GROW AND EVOLVE YOUR BUSINESS

BEIU
Buckingham Enterprise & Innovation Unit

basck

Grant Thornton

WHITESPACE

JONATHAN REUVID

GROW AND EVOLVE YOUR BUSINESS

UNIVERSITY OF
BUCKINGHAM
PRESS

University of Buckingham Press Ltd
51 Gower Street, London, WC1E 6HJ

info@unibuckinghampress.com
www.unibuckinghampress.com

 British Library Cataloguing in Publication Data available.
First published in the United States of America by Oceanview Publishing, Sarasota, Florida | www.oceanviewpub.com

Print ISBN 978-1-915054-45-6
Ebook ISBN 978-1-915054-46-3

Set in Times.

LIST OF CONTENTS

LIST OF CONTRIBUTORS

Professor Nigel Adams is a Professor in Professional Practice and the first Director of the Buckingham Enterprise and Innovation Unit (BEIU) at the University of Buckingham. He advises, supports and mentors undergraduate students in the business aspects of the innovative, two year (8 term) BSc in Business Enterprise (BBE) Venture Creation Programme. Nigel is Chairman of all the businesses that BBE students must establish and run as an integral part of their honours degree in Business Enterprise. He alsoadvises and mentors other university students, staff and local people who want to start a business or grow their businesses.. Nigel is an experienced international business adviser with more than 40 years' experience in business, enterprise, management, marketing and counter-trade. He was based in Poland from 1993 until 2002, working on Polish state company restructuring projects as a British Government Know How Fund Management Adviser.

Carrie de Silva lectured in law and Taxation to prospective rural chartered surveyors at Harper Adams University for over 20 years. She is currently a visiting Professor at the Royal Agricultural University and a consultant with a great interest in life-long learning and developing engaging and pertinent CPD works in the land-based, property and equestrian sector, for example delivering legal training to residential surveyors for Sava. Along with this, Carrie researches various historical matters, particularly early women in the professions. She has an interest in the legal frameworks of owning and managing the rural landscape, professional negligence and civil liability in the land and property sector and criminal liability for personal injury and death. Carrie has written widely in academic publications, authored books in her areas of interest, including *A Short History of Agricultural Education and Research, First Women, Equine Law, Negligent Valuation Casebook* and *Health and Safety Casebook* and has co-edited *Galbraith's Construction and Estate Management Law* along with producing several entries for the *Oxford Dictionary of National Biography.*

Dr. Mark Graves has an MEng degree in Engineering Science and a PhD in Computer Science (real-time image processing). He spent 15 years running software development teams in Europe, the USA and India in fields ranging from wireless sensor networks, neural network process control and web and mobile application development, before moving into the field of R&D Tax Credits in 2010. Mark has prepared over 1,500 R&D claim submissions and, having successfully handed a number of HMRC enquiries into software claims, has a detailed understanding of how HMRC Inspectors determine the technical eligibility of a claim. He has a postgraduate certificate in Intellectual Property Law and is a Certified Patent Valuation Analyst. He has personally invested in over 200 technology start-up companies and can advise on loan and equity financing for early-stage technology companies.

Margit Hoehne is CEO of patentGate GmbH since 2008. She has 20 years' experience with patent information, starting as a research assistant at PATON, the patent information centre in Ilmenau, Germany. Since then she has specialised in developing solutions for in-house patent monitoring workflows. Margit has a degree in business and computer science from the Technical University Ilmenau.

Nick Ioannou is an IT professional, blogger, author and public speaker on cloud and security issues with over 20 years' corporate experience. As an early adopter of cloud systems, he has been paying for the privilege of bug testing them ever since. He started blogging in 2012 on free IT resources (www.booleanlogical.com) currently with over 500 posts. Nick is the author of *Internet Security Fundamentals, A Practical Guide to Cyber Security for Small Businesses* and *A Practical Guide to GDPR for Small Businesses* as well as a contributing author to three editions of *Managing Cybersecurity Risk* and *Conquer the Web* published by Legend Business Books.

Gregor Kleinknecht LLM MCIArb is a dual qualified German Rechtsanwalt and English solicitor. Following a career at international law firms in the City of London, Gregor founded and led the award-winning boutique law firm Klein Solicitors. Gregor joined Hunters Law LLP upon the merger of the two firms in February 2014. Gregor has a strong and broadly based contentious and non-contentious IP practice, focusing on brand protection, and the exploitation, protection and enforcement of trade marks, domain names, design rights and copyright. He advises and acts for a wide range of businesses, from small, innovative start-ups and high growth companies to family companies and multinational enterprises."

Natalia Korek is an IP strategist and Managing Director of Basck, an Intellectual Property Consultancy specialising in building commercially focused IP portfolios for fast growing brands and tech companies. Having worked in IP for the past 9 years, as well as taking part in a start-up journey herself, she has gained a unique blend of legal, business and analytic skills that allows her to understand a wide spectrum of businesses regardless of their size or stage of growth. Natalia champions data-driven decisions, not only supported by business's own objectives but also justified by the market and competitors' activity, all in the pursuit of maximising the value of intangible assets. She frequently holds workshops and presentations for start-ups and investors, and is also a mentor of UKTI's Global Entrepreneur Programme (GEP). Natalia holds a Master of Laws degree from the University of Wroclaw.

Julia May is not only a prize-winning Chartered Accountant and Chartered Tax Advisor (ex- Big4) but also has a BEng Honours Degree in Engineering Science and broad-based industry experience at an international geospatial software house, an IT consultancy and other cutting edge business before setting up her boutique R&D Tax Credit Advisory. Having saved clients over £55 million in tax savings and cash rebates, Julia liaises with in-house finance teams to ensure all eligible costs are fully claimed. She liaises with your external accountant on the preparation of the tax computations and filing submission and communication with HMRC. Julia's reputation within the industry resulted in her being invited to join the HMRC Consultation Committee on R&D Tax Credits, enabling her to further develop her relationships at HMRC developed over many years.

Gary McGonagle is a founding partner at Howman Solicitors and has specialist knowledge in Corporate and Intellectual Property law. He was previously a partner in a city law firm and a media and entertainment law firm in London. He can draw on a wide range of commercial experience having also worked as an "in-house" lawyer for a FTSE listed international fashion company. Howman Solicitors is a West-End based firm of solicitors, with an ethical and modern approach. It builds strong and long lasting client relationships and helps its clients achieve and develop their business strategies.

Paula Mugisa is a business development consultant and business coach for mainly African female entrepreneurs, with over 10 years' experience in supporting MSMEs to ideate, start and grow businesses. She has coached over 4000 entrepreneurs through free webinars and paid programmes offered by Teesa Advisory services, of which Paula is the sole founder, that creates online business resources for Entrepreneurs. In 2020, Teesa launched their Online Small Business Fundamentals Course for African Entrepreneurs / Titandike Course which is already being used by 90 entrepreneurs. Paula helped design the Small Business Curriculum initiated by the National Social Security Fund (NSSF) Uganda and funded by the Master Card Foundation. She has successfully managed business development and enterprise projects on behalf of the United National Development Programme Uganda, TMR International Hospital, Ultimate Adventures Africa and Post Man Uganda among others. Paula is a Business Enterprise graduate from the University of Buckingham with First Class Honours and was top of her class/cohort in her graduating year. She is an Innovation Award winner of the Oxonia Enterprise and Research Foundation for the development of a Student Resources Mobile Application Platform. She is a Member of the UNCTAD eTrade for Women Community and was previously a Foreign Service Office diplomat with the Ministry of Foreign Affairs, Uganda.

Agnieska Musial is an IP strategist and General Manager of the EU Office of Basck, an Intellectual Property Consultancy specialising in building commercially focused IP portfolios for fast-growing brands and tech companies. Her focus is on assisting clients to build their international portfolios. Agnieska holds a Master of Laws degree from the University of Wroclaw and is on the path to qualify as a Polish patent and trademark attorney and European trademark and design attorney.

Vijay Rathour is a partner at Grant Tjornton UK LLP where he is head of the Digital Forensics Group. He has managed data breaches ranging from limited but highly sensitive losses of data by government agencies to the theft of over $100 million through intrusion and manipulation of SWIFT systems in a client bank. Vijay works at the interface of legal and clinical teams, providing experience in strategic guidance and crisis management, regularly reporting to Boards and oversight committees. He is an ethical hacker and enjoys a role on the Committee of the Cybercrime Practitioners Association. He is also engaged by the Ministry of Justice to re-draft the Civil Procedure Rules on Electronic Disclosure and Investigative techniques for the modern era.

Jonathan Reuvid is Editor-in-Chief of University of Buckingham Press and a partner in Legend Times Group. He has been writing and editing books on international trade and investment for more than 25 years and has more than 90 editions of over 35 titles to his name as editor and part-author including *The Handbook of International Trade*, *The Handbook of World Trade, Managing Cybersecurity Risk* and business guides to China, the 10 countries that joined the EU in 2004, South Africa and Morocco. Before taking up a second career in business publishing Jonathan was Director of European Operations of the manufacturing subsidiaries of a Fortune 500 multinational. From 1984 to 2005 he engaged in joint venture development and start-ups in China. He is President of the charity, Community First Oxfordshire.

James Timohy Taylor is a partner in Whitespace and Innovators Highway. He is a senior banker and corporate manager having worked in North and South America, Europe and the Middle East for multi-national banks, asset managers and fintech organisations. These international experiences provide perspective on producing for our clients bespoke business plans and Investment Memorandums. He advises clients and investors on protecting and participating in Intellectual Property, which can "make a difference." Having managed private bankers on three continents his global contacts provide valuable partnerships to our entrepreneurs. The experience of guiding family offices and introducing asset managers increases the professionalism necessary to provide capitalisation of our best ideas.

Karren Whitely-Brooks founded Whitespace at the request of her successful client base from the London Leadership Centre. She is passionate about global consciousness and the neurosciences, which help explain the emotional and mental performance required for the attainment of success and happiness. Karren is an innovative media entrepreneur and brings that valuable experience to her advisory services for business, legacy families and elite sports, organisations and athletes. She is known for her provocative interviews and remarkable breakthrough results with her clients. Karren is the author of *Spiritual Currency - Life's Capital.*

Grant Thornton

MayFigures

basck

INNOVATORS
HIGHWAY

BEIU
Buckingham Enterprise & Innovation Unit

PART ONE - INNOVATION IN A CHANGING WORLD

1.1 DEVEPLOPING AND MAINTAINING AN ENTRPRENEURIAL MINDSET

Nigel Adams & Paula Mugisa

This book has been designed to help you to grow and evolve your business. You will find in each of the chapters very useful information and experience from experts who will help you to develop your skills and knowledge to achieve your objectives in this post-pandemic, post-Brexit world. In this chapter, I will, together with one of my graduates, Paula Mugisa, provide some guidance on developing and maintaining the enterprising/entrepreneurial or "can-do" mindset, as we believe this will help you to continue to grow and evolve your business or start new ones.

PASSION IS PARAMOUNT

I have found that during the past sixteen years our BSc (Hons) in Business Enterprise (BBE) students have gone through all the ups and downs that any new or growing business will face. We have prepared them to "expect the unexpected" and be willing to "pivot" their business idea or even the direction of the business to enable it to be successful. Our advice and support has always been aimed at helping them to develop the tenacity and resilience that all founders and leaders of businesses will need. We have done this for many years and did not realise how important these attributes would become during the pandemic. Most of our students realised quite quickly that the world had changed and that they had to accept it. As a result, they recognised that they had to completely change their businesses. Those who did not change their approach soon found that their businesses could not succeed. Not being prepared for this situation and having no alternative plan, they had close down their businesses.

My first advice when developing and growing a business is that you must be passionate about its aims and how it can solve and continue to solve your customers' "pain-points". Your commitment to your business and desire to see it succeed will be vital to help you to get through the tough times you will inevitably face. If your business has survived or even prospered in the last two years, you will know exactly what I mean.

You will also need to maintain your passion as you grow your business or as you see opportunities to develop new businesses. In either case, you must also ensure that your staff, especially your senior management team, have a similar passion and enthusiasm to work on growing the business or starting another one. During the years that we have been running the BBE programme, we have found that if one of the joint founders of a business does not have a real commitment to it, the business is unlikely to be successful, unless they leave.

FROM ENTREPRENEURSHIP TO BUSINESS MANAGEMENT

Another factor that you must consider is your own attitude towards growing your business. Are you the type of person who gets bored with the day-to-day management activities of a growing business? If you recognise that you are more interested in looking for new opportunities, this approach is not good for a growing business, where the management team must concentrate on overcoming all the day-to-day challenges of business growth.

If this is the situation, you have several choices: you could hire appropriately experienced directors and managers or develop your current staff to take on these important management roles, whilst you concentrate on what you enjoy, starting and developing a new business; alternatively, you could choose to sell the business to a competitor or suggest a management buy-out to the senior members of your team. This would not only free you to do what you enjoy doing, but also provide seed-corn finance to support your new business idea.

One of our visiting entrepreneurs explained to our students that, quite early in his career, he realised that he was a "serial entrepreneur" and so would only start a new business if he knew how he was going to exit as soon as he became bored with its day-to-day management activities. If you are this type of person, I suggest that you consider adopting his approach. If, however, you feel that you can adapt to managing a growing business, then you should also remember to ensure that you develop the skills and knowledge you will need to manage a larger organisation. You must find and take the appropriate higher education or training courses that you will need. This will also be essential for your management and staff who are growing the business with you. You will all need to develop the different skills that will be needed in your larger organisation, as you face new challenges.

CONCENTRATING ON THE CUSTOMER

Maintaining concentration on your customer is also vital as you grow the business. You must engrain a "customer-oriented" approach in all the new people you employ. As our students have found, it is relatively easy to keep your customer at the forefront of your thoughts in a start-up or small business; the challenge is to maintain this approach as you grow the business. Inevitably, you will become involved in all the activities of the company as your business grows and you might not remember the importance of satisfying your customers' needs. The result can be disastrous if the "customer orientation" of your business reduces, and you are no longer providing what they want at a price they can afford, as then you will lose your customers.

How can you stop this from happening? First, the appointment of a well qualified and experienced Marketing Manager or Director is essential. When hiring this person, you need to be aware of the differences between a small, but growing business and a larger organisation. You will need to find a Marketing Director or Manager who has experience in your size of business; if they are from a much larger business, the might find it difficult to adapt to the new environment which is more "hands-on".

THE VALUE OF MAINTAINING UNIVERSITY CONTACT

Another important point that we learned is the need to combine academic research and models with a practical approach. If your business is to grow and evolve you must be aware of the ever-changing environment that you are working in and be aware of new techniques that are being developed. Maintaining contact with your local university and those who are researching in your area of business will help you to keep up to date.

You need to develop and maintain a positive and enterprising mindset. Maintaining such an approach is difficult if you are surrounded by pessimistic and negative people. One way to overcome this problem is to check if your local university has an Enterprise Hub or Innovation Centre. There where you will find a combination of entrepreneurial academics and students of all levels and an atmosphere that encourages growth and development. The people you meet will also question you about your business and the way you operate it, but they will do so in a positive and encouraging way and will introduce thoughts and ideas that you have probably not considered.

Working with your local university's enterprise and innovation specialists and their students and research colleagues will also help you to develop another trait that we encourage in our students: the need to view change and innovation as a natural part of life. You should equip yourself and your staff to cope with environmental and organisational change and encourage a positive attitude towards change, innovation and enterprise. This will mean that you must remember to maintain and develop the quality of your management and staff by continuous personal development through appropriate training programmes in which your staff want to engage.

As your business grows, you will need to develop more and different types of contacts and, as with the start-up or new business stage of your company, networking (suppliers, service providers and customers) will continue to be a great source of information and opportunities to promote your business. We introduce our BBE students to the importance of networking and developing useful business and other contacts, as soon as they start their businesses. We teach them how to find and use appropriate networking groups and to avoid those that are there just to make money out of the participants. You should remember to keep in contact with the network you have developed.

THE ONGOING NEED FOR INNOVATION

There is an on-going need for you to develop innovative new ideas and to translate them into new products or services or even new business ventures, whilst maintaining your customer focus. This approach will keep you ahead of your competitors; so it must be an integral part of your business strategy. Again, it is not only you and your management team who should be looking for new ideas. Remember that your front-line staff, at any level, are the people who meet your customers and they are an excellent source of new ideas and different approaches to solve the "pain points" that your customers encounter. Look for front-line staff who are not only "customer-focused", but are able to identify opportunities for new products and services that meet customers' needs.

We develop in our students an appreciation of the value of life-long learning and encourage them to embrace enquiry, study and knowledge creation, both in an organisational context and as a valuable activity for society in general. You will read in other chapters of this book and also be aware of, in your day-to-day work, the new challenges that you and your staff are facing. These include cyber threats, AI, government regulations that keep changing, new digital marketing techniques and the threats from new types of digital competitors. This complex world re-emphasises the importance of continuous training for you and your staff, especially in difficult times for your business.

As I mentioned at the start of this chapter, I have asked one of my successful graduates, Miss Paula Mugisa, to review for you her experience of being a student on our BBE programme. I have also asked Paula to present the ways in which she has used the knowledge, skills and experience gained when she was at the University of Buckingham in her business in Uganda. I am sure that Paula's development during the two years she spent with us, and her subsequent experience in Uganda, will provide information that you can reflect on and use in the development of your own business. I have added a few comments (in italics) within Paula's paragraphs to emphasise the entrepreneurial approach that she has developed.

PAULA'S JOURNEY

My name is Paula Mugisa. I am a graduate of the BSc (Hons) in Business Enterprise (BBE) at the University of Buckingham. I am going to present my learning and experiences on the BBE Venture Creation Programme and their application since I graduated.

As part of the BBE undergraduate programme, students are required to start a business as an integral part of their honours degree. One of the most positive opportunities I gained whilst studying BBE is the freedom and independence to explore ideas. I wanted the freedom to be able to choose something that I am passionate about and had deep meaning to me. At the start of my degree programme, I was keenly aware of the huge advantage I had of being on the BBE Programme, compared with many of my former classmates in Uganda. I wanted to share some of these experiences with people back home, so that they could also learn and make something of themselves. So, I developed and implemented a business idea to aggregate educational resources onto a platform that can be accessed by those without the opportunity to get a high quality education abroad. (*Giving back is quite common amongst the entrepreneurs we work with.)* I would not have had the opportunity to do this without being given the leeway to explore and implement what was most important to me, instead of being limited and told what I could or couldn't do.

Exploring, choosing and developing a business idea is only one part of the entrepreneurial journey; implementing it is a whole other ball game. I realised early on that there are so many naive assumptions that new entrepreneurs make, and by no means did I skip this phase. The BBE Programme gave me an open landscape to test, fail, pivot and re-start the idea I was building. I was overly ambitious and naive in the initial conceptualisation of my business idea. As a result, my colleagues and I were denied funding during our first attempt at the pitching to "Buckingham Angels". However, we didn't give up. *(Research into entrepreneurship has found that tenacity is an entrepreneurial characteristic.)* By the end of the BBE Programme, we had raised £4,500 in funding, developed a Minimum Viable Product of the Platform, launched it on campus, acquired 400 initial downloads on the week of our launch and won a £1,000 Innovation Award at the Oxonia Enterprise and Research Conference in Oxford. These experiences have provided the foundation of my entrepreneurial journey. I learned that failure is the best way to learn and pivoting i.e. changing your course of action, is par for the course, as one gets closer and closer to really understanding the value we offer in the market and how to acquire the right customers to serve and buy from us. *(Failure is not normally encouraged in universities, but in Buckingham we recognise the importance of learning from failing.)*

Finally, I will mention that the BBE Programme offered me multiple opportunities, as a student, to engage with the real world outside the university. This gave me a real idea of what it would take to implement an idea, bringing onboard partners and supporters for the idea and gaining initial traction. By meeting other entrepreneurs and professionals we also acquired different ways of looking at things, an analytical thought process and a mindset of thinking-out-of-the-box. With every external engagement all I saw were possibilities and I was greatly inspired to do more with my life and take advantage of the opportunities that I had been given and have an impact on many others. *(Students studying academic models and theories and then trying to implement them within a real business environment is an important factor in the BBE Programme.)*

Naturally, the inspiration that I acquired gave way to grand ambitions. I had added pressure to prove myself, having come from an underdeveloped country like Uganda. I also wanted to return and make something of myself by bringing great value to my people. The single, most repeated phrase that I often heard Professor Nigel tell me was, "Paula, slow down!" At the time, I perceived being asked to slow down as being pulled back. I wasn't concerned about my mental health or overall health; I was only concerned with winning. Professor Nigel advised me to work with colleagues in my class to build a team around the idea that I wanted to implement and I couldn't have been more crushed. I believed that other people would slow me down and I desperately wanted to stay a "one-woman show". As you may already be able to tell, this guidance turned out to be very useful, though it was hard to accept at the time. It is likely that I wouldn't have completed my degree programme or achieved what we did without the support of a team and guidance from Professor Nigel. The lesson of "letting go", asking for help and letting others support you is one that I am learning and re-learning, as I grow as an entrepreneur. *(Research has found that Paula's original approach was similar to many other entrepreneurs.)* I now appreciate much more the benefit of a sustainable long-term business growing with the support of a team, rather than gaining quick traction in the market too fast and burning-up because ultimately, the business was a one-woman show.

On graduation BBE gave me:

- Credibility: Having completed an undergraduate Venture Creation Programme, achieved a first class honours degree, started a business, acquired funding and won an innovation award, my profile stood out immediately.
- A first job: I was able to secure a job as a Foreign Service Officer at the Ministry of Foreign Affairs in Uganda. Acquiring the position with 18 others out of over 1,900 applicants was something to be proud of.

TRANSLATING THE BBE EXPERIENCE INTO PRACTICE

However, if you have worked with any government institution, especially those in developing economies like Uganda, you quickly realise that "majority-think" is applauded over being enterprising and it may not be the best fit for a "know-it-all" young, ambitious woman with something to prove. I quickly got frustrated and left my permanent and pensionable government job within two years for the world of business. To this day, I still think it would not hurt our ministries to operate with an entrepreneurial mindset, embracing new ideas and innovation. We really would be able to achieve unprecedented feats for a lot of deserving and many times impoverished groups of people.

After resigning my job as a civil servant, I set up a non-traditional, micro and small business advisory firm for African Entrepreneurs called Teesa Advisory Services. BBE gave me a reliable framework on how to start and grow a new business anywhere in the world, in the form of high-quality business resources, acumen and enterprise experiences. With this powerful knowledge base, during the years since starting, I have worked on filling-in the nuances of doing business in Uganda and in Africa to find a model that works for African entrepreneurs and produces results in our market.

In the three years since starting Teesa, we have helped 15 small and medium-size enterprises improve their business operations; we have worked on enterprise projects with the National Social Security Fund in Uganda and UNDP Uganda. We have supported two start-ups to build mobile application platforms and launched an on-line business course and business coaching programmes that have directly helped over 100 entrepreneurs. We have also created multiple free business resources including webinars that have reached almost 4,000 local entrepreneurs and others throughout Africa.

We have also pivoted our business model three times in three years. *(This shows the way in which Paula has used the enterprising approach we encouraged in her and recognised the need to adapt her business to the challenging environment that she is working in.)* We are currently building a strong enterprise platform on the basis of all of our learning about enterprise in the African context. We intend to scale-up beyond Uganda, firstly to the East African Region and then to the main regional hubs across the African continent.

Despite some positive traction, there have been numerous challenges developing a business in Uganda.

