Protecting your ideas

IP Community Guide to useful sources to help understand who is committing digital IP infringements & online attacks against SMEs & what is motivating them

1. Understanding Cybercrime

Researcher and academic, David Wall (2001), identified a typology of cybercrime which categorised the various malicious activities into four broad categories. These categories allow us to understand the type of criminal activities as well as the behaviours of the offenders who perform them.
Wall identified the categories as follows:

1. Cyber-Trespass
2. Cyber-Deception and theft
3. Cyber-porn and obscenity
4. Cyber-violence

For the purposed of this guide, the focused will be on the first two categories.

Cyber-Trespass

As the name suggested, Cyber-Trespass relates to the unlawful act of crossing a digital boundary of ownership to gain access to (trespassing) another's property (computer or system). These activities include malicious hacking and the transmission of viruses, trojans and malware.

Cyber-Deception and Theft

Enabled by technology and its increasing user friendliness and accessibility, Cyber-Deception and Theft refers to:

- **Deception**: using digital platforms and channels to deceive unsuspecting and vulnerable users online. These include phishing emails where mass dissemination of emails containing malicious attachments or links to gain access to user's personal information and systems. Offenders wait for the users to click on the links or open the attachments and then gain access to their machines and system to source personal data and/or Intellectual Property.
- **Theft**: this relates to digital piracy and the illegal copying of media for unauthorised and unlicensed use and consumption.

Wall's typology is one theoretical explanation of cybercrime, and is being used in this guide to apply a structure and format to the discussion and information sharing. By categorizing the criminal behavior into these four silos, we are able to address the context of threats to businesses Intellectual Property in a controlled and sequential manner.

For more information on Wall's typology of cybercrime see his 2001 book, Crime and the Internet (Routledge). This work is also summarised by Thomas Holt in the book titled "Cyberpsychology" edited by Alison Attrill (2015), chapter 8 entitled Cybercrime and Deviance.

2. Perpetrators of IP Cybercrime

The UK Government National Cybersecurity Strategy (2016-2021) identifies the perpetrators of IP Cybercrime as:

Cyber criminals

The strategy deals with cybercrime in the context of two interrelated forms of criminal activity:

- *cyber-dependent crimes* – crimes that can be committed only through the use of Information and Communications Technology (ICT) devices, where the devices are both the tool for committing the crime, and the target of the crime (e.g. developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity); and
- *cyber-enabled crimes* – traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and data theft).

Much of the most serious cybercrime – mainly fraud, theft and extortion – against the UK continues to be perpetrated predominantly by financially motivated Russian-language organised criminal groups (OCGs) in Eastern Europe, with many of the criminal marketplace services being hosted in these countries. However, the threat also emanates from other countries and regions, and from inside the UK itself, with emerging threats from South Asia and West Africa of increasing concern.

Even when key individuals responsible for the most damaging cybercriminal activities against the UK are identified, it is often difficult for the UK and international law enforcement agencies to prosecute them when they are located in jurisdictions with limited, or no, extradition arrangements. Ironically, the internet both enables increased business opportunities, while also increasing opportunities for cybercrime offences and decreases the ability to enforce domestic laws.

These OCGs are principally responsible for developing and deploying the increasingly advanced malware that infects the computers and networks of UK citizens, industry and government. The impact is dispersed throughout the UK, but the cumulative effect is significant. These attacks are becoming increasingly aggressive and confrontational, as illustrated by the increasing use of ransomware, and threats of distributed denial of service (DDoS) for extortion.

Whilst OCGs may pose a significant threat to the collective prosperity and security of the UK, equally of concern is the continuing threat from acts of less sophisticated but widespread cybercrimes carried out against individuals or smaller organisations.

States and state-sponsored threats

A Report published by the Commission on the Theft of American Intellectual Property (2013) noted, "*In a world where the highest-value assets are intangible and easy to transfer over networks, espionage has taken on a new dimension…In the rapidly evolving landscape of*

cyberespionage, it has become clear that not even the smallest organizations or lowest-level employees are safe from attack. Of equal concern is that effective and deeply penetrating cyberattacks are occurring across a broad spectrum of IP-intensive industries." The Report goes on to name China and Russia as the main culprits in this world of Trade-Secrets Theft.

For its part the UK Government notes it regularly sees attempts by states and state-sponsored groups to penetrate UK networks for political, diplomatic, technological, commercial and strategic advantage, with a principal focus on the government, defence, finance, energy and telecommunications sectors.

The capacity and impact of these state cyber programmes varies. The most advanced nations continue to improve their capabilities at pace, integrating encryption and anonymization services into their tools in order to remain covert. While they have the technical capability to deploy sophisticated attacks, they can often achieve their aims using basic tools and techniques against vulnerable targets because the defences of their victims are poor.

