IP Wales

Protecting your ideas

SME Guide to IP Cybersecurity

IP cybercrime

Intellectual Property (IP) is the area of law used by businesses to differentiate their products and services in the commercial marketplace via distinctive branding or endorsement; new inventions or creations; novel appearance or design. IP can be a critical asset for your business but one which is at risk of attack from cybercriminals if your business trades online, has a website or even just email.

IP crime is traditionally viewed as counterfeiting (false branding) and piracy (illegal copying) but cybercriminals are increasingly coming to recognise the value of confidential data held by your business, be it sensitive information about your business operation or customer information such as credit card details (note EU General Data Protection Regulation 2018).

Your Trade Secrets which may be subject to online attack include:
technical & scientific data – formulas; software code; know-how details; product information relating to design/composition/performance; manufacturing information relating to raw materials; refining processes; specialised machinery.
commercial data – business plan; marketing strategy; contract terms; supplier arrangements; customer profiles/preferences/requirements; sales methods.
financial data – internal cost structure; price lists; salaries.
negative data – dead-end research projects; failed manufacturing processes.

In reality, any data which could be of value to your business is a worthwhile target for the cybercriminal. Attacks on data are happening with increasing rapidity and ever more complexity. Zero-day vulnerabilities (where hackers have discovered and exploit a software security breach before a fix is available) are increasing exponentially. When compared to making money from traditional crimes against tangible property cyberattacks on SMEs is a relatively low-cost and low-risk proposition, especially for those residing in jurisdictions where the activity is not actively prosecuted by State authorities.

Dispelling myths

My business is too small to be a target and does not have data worth stealing – in the two seconds it has taken you to read this 25 people online just became the victims of cybercrime. Cybercrime is often indiscriminate in nature. Research carried out by IP Wales for the Welsh Government in 2011 reported over 50% of our respondent SMEs had been subjected to malware (malicious software) attack in an era of 2.3 million items of malware, as compared to over 430 million items of malware today.

My free software protection does the trick – whilst free cyber security solutions are readily available they do not offer comprehensive protection (Fazio Mechanical is thought to have used a free version of malware protection – see below).

My computer is a Mac so I'm safe - with tight security features and a largely virus-free ecosystem Apple users might be forgiven for having a greater sense of protection. However, the 2016 'Transmission BitTorrent app hack' shows the danger of any complacency and cyberattacks on the Apple mobile devices platform are increasing in regularity.

Types of cyberattack

'*Network confidentiality*' – the main IP cyber threat, the aim here is to steal or release confidential data held by your business. Research carried out by IP Wales for the Welsh Government in 2011 reported over 80% of our respondent SMEs did not scan staff emails for confidential data or have any controls over the use of USB sticks at work, 70% did not encrypt customer payment details and nearly 40% did not encrypt their wireless network. In 2013 US retailer Target was the subject of a network confidentiality attack which resulted in the loss of sensitive data relating to 70 million customers, including 40 million credit card numbers. The hack resulted in over 90 lawsuits being filed against Target by customers and banks for negligence and compensatory damages. Whilst Target had just spent U$1.6m on a malware detection tool, investigations revealed the hackers acquired the data through Fazio Mechanical (a third party supplier of less than 100 employees) by accessing the network credentials given to it by Target (an attack technique known as 'island hopping', where the cybercriminals target the weakest link in the cybersecurity chain).

'*Network availability*' – typically known as denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks, the aim is to render the web site inoperable by flooding it with a massive number of requests (e.g. a 'botnet attack' – co-ordinated attack using hacked PCs, printers & web-connected 'smart' home devices such as CCTV cameras, kettles, toasters etc. under the "internet of things"). Following a US Secret Service investigation in 2016 Frazer-Mann of Elite Loans admitted five charges in Cardiff Crown Court of commissioning DoS attacks on rival pay-day loan companies. He offered hackers from Costa Rica U$100 to take competitor websites down.

'*Network integrity*' – the aim is to cause damage to hardware, infrastructure, or real-world systems. Delivered by a rogue employee using a USB drive the 2012 'Shamoon hack' on Saudi Aramco's computer network resulted in 30,000 company computers requiring replacement.

The techniques used by cybercriminals to give effect to these attacks, targeted or otherwise, include:
(Spear-)phishing/smishing – an innocent looking email or sms message (to a targeted individual) enticing them to click on a link or download a file which then infects the user's system, spreading to infect other users. With so much information now publicly available about targeted individuals on social media cybercriminals are becoming increasingly sophisticated with their 'baiting' email or message.
Watering-holes & exploit kits – a compromised web site with predator code waiting to exploit the unsuspecting visitor.
Ransomware – be it 'locker ransomware' (locking the screen) or 'crypto ransomware' (preventing access to your own files or data via encryption – see the 'wcry'/'WannaDecrypt0r' attack on the NHS in May 2017).