- Lack of integrity and short-termism. There is still a pervasive culture of corruption in most institutions and a strong pattern of entrepreneurs being taken advantage of by their partners and associates for monetary gain that increases people's reluctance to do business. On top of this, in Uganda many people are complacent i.e. not willing to work hard to achieve more and are commonly found to be pursuing short-term, too-good-to-be-true projects that promise and rarely deliver huge financial gain.
- Under value/under estimate the contribution of young people to the economy. Despite the fact that young people are the majority of most populations in Africa, many key leadership positions are held by people in their fifties or older with minuscule youth representation.
- "Group-think" is also greatly encouraged, while simultaneously shooting-down innovation or any new ideas.
- Gender Disparity is common, as in the rest of the world; few women sit at the table of key business conversations or institutions that affect the private sector. This leads to a number of policies that, on paper, favour marginalised groups, but in practicality do not meet the growing needs of women and young people who often need to provide for themselves.
- In Uganda, the government is still the biggest spender in the economy and the private sector maintains low purchasing power, making it difficult for many local businesses without the ability to scale-up to regional markets to survive.

- Ugandans also typically lack the culture of sharing experiences and knowledge, resulting in very few sources of local enterprise education. The country also lacks examples of entrepreneurs who have shown a success path and whose strategies can be duplicated by newcomers in the market.

Despite the challenges, I fully intend to keep Teesa Advisory Services going and one day realise my dream of leaving a strong legacy of positive impact on entrepreneurs across Africa. *(Again, Paula is showing the tenacity that is needed to start and develop businesses.)*

My final piece of advice to aspiring and existing entrepreneurs is to pursue a business that aligns with your purpose and for which you have a passion; then to find a way that your idea can scale-up beyond your immediate environment.

About the Buckingham Business Enterprise BSc

In January 2006, the University of Buckingham launched what was believed to be the world's first undergraduate Venture Creation Programme (Lucken, 2012). Students on the university's BSc Business Enterprise (BBE) programme must start and run a real business, as an integral part of their Honours Degree. In addition, as for most students at Buckingham, they must achieve their honours degree in just two years (eight terms). If their first business fails, then the student must start another one. Several graduates have run two or three businesses during their time at Buckingham.

1.2 LOOSE LIPS AND LEAKY SHIPS – CYBER SECURITY AND PROTECTING THE CORPORATE ORGANISM INSIDE AND OUT

Vijay Rathour, Grant Thornton UK

Criminality is unquenchable. Outside of the realms of science fiction like *Star Trek* and *Demolition Man*, the criminal tendencies of aberrant portions of society are unlikely to ever vanish entirely. And with criminality invariably comes an attraction to opportunistic theft or fraud for financial gain. Data theft, industrial espionage and cyber crime provides the would-be felon with a potentially unlimited opportunity to line his or her pocket with barely a risk of sanction or capture. What can polite society to do protect itself, if anything?

Cyber crime is currently ranked as the third most severe risk likely to befall global organisations. The annual Allianz Risk Barometer surveys organisations and over 2,700 global experts to rank the top business risks. Cyber has been moving up these rankings and indeed in 2020 became the top ranked risk for the first time in the history of the barometer. 2021 has of course seen the global impact of the pandemic (second place in 2021). Associated with the pandemic, but the historical top risk, is the impact of business interruption. This has been especially exacerbated by Brexit and other geopolitical machinations.

BLACK SWANS AND WHITE HACKERS

For the majority of organisations that become victims of a cyber or data incident, whether through external hacks, insider risks or data thefts such as recent publication of highly sensitive banking records regarding global politicians, the impact is swift and expensive. Indeed for some businesses, the impact can be fatal. I have led cyber incident response teams for over a decade and in that time I have seen numerous clients that have been so wounded by the attack that their customers depart for competitors, regulatory fines have been levied that are beyond any black swan planning scenarios, external audit firms will refuse to sign off on the financial stability of the organisation, and reputational harm leaves the business with no hope of a return to the halcyon days before the reality of cyber risks struck them.

Financial harm may well be an immediate concern, through the loss of valuable intellectual property or customer information. However, the reputational harm and the damage to the public perception of the business can cause a loss of confidence by customers, investors, shareholders, insurers and regulators. Would you choose to fly with an airline that can't keep its computers online, or a social media platform entrusted with your secrets, when it can't keep its own source code and databases private?

Cyber incidents are inevitable and regulatory scrutiny and a customer base that votes with its wallets means that preparing for, managing and regaining control in a cyber crisis is no longer merely an option for businesses, but should form an essential part of the contingency planning in any organisation.

TIME IS MONEY

Annual studies by the Ponemon Institute LLC rank the newest and greatest impacts of cyber attacks and provides a cacophony of supporting numbers and charts to help communicate the blunt reality that cyber crime is costing more, hurting more and occurring more. The study shows the average cost of a data breach is around £2.8 million when factoring in valuation impacts, reputational harm, customer churn and regulatory sanctions. The average cost per customer record lost is around £110; this year my team has worked with organisations that have had over 1 billion customer records exfiltrated (i.e. stolen) by the interlopers, and in an increasingly connected and online world, these astronomical numbers will only increase.

It is a common modus operandi for the attackers to seek to identify your "crown jewels", gain the maximum financial value from your data, whether by stealing it for your competitors, the press or a foreign nation state; they may be aiming to steal funds from you, your bank and your customers, or merely to cause the maximum carnage to encourage you to pay a ransom to allow you to regain control of your systems.

Lockheed Martin, the aerospace engineering business, developed their "Cyber Kill Chain" framework that codifies the typical stages manifested by cyber attackers seeking to take control of your systems. Moving chronologically through the phases of a cyber attack, these are stated typically as:

1. Reconnaissance
2. Weaponisation
3. Delivery
4. Exploitation
5. Installation
6. Command and Control
7. Actions on Objective

These seven stages reflect the practical stages of many cyber attacks, although some may be truncated or side stepped due to circumstances such as readily available entry points, stolen passwords or weakened security.

Speculating on the psychopathy of the criminal, we would expect that speed would be of the essence and getting in and out as quickly as possible would be prudent. However, the average time to identify a breach was 207 days in 2020 with around another 73 days to contain it, meaning that it takes the average business around seven months merely to determine that the attackers had been inside their data environment, identifying crown jewels, spying on Microsoft Teams calls and emails, and determining how to cause the most pain and achieve the greatest financial value. And of course, like all of the best criminals, the best hackers won't get identified at all, and that 207 day window may be indefinite. If the data is silently leaked to a competitor or rogue nation state, the victim may never even realise that data has been stolen or tampered with.

The Kill Chain will strongly advocate cutting the hackers off as early as possible – the more time they have the longer the infection can spread through the open wound. Thus strong external defences such as firewalls and Data Loss Prevention systems will provide an external "radar". While equally robust internal security mechanisms such as Bastion servers and Micro Segmentation will hinder the ability of the hacker to move "laterally" within your IT estate and to trigger "exploitation".

THE ORGANISATIONAL ORGANISM

Complex data estates create complex governance problems. Indeed, the word cyber is derived from the Greek word "kubernētēs", referring to the steersman of a vessel. It references the concept of governance of complex systems and organisms. My client that suffered from a data breach of systems containing over one billion data subject records had an enormously complex data estate, fortunately coupled with effective and efficient segmentation approaches. However, notwithstanding this "fencing off" of functions within the beast, the overall complexity was such that the business could spend years seeking to identify which parts of its business were potentially touched by the "threat actor", and even then, it rapidly became cost disproportionate to seek to do so with accuracy – a cost of millions of dollars and many months of analysis.

It is an essential lesson to take stock of how the data organism grows and evolves. As it achieves an enviable scale of complexity and breadth, it is prudent to reassess whether what was appropriate at its birth is still appropriate during its adolescent years. Technologies evolve continuously, with once novel approaches such as Multi Factor Authentication now effectively mandated by most cyber insurers, auditors and data regulators. Strong encryption mechanisms continue to be created and gain credence and usage. Indeed evolving and currently expensive approaches may become commonplace, such as "homomorphic encryption", an approach of using surrogate data in place of the original, unencrypted data, in such a fashion that the surrogate creates the same outputs as the "real" data, without risking a leak of the real data whilst the data is "in transit".

DIGITAL EVOLUTION

The forms of data evolve continuously, as does the security required to contain it and prevent it from being used against its controllers, processors and creators. Who would have thought that a short form messaging platform (around 15 years old) designed to share 280 character long text messages, could result in the election of presidents, the toppling of nation states or the mobilisation of a populace seeking racial or environmental change? But for every tweet, there is a reciprocal data set – a database gets populated, metadata gets created, a censor or keyword list gets animated, governmental security agencies and national "firewalls" get triggered… for every frivolous data point there is a digital footprint that will be indelible.

Understanding what information you hold and how much of it is potentially valuable to a hacker is vital to ensure that your defences are robust, proportionate, defensible to a regulator, and cost-effective in all of these circumstances. Accessing and exfiltrating a customer database that holds a million records can be the work of minutes or hours by a motivated hacker, and the financial fallout will invariably outweigh the cost of implementing appropriate defences against theft.

Cyber has a "long tail" – the impact of a cyber incident will continue long after the 280 days or so required to identify that the business has become a victim of a cyber attack and to repair the damage. However, the financial impact on market valuations and brand can be immediate but last long past the containment of the cyber event. Studies have shown that it can take around 60 days for organisations to begin to demonstrate a return to a neutral or positive financial sentiment following a public crisis, although many will fail to return to normality even nine months after the incident.

The financial impact flowing from a data breach can clearly be great, but while less obvious at first, the longstanding harm can be even more marked. Data and financial regulators, and increasingly, third party liability claims, often follow serious security breaches. Highly regulated industries such as pharmaceuticals, health and the financial sector, and any holding large quantities of 'personally identifiable information' about consumers, are likely to come under the microscope. Recent attacks on banks, airlines and food manufacturing organisations, amongst others, have shown that consumer trust is easily lost, whether the true impact of the breach was great or small. Once lost, that trust can be difficult or impossible to re-establish.

DARK DATA SUPERSTORES

Your financial data may of course be a target, but increasingly its intellectual property is perceived by the hackers as worth holding to ransom. Recent hacks on social media platforms that resulted in the entire source code of the platform, including its back-end infrastructure, its mobile telephone apps, its security protocols, and the commissions it pays to its creators have scandalised the platform. A knock-on benefit for would-be competitors sitting in less responsible IP jurisdictions is that they have been afforded a multi-year head start in how to establish a globally scalable social media platform, worth millions. And the grey-market version 2.0 will no-doubt be hardened against the very cyber vulnerabilities that provided that springboard!

LEARNING TO BLEED LESS

George S. Patton Jr. stated that *"he who sweats more in training bleeds less in battle."*

If your information is valuable – either to you, your competitors, or to the dark-web market economy of intellectual property traders and credit card thieves – hackers will be seeking to breach your security. Many organisations have found themselves forced to make a hurried PR statement regarding the potential damage they and their customers have suffered, without the luxury of time to investigate the breach fully. This can lead to even greater embarrassment and confusion, as the circumstances evolve and the true facts and impacts, positive or negative, come to light.

Contingency plans can and should be made – the military adage that "no plan survives first contact with the enemy" is, in my experience, unfortunately more often true than not when dealing with a cyber crisis. However, the worst plan is no plan at all, and more than half of the data breaches my team engages with are for clients with no mature cyber response, or indeed a generic and untested crisis response plan.

We live in an age of instant information gratification and social media networks will be digesting and commenting on perceived failures following a breach even before your staff are aware of it. Again, referring back to the Kill Chain model, preparation is critical as the time to detect and respond is a key factor in perceived successful resolution of a crisis.

REGULATORY SCRUTINY - ALWAYS WATCHING

Currently, there are no defined legal standards of cyber preparedness for most business sectors operating in the UK. A small number of industries have more guidance – financially regulated business, telecoms, pharmaceuticals etc. However the majority of us are generating and processing ever-greater volume of valuable personal and commercial data every day. There are many ways for businesses and individuals to help themselves and secure their environments, staff and data, at little additional cost to their current posture. The risk is inevitable and growing, and thus in our experience the greatest regulatory hammer will fall upon those perceived to be flippant about risks, underinvesting or entirely avoiding the expectations of good data governance.

In the UK, cyber incidents that result in the loss of a volume of sensitive personally identifiable information will be potentially come under the scrutiny of the Information Commissioner's Office (ICO), an independent supervisory authority reporting directly to the UK parliament. The Information Commissioner publishes *Good Practice Notes* on the management and notifies breaches of data security.

Considerable fines have been levied against organisations that the ICO has determined have failed to adequately "mitigate" against the risks of cyber attacks. Although the large fines may be instructive, the *reduction* in penalties provide even more opportunities to learn how not to come under the ICO's gaze. I strongly recommend studying published *Penalty Notices* to learn what the ICO regards as beneficial mitigations that are likely to earn brownie points in future incidents.

Penalties will follow if the ICO is satisfied that the data controller either deliberately contravened the UK's Data Protection Act or knew, or ought to have known, that there was a risk a contravention that would occur that was likely to cause substantial damage or distress, and failed to take reasonable steps to prevent it. Although this seems like a high threshold, the organisation's attitude to risk and efforts to prevent data leaks will be a factor in the ICO's findings.

Where the ICO has been persuaded by "regulatory advocacy", i.e. efforts by teams such as my own, fines have been dramatically reduced. These efforts to contextualise the specific workings of the organisation's data environment, cyber infrastructure, hinderances to otherwise "common sense" implementations of Multi Factor Authentication, device encryption, operating system updates, and demonstrating a healthy attitude to lessons from regular penetration test, can all persuade the ICO that a regulatory intervention is not required. Expert guidance should always be sought when examining how your business takes in, stores and processes data, particularly when it is potentially valuable or sensitive. "Perfect security" may be unattainable, but demonstrating a healthy attitude to investing in "mitigations" can strongly dispel the QED assumption that a breached organisation is not respectful of data and security expectations.

The Information Commissioner's Good Practice Notes provides helpful, high-level guidance on issues to be aware of whenever dealing with valuable or sensitive data, and on when the ICO should be notified in the event of a security breach. However, there are sensible practical steps that can and should be taken in anticipation of a breach being discovered – in the hope of both reducing the risk of an actual security failure and improving the management of it if the worst should occur. Some of these steps originate in legislative guidance, but most are the result of good contingency planning and security awareness.

The DPA provides some guidance on relevant considerations, including the potential harm flowing from the security breach, appropriate technical and legal guarantees of the measures in place to prevent a breach, and the risk of a data breach by employees. ICO guidance also advocates good 'data hygiene' – the implementation of appropriate privacy considerations at the design stage of a data system, including encryption mechanisms.

KILLING THE KILL CHAIN

Failure to invest appropriately in adequate systems and controls when dealing with confidential information is a common focus of the Financial Services Authority, and numerous high-profile fines have been issued against businesses and senior individuals found not to have invested financially and engaged mentally with these precautions. The risk of litigation and the liability for failing to follow proper practise can be considerable, even when the failings themselves are relatively slight or flow from the failings of a third-party sub-contractor.

Vicarious liability and responsibility flowing from the loss of confidential data can dramatically complicate the risk landscape: following the global pandemic we have seen increasingly severe impacts stemming from a breakdown in supply chains. One cog may well impact a myriad of others, and failure to secure your billing system against a cyber attack, resulting in the inability to ship widgets from your manufacturer to your retailer, resulting in the loss of a contract in the construction of a factory complex, could all result in financial losses and liabilities flowing back to a singular oversight in cyber security infrastructure.

What is the cost of good cyber security? The answer to the six million dollar question should be significantly less – studies suggest that a good metric is about 0.5% of global revenue should be spent on cyber security, as distinct from about 9% on IT specifically, for a mid size organisation. That study suggests spending about £1,500 per full time employee to keep them safe from would-be hackers.

Businesses should take reasonable measures to prevent cyber attacks. Although the hackers' ingenuity knows no bounds, sensible measures can dramatically reduce the risk of an opportunistic attack. Strategies might include:

Restricting employee and contractor access to information on a 'need to know' basis. Well accepted strategies of Identity and Access Management such as the use of robust passwords and rigorous data compartmentalisation are important in the event of a system compromise, as well as in limiting the risk of data leakage by authorised system users and rogue employees. The recent Pandora Papers leak may well speak to how data can be appropriately packaged to minimise the risk of inappropriate leaks.

Organisations should consider what data they have held, hold and plan to hold, and limit this as proactively as possible. Fines that are levied *per record accessed* will cause considerable chagrin when the records accessed were vestigial, relating to customers and services historical to current operations.

Divide labour but keep teams connected. Protocols should be crafted, enforced and provided to employees and other relevant consultants and sub-contractors with assurances that they understand their content. This should ensure that any suspected data loss or intrusion is communicated to relevant staff in your organisation without delay.

My team have recently supported a global food and beverage manufacturer that had misconfigured a data server, resulting in inappropriate data leaking to incorrect recipients for over five years before the problem was observed, and even then merely by luck rather than prudent governance. The innocent victim that had received tens of thousands of emails regarding other customers' data had attempted to alert the client multiple times in various years, but divisions in team responsibilities meant that they failed to connect the dots and provide a resolution to the issue. Fortunately this data was not terribly sensitive, but with systems containing tens of thousands of data rules, it is almost impossible to ensure that human error is entirely eliminated – studies suggest that some 70% of cyber data breaches occur due to human factors.

Expert advice can assist in designing IT infrastructure and protocols and dramatically reduce the risk of data leaks and breaches. These "playbooks" and protocols should be regularly tested and updated both internally and also by security experts who can stress test them and to help ensure that they are robust against modern and evolving attack mechanisms.

Encryption and Authentication. All devices that store or facilitate access to sensitive data should provide for adequate levels of encryption to frustrate efforts by opportunistic attackers to access and/or exfiltrate the data. Effective Identity and Access Management policies should enforce healthy password policies to ensure that they are strong enough and regularly rotated to prevent the proliferation of "password stuffing" attacks facilitated by passwords stolen in other attacks being used against different targets.

Multi Factor Authentication coupled with healthy password policies can dramatically reduce the success of the vast majority of cyber attacks. These policies are relatively cheap to implement and provide some of the best "bang for the buck" in an organisation's cyber security posture. However, failure to implement these highly cost-effective and cyber-effective functions will certainly attract regulatory and audit scrutiny and increase the cost of cyber insurance.

Implement appropriate system segmentation and physical and electronic security. Much like the rationale for deploying fire doors, it is unwise to connect every computer in an organisation to every other system. Segmentation of networks can be enforced both physically and digitally, frustrating efforts of attackers to move from one impacted computer system to another trivially.

Segmentation of networks into virtual trees and branches (VLANs), including internal and external wired and WIFI networks, again can dramatically reduce the risk of cross fertilisation of hacking exploits from one "attack surface" to another. Systems can be enforced to control and detect unauthorised data flows from email or Internet access on machines with access to sensitive data.

Highly sensitive systems such as SWIFT payment gateways may warrant the use of an 'air gap' to eliminate the possibility of any external network access to the host machines.

THE DEFINITE INDEFINITE

It is inevitable that the majority of businesses have either been successfully breached, or are currently being probed by cyber attackers. Even where the best precautions have been taken, the worst can still happen. If it does, you should be in a position to respond quickly and proportionately to the inevitable black swan event. The Ponemon study tabulates the "Impact of 25 key factors on the average total cost of a data breach", and the top "mitigating factor" most likely to result in a rapid and successful response to a cyber attack is "Incident Response Testing". This is followed by business continuity planning and the formation of an Incident Response readiness team, which in my mind are a spectrum of the same underlying goal – preparing for the inevitable breach.

Again, the sooner the "kill chain" is circumvented, the less impactful the breach and the greater the likelihood of identifying and ejecting the hacker before damage can occur.

Organisations should draw up a plan of best practices to follow in the event of a breach and ensure staff are familiar with it. A response strategy should, at a minimum, address the following:

Define the incident. A data incident can cover a wide spectrum of circumstances includes situations where confidential information has potentially been compromised, whether by hacking attempts, theft, loss, or accidental disclosure to unauthorised individuals. Loss of data or penetration into your system will not necessarily mean that material can be used by wrongdoers.

Effective mitigations may mean that the detected incident doesn't escalate internally to the status of a "crisis", and such an incident may cause concerns internally, but will not necessarily pass the threshold of being a 'reportable' breach. Expert advice may be required to determine whether the data has actually been compromised, especially to allay future allegations of the organisation choosing to bury an otherwise reportable event.

Train an Incident Response team. This team should be composed of legal counsel, internal and IT security personnel, human resources personnel and representatives from your cyber security experts. Members should be aware of their responsibilities within the team and how they are expected to contribute to identifying, stemming and preventing breaches.

Create a response plan. The steps to take in the event of a suspected breach will include assessing the nature of the cyber incident, assessing the thresholds required to invoke contingency plans, and possible internal and external communications, amongst others. It may be appropriate to appoint experts to conduct "cyber health checks" and Red/Blue teaming, where ethical hackers will be appointed to seek to overcome your own internal defence teams.

It is prudent to invest in a "Digital Risk Quantification" assessment to quantity the impact of the cyber investments currently made or outstanding by the organisation, and these should include assessments of third parties and suppliers flowing to and from you.

Communications. It is essential to test protocols and plans – corporate muscle memory can destroy confidence in well-crafted crisis response plans. If a breach occurs, staff, executives and PR teams should be able to respond promptly and at the right level of seniority. It is essential to ensure that there is neither decision paralysis nor the risk of maverick decision-making that can result in even costlier consequences. Examples might include plans to erase all computers impacted with a piece of malware and to immediately restart operations. This otherwise sensible step may risk the destruction of valuable forensic evidence that may be requested by regulators, customers and insurers, and could suggest that the organisation has been unable to follow a prudent and planned crisis response plan.

Preparation for a data breach will assist in the speed and thoroughness of the organisational response. However, these plans should be regularly tested, with thorough, documented risk assessments, to ensure that staff and systems are well prepared and criticisms are addressed.

Putting it into action. Through regulator testing, in the event of a cyber attack or data breach, the pre-planned processes will help to ensure legal compliance, identify data exposures and to minimise costs. Expert assistance from data-security experts will help to ensure that incidents are thoroughly investigated and appropriately documented, and also provide the air of objectivity unfettered by internal corporate pressures to get back to BaU.

CONCLUSION

Cyber security incidents are inevitable and if you have not already responded to one, you may already have suffered one unknowingly. Attackers are tenacious, intelligent, organised, and can compromise your data and systems both from within your organisation and from outside. Effective planning and investment in TTPs, tactics, techniques, and procedures, can reduce the risk – even if your data is accessed inappropriately or lost – of material being sold on or used against you, creating a notification burden.

Effective preparation, physically, electronically and psychologically, can help to ensure that you are able to deal with problems quickly and effectively and to minimise the risk of financial harm, brand damage, and regulatory sanction.

1.3 INCREASING YOUR BUSINESS VALUATION WITH INTELLCTUAL PROPERTY AHEAD OF FUNDRAISING AND EXIT

Natalia Korek, Basck

The COVID-19 pandemic has had a profound impact on the global economy. With many people having lost their jobs or had their incomes significantly reduced, there has been a surge in new businesses. In the UK alone, more than 400,000 start-ups were formed in 2020. For many of these new businesses, securing additional funding from investors is an important stage in their growth. To obtain such additional funding, it is usually necessary to provide investors with a business valuation.

Ultimately, the higher the valuation, the smaller the share of your business you will have to trade in return for the additional cash injection. There is only so much one can achieve when it comes to valuation if valuing solely based on cash in the bank, past revenues and tangible assets. For early-stage businesses, without a great deal of revenue or even no revenue at all, Intellectual Property and intangible assets can be key in achieving the desired valuation.

