Protecting your ideas

IP Community Guide to SMEs Reporting IP Cybercrime

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 a business but one which is at risk of attack from cybercriminals if the business trades online, has a website or even just email.

In the USA IP Crime is viewed as Copyright Infringement (17 U.S.C. §§ 102(a), 106); Trademark Counterfeiting (15 U.S.C. § 1127), and Trade Secret Theft (18 U.S.C. §§ 1831, 1832, also note the Defend Trade Secrets Act 2016 codified at 18 U.S.C. § 1836). Trade secret law prohibits the unauthorized disclosure of any confidential and proprietary information, such as a formula, device, or compilation of information but only when that information possesses an independent economic value because it is secret and the owner has taken reasonable measures to keep it secret.

In the UK 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 (undisclosed information) held by your client's business, be it sensitive commercial information about their business operation or personal information held on customers, such as credit card details (note EU General Data Protection Regulation).

Broadly speaking, confidential business information which provides an enterprise with a competitive edge and is kept secret may be deemed a trade secret. The unauthorised acquisition, use or disclosure of such secret information in a manner contrary to honest commercial practices by others is regarded as an unfair practice and a violation of the trade secret protection.

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 of value to your client 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 criminals residing in jurisdictions where the activity is not actively prosecuted by State authorities.

When does an IP violation become a crime?

Trade Mark Counterfeiting:

Specific offences are created under Section 92 of the Trade Marks Act [TMA] 1994, in addition to which there may be relevant 'lifestyle offences' under Schedule 2 to the Proceeds of Crime Act [POCA] 2002. However, it might be noted that simple possession of counterfeit goods will not necessarily be an offence under the TMA, unless specifically proscribed under alternative legislation (e.g. Section 16 of the Forgery and Counterfeiting Act 1981). The TMA requires that a person acts without the consent of the trade mark owner with a view to making a gain for themselves or somebody else, or acts with intent to cause loss to another person. 'Grey market' goods (genuine items bought and sold outside the manufacturer's authorised trading channels) are not counterfeit but goods advertised as replicas can still be.

Copyright Infringement:

Specific offences are created under a number of sections of the Copyright, Designs and Patents Act 1988 (as amended) which are predominantly focused upon those who infringe copyright in the course of business, or for commercial purposes, or to such an extent as to prejudicially affect the owner of the copyright e.g. Section 107 making, dealing, possessing communicating infringing works; Section 198 making, dealing, using, communicating infringing recordings; Section 296ZB devices and services designed to circumvent technology protection measures of the copyright owner; Section 297 fraudulently receiving programmes or using unauthorised decoders. Some offences (e.g. 107(1), 107(2), 198(1) and 297A are 'lifestyle offences' by virtue of Schedule 2 to the Proceeds of Crime Act [POCA] 2002.

Online taking or hostaging of Trade Secret data:

Within UK law enforcement cybercrime is categorised as being cyber-enabled crimes (e.g. offences such as cyber fraud, harassment or grooming) and cyber-dependent crimes (e.g. offences contrary to the Computer Misuse Act 1990).

Before the Computer Misuse Act (CMA) prosecuting the theft of information stored on computers proved problematic, as information did not fall within the definition of 'property' under Section 4(1) of the Theft Act 1968 (see *Oxford v Moss* [1979]). It was also a matter of controversy whether the hacking of information stored on computers fell within Section 1 of the Criminal Damage Act 1971 (see *R v Whitely* [1991]). A prosecution under Section 1 of the Forgery and Counterfeiting Act 1981 - given a computer could not be considered the 'victim' of a deception under the Theft Act - proved equally unsuccessful, when the criminal courts concluded no 'false instrument' had been created (see *R V Gold* [1988]). For these reasons the Law Commission advocated in 1989 the creation of the first piece of computer-specific legislation to "*more effectively*" deal with the growing trend of problems associated with the misuse of computers and computer systems.

Enacted in the following year the CMA provides for criminal sanction against online attacks relating to 'undisclosed information' (see Article 39 of the Agreement on Trade-Related Aspects of Intellectual Property Rights [TRIPs Agreement]). Section 1 creates the basic offence of unauthorised access; Section 2 unauthorised access with the intent to commit further offences; Section 3 unauthorised acts with the intent to impair the operation of a computer. Since the CMA came into operation two additional offences have been created – Section 3A making, supplying or obtaining articles for use in an offence under the Act i.e. 'hacking tools' (introduced under Section 37 of the Police and Criminal Justice Act 2006) and Section 3AZ unauthorized acts in relation to computers which cause/create risk of serious damage, implementing EU Directive 2013/40 on attacks against computer system i.e. situations where the level of harm inflicted by a large-scale cyberattack warrants a prison sentence greater than 10 years (introduced under Section 41 of the Serious Crimes Act [SCA] 2015).