Cyber espionage

Disgruntled employees, hackers, hacktivists, industrial competitors may not be the only potential intruders into your network. An American IP Report published in 2013 estimated the annual losses to IP theft, primarily from China, exceeding U$300 billion with many attacks targeted against SMEs. In 2014 the US Justice Department indicted 5 officers from China's People's Liberation Army Unit 61398 for stealing intellectual property to help China's state-owned and state supported enterprises, a charge denied by a Chinese spokesperson.

Data content driven business

If yours is a data content driven business then you need to be able to monitor both the unauthorised and unlawful promotion and distribution of your digital content e.g. files of films/tv programmes, music, software, computer games, books, reports or 3D printing designs.

A Report published by the World Intellectual Property Organization (WIPO) in 2015 predicts that most firms will soon need to familiarise themselves with the legal realities of the 3D printing 'revolution'. The Report notes that the distinction between industrial versus personal 3D printing (also known as 'additive manufacturing') is fading as the personal segment of the market becomes more commercial but *"personal 3D printing potentially raises issues of large-scale infringement of existing IP rights. Underlying this challenge is the tension between what is legal and what is enforceable in practice".*

Established in 2013 under funding from the UK Intellectual Property Office, the City of London Police established the world's first Police Unit dedicated to combating IP Crime. The Police Intellectual Property Crime Unit (PIPCU) has a wide remit under which to launch initiatives such as 'Operation Creative', which targets websites that provide free illegal downloads of films & music in order to draw down online advertising revenue. However, these sites typically operate beyond PIPCU jurisdiction, so the policy has had to become one of disrupting rather than dismantling this borderless online IP crime.

The commercial strategy for addressing the unauthorised/unlawful use of your digital content is for your business to determine, with legal compliance/policing & enforcement often treated as two sides of the same coin. Microsoft's Digital Crimes Unit (MDCU) uses the civil law (with its lower burden of legal proof) to take action against cybercriminals, while seeking to work with national law enforcement to seize their physical infrastructures.

IP Cybersecurity

If data is the raw material for the new information age, then cybersecurity is the prerequisite to businesses operating securely within the new digital environment.

We are familiar with security precautions safeguarding the tangible property of a business but unlike the burglar alarm which only alerts the business to an intrusion and hopefully deters, cybersecurity can proactively protect your intellectual assets by blocking the majority of intrusions into your network before infection. It can rapidly detect and remediate any infection which has infiltrated your network. It can also stop data breaches from lost or stolen end points (desktops, laptops, tablets, smartphones, USB sticks etc.); safeguard online financial transactions; secure your password management; manage back-ups. It can even pre-empt future data attacks via automated risk assessments.

Cybersecurity is mission critical for any IP active business with an online presence. A failure of cybersecurity carries with it the risks of:

- *Leakage of sensitive data* – allowing both internal and external attackers to compromise confidential business/customer data held by your business or conduct unauthorised releases of sensitive information, causing reputational damage and a loss of trust in your business.

- *Import/Export of Malware* – importing of malware into your network and/or the exporting of malware to your business partners or the general public at large.

- *Your exclusion from Supply Chains* – excluding your business from supply chains to prevent attackers from inflicting reputational and/or financial damage to partner organisations and their customers (‘island hopping’).

A breach of your firms’ cybersecurity is at best an inconvenience and at worst could prove critical for the survival of your business. Yet in research conducted by IP Wales for the Welsh Government only 1 firm allocated 10% or more of their IT budget towards cybersecurity measures. Recent research into 500 UK SMEs funded by Trend Micro (see below) revealed that over half the firms surveyed had no internet security tools to protect their business from cyberattack.

Officially launched in February 2017 the UK National Cyber Security Centre (NCSC) – a part the UK Government Communications Headquarters (GCHQ) - has warned SMEs,”*if you openly demonstrate weaknesses in your approach to cybersecurity by failing to do the basics you will experience some form of cyberattack…**doing nothing is no longer an option***”.

Planning your IP cybersecurity resilience

Preparations for a cyberattack on your business should include (a) vulnerability mitigation measures and (b) developing an incident response and disaster recovery capability i.e. a well-tested plan of what to do if those prevention measures fail.

Vulnerability mitigation measures

Preventing, detecting or disrupting an attack at the earliest opportunity limits potential business impact and reputational damage. ***Cyber Essentials*** is the UK government's minimum standard of protection for IP cybersecurity and promotes the use of[1]:

- *Firewalls & internet gateways* – detect and block executable downloads, block access to known malicious domains and prevent users' computers from communicating directly with the Internet.

- *Malware protection* – establish and maintain malware defences to detect and respond to known attack code.

- *Patch management* – patch known vulnerabilities with the latest version of the software.

- *Whitelisting & execution control* – prevent unknown software from being able to run or install itself (including Autorun on CD & USB drives).

- *Secure configuration* – restrict the functionality of every device, operating system and application to the minimum needed for your business to function (note the need here for *Cloud* security principles).

- *Password policy* – ensure an appropriate policy is in place.