Intellectual Property Rights and intangibles are often treated as interchangeable whereas there is a subtle difference between them. Intangibles, in general, are those assets that lack physical substance, which make them difficult to quantify, describe and capture. Intangibles might be divided into three sub-categories:

- **Intellectual Capital** - people's expertise e.g., knowledge, skills, know-how, experience and relationships within the company.
- **Intellectual Assets** - company's management e.g., processes, datasets, plans, specifications, contacts, supplier lists and sales leads.
- **Intellectual Property** - the most tangible form of intangibles, i.e., patents, trademarks, design rights and copyright. These rights are publicly available. Trade secrets are also a form of Intellectual Property; however, these are confidential.

Due to the tangible nature of Intellectual Property, it can be easier to assign a value to it, or at least to convince a potential investor of its intrinsic value. For example, a copy of a patent application or a trademark certificate can be sent to an investor to provide them with something physical they can see and hold in their hands. Furthermore, Intellectual Property rights may be more easily quantified. For example, many investors will perceive owning five patents as being five times more valuable than owning one patent. Intellectual Property can therefore provide a powerful tool for increasing the valuation of your business.

Intellectual Property Ownership

Have all your employees signed their employment agreements including an Intellectual Property clause? Is everyone who contributed to your business's Intellectual Property an employee? Did the contractors and directors assign their IP rights to the company?

Ownership (or rather lack thereof) is the number one reason for Intellectual Property issues and the one most likely to be picked up on in the due diligence process. Make sure to put written agreements in place as early as possible to avoid potential issues later, even if dealing with close friends. Transparency in the founders' ownership from an early stage translates into a solid foundation of the business culture when it comes to dealing with formalities. It is absolutely critical to have "your ducks in a row" especially before your investors' lawyers have gone through your documents with a fine-tooth comb, reporting on potential issues.

Relationship with universities

Are any of your employees employed as a researcher at a university? Did you use university resources to develop your research? Are there clear-cut agreements in place with the respective university regarding IP ownership?

Relationships with universities are another big red flag in any due diligence process, most often because of the lengthy agreements governing joint projects. These agreements are finalised after months of negotiations and therefore great care has been taken in their review. Most common pitfalls include, for instance, very loosely defined IP background (i.e. what you bring to the table) and foreground (i.e. what you develop together based with the help of each other's background IP). A vague definition that becomes contentious can at best, cost you additional royalties to be able to commercialise the subject IP and at worst, restrict your own freedom to operate.

Registering Trademarks

Have you come up with a name and/or a logo for your company? Have you carried out a Trademark clearance search? Have you checked whether the domain name for your business name is available?

Trademarks are used to identify the origin of goods and services, and can be used to protect a brand from imitators. Trademarks are often overlooked by new businesses. It is important for a new business to check that the name they wish to use is not already in use by another entity. This can be done by carrying out a simple trademark clearance search. Having established that a name is not already in use, registering the name as a trademark is a quick and cost-effective way to add value to your business and protect your brand. Furthermore, if you have designed any logos, you can and should file these as separate trademarks, which will further add value to your business.

It is also important to check whether the domain name of your chosen business name is available and to register it as soon as possible. If your chosen name is not available, it is worth checking to see if the owner would be willing to sell it to you, or alternatively, if another name associated with your business or brand is available. Simply owning relevant domain names in itself can add significant value to a business.

Filing Patents

Have you developed any product or service that is completely novel and inventive? Does your methodology offer an improvement over the existing solutions?

Patents should be viewed not only as a legal tool but a commercial one — one that is deeply embedded in your business strategy. There is no "one size fits all" IP strategy but it is important to understand all the perks that come with your investment in patents and use these to their full potential. Patents can help your business gain and retain competitive advantage, and therefore increase the business value. You might never need to use them for defence purposes but even without this, they open up additional opportunities. Holding granted patents in any infringement case means that you have a much better position to negotiate a cross-licence or countersue. You can use patents as an offensive strategy and restrict your competitors. This means you can open a licensing conversation in which you set the terms and gain access to your competitors' IP in return. You can divest of patents that you no longer use, or you can seek licensees to create additional revenue streams through royalties. Owning patents equals having opportunities.

Investors like to see patents even in their "*patent pending*" state. If your technology is disclosed in a patent application, it is kept in the best technical ledger on the planet. It means it has been reviewed and classified using the international patent codes. These codes are universal and used globally to reference different types of technologies. This makes your invention much easier to find. Patent examiners from other countries can use it to refuse other applications that aim to obtain exclusivity over the same technology. Even if you do not end up getting a granted patent, at least you have established a publication block for anybody else.

Alternatively, you could opt to publish in well regarded and established magazines to achieve the same effect but these usually have very strict publication criteria. Some require a very-detailed level of disclosure, which might be particularly troubling for software inventions where snippets of the code are requested. With patent applications you are in full control of the level of disclosure.

There is a common misconception held by many businesses that it is not possible to obtain patent protection for software inventions. This is perhaps not unsurprising given how confusing the law can be around patenting software. In both the UK and Europe, scientific theories, mathematical methods, business methods, and programs for computers are all excluded from patentability, which could well lead one to believe that it would be impossible to obtain a patent for a software invention. However, these are only excluded to the extent that the invention relates to that thing "as such". Therefore, it can be possible to obtain patent protection if the software can be shown to give rise to benefit in the real world outside of the computer. For example, the use of software in a braking system for a car that results in improved stopping time could potentially be patentable.

There are more financial benefits of owning patents such as tax breaks. Most countries offer a tax scheme that allows companies to claim back part of their R&D expenditure as a tax relief against their corporate tax (e.g., R&D tax credits). The UK taxation system provides yet another tax relief that allows halving corporation tax based on a granted UK patent (see: Patent Box). As a start-up, you might not return profits for a few years whilst scaling the business but the process of obtaining a granted patent can also take a few of years. Early patent submission puts you in an optimum position to be ready for a tax break claim once the company grows to the size that warrants it use.

Freedom to Operate

Do you have freedom to operate in the market you operate? Did you check if you have Freedom to Operate in markets where you want to scale to?

This is a very frequent question asked by investors and the answer depends on the stage of the business you are at. Freedom to Operate tends to be a costly project to conduct and it is also very often misunderstood as a simple patent novelty search. The differences between the two are quite substantial though, see below:

	Patent Novelty Search	Freedom to Operate
Input	Description of invention to be patented	Description of the actual product or service as commercialised
Scope	Non-exhaustive search	Exhaustive search
Territory	Global	Selected territory only
Sources	All patent literature (granted patents, pending applications and expired rights) and non-patent literature (science journals, online blogs)	Only active patent rights i.e. granted patents and pending applications
Aim	Reveal the closest prior art to the subject invention	Check if there are any rights that could be infringed if the subject product or service was commercialised

If investors are asking about Freedom to Operate at the very early stages of the venture, some businesses might think that the best practice is to instruct patent attorneys to perform it as soon as possible, even before the product has been launched. However, the drawback is that its cost will likely take the entire budget accommodated for building the IP portfolio. From our experience, filing your own patents, trademarks, and handling any IP ownership formalities is far more important. The reality is that at the point of commercialising, you will likely have the funding to make any changes to your product or service to navigate around the granted patents of your competitors. Start-ups should be encouraged to perform patent novelty searches on their inventions as early as possible but perhaps hold off on an expansive (and expensive!) Freedom to Operate until it’s viable to perform it. At the early stages, you should be able to tell your investors with confidence that you are not aware of any patents that would stop you from commercialisation. Patent novelty searches and even instructing your internal team to read through the patent literature should allow you to achieve this.

However, businesses that produce tangible products should not delay Freedom to Operate searches for too long. Product changes will likely incur higher costs than performing the said search at the point where ordering large product quantities with manufacturers are imminent.

Intellectual Property Policy and Processes

Are your team members clear on what Intellectual Property is and what the business wants to protect? Are there clear processes in place for identifying protectable assets and working with external counsels? Has an inventor incentivisation programme been set?

Intellectual Property as a function within a business usually lies with the CEO or CTO at the early stages, which creates bottlenecks. C-level executives are aware of how critical protecting their IP assets is, but together with fundraising, business development and day-to-day running of the company, it simply falls to the bottom of the priority list. Creating an innovative culture across the team is critical for technology rich companies to allow the founders to get on with their business priorities, whilst making sure the innovation that underpins the business is protected. This takes training and setting right processes in place, for instance the process of identifying patentable inventions.

Disclosing potential patent candidates early and with a sufficient level of detail required for performing necessary searches and drafting allows for efficient collaboration between the technology teams and lawyers. It also helps avoid common mistakes of early disclosure and creating prior art against your own patents.

Fostering Intellectual Property culture and giving your team members the chance to participate in the IP process from day one provides them with the feeling of belonging and incentives to take ownership of the company's innovation. This, as a result, builds yet another intangible asset which increases the business value; a team that not only has strong work ethics but also a fantastic culture, with high employee retention rates.

In order to do this, two things are critical: training and transparent policies. A workshop to educate your team about Intellectual Property will take you a long way. It does not need to be very detailed or long, it is all about building awareness about IP in general. Setting an IP policy will complement it. As such, it should be a part of an employment contract, in the same way as, for instance, maternity or whistle-blowing policies are. The policy IP should govern matters such as:

- invention capture process
- financial incentives for patent inventors
- infringement management
- open-source handling
- IP registry management
- IP functions across the company
- IP reporting structure

Enforcement Strategy

What is your IP enforcement strategy? What is your goal? What is your bottom line in negotiations? How do you approach different parties? How aggressive are you willing to be? How much are you willing to spend? Is there an emergency IP budget set for this?

If you are unsure of what you would do if you came across a potentially infringing product or service, you should probably answer the above questions before such a situation arises. Any contentious issue will affect your emotions and the last thing you want to do is for your emotions to influence your judgement. Take all the questions above and create a methodology of assessing potential IP issues. Start a list with categories of different parties you have encountered in enforcement to date and set a plan of actions and how you escalate the issue gradually with each category. You can also take the opposite approach, focusing on how you step down from the initial demands and what your bottom line is. Make it clear to your enforcement team what you consider a critical issue and what merely needs monitoring to see how it progresses. Leave enough breathing room to make decisions that fall beyond your methodology but be sure any such decision follows the general guideline, and you can justify taking or not taking an action. The worst you can do is make inconsistent choices that in turn might weaken your brand as your infringement boundaries become muddled and decisions unforeseeable.

If you open Pandora’s box, you need to be sure that you are ready for it. Your investors will appreciate that you have a transparent strategy and that you are willing to go to great, but reasonable, lengths to protect your business, and as a result, protect their Return on Investment.

Intellectual Property Insurance

Are you aware of any parties that might be copying your product or service? Is there a risk that you might be sued for IP infringement?

Once upon a time, IP insurance as a product was so expensive that it fell absolutely outside the reach of any SMEs. Nowadays, one can obtain a policy that works both defensively (covering costs of legal proceedings against you) as well as offensively (covering costs of you pursuing legal proceedings against a third party) at a relatively modest cost of a few thousand pounds annually. IP insurance cover is not yet a standard “tick box” on an investment due diligence sheet but with its affordability I would expect it to become one, just like professional liability insurance is.

Conclusion

For any new business, investing in Intellectual Property is not only a powerful tool for increasing the valuation of the business, but also a valuable asset that can protect your brand and give you a strategic advantage over your competitors.

1.4 BRAND STRATGY FOR SCALE UPS: PROECT YOUR VOICE

Natalia Korek and Agnieszka Musiał, Basck

Your brand is the voice of your company; it will reflect your goodwill and reputation built up as a result of years of hard work. What if you picked a voice at the outset that can be easily silenced or one that is heard differently depending on who is listening to it? Or a voice that can simply be lost in the crowd?

It is surprising to discover how many companies draw inspiration, either expressly or subliminally from existing brands already recognised and advertised in their business area or a closely related business area when selecting a new brand name. Needless to say, those imitation brand names, if adopted, are likely to be silenced at birth by swift and successful legal action which will leave you out of pocket and right back where you started. Then there are those brands which sound fine in English, but speak with a very different voice when heard in another language; this said, surprisingly some prominent brands survive despite this oversight:

- *Vauxhall/Opel **Nova®** for cars - where "No va" in Spanish means "does not go"*
- ***Irish Mist®** for liqueurs - where "Mist" in German means "manure*

Finally, there are brands whose voice can be lost in the crowd. Brands which are prone to falling into this category are those which are developed for products for short term or seasonal lifecycles. This is seen frequently in industries such as cosmetics or fashion where the tendency is to pick a name which is more descriptive of the look and feel of the product or the benefits it provides. A number of competing products jostle for position on the shelves where the brands are made up of the same or very similar descriptive words and, as a result, their voices are diluted or weakened. They cease to be the voice, which can clearly denote the origin of a particular product and is the essential function of a brand and its legal reflection; the trademark.

CREATION: the voice that reflects who you are, not what you provide

When there are so many competing demands on the funds of an expanding business, it might be counterintuitive to choose to set aside funds for a creative agency to help you create your brand[s] with you. However, developing the brand personality and the values you want your brand to represent from the outset, will pay dividends in the medium to long term, generating the distinctive recognition, customer loyalty and goodwill behind the brand which will sustain your business development in both good as well as challenging economic circumstances.

For many FMCG brands, new brand creation will invariably result in highlighting some quality or benefit of your product or services in the name itself; the trick will be to ensure that the resulting name, even if containing a descriptive element, falls on the right side of the line, so that the selected name is also sufficiently legally strong to be enforceable against imitators and copycats. For this reason, it is important to ensure that you have a trademark advisor participating at the workshops with the branding agency to act as a foil to the creative professionals.

In more highly regulated industries, such as the pharmaceutical or agricultural industries, the ability to be creative around the choice of brand name is much more prescribed, because of the overriding imperative around patient/consumer safety; i.e. you cannot describe the efficacy or other characteristics of a product in the brand name if it has any potential to mislead. Hence the choice of brand names in these industries inevitably gravitates towards invented names, which also make for the strongest legally enforceable trademarks.

CLEARANCE: the voice that can be heard

IP practitioners take various approaches to conducting trademark checks in the Trademark Registries in order to advise their clients as to their brand's availability for use and registration. Much is dictated by the budget a company has to invest behind those activities. The cost of full availability searches for a mark in multiple countries is likely to be more expensive than the cost of applying for and straightforward prosecution of the trademark through to registration in those same countries.

For a company with plans to expand in one or more markets outside its first core market, one approach is to carry out full searches in line with the timings of your launch plans in those countries with less rigorous searches [identical/near identical] in countries which are further down that launch plan. If all searches look fairly positive, then file trademark applications immediately in all countries searched. The advantage of this approach is that the registration process in the countries in which you have carried out the less rigorous searches will throw up any significant third party trademarks as part of that process. In many countries, you can obtain a registration within a year and you will know of any significant obstacles well before that.

This approach also works in regulated industries where the name has also to be approved as part of the Regulatory process and the commercial launch of the product may be 5 or more years down the track from the time you are creating and clearing brand names. In those circumstances, you will be searching for a first choice brand name and several backup names and can allow for an attrition rate, either as a result of the regulatory or Trademark registration process. The only difference in approach here is that you would carry out your full searches only in your must have countries which will probably, but may not necessarily, coincide with your list of first to launch countries.

The most important point to note in this context is that the most important advice, which is based on clearance searches, is freedom to operate. If you launch your new brand in a country and are successfully sued in the courts of that country for trademark infringement, then a company will have to immediately cease use of that brand, withdraw all marketing and publicity already in circulation associated with that brand and pay damages to the successful party to compensate them for their loss of profits. It is therefore vital to create a branding strategy that does not only rely on the main brand name. Put the same emphasis on building and protecting your logos, straplines, product names etc. Any of these might eventually become your fallback plan and allow your business smooth transition from one name to another, without losing a significant amount of goodwill accumulated in the previous name.

EXPANSION: the voice that is ready to echo without borders

The trademark registries around the world are crowded, particularly when you are trying to protect Trademarks in popular business sectors. For a scale up company, the holy grail is to build and then protect a global brand, whatever that may mean for your business. At a minimum, this will mean trading with a single brand in all the countries in which your products and services are on the market. The obvious reason for this is enhanced brand recognition which, in turn, increases bottom line sales. It is rare that a company will achieve this holy grail without overcoming some legal challenges. Even the largest companies have not overcome insurmountable obstacles for some of their brands.

- *The car brand is **VAUXHALL®** in some countries, **OPEL®** in others.*
- ***MARATHON®** chocolate bars are **SNICKERS®** chocolate bars in some countries* during the prosecution process when they are raised as obstacles to registration. A good trademark attorney will use a variety of skills and tools in their toolkit to obtain commercially acceptable coexistence agreements with a third party which may be country or regionally specific or global in application.

Another point to consider is how your brand will be perceived by consumers in various countries. We have already mentioned how a simple difference in the understanding of the same word in different languages can entirely alter the perception of your brand. However, during your international expansion, you may find out that in addition to linguistic and alphabetical issues, cultural, psychological, or even historical differences may also cause consumers from different countries to respond to your chosen brand name differently. Some people may prefer the brand to be in their own local language, while others end up responding better to a foreign-sounding name. These and other preferences may affect your commercial success. Nevertheless, using different local names does not mean that your brand or products are not global and there are ways of ensuring that consumers will see that these names are related.

Unilever's Hearbrand Family of ice creams contains OLA®, ALGIDA®, FRIGO®, ESKIMO@ and few other ice cream brands in different regions, which, however, are all used with the same device element and in similar colours.

REGISTRATION: the voice that is the only one listened to

A Trademark registration gives the registered proprietor, on paper, the exclusive right to use the trademark for the goods and/or services for which it is registered. By definition, this is a monopoly right, which is the only form of intellectual property that can last forever, so long as the registration is renewed, usually at 10-year intervals. A portfolio of Trademark registrations supported by commercialisation of the brand in the relevant countries can be a company's most valuable asset. In order to illustrate this, consider a theoretical investment decision which gave the investor the choice between purchasing the COCA COLA® Trademark portfolio together with the trade secret recipe for the soft drink as opposed to purchasing all the manufacturing sites and bottling plants which COCA COLA® owns to produce and distribute the product. The right to affix the trademark COCA COLA® to the drink as opposed to access to the means of manufacturing and distributing a generic product from those premises is likely to be far more valuable, even if the investor had to invest in new manufacturing facilities or license others to manufacture.

The challenge is to ensure that the company's Trademark protection continues to reflect its commercial footprint as the company grows. To give sufficient attention to this, among all the other priorities, is a challenge by itself. New Trademark applications must be placed on file well in advance of entering new markets. The more successful a brand becomes, the more likely an opportunist is to file a speculative Trademark application for your brand and then attempt to hold you to ransom, demanding payment for its assignment back to your company.

In addition to securing all relevant Trademarks, a company must not forget domain names! Register your top-level domain names [TLDs], country level domain names [CLDs] or generic TLDs (gTLD) incorporating your brand names. Once you grow, you could even try to apply for your own gTLD. The practice of domain name squatting and exhorting payment for the return of those domain names to their rightful owners is rife. As opposed to what some entrepreneurs are led to believe: holding all domain names does not mean you do not need a Trademark anymore. Similarly, having registration at Companies House is not considered an alternative to Trademark rights, which are the only rights providing you with exclusivity to the name in the selected business fields.

MANAGEMENT: the voice that does not need backup singers

The routine management of your registered rights means you will need to keep good records of the use of your brands. A certain percentage of your portfolio will fall due for renewal every year. This is not in all cases as simple as paying a fee; in some countries proof of use is required as a condition of renewal and, in others, additional supporting documentation. Every company should pay great attention to maintenance as, once rights are lost, it is not straightforward to restore them and third parties may well have already taken advantage of lapsed rights to jump in and file a Trademark application for the brand for which you have done all the hard work to create and build a reputation.

As you build and develop the profile of your brand, it will pay dividends if you keep an eye on the competitor landscape. As a minimum, you should be watching the publication of conflicting Trademarks on the main national and multinational (e.g. European Trademarks) registers so that you can challenge conflicting Trademarks within the relevant prescribed timescales. You will probably need a similar watch service in place to alert you for conflicting domain names.

Counterfeiters will only reproduce branded products where they can make the highest profit margins on sales. Imitation is the sincerest form of flattery in this context and your brand has definitely met the threshold to merit this criminal activity if counterfeiters target it - this is not of much comfort of course! There are management tools you may wish to invest in which will trawl the Internet and alert you to the sale of potential counterfeit/lookalike products. Online marketplaces have dedicated teams to deal with counterfeit claims but they will not take action unless your brand is registered as a Trademark in the relevant country of issue. Likewise, if the look of your packaging is unique - register it as a design to allow for smooth handling of any counterfeit issue.

However, performing internal due diligence is just as important as having an external one. Having an internal Brand / IP Policy document setting out the internal rules regarding the use of your brands, which should be followed by your entire team will ensure that you have the correct and genuine use of your brands properly documented. At first, this may sound like an unnecessary formality, but you will quickly realise that it is not easy to prevent your brand from becoming generic or diluted. For example, did you know that in any product descriptions or articles, the brand name should be used only as an adjective? Even if you did know that, it is almost certain that not everyone in your team does. Remember that it is not only the marketing team that should follow your Brand Policy, but all other team members too, especially when speaking about the company and its products on social media and at events. The more conscious your team is, the easier it will be for you to enforce and prove the use and reputation of your brand in the future.

The principle advice is, that, as your company scales up and your brand becomes increasingly prominent and profitable, you need to be increasingly proactive to police and monitor the integrity of your brand and take action, where necessary, to enforce your registered rights which are the legal foundation of that brand.

ENFORCEMENT: the voice that is firm and assertive

You are taking proactive measures to police your Trademark rights as discussed in the previous paragraph. It follows therefore that you need to be prepared to maintain the competitive space around the legal monopoly you have obtained by virtue of your portfolio of Trademark registrations. You need to be proactive in opposing conflicting marks, particularly in your key markets. Additionally and hopefully, more rarely, you will need to enforce your rights through the courts if necessary. For that you will need to allocate a litigation war chest each year to take on these conflicts.

As a rule of thumb an average business spends an estimated 10% of their revenue on all IP protection annually [including Trademarks]. However, that is not the end of the financial provision you should make; an additional 10-15% of that IP budget should be set aside for legal enforcement activity to cover the range of activity described above. This percentage will grow significantly if you happen to find yourself on the receiving end of a successful litigation.

Failure to enforce your legal rights leads ultimately to dilution of your brand and of course a negative impact to your business health and bottom line.

ENJOY THE JOURNEY: brand strategy to follow your business

The best brand strategies we have seen are those where there is a close cooperation and clear communication between the main stakeholders at the very outset. Discussing the brand values, understanding the company’s vision and growth plans requires involving both the top decision makers of the company as well as brand designers and IP practitioners. Only a strategy that takes into account and understands the perspectives of all parties will allow the creation of a brand that has a clear pathway to grow and support the business’s aspirations. Additionally, engaging all the top stakeholders early on and getting their clear sign off to establish default instructions will allow them to delegate and get on with the other tasks demanding their time.

In summary, as you scale up, a strong, well-protected brand is crucial to your business’s success. There is a clear and direct causal link between repeat sales and increased profit margins to the strength of your brand, so it is worth spending more time and allocating budget to get it right from the beginning rather than executing the trial and error strategy which ultimately often results in a bigger cost allocation.

1.5 RAPPORT

Karren Whitely-Brooks, Whitespace

"Raise your words, not voice. It is rain that grows flowers, not thunder."
— *Rumi*

As we return to normalcy in the post-pandemic environment, we are logically re-examining the basics of our business practices. As consultants here at Whitespace, we are frequently requested by our corporate clients to help them improve their relationships. These relationships are not just with their clients but with their colleagues and stakeholders, as well.