How to recognise becoming the victim of an IP cyberattack

The Institute of Directors has warned that on average it takes 120 days for a business to know that its data has been compromised.

Cyberattacks targeting IP are often asymptomatic (because the attackers have covered their tracks). They often take place over a long timeframe and can be aimed at differing aspects of the organisation. So unless a client business takes active steps it is unlikely to be in a position to recognise that it has fallen victim to an IP cyberattack.

There are many different ways in which a IP cybersecurity incident can be identified:

• Alerts generated by technical monitoring systems: such as Data Loss Prevention (DLP), Intrusion Detection Systems (IDS), antivirus software, and log analysers – having a blind 'fit and forget' trust in monitoring tools should however be avoided. Client firms should ensure they have access to the request skills to analyse such data effectively.

• Suspicious events reported, for example, by employees or customers.

• Anomalies detected by audits, investigations or reviews.

• Cyber threat intelligence e.g. Cybersecurity Information Sharing Partnership (CiSP) – membership of which is open to any UK registered company or other legal entity which is responsible for the administration of an electronic communications network in the UK and is sponsored by either a government department, existing CiSP member or a regional Cyber PROTECT police officer or industry champion.

Why report IP cybercrime

By definition a 'Trade Secret' loses its commercial value when it is no longer secret and when looking to retain commercial trust there is a natural reluctance on the part of most businesses to report that they have fallen victim to a breach of their IP cybersecurity[1], albeit such victims are not alone – the Institute of Directors reports the UK's 5.4 million small businesses are collectively attacked more than seven million times a year, with 66% falling victim to cybercrime in the last two years.

Nevertheless, the effective prosecution of IP cybercrime requires substantial assistance from its victims, with law enforcement authorities unable to act in many cases unless the crimes are reported in the first place. Additional to statutory reporting requirements the US Department of Justice has set itself the goal of making it as easy as possible for victims in the USA to report incidents of IP cybercrime to law enforcement authorities, using departmental press releases to promote high-profile instances of prosecutions for trade secret theft.

SME Client firms with Cyber and Data Insurance (see our ***Guide to SMEs Outsourcing Cybersecurity Incident Response & Data Recovery Activities***) are likely to find themselves under an obligation to report cybersecurity breaches when claiming under the Policy. Other than under such insurance, few SME client firms will have access to the digital forensic expertise possessed by law enforcement to conduct a full investigation.

Unlike the Police and other government agencies[2], SME client firms do not possess the legal powers to engage in retaliatory offensive cyber activities, as part of active cyber defence.

[1] Only 26% of firms did so under the latest UK Government Cybersecurity Breaches Survey (2017) – excluding reporting to outsourced cybersecurity providers.

[2] See further amendments to the Computer Misuse Act 1990 introduced 3rd March 2015

How to report IP cybercrime

Online counterfeiting & piracy

Local trading standards is the leading authority for enforcing criminal legislation relating to piracy and counterfeiting. Within UK law enforcement there are a number of externally funded specialist units to investigate specific types of perceived fraud which impact on particular sectors. One such specialist unit is the Police Intellectual Property Crime Unit (PIPCU) based within the Economic Crime Directorate of the City of London Police, the UK National Lead Force for Fraud. Funded by the UK Intellectual Property Office (IPO) [£5.56m 2013-2017] the Unit is dedicated to tackling serious and organised counterfeiting & piracy (excluding pharmaceuticals, foodstuffs, alcohol, tobacco or currency - unless exceptional circumstances apply) with a focus on offences committed using an online platform. There are a number of factors considered by PIPCU in their case acceptance process, not least the likelihood of a successful outcome. PIPCU works with the IPO Intelligence Hub (UK point of contact for Europol's IP Crime team) to target international organised criminal groups [OCGs], especially where there is the potential to cause physical harm to individuals and the general public.

Online taking or hostaging of trade secret data

Action Fraud is the UK's national reporting centre for all incidents of cybercrime and fraud, with reports able to be made online or via telephone. However Action Fraud is not in popular use with firms who have fallen victim to online attack[3], leading to concerns about an under-reporting of the online taking or hostaging of trade secrets.