- *User access control* – limit normal users' execution permissions and enforce the principle of least privilege.

If your business falls victim to a network availability or network integrity attack it will be self-evident but network confidentiality attacks are often less obvious. Internal system monitoring & external surveillance (e.g. dark web) provides a capability to detect actual or attempted attacks and is increasing in importance to comply with legal or regulatory requirements.

[1] Common Cyber Attacks *Reducing the Impact* (NCSC)

Other controls to mitigate the various stages of a cyberattack include:

Survey stage

- User education & awareness – train all users in the risks of public disclosure and spear-phishing techniques.

Delivery stage

- Network perimeter – block insecure or unnecessary services or only allow access to permitted websites.
- Malware protection – block malicious emails and prevent malware being downloaded.
- Password policy – improve the quality of passwords and lock user accounts after a low number of failed attempts.
- Secure configuration – restrict system functionality to the minimum needed for business operation on every device.

Breach stage

- Patch management – apply patches at the earliest possible opportunity.
- Monitoring – monitor and analyse all network activity to identify any malicious or unusual activity.
- Malware protection – protection within the internet gateway can detect malicious code.
- Secure configuration – remove unnecessary software and default user accounts. Change default passwords and ensure automatic features that could activate malware are turned off.
- User access – restrict the applications, privileges and data that users can access.
- User training – valuable in reducing the likelihood of successful social engineering attacks.
- Device controls – prevent unauthorised access to critical services or inherently insecure services that may still be required by the business.

Affect stage

- Planned controls for a bespoke capability attack – whereas the aforementioned controls can combat attacks using commodity (known) capabilities they are likely to be less effective against new malicious code or ‘zero day’ exploits.

Developing an incident response and disaster recovery capability (planning for the worst)

The NCSC has made clear that all SMEs can expect to experience a cybersecurity incident at some point and, "*investment in establishing effective incident management policies and processes will help to improve resilience, support continuity, improve customer and stakeholder confidence and potentially reduce any impact*."

Planning a cybersecurity incident response capability requires good preparation and a comprehensive review of the state of readiness of your business.

In terms of response, each incident will necessitate a proportionate response – overreacting can be detrimental.

The designated member(s) of staff should:

- Verify the breach and work to contain and then eradicate it.
- Confirm the extent of the breach and the data/services which have been affected.
- Identify the risks arising to the business and others from the breach.
- Implement any recovery of data via back-up files and recover any systems and connectivity.

In addition to keeping other members of the business apprised (ensuring media dialogue is co-ordinated through one person/team operating under legal advice), relevant parties who may need to be informed include the Police/Action Fraud; Banks/Credit Card Companies; Regulators (note the 72hr reporting deadline under GDPR 2018)/Insurers (SRA in the case of Solicitors) and potentially 'Data Subjects".

Litigation risk will need to be assessed and once matters have been addressed your business will need to conduct a structured review and lessons learned exercise.

Deception Technology

In recognition of the fact that no organisation can mount a perfect digital defence some businesses are reported as having employed deception technologies to hide their valuable data i.e. creating a shadow network to divert and mislead the malicious intruder into wasting their valuable resources.

Top 5 Corporate Endpoint Security Leaders

At the time of writing the International Data Corporation (IDC) has identified the following suppliers, prioritised by market share:

1. *Symantec* – (Head Office: USA) the company has recently reduced the number of versions of its Norton Antivirus line for SMEs.

2. *Intel Security* – (Head Office: USA) formerly McAfee.

3. *Trend Micro* – (Head Office: Japan) in 2015 the company funded research into 500 UK SMEs which revealed only 18% thought they had data worth stealing.

4. *Sophos* – (Head Office: UK) the company has placed an emphasis on serving the needs of SMEs.

5. *Kaspersky Lab* – (Head Office: Russia) the company is developing a US federal arm to bid for US government contracts.

To build an effective IP cybersecurity resilience for your business may require the selection and management of external suppliers beyond just malware protection. External support for a cybersecurity incident response, as well as STAR (Simulated Targeted Attack & Response) penetration testing, can be provided by UK approved member firms of CREST (visit www.crest-approved.org).

5 lessons you can learn the easy way

- You may not be able to stop your business becoming a target for cybercriminals but there is a lot your business can do to protect itself from becoming the victim of cybercriminals.

- Programmes which have not been updated are the number one route used by cybercriminals to 'hack' businesses. Using pirated software, inadvertently or otherwise, exposes your business to far greater digital risk.

- Working on the move is now part of everyday life and cybercrime is increasingly directed towards mobile devices. Using unprotected wi-fi (e.g. public wi-fi in coffee shops & airports etc.) carries an increased risk of your data being intercepted.

- Users can be a significant source of vulnerabilities. Using the same password in both a professional and private context should be avoided. However strong it may have been, a compromised password used for multiple purposes can lead to an even bigger security breach.

- Trusted sources cannot always be trusted as they may have been compromised. It is becoming ever more difficult to identify baiting emails under 'spear-phishing'.