We like to begin with the fundamental concept, which we think is most important: that of rapport. We state unequivocally that "rapport is above everything."

The accepted definition of rapport is:

'a close and harmonious relationship in which the people or groups concerned understand each other's feelings or ideas and communicate well.'

Every business and, indeed, every positive human interaction desires "harmonious relationships" and indeed better communication; but how is that achieved?

Here are six simple rules for building rapport:

- Put on a smile
- Show genuine interest
- Listen actively
- Use people's names when possible
- Keep their interests at the forefront
- Sincerely, make them feel important

The problem with these simple suggestions for building rapport is that one may be inclined to fake it. One can put on a smile and pretend to be interested, like a telephone marketer who feigns interest but needs to deliver their pre-prescribed script. We have all had the unsolicited call offering cheaper energy or better 'phone service', which is not only a nuisance but is the ultimate phoney attempt to build a relationship based on the assumption that we need their service.

One may very well have a product or service, which one knows the prospect needs. The importance of the communication of that offering is to make the prospect aware, or come to the personal conclusion that they need the offering, not because we need to sell but because they will be better off by purchasing our offering. The communication which creates this needs awareness requires an empathy for the condition and problems of the customer which may have nothing to do with the solution we are offering, but by paying attention and listening actively, one improves the relationship and increases the possibility of a positive outcome.

The importance of being present can be demonstrated by those who actively listen. We literally give value to our relationships by paying attention to the communication process. Not the perfunctory, “ok” or “uh huh” but the true reply of understanding and receipt of the energy accompanying our communication.

One interesting derivative of this relationship principle is that where your attention goes, your money goes. So, it is the forethought of our firm intention coupled with the paying attention of active listening, which produces the results of improved relationships.

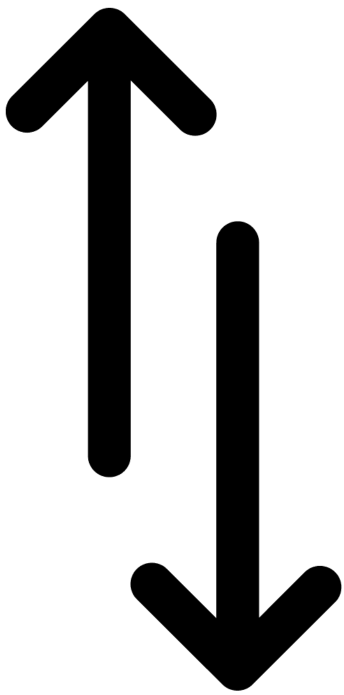
While the engagement and involvement described above are nothing new, we like to step back and request that you first review your intention. If you agree that you would like to have re-energised and more valuable relationships, then before everything, you must make that a firm intention and indeed, a companywide commitment communicated throughout your organisation.

Early in my consulting life, I was invited to speak at a conference on a cruise ship off the coast of Southampton, England. One of the other guest speakers was Stephen Covey, author of the bestseller, *7 Habits of Highly Effective People*. We discussed relationships and communication and I frequently recall something, which helps one distinguish and recognise the trustworthy and valuable relationship from the ordinary and unimportant relationship. Covey stated, “most people don’t listen with the intention to understand, most people listen with the intention to reply.” Another of his memorable sayings was "people don’t care how much you know until they know how much you care."

It is one’s ability to actively listen, with interest and care, which earmarks the empathetic, the person with whom we are able to relate. Relationship building requires focus and the decision or intention to improve. The next time you interact with an important relationship, take the time to ask yourself:

- How did they feel?
- Did you enquire about and understand their feelings?
- How did you leave them feeling? More positive or less?

The American psychologist, Karen Rook, investigated the research on positive and negative influences on relationships and concluded that because of the variability of the human psyche all relationships are either improving or deteriorating but are never static.



If one accepts that our human relationships are either heading in a positive or negative direction, the question is; how do you improve one's connectivity to move positively in an upward progression?

You may have heard from isolated acquaintances lamenting during this pandemic that they don't have anyone to talk to. However, have you ever heard someone say they would like to have someone who they could listen to? The more valuable ability would be the skill of active listening, one who receives and empathises with other peoples' feelings. It is a considered value we place on active listeners, who not only hear but comprehend, who not only receive our communication but who empathise with our feelings that is a desired skill to improve connectivity and relationships.

At the beginning of this discussion, we quoted the Persian poet, Rumi, who said, "Raise your words, not your voice." We have all witnessed and most probably fallen into the tendency to raise our voice, possibly to someone who doesn't understand

English or does not comprehend our words, as if being louder will help. The human reaction is to believe that the receiving party may be hard of hearing, while it may be more likely our inadequacy of expression, which is the culprit for faulty understanding.

This quote from Rumi also speaks to the importance of rain that grows flowers, which is comparable to the positive movement in the connectivity of our relationships, which flowers with frequent and patient communication. Rumi continues by cautioning against the fury and expression of frustration, which often precedes communication that is not received, and leads to one raising the voice; the thunder which can be surprising and disconcerting.

In every business the issue of relationships both more and better is at the heart of success. In our consultancy practice we ask the leaders to step back and say what is it we need in terms of relationship growth? This analysis is key to understanding our objectives. We would categorise relationships in business in four main cornerstones to build a stronger corporate foundation. These cornerstones are collaborators, clients, investors, and suppliers.

1st: Collaborators

a. Creators
b. Executors

We all need teammates and as you build your company personnel, you will realise that not all creators have the patience or persistence to execute the vision. So, company directors need to ask themselves, what types of relationships do we need to make the company better? Seldom, do the creative visionaries have the skills and personality required to execute the programme and vice-versa.

2nd: Clients

a. Current
b. New

Every company wants more and better clients, which they might call "users" or "subscribers" or a variety of other terms. It is important to increase the current clients' relationship before the company starts to pursue new users of their products or services. The popular business speak term is "share of the wallet;" that is to say a broader and more remunerative relationship. Every company can improve their current client relationships by analysis of what they like and need and what appears to be inadequate in the current client experience.

New clients will be attracted to new offerings but also different demographics may be attracted to your offering by taking a new and different marketing approach, which may include social media and third-party endorsements.

3rd: Investors

a. Capital
b. Expertise

All business needs capital to grow and, in early stages, relationships with wealth and the ability to invest in our vision are key to success. The requirement of ethical money was never more important as regulators and journalistic investigators are constantly pursuing the provenance of investment funds. The offering of equity in our companies to friends and family and interested investors requires detailed due diligence to understand if the relationship which accompanies the capital and their source of funds is one which will enhance the reputation of the company.

4th: Suppliers

a. Service Providers
b. Product Providers

Every business requires a quantity of relationships, which supply us with services and products and are key to our success. All too often we are focused on price and speed of delivery rather than our actual relationship with these Suppliers. It is important to review not just the contracts but also the relationship managers from our company in charge of these important providers. Are we?

If you have made the decision to improve your relationships, congratulations! Here is a simple chart for any organisation to analyse where they are and where they want to go. Independently of the size and complexity of one's company, we simply categorise business relationships into: Collaborators, Clients, Investors, and Suppliers. The chart is designed to represent the intention to build better relationships by giving a mathematical measurement of the number and quality of these relationships. At any point in time, the trend in the number and quality of relationships may be increasing or decreasing. On the next page is a visualisation to assist your strong intention.

Collaborators in the graph below can be permanent employees or part time partners who help produce the goods and services for the company. While every company wants growth, the management of the employee relationship and the size of the employee population are key metrics in determining the efficiency and ultimately the profitability of the company. In the young company example in the graph below, there are only 30 collaborators with relatively high quality of relationship rating of 70. The challenge for every company is to maintain or improve relationships as the size of the enterprise grows.

In every business the number of clients and the quality of the relationship is key to financial success. In the chart below the young enterprise has 90 clients but the average relationship is only a rated 50, possibly because the clients have only interacted with the company a few times. Obtaining client satisfaction and repetition are keys to improving the average relationship and programs designed to engage, reward and understand the new clients are important in every business. This company should examine how to increase both the quantity of and relationship quality of their clients.

Ideally investors will bring not only capital but also expertise and a network of valuable contacts to enhance your value proposition. They exist in every company relationship and those who may not have capital but can provide knowledge, and "sweat equity" of experience will provide added value to your company.

You may have other names or subdivisions for these relationships, but every company has investors sometimes called "owners" or "shareholders". The capital of these investors is the life-blood of the company and gives the managers, directors and leaders of the corporation the ability to produce their products and services. The chart above shows this young and small enterprise to have only 5 investors who rate a qualification of 80 in terms of their importance and quality of relationship. These relationships are often family and friends in start-up companies and communication can be frequent and detailed. Larger corporations may have thousands of anonymous shareholders provided by the capital markets, but who nonetheless, require earnings reports, shareholder relations and meetings to make sure that the value of the relationship is nurtured.

While suppliers for any enterprise are important, the entire supply chain must be considered. In the recent logistics crisis in Britain, it appears immigrant workers who have returned home due to the combination of the global pandemic and Brexit are threatening the supply chain in a variety of important business components, notably fuel and construction materials. In the above graph, the new enterprise has an alarmingly poor relationship metric of 40 for the 20 important suppliers to the company. While the infrequency and anonymity of many suppliers may make relationship building difficult, the importance of obtaining alternative suppliers and building solid relationships was never more important.

Rewarding relationships

We all like the concept of getting paid but seldom stop to contemplate the meaning of "paying attention." This colloquialism incorporates the concept of exchange of value implicit in the act of payment and combines it with the attention and presence required to actively listen. We literally give value to our relationships by paying attention to the communication process. Not the perfunctory, "ok" or "uh huh" but the true reply of understanding and receipt of the energy accompanying our communication.

One interesting derivative of this relationship principle is that where your attention goes, your money goes. So, it is the forethought of our firm intention coupled with the paying attention of active listening, which produces the results of improved relationships.

Three examples of the emotional and psychological feelings one has in the exchange of money will help in understanding possible obstacles to building better business relationships.

- What is my rapport with money?
- What mood am I in when I hand over money for payment?
- What is my persona when I receive money?

We all know people who think money is evil and something to fear. These negative attitudes and influences can inhibit the commercial relationship. It is axiomatic with words like "tight" and "stingy" that some people are overly frugal and careful with paying their legitimate share. When we find ourselves disappointed or hesitant in paying it may be that our expectations exceed the anticipated value of the goods or services we are purchasing. In all cases, realistic expectation management will increase and enhance our ability to have a positive business relationship.

When examining one's attitude toward relationships, it is worthwhile to notice one's attitude to paying for services or being paid for one's work. Do we appreciate the exchange or are our expectations not being met when we receive less than we think the value of the exchange should provide? Aspiration to receive more is a human condition but unrealistic expectations can lead to poor relationships between our employer or shareholders. Managing expectations in terms of what one's work is worth and what one expects in payment are important abilities to improve the business relationship.

One may very well have a product or service that one knows that the prospect needs. The importance of the communication of that offering is to make the prospect aware, or come to the personal conclusion that they need the offering, not because we need to sell but because they will be better off by purchasing it. The communication, which creates this, needs awareness and requires empathy for the condition and problems of the customer which may have nothing to do with the solution we are offering; but, by paying attention and listening actively, one improves the relationship and increases the possibility of a positive outcome.

One technique for improved phone connectivity is by practicing a simple Whitespace drill on the next few calls you have; try to understand three things from the recipients of these calls.

1. Where are they?

You may think they are in their office, or are they? We have all diverted our phones to our mobile because we had other, outside the office requirements. Without being too intrusive or nosey, one can both inquire about the location and earn the right to continue with the reason for your call by asking simple questions about how their day is going and is this a convenient time? The trust building aspect of being respectful of your relationship's time and environment will increase your connectivity and improve your communication. At the end of your call review, make note of what you learned about the environment of the person you called.

2. Did they understand your communication, reason for your call, message you wanted to deliver?

Frequently, one finishes a call and doesn't take the time to understand the effectiveness of the communication. Make note of whether you heard acceptance and agreement of your message. Did you just assume that your communication was effective?

We have all heard the derivation of the word "assume" to mean an ass out of you and me. Acknowledgement is not necessarily an agreement. 20th-century sales techniques placed great emphasis on getting prospects to say "yes" by an almost hypnotic and frequent insertion of subliminal questions such as "is that ok?", "Do you understand?", "Do I make myself clear?", "you know what I mean?", "are you with me? etc. The theory of this technique was not to actually produce understanding with your communication but trick the client into agreement. In this second technique, practicing a post-call review will increase one's intuition and assessment of the energy of the relationship and the communication.

3. What is the follow-up, next steps, agreement, call to action?

All too often we finish our communication with a goodbye and a possible salutation for having a good day without asking for, or deciding on, next steps. Again, the firm intention, to get to the result of the desired goal, which might be a face-to-face meeting, a concrete proposal or possibly a buying decision, is often forgotten in the cut and thrust of the conversation. Make a note of the conclusions, agreements and next steps including what the recipient of your call has promised to action.

We often ask new relationships, when speaking about others, "What's your connection?" We may be seeking to understand the contractual responsibility of the connection or the commitment to the proposition but in either case we are attempting to realise the energy. We have all struggled with different plug sockets and voltage on our travels. Matching the right plug and transforming the energy will be key in getting our electrical apparatus to function and it is equally key to making sure the energy in our relationship is functional.

Energy can be transmitted more effectively when focus and presence are combined in the communication process. In summary, to begin with the firm intention to build better relationships will increase one's presence and harmonise one's energy. The constant analysis of where we are in the relationship graph will help build a stronger and more successful company.

1.6 INNOVATION - THE LONG AND WINDING ROAD

James Timothy Taylor and Karren Whitely-Brooks, Whitespace

...The long and winding road
That leads to your door
Will never disappear
I've seen that road before…
Sir Paul McCartney, 1969

If one thinks about innovation and inventiveness, then undoubtedly when reviewing creative hallmarks of the last 60 years the musical genius of Sir Paul McCartney will figure in the discussion. Sir Paul was said to have been inspired by a Scottish road near Campbeltown, which led to a farm he purchased in 1969, when he wrote the lyrics to *"The Long and Winding Road."*

Barry Miles, who wrote a biography describing McCartney, said the song was about the "unattainable; the door you never quite reach". No doubt the song is symbolic of the twists and turns that commercialisation of any creative expression inevitably confronts. This song was cited in High Court hearings as evidence of the "over-production" of Sir Paul's music, which contributed to the demise and break up of the Beatles.

Creative innovation, whether found in the Arts, Sciences, Engineering or other specialisations, produces a myriad of long and winding twists and turns on the road to commercial success. We at Innovators Highway, provide a road map to entrepreneurs to assist them on the treacherous journey to protect, produce and profit from their creativity.

If one enumerates the important factors required to Protect, Produce and Profit from Intellectual Property the following formula may prove helpful...

===

Ideas+research+development+patent+testing+investment+production+ planning+marketing+capital structure+demonstrated profitability = **Successful Exit**

==

While specialist companies exist to navigate each of these critical factors, the majority of entrepreneurs fail to understand the complexity of the entire equation and the importance of understanding the different exit opportunities which may include partnerships, trade sales or capital market public listings. The commercial detours along the innovators highway contribute to the amazing statistic quoted in the US periodical, *Forbes,* which stated that "Of today's 2.1 million active patents over 95% fail to be licensed or commercialised."

UK investment in "protected intellectual property rights is over £100Bn but the hidden dimension of unprotected and uncommercialised ideas is an iceberg of opportunity estimated in over £900Bn." *Source: UK Intellectual Property Office 2019.*

Much the way one plans a substantial road journey by checking one's vehicle, the roads and detours by employing a GPS navigation system and understanding the best exits to lead to one's destination; such planning is required by a successful entrepreneur.

The statistics of unused good ideas begs the question of why so many *inventors* cannot be classified as *innovators?* And what distinguishes between invention and innovation? We look for investors in good ideas with good strategies and controlling the Intellectual Property increases the attractiveness to invest in the good idea.

WHY INNOVATE? WHAT DOES IT REALLY MEAN?

If you take it as a given that innovation is necessary for any business, and indeed society, to advance and flourish, then you may be reading this chapter to find an edge in your quest to improve your company. If however, you are an ***inventor***, then you may ***not*** have the requisite mindset to be an innovator. Common wisdom would argue that if one can invent something then, surely, one is automatically an ***innovator.*** The confusion begins when one reviews the popular definitions for the noun, ***innovation***. The Merriam-Webster Dictionary offers these definitions: ***1. The introduction of something new*** and goes on to state its second most common definition, ***2. A new method, idea or device.***

When one explores other information sources such as Wikipedia, they begin with the same definition for innovation as "*something new*" but expands on the idea by stating, "*innovation takes place through the provision of more-effective products, processes...that are made available to markets, governments and society"*. If however, the inventor who builds a ***better*** mousetrap does not require a-***brand new***-mousetrap and the inventor is able to commercialise and positively affect society with his mousetrap, then that inventor is truly an innovator. Innovations may thus be incremental improvements, which satisfies our clients needs and demands rather than just something new or different.

The futurist and author, Jacob Morgan, gives a more easily understood example, which is important if you and your company want to innovate. He asks, "Is Google Glass an invention or an innovation?" And offers in contrast, "is the Apple iPhone an innovation or an invention?" This is not just a discussion of semantics but goes to the core of the dilemma. If the invention of Google Glass, while novel and definitionally appearing to be an innovation, remains an oddity with little commercial acceptance or demand, then the invention of Google Glass, he argues, is ***not*** an innovation. The iPhone, Morgan states, is "both new and has had a profound influence in the way we communicate, store and access data," which makes it truly an innovation. It is as Wikipedia offers, "the more-effective" inventions, which results in an innovation and the inventor and his company to be classified as an innovator.

Most everyone would acknowledge that Elon Musk is an innovator, with success in his electric car company, Tesla. Yet the inventor who inspired Musk to use his name and indeed, some of his technology is the inventor Nikola Tesla, who never attained true commercial success despite registering almost 300 patents for his intellectual property.

"Invention is not enough. Nikola Tesla invented the electric power we use, but he struggled to get it out to people. You have to combine both things: invention and innovation focus, plus the company that can commercialise things and get them to people.".

Larry Page Co-founder of Google

Trading in IP – A Good Idea.

The traditional route of investing in an early stage business that has a "good idea" is completely reliant on the quality of the management delivering the business performance. Yet the reason for the investment was the "good idea".

Most "good ideas" are defined as intellectual property (IP) in the business and the protection and exploitation of them are the key to success of the business.

One of the best forms of protection is patenting, this protection process gives the rights to the patent holder to uniquely exploit the "Good Idea" for a period of 20 years.

A business may have patents on its books, but they are not in the assets of the business as many investors believe. Quite often the patent is owned by an individual who is a member of the business, not the business itself. Although there may be assignment of the patent to the business, the issues of ownership and value become less transparent if the business starts to fail.

Business valuation is generally based on a multiple of profit generated from the exploitation of the "good idea" – these profits are likely to be generated by the good idea, so why not own the "good idea" and take a revenue from the "good idea" for the life of the patent as opposed to investing in the business? Or where possible – do both.

This is a hedging process and therefore de-risking the investment and generating returns to the investor are not simply based on some share sale event. Failure of the management to deliver the “good idea” should not be because the good idea failed, just the exploiters. Moving the good idea to a better management team must be an option for the investor, or simply having the right to sell the good idea allows for some investment recovery and return should the business not deliver its expectations.

Assignment of patents is a legal process that allows shared ownership of the patent. The process can be defined through a formal contract alongside a legal agreement prepared by a patent attorney to ensure ownership is vested in the investor.

The assignment and the contract can define all the rules surrounding the rights and benefits for the investor in protecting their position in respect of the “good idea”.

The marketplaces for tradeable share transactions are well understood; the reality for share transactions in closed companies however remain: willing buyer – willing seller, generally based on calculated multiples on future profits. These remain at best extrapolations from predictions made by the management team and their advisers to facilitate finance to deliver the “good idea”.

Validating and defining the “good idea” and therefore developing a price and value model for the future revenues will allow better assessment of the success opportunity.

The world is changing, and trading of Intellectual property will become commonplace in the future.

An example of this change is IP Marketplace:

At IP Marketplace you can put your patents, patent applications, utility models, design, and trademarks up for sale or out-licensing. You can also use IP Marketplace to search for IP rights to buy or license in. The website is managed by the Danish Patent and Trademark Office. It’s free of charge for both buyers and sellers.

- https://ip-marketplace.org/

‘INTENTIONS HAVE NO INTELLIGENCE’

Unfortunately, the word ***new*** and the promise of innovation has become ubiquitous in our lives as any visit to the supermarket will attest. It is obvious in every aisle of our shopping that ***new*** and ***improved*** can apply to everything from apples to zucchinis. All too often, leaders of business have a mindset which says, ‘innovation is just some business school hype or marketing speak.’ The scepticism surrounding innovation is that it has little relevance to the day to day operation of the company. We strongly suggest the company's “vision” or “mission statement,” which is necessarily a broad generalisation to be delivered over a long period, should include the ***intelligent intention*** to innovate. The company's long view must be accompanied by the short-term deliverable projects, which will become commercially viable and make a difference to our clients and shareholders.

The following diagram demonstrates how the importance of long and short-term goals relate to a company's ability to innovate. We would argue that in all three areas of Mission, Strategic Goals and Operating Objectives there must be a stated and determined intention to innovate; not lip service, but a firm and communicated intention; not just a hope but an intelligent intention.

The requirement for specific and short-term projects to produce commercial success is the test, which will prove whether the new product or process is truly innovative.

Ever since Peter Drucker argued in the *Harvard Business Review* in 1996 that "Innovation is the specific function of entrepreneurship," business consultancies have been attempting to assist companies to change their mindset. Drucker's premise instructs companies to promote "wealth producing resources" as a fundamental goal for their employees. As the 21st-century continues to make great advances in artificial intelligence, it appears that business leaders may be now hoping that technology will provide these much sought-after resources and innovations.

WILL ARTIFICIAL INTELLIGENCE ASSIST INNOVATION?

Arvind Krishna, Director of IBM Research says, "Faced with a constant onslaught of data, we needed a new type of system that learns and adapts and we now have that with AI. Krishna further states, regarding the use of AI in business innovation, "What was deemed impossible a few years ago is not only becoming possible, it’s very quickly becoming necessary and expected.”

In just the last decade AI has exploded because of the combination of big data with powerful (GPUs) graphics processing units, which has benefited from employing the well-known model of Deep Learning. We all remember the stories of Deep Blue which was programmed by the forefathers of IBM Research back in the 20th-century and which culminated in a competition with the Russian Chess Master, Gary Kasparov in 1996. It was IBM’s Deep Learning that allowed the computer to analyse millions of chess moves and which revealed Artificial Intelligence as one of the most important technologies to be developed in the 21st-century.

It is this Deep Learning popularised by Deep Blue, which will be educated by Deep Reasoning in order to create a new technology, enabling machines to conduct unsupervised learning. It is the human brain function of unsupervised learning, which continues to baffle the technologists. IBM Research is attempting to make machines curious and to seek answers. These machines will indeed produce new questions, as they learn from each other, but this is proving far more difficult than the much-discussed language and image recognition applications.