Two Regional Organised Crime Units (ROCU) operate in Wales – TARIAN (covering the Gwent, South Wales, Dyfed-Powys police force areas) & TITAN (covering North Wales along with Cheshire, Merseyside, Greater Manchester, Lancashire, Cumbria police force areas). The National Cybercrime Unit [NCCU], as part of the National Crime Agency [NCA], leads on UK national police responses to the most serious cybercrime, working with the National Cybersecurity Centre [NCSC], which co-ordinates governmental responses to national cybersecurity threats.

[3] Less than 2% of the firms who had fallen victim to a cyberattack reported it to Action Fraud under the latest UK Government Cybersecurity Breaches Survey (2017).

How to assist law enforcement

In a digital world where evidence can disappear at the click of a mouse or the tap of a smartphone it is little wonder that UK law enforcement looks to operate under the 'golden hour' principle for cyber offences – effective early action by a 'First Responder' can result in securing significant digital data that would otherwise be lost to an investigation through being dumped or overwritten (see ACPO *Good Practice Guide for Digital Evidence* 2012 & College of Policing *Authorised Professional Practice-Investigation* 2016).

Data evidencing the interaction between the victim and the offender's attack infrastructure is usually in a volatile state and can cease to exist when power is shut down to a system or hardware, such as a server. Information regarding network connections and system processes often exists in the form of event logs, which may have limited duration or are otherwise capable of being deleted remotely, yet it is within these event logs (and registry files) that suspicious activity can be detected. Any communication from the cybercriminal (including email headers – also known as source code) will also need to be evidentially secured, as it may contain valuable information to help identify the suspect.

We have already noted (see our ***Guide to SMEs Outsourcing Cybersecurity Incident Response & Data Recovery Activities***) that many organisations carry out the role of 'First Responder' themselves, dealing with all the initial activities prior to the more detailed investigation. SME Client firms may therefore find themselves in the situation of having to capture this digital evidence for themselves and should look to plan in advance for this eventuality.

Notwithstanding the 'golden hour' principle UK law enforcement has been advised to prioritise the future prevention of cyberattacks over a current investigation, especially in the case of a cyberattack affecting the day-to-day operation of a business.

Accurately assessing the risk

A recent UK government survey (2017) recorded cybersecurity breaches resulting in the loss of trade secret data at only 1% of the firms to have identified a breach or attack in the previous year. This might lead some client SMEs to conclude that the threat poses a low level of risk to their business.

It was noted in the same survey however that protecting commercial trade secrets, IP or other assets (e.g. cash) was the second most important driver for investment in cybersecurity (28%), with protecting customer data the highest driver (51%)[4] .

There are a number of reasons to conclude that there is a significant under-reporting of online attacks targeting trade secret data:-

1. the survey finding is at odds with evidence presented from the US - *"total annual losses due to stolen IP are in the hundreds of billions of dollars."* The IP Commission Report on the Theft of American Intellectual Property (2013)

2. the survey finding is at odds with evidence presented from the UK Government - . "given the industrial-scale theft of intellectual property from our companies and universities," Robert Hannigan, Director GCHQ, March 2016

3. Firms may not be aware that they have fallen victim to an IP cyberattack – see *How to recognise becoming the victim of an IP cyberattack* above

4. Firms are reluctant to report IP cyberattacks – see *Why report IP cybercrime* above

5. The reporting structure for the UK is not in popular use – see *How to report IP cybercrime* above

6. The priority is avoiding future cyberattacks rather than reporting & investigating previous cyberattacks – see *How to assist law enforcement* above.

[4] EU General Data Protection Regulation (GDPR) comes into force on 25th May 2018, with the threat of fines increasing from the current maximum of of £500,000 under the Data Protection Act to:-

- Up to 2% of annual worldwide turnover of the preceding financial year or 10 million euros (whichever is greater) for violations relating to internal record keeping, data processor contracts, privacy impact assessments, data security and breach notification and data protection by design (amongst others); and

- Up to 4% of annual worldwide turnover of the preceding financial year or 20 million euros (whichever is greater), for violations relating breaches of the data protection principles, conditions for consent, data subject's rights and international transfers.

Further reading

This Guide is intended for educational use only and uses selected text and adaptations from:

Michael Betts (Consultant Editor Commander David Clark, City of London Police, Police National Coordinator for Economic Crime), *Investigation of Fraud and Economic Crime* (OUP 2016)

U.S. Department of Justice Reporting Intellectual Property Crime, *A Guide for Victims of Copyright Infringement, Trademark Counterfeiting, and Trade Secret Theft* (2nd edition, 2016)

CREST *Cybersecurity Incident Response Guide* (2013)