The emotional side of facial recognition, for example, and the reasoning which humans develop from a young age, is much more difficult for Deep Learning to grasp. Computer scientists are working with neuroscientists and psychiatrists to help the advanced computer facial recognition of emotional indications. Dr. Fei Fei, Professor of Computer Science at Stanford University says AI image recognition struggles to identify and interpret emotions; the computer’s cognition is similar to the human condition classified as Alexithymia. This is a condition which inhibits some humans from both expressing and recognising emotions, often accompanying Autism and other psychological disorders. IBM research, however, has made great strides in image recognition which is helping identify and diagnose a variety of illnesses and pathologies.

One example of AI image recognition is the computer application, which assists the clinician in recognising melanoma lesions on human skin. While a clinician may be confident in recognising a certain type of lesion within a predominant racial skin colour, they dramatically increase their diagnostic ability with the AI database. The computer is able to compare, select and identify from a much greater range of images and skin tones and alert the doctor to possible areas of concern from patients they are not accustomed to treating. The use of AI in pathological recognition and diagnosis meets the societal impact criteria for innovation.

...Who's zoomin' who?
Take another look, and tell me babe
Who's zoomin' who?
Who's zoomin' who?
Aretha Franklin 1985

The iconic American soul music singer, Aretha Franklin, sang *Who's zoomin' who?* in 1985. When interviewed and questioned what the title lyrics really meant she responded, "in relationships, the game always has one partner who thinks they are fooling the other."

The use of the Zoom application or Microsoft Teams or even Apple's FaceTime has led to the ability to connect over the Internet rather than having to go to an office or a physical meeting place. While the advancement and economic cost of online meetings has been a salvation for many companies during the pandemic, many business consultants have studied the differences and effectiveness of working from home.

While the mastery of the technology is important, we would like to concentrate on the concepts of presence and emotional connectivity, which can be improved with physical meetings. Make the effort to visit.

One popular digital consultant lists 5 main reasons physical meetings are important. The present London Mayor, Sadiq Khan, concurs and is worried that office real estate and the corresponding tax base is in decline with the use of stay at home office meetings. Mayor Khan has urged city's office workers and businesses to embrace post-pandemic hybrid working, with staff returning to offices for one or more days a week, as the prospect of more after-work socialising gives London's hospitality sector a much needed boost.

Whilst there are many good reasons for physical business meetings here are 5 important considerations:

1. It Gives You the Chance to Understand their Body Language
Are they connected to your conversation, what signs of being present and relating to your presence are evident?

2. It Helps You to Focus
Fewer distractions from family, pet, and household issues.

3. It Is Appreciated By Clients
A chance to physically deliver literature or show and demonstrate products

4. It Helps Develop Trust and Transparency Easily

The hospitality required to have a guest and be a guest increases the connectivity.

5. It Proves to Be More Effective

Follow up, objections and plans for action are more easily agreed face-to-face.

In summary, it is more difficult to be "zoomin" or playing a game like the Aretha Franklin song suggests, when one is physically present rather than speaking over a virtual meeting service.

We at Innovators Highway realise how long and winding the road to commercial success can be. We begin with the firm intention to innovate not just invent and we realise the entire journey and myriad detours must be contemplated and anticipated from the beginning.

PART TWO - REVISITNG THE FUNDAMENTALS

2.1 BUSINESS STRUCTURES

Gary McGonagle, Howman Solicitors

INNOVATION

With the advent of artificial intelligence, the world is currently on the cusp of a new industrial revolution. The recent, and continuing, COVID-19 pandemic will invariably lead to artificial intelligence being required and accepted by the general population. Businesses need to be ready to adapt and change. Such adaptation will further bring to the foreground intellectual property law and the ability of business entities to develop, exploit and protect their intellectual property. To accomplish their aims, business entities must choose the correct business structure to allow their innovation to flourish and be protected.

CHOOSING THE RIGHT STRUCTURE

To help you identify the correct structure you should consult with your accountant and lawyer to look at the various options that are available to you. The correct option for you will depend on a number of variables, for example:

- the size of your business;
- your tax structure;
- whether you wish to seek external investment;
- whether you wish to form a joint venture with another person; and
- your appetite for risk.

TAX

The tax benefits/pitfalls of each business structure are outside the scope of this chapter. However, taking tax advice should be one of the pre-cursors for launching your products, setting up your business structure or analysing how best to exploit your innovative intellectual property.

HOW TO DECIDE WHICH STRUCTURE IS CORRECT

Currently, there are a great variety of business structures to choose from. They provide flexibility in management and budget, although some options may be immediately discounted, as it would be unlikely that you would choose to exploit intellectual property through some of those structures. For example, Charitable Incorporated Organisations (available for charities or charitable groups) or Community Interest Companies (intended for social enterprises that want to use their profits and assets for the public good) are unlikely to be utilised for exploitation of intellectual property unless, it was specifically for a charitable purpose or the public good.

In this chapter, we will therefore concentrate on the more familiar business structures and consider the benefits or drawbacks of each. To draw a fair comparison between the various business structures we need to utilise the same comparables. In my experience, the following comparables are the main driving factors behind deciding which business structure to choose:

- **Speed & Costs**

  How quickly can you get up and running? Will there be large set-up costs and ongoing costs?

- **Liability**

  If the business structure is sued or gets into financial difficulty, who will be potentially liable for the losses?

- **Finance**

  Can the business structure easily raise finance? In the intellectual property sector, research and development is a necessity and can be very costly. Therefore, the more options you have to finance, the better.

- **Confidentiality**

  Under this heading we will consider what filings and disclosures are required in relation to each business structure. This should not be confused with the disclosures that you would be required to make in relation to the intellectual property that you are seeking to exploit. For example, if you are exploiting a patent then you will be required to have disclosed details of the invention when you made your application for a patent.

- **Potential for investment**

If third parties can invest into your business structure, then you can use the money that they invest to research, grow and develop. If you need a lot of research and development, then this will be a key factor for you to consider.

- **Business perception**

Under this comparable we will identify how your competitors, suppliers and clients will perceive your business structure.

TYPES OF BUSINESS STRUCTURE

Sole trader

This is trading on your account (i.e. as an individual although, you may adopt a trading name).

Speed
Very quick, there are no legal formalities to comply with.

Costs
To start, there are no costs involved and ongoing costs will be basic accountancy charges.

Liability
You are fully liable personally, so this is a big negative.

Finance
You can borrow but you cannot offer security above your personal liability (i.e. you cannot create charges over your business structure to enable borrowing).

Confidentiality
No disclosures are required outside your basic tax return.

Potential for Investment
No potential.

Business perception
Other businesses are likely to view you as a young/basic business.

General Partnerships

The Partnership Act 1890 defines a partnership as, 'the relation which exists betweenpersons carrying on a business in common with a view to profit'.

Speed

You can start a partnership without a partnership agreement and be governed by the Partnership Act 1890. However, this out-dated piece of legislation should be avoided unless you want business uncertainty. Therefore, it is advisable that you put in place a partnership agreement before you set up. This may lead to a delay in getting started.

Costs

Start-up costs are limited and ongoing costs will be basic accountancy charges although that can vary depending upon what sector you are operating in. That said, you should engage a lawyer to draft a partnership agreement to avoid uncertainty.

Liability

Partners are fully liable personally, so this is a big negative.

Finance

You can borrow but you cannot offer security above your personal liability (i.e. you cannot create charges over your business structure).

Confidentiality

No disclosures are required outside your basic tax return.

Potential for Investment

No potential.

Business perception

With the advent of Limited Liability Partnerships the general partnership was seen to have had its day. It seems that in recent years, this viewpoint has now been rejected as people still consider that the confidentiality benefits offered by a general partnership can be attractive if they wish to keep their success under the radar.

Limited Liability Partnerships (LLP)

Members of an LLP have limited liability, which is very attractive. The LLP is a separate legal entity but is taxed as a partnership and it has the organisational flexibility of a partnership.

Speed
You will need to incorporate the LLP at Companies House and put in place a limited liability partnership agreement, which can lead to a delay in set-up.

Costs
Initial costs will be a registration fee with Companies House and a limited liability partnership agreement. Ongoing costs will be preparation of accounts and making basic filings of a confirmation statement at Companies House.

Liability
Members' liability is limited to their capital share; therefore they are not personally liable above that sum (except in limited circumstances).

Finance
You can borrow and can create floating charges rather than be restricted to having to offer personal liability as per a sole trader or a general partnership.

Confidentiality
You must file with Companies House your accounts, registered office details, members' and designated members' information. Any limited liability partnership agreement between members is a private document that is confidential to the members and does not need to be registered at Companies House.

Potential for Investment
You cannot raise money by issuing shares, although there is the potential that an investor could invest capital and become a member/designated member. That said, this is a pretty inflexible investment route.

Business perception
Although LLP's have been very popular with the professional services sector, for example, solicitors, they have not had the same popularity with intellectual property rich companies. Therefore, business perception may be neutral.

Limited Company

A limited company is probably the most commonly used and flexible business structure. A limited company has its own separate legal personality and has shareholders and also directors, the latter who direct the company's day-to-day activities.

Speed

You will need to incorporate the limited company at Companies House. This can be done on the same day, for an additional fee. Additionally, you may wish to have tailored articles and a shareholders' agreement, although this is not a legal requirement.

Costs

Initial costs will include a registration fee with Companies House and, ideally, tailored articles of association and a shareholders' agreement (i.e. regulating how the share-holders conduct themselves). However, if you are setting up a company on your own you can rely on the model articles and would not need a shareholders' agreement. Ongoing costs will be preparation of accounts and making filings at Companies House.

Liability

Shareholders' liability is limited to any sums unpaid on their shares. The share capital should also be available on a winding up. Therefore, it is always better to ensure that a limited company's overall share capital is fully paid up and that the total share capital is not an excessively high figure (for example, you can have 10,000 shares with a nominal value of 0.01 pence each that would amount to a total issued share capitalof £100).

Finance

A limited company is the most flexible method for raising finance. You can borrow, create floating charges and issue loan notes.

Confidentiality

This structure requires the most disclosure. You must file with Companies House your accounts, registered office details, director and shareholder information and certain information regarding shareholder resolutions.

Potential for Investment

A limited company can, within certain legal parameters, allow you to seek investment or take investment from certain individuals or other entities. This is a well-worn path with investors looking to invest in a company for shares. This can clearly be greatly beneficial for an intellectual property rich company as intellectual property companies can require large sums of capital to develop and exploit their innovative ideas.

Business perception

A well known business model which will be viewed as standard.

OTHER INFLUENCING FACTORS

Retaining talent

The core of any business is its employees. In intellectual property rich companies the key employees are the developers and exploiters of their intellectual property. Competition to retain and develop these talented individuals has never been higher and, given the expanding global job market and the United Kingdom's exit from the European Union, British-based businesses will always have to work hard to retain talent. A limited company does offer the business a way of incentivising those individuals to stay. For example, you can incentivise by issuing share options or by creating an EMI Scheme (i.e. a tax-advantageous employee share scheme). These types of incentives will allow individuals a share of equity now and/or in the future.

It is true that LLPs and general partnerships also offer the option to incentivise and retain talent; however, they are less flexible. Additionally, offering an individual partnership, in a general partnership, may also be counterproductive as they may be intimidated by the prospect of becoming personally liable for any losses.

Ring fencing

Ringfencing an asset describes a procedure whereby you identify an asset in a business structure that you want to protect and you structure your business to protect that asset. For example, you could ringfence an asset by deciding to transfer that asset, for an appropriate value, to another entity in order to separate the asset from another area of the business. This can be a sensible step to take, however, it is only worthwhile taking with the correct business structure. Ringfencing would be most beneficial if used by a limited company or an LLP. An example of ringfencing would be if a trading entity owns a patent and wants to diversify into another area of business. This alternative area of business may be more risky, in which case the business could set up another limited company to start the more risky area of business or, alternatively, transfer the more valuable patent to another limited company. Therefore, if the "risky business" limited company entity fails, it reduces the risk of the patent being lost in a potential liquidation scenario.

THE PITFALLS

The majority of problems occur where a business rushes to adopt a business structure without any consideration of its ultimate future aim or without taking appropriate advice (tax or accountancy). This can lead to tax problems, potential personal liability or curtailed expansion. Some of the potential pitfalls are:

No written agreement

Businesses that are a general partnership, an LLP or a limited company may require their main protagonists to organise themselves and sign up to an agreement that determines what should happen if, for example, someone wishes to leave, they die or they wish to sell. Without such an agreement in place that specifies how this should be done the parties may find themselves in disagreement, the business may stagnate or the parties may, at worst, find themselves in court seeking a resolution.

Compromised intellectual property

If the main asset of your business is its innovative intellectual property, then to lose control of it is a disaster. This can happen if:

- you enter into a business structure with third parties who do not share your vision;
- you do not have appropriate agreements in place to control the business structure, the individuals or the usage of intellectual property; or
- you do not ringfence the intellectual property and protect it from insolvency or bankruptcy proceedings.

Summary Table

Structure	Benefit	Negative
Sole trader	Low cost. Easy to set up. Basic financial reporting.	Full personal liability. Lacks business credibility in market.
Partnership	Low cost. Easy to set up. Basic financial reporting. More potential to raise finance.	Full personal liability. Can lack business credibility in market. Can reduce expansion due to personal liability risk.
Limited liability partnership	Less personal liability. LLP is a separate limitedentity and can enter into contracts.	More ongoing costs. More disclosure (e.g. partners must disclose income in accounts).
Limited company	Less personal liability. Better market perception. Better ability to seek finance and raise investment.	More ongoing costs. More disclosure (e.g. annual accounts and financial reports must be placed in public domain).

2.2 COUNTERMEASURES TO ADVANCED THREATS

Nick Ioannou, Boolean Logical

Every organisation faces cyber threats and while security certification schemes like Cyber Essentials help protect against around 80% of the common threats likely to be faced, what about the uncommon threats, or advanced threats? What can small and medium organizations do to protect themselves when they are targeted by malicious threat actors with more resources and expertise than the common cyber criminal?

In the same way that if your home is targeted by a professional burglar, a standard alarm system won't be of much help. Though truth be told, a more advanced alarm system may have 'convenience features' for the owner, which in turn allow opportunities for the burglar to surreptitiously attempt to clone the proximity fob to deactivate the alarm. In a similar vein, many top of the range cars are stolen in seconds using technology to boost the signal from a keyless entry fob, which is then cloned, giving the thieves full access to the car. The owners are often clueless that their car has been stolen until they leave home in the morning.

Cyber-based advanced malware threats likewise are only typically discovered in the fallout from the data breach, extortion, or theft that resulted. Assuming that they are discovered at all, as many are specifically designed to remain undetected for months, if not years. That said, just because part of the malware is advanced, it doesn't mean all elements have to be, as deception, theft, and social engineering can all be used as part of the chain of events leading to an infection or compromise. At the other end of the scale, there is zero-click malware like NSO Group's Pegasus spyware, which made the news due to the number of high profile and prominent individuals whose smartphones were infected without any user intervention.

Advanced threats can also be hidden in plain sight, via third-party compromises, leading to supply chain attacks to modify the code base of trusted software or devices via routine security updates. Another supply chain attack is via modifying open-source software code libraries, which are used by multiple software vendors within their own products. Fileless malware and 'living off the land' techniques use in-built functionality in the operating system to carry out their functions, while other advanced malware has been known to receive instructions via innocent-seeming posts on social media platforms like Twitter.

While most advanced threats are targeted, anyone can fall victim to them. They could merely be a stepping-stone towards an end goal, or part of the 'smoke and mirrors' distraction used to hide the true target or goal. Malware can also be coded to do multiple things and just because it says it's ransomware and is displaying a ransom demand, that doesn't mean that is all it's doing, or was even the primary objective. So what can be done to implement countermeasures to detect and stop these advanced threats?

The What

To start with, the maxim 'know thyself' comes to mind. Understanding the attack surface of an organisation translates to knowing what there is to attack. Whether it is computer endpoints, IoT (SMART devices), cloud services, WiFi, NFC, software, email, mobiles, network appliances, or third-party vendors, the list is constantly growing and changing. What was not a possible threat vector last month could now be, following a change in connectivity or functionality. And let's not forget the human element, as people join, move within and leave organisations on a frequent basis. Additionally, threat actors can physically introduce devices like keylogging mice and keyboards or devices to facilitate remote access. Back in 2013, £1.3m was stolen from Barclays bank when a fake IT engineer managed to install a remote keyboard video mouse (KVM) device at a London branch.

Knowing what you have in great detail allows you to see what routes threat actors could use to potentially compromise the organisation, so you can do something about closing off or narrowing those routes. While many organisations maintain asset lists, it is often neither detailed enough or updated quickly enough to be of help in identifying where security resources need to be allocated, leaving gaps that could be exploited. Legacy technology creep can also be an issue as much as the introduction of emerging technology, so robust processes are needed for what is introduced, maintained or retired from the organisation. Now, many people confuse robust with complicated, but processes need to be clear, relevant and easy to understand, otherwise they won't be followed.

The Where, Who and Why

After working out what you have, the next question is asking 'where' it all is. Some of this is self-explanatory, in the case of cloud services, while others are portable and more tied to a person or team rather than a physical single location. This leads to the 'who' element of the asset list. Often missing is the current accountable person or team responsible who would be following any processes regarding that asset. Finally, we have the 'why', the business justification for literally why a service or device is in active use.

For ease, you can tie the 'why' to business functions or departments, like HR, finance or email security, network security, etc.

The whole point of asking these questions is to be able to make changes in order to lower the risks the organisation faces, by addressing any surprises or missing information in the answers. If the attack surface can be reduced by removing some of the 'what', which is no longer necessary, defunct, or duplicated, then these are quick gains. The same applies to removing assets as the 'why' is no longer valid. Just because something was expensive when it was purchased, if it is no longer supported and has no business justification anymore, it's best to remove it, as it is a risk.

Third-party compromise is always a potential risk, which can be reduced by using third parties that have visibly invested in their security like bug bounties and regular security patches. Also, creating a set of due-diligence questions to ask all existing and new suppliers will help identify those who value both their security and the security of their customers.

Reducing the Attack Surface

Removing may equal reducing, but reducing does not always equal removing, as there are many options to reduce the attack surface presented to the outside world. Operating systems and software applications may have upgrades to newer more secure versions, as one such option. Alternative operating systems like Chrome OS on Chromebooks removes the majority of possible malware infections compared to Microsoft Windows. Another is replacing laptops with iPads, for similar reasons, where it is both feasible and practical for the end-users.

Users can still be compromised though, through social engineering, phishing, and a whole host of other scenarios designed to glean credentials and information. This is where relevant, engaging cyber security awareness training can help reduce the risk of users falling victim to these manipulations, as well incident response training (insofar as) to know how and who to alert. Users are considered the last line of defence, so reducing what they are exposed to beforehand makes logical sense, as even the most highly trained user can make mistakes.

As emails are one of the most heavily targeted entry points for many threats, whether advanced or not, filtering emails before they arrive can greatly reduce the burden on users to distinguish between the legitimate and malicious. Many modern email systems either have features to do this or have a wide range of third-party offerings or even have a mixture of both. It is a good idea to block email attachments containing non-standard and executable file types. Believe it or not, there are over 90 Windows file types that could be executable programs or used as part of a 'living off the land' type attack. These utilise existing functionality within the operating system like Microsoft's PowerShell, a command-line shell, scripting language and configuration management framework. A simple rule in email systems (even Office 365) can block them from ever being delivered to users. You can find my free step-by-step instructions for Office 365 at:

www.booleanlogical.com/office-365-security which includes the full list of file types to block.

Many malicious emails are technically benign but reach out to the Internet, so filtering web traffic is the next logical step. This can be achieved through virtual private networks (VPNs) or a myriad of web security solutions. Cloud-based solutions such as Censornet, Zscaler, or Cisco's Umbrella offer protection regardless of where the user or device is currently located. Many premium antivirus solutions also offer a high degree of web filtering, as do many modern web browsers (if you choose to turn on the features). Each offering has its own strengths and weaknesses, so layering up may be the way to go if budgets allow. Another area to look at is the Domain Name System (DNS) which every Internet connected device uses, by choosing a security filtered service like Quad9.net (which is also free, though there are paid-for offerings too from other vendors) and changing the network settings of devices and computers.

Secure Configuration

Once the What, Where, Who, and Why has been answered and the attack surface reduced, it is a case of asking 'has everything been securely configured?' But what does this mean in practice, as a yes or no answer is not very helpful? Mostly it is a case of making a list of questions and picking the ones that relate to a particular device or service. Questions such as, is the asset fully up to date with regards to the operating system or firmware? Are all the security patches applied? Are appropriate user accounts configured with unnecessary accounts removed? Are the permissions set correctly for the user accounts? Are unnecessary optional features and services turned off?

There are many guides on 'hardening' devices like servers, as well as best practice guidelines for just about every asset. The important thing is that there is a repeatable process to follow for the secure configuration of assets. The keyword is repeatable, as this is not a one-off exercise, which is where people tend to go wrong. Re-checking (or if you prefer, auditing) that the process is still correctly applied after a set period of time, for instance quarterly, will help plug configuration related security gaps that can develop over time. Ongoing patching needs to be updated less than 2 weeks from the patch release date. Weekly checking and auto-update settings can help achieve this, if patch management solutions are not in place.

Next, does the idea of six degrees of separation apply to all your systems? Or, to put it another way, are all your systems interconnected? While individual assets may be securely configured, that doesn't mean they can never be compromised, and if everything is connected to everything else, there is the potential for malicious actors to move from system to system. Network segmentation can stop this and reduce the possibility of what appears to be a minor IoT or SMART device being a route into the entire organization. One easy way of achieving this is to use a separate Wi-Fi network or a 4G/5G router for cloud-managed devices that just need Internet connectivity to function. Separation of duties can also greatly reduce malicious lateral movement and can be as simple as using different admin accounts with different credentials for core services, rather than one master administrator account.

Access Control

Many user identity related risks can be reduced through additional access controls like two-step authentication (AKA 2fa or two-factor authentication), which stops most unauthorised access through credential stuffing and brute force attacks. Many online services already feature 2fa, so in many cases it is a case of turning the feature on and educating users. SMS text message based authentication is less secure than smartphone authenticator apps though, as they can be subjected to a SIM-swap attack, which if successful effectively puts them in the hands of the malicious actors.

Identity management is key to making controls such as a zero-trust security model and context-aware access effective in only blocking unauthorised users. These controls can take into account the user credentials, device, location, time, IP address, and a whole host of other factors to establish authorisation. Once identity is confirmed, for both convenience and increased security, Single Sign-On (SSO) solutions remove the risks of users having to know multiple passwords, in the same way that Privileged Access Management (PAM) solutions can also remove the risks of users having admin rights and being tricked into giving up their credentials.

While not strictly an access control, application control solutions restrict which applications can be run, limiting them to a defined list and effectively rendering new unknown and unauthorised software unusable. It is even built into Windows 10 and 11 for free as Windows Defender Application Control, though there are also many third-party offerings like Heimdal's affordable combined PAM and application control solution.

Visibility

Once all the security controls have been put in place, visibility of your assets is key, together with an understanding of what is 'normal' for your organisation with regards to network traffic and device activity. There are many tools and solutions available, all with their own acronyms such as Security Information and Event Management (SIEM) platforms, Security Orchestration and Automation (SOAR), and User Event Behavioral Analysis (UEBA) to name a few. Add in AI and machine learning and these systems can easily absorb the bulk of a healthy security budget in many organisations, introducing risks and gaps where budgets are too stretched. A pragmatic approach is needed for most small and medium-sized organisations.

If you still have people based out of a static office, then a good cloud-managed Unified Threat Management (UTM) firewall will give you visibility of all the devices on the network that connect to the Internet and where that traffic goes. In addition, cloud web proxy type services (like CensorNet) offer real-time traffic inspection, together with advanced anti-malware, no matter where the device is located, as well as providing full visibility of everything connected to the service and their network traffic.

Visibility can also be achieved by deploying management agents onto devices, whether standalone like mobile device management (MDM) or as part of a security solution. They allow the enforcement of security policies such as drive encryption and application vulnerability patching. Though visibility of online services may be a lot harder to achieve unless the service offers auditing or logging features. I'd go so far as to recommend changing where possible any online services that do not offer detailed logging and reporting of users' activities. If you do not know what is going on when things are normal, how will you know if anything is untoward? For example, can your cloud backup service be accessed from anywhere in the world and everything downloaded, without anyone being alerted to the fact that someone has signed in?

Forensics and Remediation

Prevention is best, but as there is no such thing as 100% security, devices and services may be compromised and remediation will be required. Many enterprise-grade antivirus solutions offer Endpoint Detection and Response (EDR) capabilities, allowing for root cause analysis and in-depth remediation to reverse all unauthorized changes by any malware. Threats come in all shapes and sizes, sometimes with multiple components each tasked with certain functions like making the malware persistent to be automatically restored after the system is rebooted. Some of the functions may be just 'smoke and mirrors' diverting attention and resources away from the real target. Working out what actually happened is no easy task and a whole body of knowledge such as the MITRE ATT&CK® Matrix has been developed to map out the common tactics, techniques, and procedures that many advanced threats use.

Many EDR solutions are mapped to MITRE ATT&CK® automating much of the process, though having a solution without anyone able to respond to the alerts is a recipe for disaster (and possibly a major data breach waiting to happen), which is why many are also available as a managed service. I currently have a solution by SentinelOne via a third-party managed service provider and pay roughly the same price as two takeaway latte coffees a month per person. Heimdal Security also offers an affordable alternative solution directly, while many of the major antivirus companies also have solutions aimed at larger organisations and varying price points.

If there is no facility for any forensic analysis, alternative remediation options include rolling systems back to a historic backup snapshot or to factory reset devices and repeating any secure configuration steps. Sometimes these are the best options regardless, so it's best to plan for them nevertheless.

Conclusion

To quote Po from the *Kung Fu Panda* movie, "there is no secret ingredient". There is no single thing you can do, no device or service you can buy that will protect you from every advanced threat because by their very nature, they are preying on often unknown vulnerabilities. Also, malicious actors purchase the very solutions claiming to thwart them, to learn how to circumvent them. The good news is that threats will rarely be 100% advanced in all the various components they consist of, so with good cyber hygiene and robust adherence to cybersecurity best practices, advanced threats can be stopped. This means that protecting an organisation is an ongoing process, not a one-off, yearly, or quarterly compliance requirement and far removed from the Hollywood glamour often portrayed as cyber security.

2.3 USING TRADEMARKS, DESIGN RIGHTS AND COPYRIGHT TO PROMOTE BUSINESS GROWTH AND INNOVATION

Gregor Kleinknecht, Hunters Law LLP

THE ROLE OF BRANDING AND DESIGN

Branding and design are key to turning innovation into marketable and commercially successful products, regardless of industry sector. Branding and design, and the associated IP rights, enhance product awareness, quality perception and customer loyalty, and help to distinguish innovative new products from those of other competitors. Brand rights are increasingly valuable and important for businesses in a global economy but, at the same time, brand protection challenges and threats to brand integrity become ever more demanding for brand owners to manage. The pronounced move to online trading during the Covid-19 pandemic, successive lockdowns of brick-and-mortar stores, as well as the implications of Brexit, have reinforced both the challenges and opportunities for growing and evolving businesses, with the strongest, most recognisable, and innovative brands continuing to prosper.

OPTIONS FOR PROTECTION

In simple terms, different IP rights protect different aspects of a product. Patents are dealt with in detail elsewhere in this compendium, and this chapter will therefore focus principally on the value of trademarks, design rights and copyright in protecting and promoting innovation. A trademark is essentially the name or sign placed on or used in connection with a product and its packaging to distinguish it from other products. Registering a trademark protects that name or sign from infringement by others although, under English law, unregistered trade names also enjoy (albeit more limited) legal protection. By contrast, design rights are concerned with the appearance of products. Again, design rights can be registered or unregistered. Finally, copyright can also be used to protect aspects of design and aims to prevent others from reproducing a protected original work. In the United Kingdom, copyright protection arises without the need for registration (indeed, there is no copyright register). New products will generally be protected by a combination of these rights, in addition to any patents that protect the underlying technical innovation of a new product.

TRADEMARKS

Trademarks defined

The Trademarks Act 1994 ("TMA") defines a trademark as any sign capable of being represented graphically which distinguishes the goods or services of one undertaking from those of other undertakings. Traditionally, a trademark consisted of words, slogans, designs, letters, numerals, or the shape of goods or their packaging. More recently, smells, sounds, colours, gestures and moving digital images have also been considered in principle as being capable of registration as trademarks. Trademark lawyers typically speak of word marks, device marks, shape marks and olfactory marks, etc. The key function of a trademark is to distinguish the products of different traders and to serve as an indication of origin; this is known as the "guarantee" function.

The legal framework

Trademarks are essentially national rights, i.e., they provide protection only in the country or territory where they are registered. In the UK, registered trademarks are dealt with in the TMA. European Union (EU) trademarks were a notable and important innovation when they were first introduced as Community Trademarks because, upon a single registration, they provide trademark protection in all EU Member States at once. EU trademarks are governed by Regulation (EU) 2017/1001 of the European Parliament and of the Council of 14 June 2017 on the European Union Trademark (EUTM Regulation). The EUTM Regulation is directly applicable in all EU Member States. Since 1 January 2021, following the end of the Brexit transition period, EU trademarks no longer cover the UK. As a result, businesses trading both in the UK and in the EU will now need to register, manage, and protect both a UK national trademark as well as an EU trademark.

Registering a trademark

Trademarks are best applied for and registered at an early stage in the product development cycle to ensure that the preferred mark is available and protected, and a branding strategy is in place, by the time the product is ready to be launched in the market. Before a trademark application is filed, it is prudent to obtain trademark clearance advice on the question whether the proposed mark is available for registration and use across the territories in which it is likely to be marketed. Possible delays and conflicts (in particular as to third party rights) can often still be avoided or resolved at that stage, for example, through a coexistence agreement, challenge of the validity or subsistence of the conflicting mark, or simply through acquisition of the conflicting right.

The UK national trademarks register is administered by the UK Intellectual Property Office ("UKIPO"); EU trademarks are administered by the EU Intellectual Property Office ("EUIPO"). Upon receipt of a trademark application by the competent trademark office, an examiner will review the application to assess whether there are any "absolute" grounds on which an application must be rejected. These grounds include, for example, that a mark is devoid of distinctive character, and did not acquire distinctiveness through use, or that the mark is descriptive of the goods or services to which it relates. If the examiner finds that there are conflicting registrations of identical or similar marks, he will notify any such conflict to the applicant and to the owner of the conflicting earlier trademark application or registration.

If the application passes this stage, it will be publicly advertised in the Trademark Journal or the EU Trademark Bulletin respectively. This stage provides third parties with an opportunity to oppose the registration of a mark on "relative" grounds, basically, on the ground that the application conflicts with rights that already exist in respect of some or all of the goods and services to which the application relates. If the application is not opposed, or an opposition is successfully resolved in favour of the applicant, the mark will proceed to registration and a certificate of registration will be issued. Trademark registrations must be renewed periodically (currently every 10 years) but are renewable indefinitely for successive ten-year periods upon payment of a renewal fee.

Nature and scope of trademark protection

A trademark registration confers on the owner the exclusive right to use the mark in connection with the goods and services for which it has been registered. The proprietor may prevent others from using the same or a similar mark in the course of trade in connection with identical or similar goods without consent and can sue for trademark infringement where this occurs. Unless an identical mark is used for identical goods or services, the owner must show that use of the mark causes, or is likely to cause, confusion on the part of the public.

If a trademark is well known and enjoys reputation, it benefits from a wider scope of protection in circumstances where the mark is used without due cause and such use takes unfair advantage of, or is detrimental to, the distinctive character or the repute of the infringed trademark. In the case of an EU trademark, this applies even if the infringing use of the mark is in relation to goods or services which are not similar to those for which the EU trademark is registered.

EU trademarks have the same effect in the EU member states as national trademarks have in the UK but with wider territorial scope. Importantly, in economic terms, a trademark registration of course also enables the proprietor to exploit his IP rights commercially, for example, by granting trademark licences to third parties within a distribution or franchising arrangement or by selling and assigning the rights to a third party.

Extending protection internationally

If an innovation is to be commercialised outside of the UK and the EU, the Madrid Protocol enables trademark registrations to be extended internationally to designated signatory countries based on their "home" registration.

Unregistered trademarks

In the UK, the owner of goodwill in an unregistered trade name may be able to protect that trade name against infringements through the common law tort of passing off. However, establishing the required evidence can be difficult and costly, in particular, in the case of new trade names, which may not yet have built up sufficient goodwill in the market place. Relying on the protection of unregistered trade names at common law is therefore no effective substitute for registered trademark protection.

DESIGN RIGHTS

The legal framework

The appearance of a functional object, or of part of an object, can be protected through registered or unregistered design rights if the statutory requirements are met. Unregistered designs are protected at a national level in the UK through the Copyright, Designs and Patents Act 1988 ("CDPA"), and registered designs through the Registered Designs Act 1949 (“RDA”), as amended first through the CDPA, then by regulation in 2001 and 2006, and more recently by the Intellectual Property Act 2014. At EU level, designs are protected by the Council Regulation on Community Designs (6/2002/EC) although the European Commission has recently undertaken a consultation on possible reforms of the European designs legislation. As with EU trademarks, since 1 January 2021, EU Registered and Unregistered Community Design protection no longer extends to the UK.

Requirements for unregistered design right protection

In order to be protected a design must:

- consist of the shape or configuration of the whole or part of an article;
- be original (which means that it must not be commonplace in a qualifying country in the design field in question at the time of its creation);
- be recorded in a design document or an article must have been made to the design; and
- have been created by a qualifying person.

If reliance is to be placed on unregistered design rights under the CDPA, it will be essential for detailed records to be kept of when the design was first created, and when articles made to the design were first marketed, so as to be able to establish the existence of a design right in any subsequent infringement proceedings. In order to assist with legal action against infringers, design documents should therefore always be signed and dated. Products made to the design should be marked with the words "Design Right", the name of the design right owner and the date when the right came into existence.

The CDPA specifically excludes design right protection where the design:

- is a method or principle of construction (as opposed to the finished article);
- comprises features of shape or configuration of an article which enable the article to be connected to or placed in, around or against, another article so that either article may perform its function ("must fit" exception); or
- is dependent upon the appearance of another object of which the article is intended by the designer to form an integral part ("must match" exception); or
- is a design for surface decoration.

The scope of the European Unregistered Design Right (described in more detail further below) is somewhat wider in that it protects designs of the appearance of the whole or part of a product resulting from the features of, in particular, the lines, contours, shape, texture and/or materials of the product itself and/or its ornamentation.

Nature and duration of unregistered design right protection

The owner of the rights in a design has the exclusive right to reproduce the design for commercial purposes by making articles exactly or substantially to that design, or by making a design document recording the design for the purpose of enabling such articles to be made, and can prevent others from infringing his design right and from interfering without the design right owner's consent with those exclusive rights (these acts are called "primary" infringements). Design right is aimed at preventing copying; importantly there will therefore be no infringement if the alleged infringer has independently created the same or a similar design.

A "secondary" infringement occurs when a person imports into the UK or has in his possession for commercial purposes, or deals in the course of a business with an article which is, and which he knows or has reason to believe is, an infringing article, without the licence of the design right owner.

Design rights last the lesser of 10 years from the end of the calendar year when articles made to the design were first marketed or 15 years from end of the calendar year when the design was first recorded in a design document (or, if earlier, when an article was first made to the design), subject to a licence as of right during the last 5 years of the term.

Registered design protection

The RDA (as amended) defines designs as features of lines, contours, colours, shape, texture or materials of the product or its ornamentation. In order to be capable of protection as a UK national registered design (in respect of the whole or part of a product), the design must be new and have individual character. These criteria are subject to an examination procedure by the registrar at the application stage. Registered designs can protect both three-dimensional and two-dimensional designs. There is a "must-fit" exemption but the "must-match" exemption does not apply to registered designs. Designs are protected as such and protection is not limited to the product to which the design was originally applied. Applications are made to the UKIPO and the registration process is relatively short and inexpensive compared, in particular, to that for obtaining a patent. The period of protection is a maximum of 25 years. Registered design right protection can be extended to other countries under the Paris Convention regime. International design registrations are possible pursuant to the Hague Agreement. Products made to a registered design should be marked with the words "Registered Design" and the corresponding registration number.

European design protection

The Council Regulation on Community Designs (6/2002/EC) established a framework for protecting industrial designs throughout the EU, mirroring the EU trademark regime, by creating a Registered Community Design administered by the EUIPO. In the EU, registered design protection lasts for 5 years and may be renewed for subsequent 5 year periods up to a total of 25 years.

In addition, the Regulation introduced an Unregistered Community Design right, which comes into existence when products incorporating the design are made available to the public in the EU and lasts for a period of three years. There are detail differences between the regimes for protecting unregistered designs under the CDPA and under European rules and an assessment must be made on a case by case basis as to which regime proves more beneficial in the particular circumstances or whether both are required.

COPYRIGHT

Basis of protection

In the UK, copyright is an unregistered right protected through the CDPA. It arises automatically for any work that has been recorded in any form and meets the statutory requirements to qualify for protection, including that it has been created by a qualifying person. Earlier legislation still applies (with some amendments) to works created while the earlier legislation was in force.

Nature and duration of copyright protection

In the context of protecting innovation, copyright is of relevance principally with regard to original design and technical drawings as well as computer programs and code.

In contrast to some other IP rights, copyright is intended to prevent copying of the whole or a substantial part of a protected work and certain other restricted acts but does not provide monopoly rights where another author has independently and without reference to the protected work created a similar or even identical work. Famously, copyright seeks to protect the expression of an idea but not the idea itself. The CDPA also seeks to prevent "secondary" infringements committed through importing, possessing or dealing with infringing copy.

Copyright usually lasts for the lifetime of the author plus 70 years from the end of the calendar year of his death. In the case of computer-generated works, copyright protection lasts for 50 years from the end of the calendar year in which the work was made.

Relationship with registered and unregistered designs

There is some overlap between the scope of design rights and copyright, in particular, since amendments to the CDPA now extend the benefit of copyright protection to industrially exploited artistic works. Where an action for copyright infringement is possible, an action for infringement of an unregistered design may not be brought.

THE IMPLICATIONS OF BREXIT

Brexit and the end of the Brexit transition period, have had far reaching implications for IP rights in the UK and, in particular, for brand protection. UK secondary legislation, implementing the provisions of the Withdrawal Agreement, revoked the retained EUTM Regulation and amended the TMA, *inter alia* to grant the holders of existing EU trademarks, a comparable UK national trademark, and to make other transitional arrangements. A comparable trademark has the same status and effect as a trademark registered under the TMA.

In the area of design right protection, transitional arrangements have also been implemented following Brexit; the UK legal framework has become more complex as a result of the creation and grant of new types of design rights to holders of existing EU Registered and Unregistered Community Designs, such as comparable design rights, re-registered designs, continuing unregistered designs, and supplementary unregistered designs.

With regard to copyright, the UK will no longer be part of the project creating the Digital Single Market and copyright protection in the UK and in the EU is already starting to diverge as a result of the EU Digital Copyright Directive not having been implemented in the UK.

BRAND MANAGEMANT AND PROTECTION

The effective management of an IP portfolio is key to a successful brand strategy and to maximising the value of IP rights. This includes not only the maintenance of registrations, and a watching brief to monitor third party applications to register potentially conflicting rights, but also an effective enforcement program to prevent, identify and pursue rights infringements. What form that enforcement action takes will depend on the circumstances of each individual case, on the rights involved, the type and seriousness of the infringement, and the identity and location of the infringer. The available options range from administrative proceedings before the competent trademark registry, or the involvement of police forces and customs or border agencies, and the instigation of criminal investigations, to domain name dispute resolution procedures and enforcement action in the civil courts, including interim and permanent injunctions, claims for damages and/or an account of profits, and an order for the delivery up or destruction of infringing articles.

2.4 KEEP INFORMED ABOUT IP RIGHTS

Margit Hoehne, Patentgate

Legal status of patents

One interesting fact about patents is the contrast between legal and technical aspects of those intellectual property rights. While the content of a patent document describes the novelty and ingenuity of a technical innovation and the claims translate the invention into comparable and enforceable legal terms, there are life phases and events that have a large impact on the legal validity of the patent.

These legal events determine if a patent is still 'alive' or is not any longer in force. Knowing this impacts questions like: Is the invention considered state of the art and can be used without infringing any patent? Can this invention be uses freely or is it necessary to license it? Has the assignee declared his willingness to grant a licence?

Introduction

A legal event is data concerning the life cycle of a patent or other intellectual property right like trademarks or designs.

They describe the steps beginning with the filing at a patent office to the end of the IP right's life. This event history shows all events and the legal status, which describes whether an IP right is still in force. It is maintained within the patent register of the filing office.

The part of the patent register that is accessible by the public contains only events for IP rights that have already been published.

A patent application will be published 18 months after filing by the patent office. If a priority is claimed within 12 months, the first publication occurs 18 months after the priority date, which is the filing date of the first filing at another patent office for this application.

The event of filing and all others that take place until the patent application has been published will not be known to the public before the publication day. They are, however, already stored in a section of the patent register that is not open to the public. When the IP right is published, all events up to that time will be available in the patent register.

Some events may occur before or after the publication, for instance the request for examination. Others, like claiming a foreign priority, take place before publication.

There are differences between legal status and legal events. The status describes in one phrase if an IP right is still in force or not at the current date. For every patent application, there is a list of legal events, which can either be neutral, positive or negative. An example for a neutral event could be the communication with the examining division. This can only be interpreted when the content of the examination report is considered. Positive events that indicate the IP right is still in force, are the payment of the annual fee or the request for examination. Other events like filing for opposition or the decision to reject indicate that the patent could be lapsed.

Most IP offices publish a weekly gazette in paper or online that lists all publications, grants, corrections, as well as legal events and changes in legal status for that week. The patent register contains all information for all IP rights at a given time. The selection of events and how detailed they are published in the register and / or gazette can differ.

The register differentiates between the date of the procedural status and the date of publication in the patent register or patent gazette.

While the date of the procedural status is the day when the event has occurred, the public will be informed about it later on the date of publication in the register or gazette.

Sometimes an event's legal effect will not occur, for instance when a missed fee payment has been rectified within a defined deadline. That means that you cannot determine with only the occurrence of a legal event if an IP right is still in force or not. It is in force while the legal status in the register is still “in force” or “pending”.

Some patent offices provide in the legal status if a patent is not in force anymore. The British Intellectual Property office indicates if a patent is “Expired”, the German Patent and Trademark office declares it “Not pending / Lapsed”. The European Patent Office (EPO) publishes no such information in the register, but has 14 different legal status values.

Indicator	Legal status
IP right in force	Examination is in progress Grant of patent is intended Opposition filed Request for examination was made The application has been published The patent has been granted
IP right not in force	Patent revoked The application has been refused The application has been withdrawn The application is deemed to be withdrawn
Granted EP patents	No opposition filed within time limit Opposition procedure closed Opposition rejected Patent maintained as amended

Table 1: Status values for European Patents

The legal status for granted EP patents is not found at a single source because after grant and the entry in the national phases the information can be found in the registers of the designated contracting states, validation states and extension states. It can be in force as long as it is still valid in at least one of those states. With the implementation of the Federated Register it has become easier to collect the legal status for all countries concerned.

The following chapters introduce public services of patent offices for legal status information: INPADOC, the largest worldwide legal status database; the Global Dossier, a service of the five largest IP offices, and EPO's Federated register with data for the national phase of European patents.

Descriptions of national register services are not part of this article; its focus is on services with cumulative data from different sources.

INPADOC Legal Status Database provided by the EPO

INPADOC is the largest worldwide legal status database. It is maintained by the European Patent office and contains about 360 million legal events and statuses.

The EPO publishes weekly statistics that show the growth of the data and which countries are covered.

An evaluation of the data of week 35/2021 shows that those 360 million legal events are related to 71 million patent applications from 54 countries. They are classified with 4700 legal event codes.

The biggest portion is data from the EPO with more than 117 million events, the IP offices of Japan, China, USA, Korea, and the World Intellectual Property Organization WIPO provided more than 20 million events each to the EPO, and together more than 218 million events.

The events represented in the INPADOC database are sometimes not as much detailed like in the register of the national IP office. The update frequency and completeness of the data is not the same for all offices.

Sometimes similar events will be grouped together in one event code or are not represented in INPADOC at all. The time lag between the occurrence of the event and the publication in INPADOC can be weeks or even months.

The average number of events per document in the database is 2.3 events, EP publications have a higher average of 20 events. The data is updated weekly.

INPADOC data is provided in Espacenet as “INPADOC legal status” and is used by commercial patent information providers for their own databases.

The legal status of a patent family can be obtained easily in Espacenet because all documents of a patent family are displayed there.

Patentscope is a service of World Intellectual Property Organization (WIPO). The database contains mainly bibliographic data from the WIPO itself and 82 other countries worldwide, but also legal status information (displayed in the tabs “National Phase” and “Documents”). There is no link between members of a patent family.

To get an overview of all legal events of a patent family, using other services to find the patent family members is necessary.

For applications filed under the Patent Cooperation Treaty (PCT) the WIPO provides the documents from the search and examination procedure as well as related documents in the file inspection. WIPO provides a statistics table on their website with information how many national phase entries in which time frame are available in the Patentscope database.

WIPO also provides a patent register portal on their website where databases, registers and online gazettes of more than 200 IP offices can be accessed

This service can be used to find information about the content of national and regional registers.

Global Dossier

Patent documents published by an IP5 Office can be accessed via the Global Dossier. This is a joint project of the five largest IP offices to facilitate the access to the file wrappers of IP5 patent family members.

The IP5 member offices are:

- European Patent Office (EPA)
- Japan Patent Office (JPO)
- Korean Intellectual Property Office (KIPO)
- National Intellectual Property Administration of the People's Republic of China (SIPO)
- United States Patent and Trademark Office (USPTO)

The table shows the data coverage of the Global Dossier.

Patent office	**Dossier type**	**Date range**	**Language**
EPA	EP and PCT applications	All (from 1977)	Original EN/DE/FR
JPO	JP and PCT applications and utility models	Application date from 01.07.2003	JP / EN (JPO machine translation)
KIPO	KR and PCT applications and utility models	Application date from 01.01.1999	KR / EN (KIPO machine translation)
SIPO	CN and PCT applications (no utility models)	Application date from 10.02.2010	CN / EN (SIPO machine translation)
USPTO	US and PCT applications	Application date from 01.01.2003	EN
WIPO *	PCT applications	All (from 1978)	PCT publication languages
CIPO *	Applications	With examination report application date from 01.08.2015	Original EN/FR
IP-AUS	Applications	Application date from 01.01.2006	EN

Table 2: Global Dossier Coverage; Source: „IP5 Global Dossier: Scope, content, availability and performance"

* While WIPO, the Canadian Intellectual Property Office (CIPO) and IP Australia are not members of IP5, they provide data to the Global dossier.

The content of the Global Dossier is nearly identical to the online file wrappers at the IP5 office. When no document exists for a legal events, for instance fee payments, there is no entry of the event in the dossier.

Cited non-patent literature is not provided in the Global Dossier due to copyright issues.

The global dossier service can be accessed via the website of any IP5 office. The layout and language of the user interface differs, but the content is the same. For publications from China, Korea and Japan, machine translations to English are provided parallel to the original document.

The number of daily requests can be limited by the office and some offices may have maintenance times where the server will be unavailable. The delay until a document is available within Global Dossier can be up to 8 weeks.

Federated Register

The Federated Register is a part of the European Patent Register and shows the consolidated status of the legal status of a granted European patent at the national offices of the designated states.

When a European patent has been granted, the tab “Federated Register” can be accessed in the European Patent Register.

34 of the 38 member states of the European Patent Convention (EPC) provide deep links into their national patent registers, so that a patent's data is directly accessible. 31 offices provide data to the EPO that is made available in the Federated Register. More offices will follow. Not all member states make their data available in the Federated Register. Cyprus, Italy and Latvia only supply links to their national register database: (Source: Federated Register – integration status 06/2021)

For each patent the Federated register contains:

- the link to the national register
- the legal status
- the application and publication number
- the applicant or proprietor
- the invalidation date
- the information since when the patent is not in force
- the last payment of renewal fees
- the date the record was last updated

For all designated contracting states, extension states and validation states that provide the data to the register. The list of states can differ for each EP patent.

Not all offices supply all the data in the table, but the EPO has documented the available coverage. For example, the data provided by the German Patent Office

(DPMA) are the legal status, application and publication number, one proprietor, fee payment and update date.

Even with the message, "*No data provided by the national patent office for this patent*" there may still be data in the national register.

The help page describes the 18 status values and their definition. The links to the national patent registers at the bottom of the Federated Register page are the same as in the table above, when the office is listed in both selections.

If the Unitary Patent will enter into force, it will be possible to get combined patent protection in 26 EU member states by requesting unitary effect with the EPO. This will affect the data provided in the Federated register.

Conclusion

There are different sources for an IP right's legal status information: patent registers maintained by the filing office and secondary sources like the INPADOC database or the Global Dossier and Federated register, that provide consolidated information from different sources.

The completeness, accuracy and timeliness of these sources may vary, so legal status information should be interpreted with care. Patent attorneys and patent information professionals who have in depth knowledge of the patent system and the available data sources can help interpret the legal status of patents.

2.5 RISKS OF UNEDUCATED RELIANCE ON R&D TAX CREDITS: SOFTWARE START-UPS

Dr Mark Graves and Julia May, May Figures Ltd

The UK R&D Tax Credit Scheme is an extremely valuable source of funding for early-stage technology companies.

The latest published government statistics for the year ending March 2020 estimate that 85,900 companies claimed R&D tax relief amounting to £7.4 billion. Given that companies can claim relief retrospectively for up to two years, the eventual figures will be significantly higher. Even so, the provisional figures represent an increase of 19% compared to the previous year.

In particular the number of first-time applicants has been steadily increasing year on year, with nearly 18,000 first-time applications representing a 25% increase in first time SME claims in March 2019 over the previous year (2020 data not available).

Information and Communication represents the largest sector (by number of claims) with 22% of the total claims, just exceeding the number in manufacturing.

An interesting recent trend is the increase in “low value” claims with over half of all claims being worth £30,000 or less.

Many of these small claims are first time claimants operating in pure R&D mode, many being pre-revenue start-ups who use the R&D tax credit cash rebate alongside early “friends and family” seed funding to develop their software to the Proof-of-Concept or Minimum Viable Product stage.

Increasingly fledgling companies are taking advantage of R&D Tax Credit Bridging Loans i.e. borrowing against future R&D tax credit cash rebates as part of a funding strategy until a successful first round of raising external capital (VC series A/Angel round or equity crowdfunding).

We have written about the opportunities to borrow against a future R&D claim round in order to extend the funding runway between equity investment rounds in a previous publication (Graves and May, 2019a) where further information can be found.

HMRC investigations

Historically, companies were able to claim R&D tax relief with minimal intervention from HMRC. Inspectors tasked with policing the claims were based at a handful of offices with limited resource. Relatively recently, that has changed: most corporation tax return Inspectors are now trained in risk assessing claims, and there are a number of government initiatives in operation to target inappropriate and fraudulent claims.

As a result, we are observing a trend of HMRC investigations into companies who, having successfully submitted one or two relatively low value R&D claims, then submit a higher value claim (often following a significant funding round with an associated increase in qualifying expenditure). These unanticipated HMRC investigations come as a shock, as having undertaken a couple of successful small value claims companies naturally feel their activities qualify without fully understanding the detail of what the legislation requires to make a valid claim.

This is exacerbated by the existence of a plethora of R&D tax credit advisors, unregulated or unqualified, attracted by high professional fees "advising" in this complex area of tax legislation, breeding inappropriate confidence in R&D tax credits as a source of easy cash.

Given that HMRC investigations can result in a substantial or complete rejection of a claim, potentially triggering penalties as high as the value of the original claim, it is vital that companies are fully aware of the scheme requirements *before* submitting a claim. This is particularly important for companies who have relied on tax advisors as when determining the penalty HMRC consider how much care the company took in preparing the claim which includes: (i) the extent the company went to in researching and understanding the scheme requirements and (ii) the steps taken to ensure the advisor is appropriately qualified and experienced in the field.

Financial aspects

R&D tax relief claims rely on two aspects:

- the financial aspects
- the technical aspects

We set out both below, with specific focus on the technical aspects facing high-growth software companies.

R&D tax relief provides a combination of corporation tax reductions for profitable companies and cash rebates through the surrender of tax losses or offsetting the additional losses against historic or future profits. Claims are based on allowable qualifying R&D expenditure. A claim is either submitted as part of the company's annual corporation tax return filing, or subsequently up to two years from the end of the accounting year.

Claims are based around specified projects, with allowable expenditure potentially including employment costs, subcontractors, materials consumed or transformed in the course of the project and software licenses.

Costs of subcontractors (corporate & individual) are subject to a number of rules which relate to the type of project funding, the relationship between the claimant company and the supplier and the terms of engagement.

There are in fact two distinct R&D tax credit schemes that interact:

(i) the SME scheme targeted at Small & Medium Sized Enterprises (defined as having <500 employees with either turnover <Euro100m or balance sheet <Euro86m).

(ii) the RDEC scheme for larger companies and certain funded/subcontracted projects.

The SME scheme is approximately three times more generous than the RDEC scheme, and under the RDEC scheme certain costs are excluded.

Most early-stage companies believe the less beneficial RDEC scheme is not relevant to them. However, if the SME received funding for an R&D project then they are precluded in most situations from using the SME scheme, and must claim under the less beneficial RDEC scheme.

Grant funding

There are particularly complex rules if the company making the R&D claim has received any form of grant funding (this now includes Bounce Back Loans, as they are a form of Notified State Aid). We have written on the topic of the overlap between grants and R&D Tax credit claims previously (Graves and May, 2019b) and so will not go further here, other than to advise companies to seek experienced professional advice from an agent experienced in dealing with the complex interaction of Grants and R&D Tax Credits.

Client funding

It is common for early-stage software companies to initially self-fund their development but, as they grow, they may enter into various commercial contracts with customers which may include payments for bespoke development, payments for bespoke versions of their software for a client, upfront license payments, SaaS deposits etc.

All of these scenarios can result in the claim being moved from the SME scheme to the RDEC scheme. Other elements are the client size and the nature of the commercial relationship.

In another publication, we have outlined the three most common commercial relationships (Graves and May, 2019b), but as start-up companies develop ever more complex business models, we are starting to see yet more complex relationships emerge.

Staff costs

Generally, for software claims the greatest cost that can be claimed is the cost of the team involved in undertaking the R&D activity, both employees and subcontractors.

For small early-stage pre-revenue companies, the first 12-18 months might be a period of high R&D activity. Each individual's involvement in qualifying R&D activity is likely to be high, particularly for technology entrepreneurs. Maintaining timekeeping records of staff activities provides support for high value robust defensible claims. In the absence of record keeping, time may be estimated at first. In these early periods, staff will therefore be legitimately claimed at a high percentage of total time.

As the company grows there will be more staff who fill more varied roles such as Application Developer, Solution Architect, Systems Testing, Infrastructure Architect, Business Analyst, DevOps, and Systems Admin. Without a detailed understanding of the technical eligibility criteria it becomes increasingly hard to know the extent to which the costs of these staff can be legitimately claimed. This applies when completing time sheets and when estimating. It can be challenging to demonstrate valid R&D activity within the R&D technical report, to avoid triggering an unwelcome (and unnecessary) HMRC investigation; HMRC resources to review software claims have increased dramatically since October 2019.

Technical Eligibility

In the following section, we aim to provide a high-level understanding of the technical eligibility criteria, with a particular emphasis on issues surrounding a scale-up stage development. This should enable companies to determine:

- whether projects qualify,
- (if they do qualify) which aspects of the project qualify and
- within each aspect, which activities qualify.

Before going into some of the specific complications for software projects (which relate to the rapid scale-up of an architecture or platform following investment funding), it is worth revisiting the two fundamental technical eligibility requirements for all software R&D claims as these are often misunderstood.

A fundamental point to understand at the outset is that just developing software in itself is not sufficient to meet the tax relief criteria, *even if* the project is difficult, expensive or novel.

We often come across clients that have been advised by unscrupulous or misguided telemarketers from unregulated advisory firms that: if they are "developing bespoke software" then they definitely have a claim.

HMRC's internal guidance in CIRDs 81960 and 81900 make it explicitly clear that this is not the case, "*The words 'research and development' are frequently used in the* *software sector and care should be taken not to assume that a commercial project fully aligns with the definition of R&D set out in the BEIS Guidelines*."

Technological Advance

R&D takes place *for tax purposes* when a project seeks to achieve an advance in science or technology.

A key point to understand here is that the advance has to be an advance in overall knowledge or capability in a field of science and technology worldwide in the public domain, and not a company's own state of knowledge or capability alone.

Frequently a software start-up company will undertake qualifying R&D in the area of expertise of the founders in developing a first proof-of-concept solution, but then the scale-up of the platform following an investment round may involve development of other areas of software such as cloud computing, serverless architectures, DevOps, microservices, test driven design etc. For example, a company having initially undertaken qualifying R&D in developing an outline solution with a monolithic architecture may then spend significant development effort in re-architecting the solution to make use of a modern microservice design architecture.

In such scenarios the company believes they can claim relief because their technology has been advanced in moving from a monolithic architecture at the proof-of-concept stage through to a microservices architecture at deployment stage. However, the test is whether this project has made an overall advance in knowledge or capability not just for the company alone.

Such a judgement can only be made by assessing the development against the baseline technology for microservice architecture software development, ideally from a peer referenced academic journal publication, recent book publication or highly credible/respected technical blog posting articles. For example, in assessing microservice claims we might compare the company's developments against the book *Microservice Patterns with examples in Java* by Chris Richardson, as well as the blog postings of Martin Fowler, as widely accepted as the pre-eminent early conceptualist in the field.

It is also important to realise that the advance should be in underlying knowledge or technology and not in the commercial output or outcome. Rapid scale-up software companies often describe their advance in terms of a commercial metric e.g. users of their platform. Whilst this is a commercial advance, it only represents a technological advance if the development of the scale-up architecture itself represents an advance in enterprise computer architectures. As HMRC themselves describe (CIRD 81960) "*what matters is technological input, rather than commercial output*".

Because of the pace of change within the software industry, HMRC inspectors have access to support from HMRC's own computer specialists in this respect, to ensure that knowledge of the industry is kept updated. The computer specialists provide advice based on their knowledge of the software industry.

Within an enquiry into the tax return, if there are differences of opinion between competent professionals working in the field (specialist area of the company's R&D project and HMRC Inspectors/HMRC software specialists) the Competent Professional at the company may be asked to provide further clarifications with reference to information in public domain that can help better articulate the advance sought and technological uncertainties faced to support the explanation of what prevented these from being readily deduced at the outset.

Technological Uncertainty

The second major requirement for project eligibility is that the project has to require efforts to resolve a technological uncertainty (even if unsuccessful).

Many companies try and argue "we weren't sure if our solution would work", which is not the same as the legislation's requirement for a technological uncertainty.

HMRC does not provide a specific definition of a technological uncertainty specifically for software projects but their overall definition of scientific and technological uncertainty for all projects is that it "*exists when knowledge of whether something is scientifically possible or technologically feasible, or how to achieve it in practice, is not readily available or deducible by a competent professional working in the field.*"

There is however a definition of System Uncertainty which can be the basis for some software R&D claims as platforms and architectures scale-up. The definition is "*System uncertainty arises because of the complexity of the entire system rather than how its individual components behave*."

In scaling-up a software technology from an initial proof-of-concept to an enterprise commercial deployment, there will often be the integration of many additional software components and technologies. In such a case, however, "*simply specifying that there was a large number of components to assemble or integrate is a general statement and does not give enough information. The company should clarify why the relevant routine or established assembly methods would not resolve the technical uncertainty*."

In many cases, the scale-up of a platform or system architecture will involve the communication or workflow of data between several third-party software and data storage tools. If, however, these software components all interface through published API standards then it will not be apparent how this represents a technological advance, which is often a trigger for HMRC inquiries.

To successfully demonstrate that qualifying activity in a project meets the requirement of System Uncertainty it is necessary to describe why routine methods or established methods could not be applied.

Typical challenges associated with software scale-up projects:

Data Volumes

Companies will often claim that a data volume scale-up from their proof-of-concept development to an enterprise scale architecture represents an advance. Whilst a given project may have some specific data scale-up challenges that represents an advance in the field and required the attempted resolution of a technological uncertainty, this cannot always be assumed to be the case. Logically, if this were to be always the case, then by definition every software development that moves to be deployed at enterprise scale would be qualifying R&D, and this is certainly not true. Hence to be able to justify that a data scale-up is an advance, there would have to be supporting documentation and data metrics showing the limitations of existing known methods of data scale-up and how the project represented an advance in this field.

Machine Learning

Often a scale-up of data volumes will be undertaken in parallel with the development of Machine Learning solutions. Given the high-tech sounding nature of Machine Learning many companies believe this is likely to qualify. However, as always it is necessary to go back to the key definitions of *the field of advance* and the *resolution of technological uncertainty* to determine if qualifying R&D really has taken place. Increasingly, there are commercial tools available, which enable Machine Learning projects to be undertaken where the Machine Learning is essentially a "black-box" engine. Such a project would not qualify, as it is a classic example of *"using advanced technology rather than advancing technology."*

It is quite rare for companies to be developing a fundamentally new Machine Learning algorithm; in many cases the project will entail manipulating the data into a suitable form for use with a known Machine Learning algorithm such as a Convolutional Neural Network. Such cases are challenging to assess because they could be the case of a routine data manipulation for use in Machine Learning (non-qualifying) or a complex data pre-processing of unstructured data into a structured data format suitable for Machine Learning (likely to be qualifying). As in many cases where the determination of the advance is uncertain, it will be necessary to intelligently compare the development against the closest baseline technology and determining how the project sought to make an improvement over the baseline approach.

Security

Often companies will develop a proof-of-concept solution for internal experimentation or testing without concerns for IT security. When the development reaches the point of commercial deployment there may well be considerable development effort and subsequent testing (penetration testing etc) in ensuring the software is secure. Whilst such work is necessary to ensure the technology can be commercially productised, it is unlikely in most cases to meet the definition of an advance in the field of software engineering as again all enterprise scale commercial software products undergo this process.

There are however specific cases where meeting the software security requirements could be especially challenging. An example might be in the field of electronic healthcare where the regulatory challenges mean that standard software security measure for routine software deployments do not meet the requirements for patient confidentiality and new methods are required to be created.

Conclusions

The R&D tax credit scheme is a superb, targeted form of funding for companies in the early stage of development leading to initial proof-of-concept of their technology. It should, however, not be automatically assumed that because a project has qualified for R&D tax credit funding to the proof-of-concept stage that much of the additional enterprise scale-up costs will be eligible. Each project needs to be analysed on its own merits with close attention by software experts to determine if the scale-up phase of the project meets the legislation's definition of R&D, specifically with regards to technological advance and technological uncertainty.

References

Graves, M and May, J. (2019a) "R&D Tax Credit claim backed short-term bridge financing for high-tech start-ups" in Growing Business Innovation – developing, promoting and protecting IP. Edited by J Reuvid, Legend Press.

Graves, M and May, J. (2019b) "R&D Tax Credit claims – an overview of the SME and LARGE / RDEC Schemes and how SME companies are affected by receiving funds from Grants and Clients" in Growing Business Innovation – developing, promoting and protecting IP. Edited by J Reuvid, Legend Press.

2.6 KEY PROVISIONS OF EMPLOYMEMENT LAW

Carrie de Silva

Introduction

Not so may generations ago, employment rights were limited, with employers having considerable powers and the employer/employee relationship not even approaching parity. Particularly since the 1960s (although there were gradual developments from the nineteenth century) there has been a growing protective framework for the employee and, more recently, the *Taylor Review of Modern Working Practices*, led by Matthew Taylor (an independent review commissioned by the government in 2017) fed into the *Good Work Plan* (2018), which set out five 'foundational principles' for the government's Industrial Strategy:

1. Satisfaction
2. Fair pay
3. Participation and progression
4. Well-being, safety and security
5. Voice and autonomy

Along with further embedding existing principles, such as those relating to pay, health, safety and welfare, and employee consultation, the *Plan* pledged to clarify employment status and enhance the rights of certain individuals, particularly those categorised as 'workers' (as opposed to employees). This chapter sets out some of the key provisions of employment law of which businesses should be aware.

Employment law is, though, complex and ever developing, so these notes are for guidance only and in many instances, further legal advice will be required, whether through online resources, such as Acas (www.acas.org.uk), or from employment professionals. All the areas outlined below are covered in detail by Acas and their website has both detailed procedural guidance on various issues (utilisation of which is mandatory in some instances, such as grievance and disciplinary procedures), along with exemplar and suggested templates for contracts of employment, home working policies and much more.

The law

The employment relationship is largely governed by the Employment Rights Act 1996, which covers a range of areas including provisions relating to unfair dismissal, redundancy, notice periods, wages and salaries, 'whistle-blowing', holidays and maternity, adoption and parental leave.

The Equality Act 2010 is the consolidating legislation covering nine protected characteristics against which it is, broadly, unlawful to discriminate. There are some exceptions.

Although covering an ever-diminishing membership, the Trade Union and Labour Relations (Consolidation) Act 1992 sets out the law governing trade unions and their relationship with individual members and employers, industrial action, collective bargaining and the statutory recognition of trade unions.

Where a business is transferred as a going concern and continues trading, the rights of workers are protected under the Transfer of Undertakings (Protection of Employment) Regulations 2006 which protect, for example, length of service.

Limits on low wages are regulated by the National Minimum Wage Act 1998 (and annually updated regulations on applicable rates).

Working time, daily and weekly rest periods and rest breaks, annual leave and night work are set out in the Working Time Regulations 1998.

There are many other regulations, and employment law has been particularly influenced by membership of the European Community (later Union) since 1973. Readers will be aware that the United Kingdom left this union on 31 January 2020. Whilst existing provisions were absorbed into UK national law, it is unclear how closely the UK will mirror European developments in future. Constitutionally, European law is irrelevant, post-Brexit, but there may be political and trading constraints on falling out of sync in certainly areas. Only time will tell.

Employment status

Readers may think in terms of a person either being an employee or, if they are not, then self-employed or working for someone else and clearly *not* an employee. But there is a further category of 'worker'. It is important to establish the correct classification, as it will impact various matters such as taxation and employment rights. Workers increasingly have *some*, but not all, of the benefits (and constraints) of employment.

Traditionally, the courts looked at what was called the 'integration test'. To what extent was a person's work *integral* to the employer's operations? This is now considered somewhat inadequate, and the modern approach is to look at numerous factors: the 'multiple' or 'mixed' test. Such factors might include, but are not limited to:

- the level of control by the employer on how and when work is carried out
- the level of managerial responsibility and autonomy for the job
- whether the worker supplies their own tools, vehicle, specialist clothing, etc.
- the method of remuneration and arrangements to pay tax and National Insurance
- the employer's powers of selection and dismissal
- whether the worker bears any economic risk
- whether the worker can benefit from good management on particular jobs (as opposed to an employee, who would not) and
- the hiring of the worker's own staff/additional workers.

This must be considered holistically, and *Ready Mixed Concrete (South East) Ltd v Minister of Pensions and National Insurance* (1968) clearly showed how apparently conflicting terms need to be reviewed for the overall balance. A lorry driver wore a uniform provided by the company, followed the instructions a company employee and obeyed company rules. These aspects suggested a contract of service (a contract of employment). On the other hand, the driver provided his own lorry, paid his own servicing costs and managed and paid his own tax and National Insurance. These factors pointed towards self-employment. As with many legal situations, the picture was not clear-cut. There were arguments for and against but, on balance, the court held the lorry driver to be self-employed.

It is important to note that the courts will look at the facts, at what is happening day to day, in addition to any legal documents or what was said.

Firms may try to draft contracts indicating self-employment, particularly with the use of 'substitution' clauses: whereby a worker could have someone else carry out the work. This would clearly not be the case in an employment contract. *Autoclenz Ltd v Belcher* (2011) confirmed that the facts, rather than the legal documentation, was the deciding factor.

Workers

Although not employees, those classified as workers now enjoy significant rights and protections. Such workers might include those working on an *ad hoc* basis, workers employed under zero-hour contracts or those working for agencies.

The term worker is noted at s230(3) Employment Rights Act 1996 but more usefully in *Byrne Brothers (Formwork) Ltd v Baird* (2002) where the Employment Appeal Tribunal found the claimants were workers, rather than self-employed, due to their dependence on one firm for work, and clearly not being in business on their own account.

More recently, the status of workers has been considered in two important Supreme Court cases. In *Pimlico Plumbers v Smith* (2018), Gary Smith claimed in the Employment Tribunal for (a) unfair dismissal, (b) discrimination regarding disability,

(c) a lack of provision of annual leave, and other matters. Mr Smith sought to establish that he was an employee and Pimlico Plumbers wanted a ruling that he was self-employed. The tribunal found that Mr Smith was *not* an employee, thus had no protection from unfair dismissal, but that he *was* a worker with Equality Act protection against discrimination and a right to paid leave. The firm appealed all the way to the Supreme Court, but the judgment remained: Mr Smith was a worker. A key feature was that he was required to undertake the work personally and that Pimlico Plumbers had control over clothing, method of operation and administration along with restrictions on any work following the termination of the relationship.

In *Uber BV & Ors v Aslam & Ors* [2021], the Supreme Court upheld the earlier judgments that Uber drivers are workers, rather than self-employed. The drivers were found to be in a position of dependency on Uber, who control how the business is run. The drivers have no real economic impact or control and can only affect their earnings by working longer hours.

Workers can be freelance (and circumstances will determine whether a worker or self-employed), engaged through an agency or on a zero hours contract (and circumstances will determine whether the individual is a worker or an employee).

Key employment rights for employees *and* workers (including most agency workers):

- entitlement to written statement of employment terms
- entitlement to pay in line with contractual terms, at or above the National Minimum Wage (maximum levels reached at age 25 with different rates for apprentices)
- entitlement to wages within the national equality framework
- entitlement to be indemnified for expenses reasonably incurred during the employment
- protection against unlawful deductions from wages
- entitlement to an itemised pay statement
- minimum statutory levels of paid holidays
- minimum statutory rest breaks
- maximum working week (48 hours on average) unless expressly opted out
- protection against unlawful discrimination
- protection for ‘whistleblowing’
- entitlement that employer takes reasonable care for health, safety and welfare as governed by the Health and Safety at Work etc Act 1974 and related regulation.
- not to be treated less favourably if working part-time.

Key employment rights for employees only:

- minimum notice periods on dismissal
- right to request written reasons for dismissal
- protection against unfair dismissal
- right to be accompanied at disciplinary and grievance hearings
- right to request flexible working
- time off for emergencies
- statutory redundancy
- rights in connection with trade union membership.

Key employment rights for employees and some agency workers:

- statutory sick pay
- statutory maternity pay and leave
- statutory adoption pay and leave
- shared parental pay and leave.

Note that agency workers do not acquire some of the rights until they have been working for 12 weeks in a job.

Vicarious liability

It is a function of the employment relationship that for wrongs (civil or criminal) perpetrated by employees, the employer might be prosecuted or sued and be found liable under the principle of vicarious liability, that is liability on behalf of their employee. This is in the absence of any fault of the employer and is a long-standing principle on policy grounds to support victims. The wrong must be broadly 'in the course' of employment and employers will insure accordingly. In recent years, this has been extended, in certain circumstances, to embrace liability for those who are considered 'akin' to employees and thus may cover some workers and others, although each case will turn on its facts.

Contracts of employment

There are many provisions, in addition to the basic framework of contract law, specific to contracts of employment. Many of these provisions cover trades unions and collective bargaining, which is outside the scope of this chapter, as are apprenticeships.

Under basic contract law, a contract of employment does not have to be in writing to be enforceable but, from April 2020, employees must be provided with a written statement of terms from the first day of their employment (Employment Rights, Employment Particulars and Paid Annual Leave) (Amendment) Regulations 2018). These regulations also expanded the detail required in the written statement.

Written statement of terms should include:

- names of parties
- date of commencement of employment
- cessation date or terms of fixed term or temporary work
- job title and details of work
- place of work
- details of any probationary period
- details of pay including method of calculation, intervals at which paid and any benefits
- an itemised payslip detailing deductions
- hours of work (including days of the week, any variations and how variation will be decided) and overtime arrangements
- holidays and holiday pay
- sickness provisions and sick pay
- pensions
- disciplinary rules
- grievance procedures
- notice periods to be given by employer and employee
- training provided by employer, any mandatory training entitlement and any training to be paid for by worker
- it would normally include maternity and paternity provisions.

There are, of course, various statutory provisions surrounding many of these factors, such as equal pay, minimum wage, maternity and paternity rights, holiday rights and more. A contract of employment must meet or exceed minimum statutory rights. It is not open to employers to ‘contract out’ of these frameworks, other than the 48-hour maximum working week (under the Working Time Regulations 1998, as amended).

Terms of employment

Ideally, all the terms and required information for a contract of employment is in a single document although terms of a contract can arise from various sources:

- written statement of terms
- written contract of employment (this may be the same document as above, but a bare statement of terms is not, of itself, a binding contract).
- terms implied by legislation or the common law

- additional communications in any form (oral or written) which may contain specific terms
- trades union collective bargaining.

Importantly, the information must be kept up to date with changes notified within a month. Note that employers do not normally have the right to unilaterally alter a contract of employment. But the terms of the original contract may have certain flexibilities for the employer built in (such as place and nature of work) to avoid future constraints and disputes.

Where a written statement is not provided, the employee can refer to an employment tribunal.

Common law terms

Where there is a contract of employment, regardless of written terms, both parties have rights and duties.

Employers' duties - in addition to the duties related to employment rights, as noted above:

- A duty to show mutual respect to the employee. The ethos behind this duty, which has emerged more recently, can be seen in the overarching theme of the Good Work Plan: that work should be 'fair and decent'.
- There is no duty on an employer to provide work but, of course, wages would need to be paid if agreed (subject to zero hours contracts).
- An employer has no duty to provide a reference. Any reference that *is* provided must, of course, be true. If untrue, there could be action for defamation of character (rare) or negligent misstatement.

Employees' duties - the employment relationship is, of course, between two parties and employees have obligations as well as rights and employees have, among other things, a duty:

- of personal service, distinguishing an employee from an independent contractor
- of faithful service
- not to damage their employer's interests or act with any conflict of interest
- not to make a secret profit from the employment; this provision has been overlaid by the law on bribery (Bribery Act 2010) and many employers have a blanket ban on accepting even modest gifts, and an employee should not accept a job from their employer's customer 'on the side'

- not to compete against the employer; clearly closely connected with other duties of faithful service and not making secret profits
- to obey the lawful and reasonable orders (orders not in breach of the law or express terms agreed between the parties) of the employer
- to carry out tasks with reasonable care and to take reasonable care of the employer's property.

Note that an employee in breach of one of these duties is, technically, in breach of contract. The circumstances will dictate whether this would amount to a fair reason for dismissal, but it would not be automatic fair grounds.

Contracts in restraint of trade

The duty not to compete with an employer may well extend beyond the end of employment. Many contracts include a 'restraint of trade' clause preventing operation in the same business in, for example, a close radius of the employer for a given period after leaving the employment and/or not approaching the employers' customers for a given period of time after leaving. The enforceability of such terms will depend on their reasonableness. A term for a shorter time and covering a smaller geographical area is likely to be more readily acceptable. The status of the employee and the nature of the industry will also impact 'reasonable' time and distance.

Maximum working week

The provisions of the Working Time Regulations 1998 can be opted out of by those over 18, although employers cannot dismiss or treat anyone unfairly if they refuse to opt out. Certain industries are not covered by the 48-hour week in the first place (e.g. armed and emergency services, domestic staff in private households), there are temporary exemptions (e.g. for seasonal workers) and certain industries are not permitted to opt out and work longer hours (e.g. airline staff, drivers of vehicles of 3.5 tonnes or more). The provisions for averaging hours (normally over 17 weeks but with industry exceptions), for opting out and the various exceptions mean that the 48-hour week is not as clear and protective as it might seem. As with many areas covered, reference to more detailed guidance is advised.

Termination of contract of employment

Most contracts of employment do not have an indicated date for termination, although some are fixed term. Where there is no express end date, then notice can be given by either party although, for an employer, this must come within a fair reason for dismissal. There are minimum notice periods of one week's notice for each year of continuous employment, up to a maximum of 12 weeks' notice. An employee must give a minimum of one week's notice although, again, the contract may specify a longer period.

It is common to require notice to be in writing (but there is no statutory requirement for this). Regardless of these provisions, either party can terminate the contract with no notice if the behaviour of the other party justifies such action. This is known as a summary or instant dismissal when the termination is by an employer.

Unfair dismissal

Employers can only terminate employment contracts for reasons deemed as 'fair'.

The Employment Rights Act 1996 sets out fair reasons for dismissal:

- the employee's capability or qualifications, including their skill, aptitude and health,
- the employee's conduct (see Disciplinary procedures, below),
- retirement of the employee (most employers no longer have a set retirement age although it is technically possible, but needs to be consistent and is open to an age discrimination claim, although employers may be able to justify in the interests of the business),
- redundancy, subject to fair process
- where continued employment would cause the employer to be in breach of a statutory duty,
- some other substantial reason justifying dismissal.

In addition to the reason, the *means* of dismissal also needs to be 'fair'. Reasonable procedures must be followed, for example, due investigation into conduct. Employers should use the Acas Code of Practice. Ultimately, in the round, was the dismissal a reasonable one in all the circumstances?

Remedies for unfair dismissal

Claims by an employee under the unfair dismissal rules are made to an Employment Tribunal, usually to be commenced within three months of the effective date of termination of the employment. Claims will initially be referred to Acas, who will mediate between the parties to reach a settlement, if possible, whether by re-instatement or financial.

An employee found to have been unfairly dismissed may be awarded:

- reinstatement of job,
- re-engagement with a job *comparable* to his or her former job or
- compensation.

All compensation consists of two elements, basic and compensatory.

Basic award

The calculation depends on a combination of factors: age, length of continuous service and weekly pay.

Age 41 and over	1½ week's pay for each year of employment,
Ages 22–40	1 week's pay for each year of employment,
Under age 22	½ a week's pay for each year of employment.

A maximum of 20 years' employment is taken and there is a ceiling on the maximum week's pay, increased periodically (£544 on 6 April 2021).

Compensatory award

The compensatory award is an amount considered just and equitable (bearing in mind a claimant's losses and expenses, including loss of future earnings). There is a statutory maximum compensation for unfair dismissal along with a basic award, which an Employment Tribunal can apply.

Redundancy

Redundancy (per s139 Employment Rights Act) is where:

- the employer has ceased to carry on business for the purposes of which the employee was employed or
- the employer has ceased to carry on business in the place where the employee was employed or
- the requirements of the business for employees to carry out work of a particular kind have ceased or diminished.

There is no entitlement to a redundancy payment if the employee unreasonably refuses suitable alternative employment.

Payments are calculated by reference to rules similar to those used in unfair dismissal awards. Note that for compensation for unfair dismissal or for redundancy, the week's pay does not normally include overtime and the calculation can be complicated where employees are on shift pattern, piece rates, or productivity bonuses, which are usually averaged over a 12-week period.

Employers must consult with trade unions (where applicable) or other representatives if sizeable numbers are to be made redundant over a short period. This duty is in addition to the obligation to notify the Secretary of State when making more than 20 redundant at the same time. If employers fail to consult, a special protective award may be made against them, which will safeguard the remuneration of employees for the period for which it is made.

Disciplinary procedures

Employers should have a disciplinary procedure in place, notified to all employees through their written statement of terms. This can help support any future dismissal cases and, more importantly, mitigate against minor matters escalating to the point of dismissal. See the Acas guidance, which supports fairness and transparency in the treatment of all employees.

Under the Employment Act 2008, an Employment Tribunal may increase an award made to an employee by up to 25% if the tribunal considers that the employer has unreasonably failed to comply with the Acas Code of Practice. An award may be reduced by a similar amount if an employee unreasonably fails to comply with the Code.

Grievance procedures

Grievance is where the employee has a complaint against an employer. Ideally, workplaces have grievance procedures in place which are clear and notified to employees in their written statement of terms. Setting up such procedures is straight forward using the Acas Code. The Acas website has exemplar grievance (and disciplinary) procedures.

Internal - Informal

Where employees have concerns, as with any legal issue, the best first step is to raise it calmly and informally, probably verbally, with many issues satisfactorily resolved by open communication. In preparation for any communication, employees are advised to refer to the Acas website. Employers in receipt of notification of a grievance should do the same. Both parties are advised to retain good notes of oral communications and confirm outcomes in writing (simply a quick email can provide invaluable future evidence and timely clarification). Employers should take informal notifications of grievance seriously to ensure speedy and effective resolution, to maintain good working relationships, and to evidence good practice (should the situation escalate).

Internal - Formal

If an informal approach does not resolve the matter, or the issue is particularly serious, an employee may wish to follow a formal procedure, setting out the grievance in writing. This should include evidence where available (perhaps a contract, payslip or photograph) and what the employee wants the employer to do about the issue. A hearing should follow, ideally within 5 days. Employees have a right to be accompanied and a written decision should be provided, normally within 24 hours.

Internal - Formal - Appeal

If the outcome is unsatisfactory to the employee, an appeal can be made and a hearing with a more senior manager or the business owner should follow, and the outcome of that meeting is final, subject to any right the employee may have to take the matter to an employment tribunal.

It is important for employers to note the following when any grievance is raised:

- that they can evidence investigation of the grievance, providing sound grounds on which to base their decisions,
- that data protection is being complied with,
- that any alleged criminal matter is referred to the police (as appropriate),
- that meetings are in a private and supportive atmosphere,
- that any mental health issues of the employee are considered (and expert referral/guidance sought as appropriate),
- that communication between employee and employer is maintained (and possibly enhanced) throughout,
- that employees are informed of their right of appeal and
- that detailed records are kept.

External – Employment Tribunal

If the matter is within the remit of an employment tribunal, then employees should be aware that there are strict time limits. This is normally three months less one day from the incident (six months if about redundancy pay or equal pay). It is a requirement that the employee informs Acas of wanting to make a tribunal claim and they will normally be offered an ‘early conciliation’ process.

Equality and discrimination

The Equality Act 2010 is the consolidating legislation, covering a range of anti-discrimination measures first introduced to the UK with the Equal Pay Act in 1970, the Sex Discrimination Act 1975 and the Race Relations Act 1976 with legislation on disability following in 1995 and 2005, and on age in 2006. The Act now covers nine protected characteristics:

1. age
2. disability
3. gender re-assignment
4. marriage and civil partnership
5. pregnancy and maternity
6. race
7. religion or belief

8. gender
9. sexual orientation.

Direct discrimination

Employers are largely well-informed that it is unlawful to treat anyone less favourably than another because of one of the protected characteristics. And that, essentially, everyone should have equality of treatment and opportunity, regardless of these characteristics. Incidents of direct discrimination are certainly far fewer than in the past.

Associates of those with protected characteristics

Employers should also be aware that it is unlawful to discriminate against a person because of their *association* with someone with a protected characteristic, for example a carer of a disabled person.

Indirect discrimination

Indirect discrimination is just as unlawful as direct discrimination and is where those with one of the protected characteristics are proportionately more likely to be affected by a requirement not, of itself, contrary to the Equality Act, for example, a stated minimum height will disproportionately impact women.

Hidden/imperceptible characteristics

Employers should note that not all protected characteristics will be obvious, such as certain disabilities, gender and sexual orientation.

Reasonable adjustment

Note that with disability, there is a requirement on employers to make reasonable adjustment. Only if the employee cannot cope after reasonable adjustment has been made, would there be an objective justification to dismiss/not employ. What is defined as a 'reasonable' adjustment will depend on the nature and size of the business, as well as the nature of the disability.

Equal pay

The Equality Act also covers the right of men and women in the same employment, and for workers and apprentices, to receive equal pay and terms. The early, blunt instrument of 'equal' pay between men and women has been refined to be consider 'like' work so that men and women in the same employment doing what is deem 'equivalent' work or work of 'equal value' must be paid the same, and on the same terms.

Justification for discrimination

There are, of course, limited groups for legal discrimination, known as 'objective justification'. This will require proportionate means of achieving a legitimate aim. Legitimate aims include health, safety and welfare but advice should be sought if trying to avoid the Equality Act provisions.

Claims

Perception of discrimination can lead to victimisation and harassment claims or claims of constructive dismissal.

Governance

The body responsible for upholding equality and human rights in England, Scotland and Wales is the Equality and Human Rights Commission and useful guidance is available on their website for employers and employees: www.equalityhumanrights.com.

Bullying, harassment and victimisation

Bullying is a behaviour which makes someone feel frightened, disrespected, 'put down', humiliated, made fun of, offended, upset or threatened. It is not, in itself, unlawful although clearly not behaviour anyone wants to see in the workplace. But it *is* unlawful if it takes the form of harassment. It may also breach the welfare parameters of the Health and Safety at Work Act, and it could give rise to a claim of constructive dismissal.

Harassment is where the unwanted behaviour of the nature noted above relates to protected characteristics under the Equality Act. It should be noted that it is the victim's perception which is important, *not* the perpetrator's intent.

It is classed as harassment:

- where the victim is *thought* to have a protected characteristic (even if they do not),
- where they are being harassed due to their link with someone with a protected characteristic and
- where they are distressed, feel their dignity is violated or that they are in a hostile environment because they *witness* harassment because of someone else's protected characteristic.

Employers should ensure:

- all complaints are taken seriously and acted upon,
- that employees know where and who to see with any concerns,
- that complainants are asked what they want to happen (but ensuring appropriate measures are taken even if the victim does not seek further action) and
- that a policy of informal and formal processes is in place, known to all and followed.

Acas mediation can be implemented if internal processes do not resolve matters speedily.

Victimisation is where someone is treated unfairly because they made, or supported, a harassment or discrimination complaint to do with a 'protected characteristic'. Where an employee feels victimised and if informal communication with a senior staff does not work, a formal grievance procedure can be raised.

Home Working

The recent global pandemic has made many employers, employees and workers consider working from home in a new light. After the restrictions enforcing home working were lifted, many employers have retained some level home working (depending, of course, on the nature of the work), for reasons of economy (such as maintaining smaller premises), productivity and staff well-being. Many staff value this, although some have inadequate home premises and find the isolation problematic. No one size fits all. Surveys have shown that most staff prefer, where possible, a measure of flexibility.

Employers wanting staff to work from home
Where employers seek to make changes to contractual terms there must be consultation and agreement from employees, including union consultation where relevant.

Employees wanting to work from home
Where employees seek to make changes, all employees (but not workers) have a legal right to make a 'statutory application' to request flexible working (under Part 8A sections 80F-I Employment Rights Act 1996). This is not just available for parents and carers, as is sometimes thought. Both employees and employers should consult the Acas guidance on this matter. Employers are required to review the matter in a 'reasonable manner' and to hold a meeting to discuss the request with the employee. But the employer can refuse the request if they have a valid reason which are listed in the legislation and which relate to practical business efficacy.

Working hours

Employees working from home are still covered by employment legislation on working hours.

Health, safety and welfare

Employers' statutory obligations regarding health and safety are still relevant off premises and a risk assessment should be carried out prior to the approval of home working, for any given individual.

Expenses

Any additional expenses an employee may incur should be discussed and agreed. This might include matters relating to health, safety and welfare such as appropriate seating, a desk of reasonable height to allow long hours, phone, broadband arrangements, computer equipment and printer, stationery, a fire extinguisher and/or other safety expenditure, home running costs such as additional heating and lighting (with a policy on how much can be claimed)

Mortgagee or Landlord

Employees should inform their mortgage lender or landlord to ensure there is no bar on home working.

Insurance

Employees should inform their home insurers and any additional expense discussed with employer. Employers should inform their insurers of the working patterns of employees, but their employers' liability insurance should cover as usual.

Taxation

Employees should be directed to explore HMRC provisions on claiming expenses and allowances for home working but not, of course, if already covered by employers.

Home working policy

It is good practice, and likely to be more common in future, that employers have a home working policy in place and a template can be found on the Acas website.

Mental Health

The mental health of employees and others has always been embraced in the statutory health and safety obligations of employers under the Health and Safety at Work etc Act 1974 where the foundation section setting out an employer's duty to employees (section 2) highlights 'welfare' along with health and safety. Such issues gained increased exposure with the instability, isolation, demanding working conditions and personal grief suffered by many in the 2020-21 global pandemic.

Employers must consider the mental health of their staff (and themselves) in their working practices and seek the available guidance. As always, the Acas website contains detailed information along with practical guidance for employers.

Dispute Resolution

As with any legal dispute, good communication is key. It is best to air issues informally, possibly verbally and then in written form. Grievance and disciplinary matters have their own formal staged processes as noted above.

For most disputes regarding employment the matter can be referred to an employment tribunal and many claims will have an interim requirement of Acas early conciliation, mediation or adjudication before going to the tribunal.

From the tribunal there may be grounds of appeal to the Employment Appeal Tribunal and from there, but only on a point of law and with permission, to the Court of Appeal.

In summary

These outline notes show that employment law is complex, not least because there are many variations on rights, often depending on the precise status of a worker and length of engagement. The law is also ever-changing. Although the regular reference to employers having policies in place might seem disproportionate for small and new businesses, such policies can be found online. Reference to these, with appropriate editing, will ensure that relevant issues have been covered. Small businesses will not have in-house professionals on the law or human resources, but a working knowledge and judicious use of online information will help anyone engaging staff or, indeed, any employee or worker, field issues before they become problems. Fulfilling such obligations is not only a legal imperative, but also a moral obligation and ensures business success by not diverting time, money and mental energy towards resolving issues which could have been avoided by being well-informed and implementing good working practices, to the benefit of all concerned.

Some key resources:

Acas - www.acas.org.uk
Citizens Advice - www.citizensadvice.org.uk
Department for Business, Energy and Industrial Strategy (embracing the Small Business Commissioner) - www.gov.uk/government/organisations#department-for-business-energy-and-industrial-strategy
Equality and Human Rights Commission - www.equalityhumanrights.com
Health and Safety Executive (HSE) - www.hse.gov.uk
Her Majesty's Revenue and Customs (HMRC) - www.gov.uk/government/organisations/hm-revenue-customs

References

Legislation

Employment Relations Act 1999 Employment Rights Act 1996
Employment Rights (Employment Particulars and Paid Annual Leave) (Amendment) Regulations 2018
Equal Pay Act 1970
Equality Act 2010
Health and Safety at Work etc Act 1974
National Minimum Wage Act 1998
Sex Discrimination Act 1975
Trade Union and Labour Relations (Consolidation) Act 1992
Transfer of Undertakings (Protection of Employment) Regulations 2006
Working Time Regulations 1998

Cases

Autoclenz Ltd v Belcher (2011) Supreme Court
Byrne Brothers (Formwork) Ltd v Baird (2002) Employment Appeal Tribunal
Pimlico Plumbers v Smith (2018) Supreme Court
Ready Mixed Concrete (South East) Ltd v Minister of Pensions and National Insurance (1968) High Court
Uber BV & Ors v Aslam & Ors [2021] Supreme Court

Other

Acas, 2020. *Discipline and Grievances at Work.* *www.acas.org.uk/sites/default/files/2021-03/discipline-and-grievances-at-work-the-acas-guide.pdf* [accessed 19 September 2021].
Secretary of State for Business, Energy and Industrial Strategy, *Good Work Plan* (Cm 9755, 2018).
Taylor, M, Marsh, G, Nicol, D and Broadbent, P, 2017. *Good work: The Taylor review of modern working practices*. London: Department for Business, Energy & Industrial Strategy.

CONTRIBUTORS' CONTACTS

Basck
Natalia Korek
Tel: +44 (0) 7455 834999
Email: natalia@basck.com

Boolean Logical Ltd
Nick Ioannou
Tel: +44 (0) 780 308 5249
Email: nick@booleanlogical.com

Buckingham Enterprise and Innovation Unit (BEIU)
University of Buckingham
Professor Nigel Adams
Tel: +44 (0) 1280 820 826 / Mobile: +44 (0) 7779 010838
Email: nigel.adams@buckingham.ac.uk

Carrie de Silva
Tel: +44 (0) 7583 144622
Email: carrie@carriedesilva.co.uk

Grant Thornton UK
Vijay Rathour
Tel: +44 (0) 20 7383 5100 / Mobile: +44 (0) 7788 418652
Email: vijay.rathour@uk.g.com

Howman Solicitors
Gary McGonagle
Tel: +44 (0) 20 7629 1801 / Mobile: +44 (0) 7887 774656
Email: gmg@howmansolicitors.co.uk

Hunters
Gregor Kleinknecht
Tel: +44 (0) 20 20 7412 5122
Email: gregor.klenknecht@hunterslaw.com

May Figures Limited
Dr. Mark Graves
Tel: +44 (0) 1727 751 080 / Mobile: +44 (0) 7754 593 562
Email: mark@mayfigures.co.uk

Julia May
Tel: +44 (0) 20 7666 3289 / Mobile: +44 (0) 7810 124799
Email: Julia@ mayfigures.co.uk

Patentgate GmbH
Margit Hoehne
Tel: +49 (0) 3677 205 9960
Email: mh@patentgate.de

Tessa Advisory Services
Paula Mugisa
Email: paula.mugisa@gmail.com

University of Buckingham Press
Jonathan Reuvid
Tel: +44 (0) 1295 738070
Email: jonathan.reuvid@legendtimesroup.co.uk

Whitespace
Karren Whitely-Brooks
Tel: +44 (0) 7710 023302
Email: karren@bewhitespace.com

James Tmothy Taylor
Tel: +44 (0) 7445 220020
Email: jtt@bewhitespace.com