Only a handful of states have the technical capabilities to pose a serious threat to the UK's overall security and prosperity. But many other states are developing sophisticated cyber programmes that could pose a threat to UK interests in the near future. Many states seeking to develop cyber espionage capability can purchase computer network exploitation tools 'off the shelf' and repurpose these to conduct espionage.

Beyond the espionage threat, a small number of hostile foreign threat actors have developed and deployed offensive cyber capabilities, including destructive ones. These capabilities threaten the security of the UK's critical national infrastructure and industrial control systems. Some states may use these capabilities in contravention of international law in the belief that they can do so with relative impunity, encouraging others to follow suit. Whilst destructive attacks around the world remain rare, they are rising in number and impact.

Insiders

Insider threats remain a cyber risk to organisations in the UK. Malicious insiders, who are trusted employees of an organisation and have access to critical systems and data, pose the greatest threat. They can cause financial and reputational damage through the theft of sensitive data and intellectual property. They can also pose a destructive cyber threat if they use their privileged knowledge, or access, to facilitate, or launch, an attack to disrupt or degrade critical services on the network of their organisations, or wipe data from the network.

Of equal concern are those insiders or employees who accidentally cause cyber harm through inadvertent clicking on a phishing email, plugging an infected USB into a computer, or ignoring security procedures and downloading unsafe content and software from the Internet. Whilst they have no intention of deliberately harming the organisation, their privileged access to systems and data mean their actions can cause just as much damage as a malicious insider.

These individuals are often the victims of social engineering – they can unwittingly provide access to the networks of their organisation or carry out instructions in good faith that benefit the fraudster.

The overall cyber risk to an organisation from insider threats is not just about unauthorised access to information systems and their content. The physical security controls protecting those systems from inappropriate access, or removal of sensitive data or proprietary information on different forms of media, are equally important. Similarly, a robust personnel security culture that is alive to the threat posed by disaffected employees, fraud in the workforce and industrial and other forms of espionage is an important element in a comprehensive approach to security.

'Script Kiddies'

So-called 'script kiddies' – generally less skilled individuals who use scripts or programmes developed by others to conduct cyberattacks – are not assessed as posing a substantive threat but due to the vulnerabilities found in internet-facing systems used by many organisations they can have a disproportionately damaging impact on an affected organisation. It is important to note that the ever-increasing sophistication of readily available malicious software packages and tutorials online results in 'script kiddies' being able to simply purchase or download increased threat capability regardless of their own technical skill set.

Terrorists

Whilst terrorist groups continue to aspire to conduct damaging cyber activity against the UK and its interests the current technical capability of terrorists is judged to be low. The current assessment is that physical, rather than cyber, terrorist attacks will remain the priority for terrorist groups for the immediate future.

Hacktivists

Hacktivist groups are decentralised and issue-orientated. They form and select their targets in response to perceived grievances, introducing a vigilante quality to many of their acts.

Digital Pirates

Although digital piracy may be related to, and result from, hacking activities, digital piracy is a form of Intellectual Property rights infringement involving the unauthorised copying, distribution and use of digital media such as commercial software, music and video materials. The pirates are those individuals who steal, replicate, distribute or even use the unauthorised media, regardless of their involvement in the theft itself.

3. Online Behaviour

The UK Intellectual Property Office (IPO) conducts ongoing research relating to copyright infringements, releasing their latest (7th) version of the *Online Copyright Infringement Tracker* in March 2017. The tracker outlines the findings of their large-scale consumer tracking study of online infringements as well as digital behaviours and attitudes of individuals aged 12 years old and above in the UK. Roughly 5,240 participants were assessed regarding their recent online behaviour and consumption of digital media.
An estimated 6,486,000 people in the UK ages 12 and over (roughly 15% of the UK population) infringed on the IP rights of copyright holders by consuming at least one item of illegal content.

(This report and the raw data captured to support it is readily available on the UK IPO page on the Government's Website: https://www.gov.uk/government/publications/online-copyright-infringement-tracker-survey-7th-wave)

Profile and behavioural trends of cybercriminals

From a demographic perspective, The UK IPO study indicated that those more likely to infringe were largely those under 35 years of age (68%), from the ABC1 group (62%), and marginally higher prevalence in males (54%). The study also outlined the findings relating to the reasons for infringing which were:

1. **Convenience**: Pirated media is easily accessible with little barriers to access;
2. **Cost**: Lack of cost involved as it is often free;
3. **Speed**: Pirated media is quick to attain

The above lends itself to a culture of immediate gratification and lack of perceived consequences.

When profiling IP Criminals we start to look to an ever-growing field of study which has emerged at the intersection of technology and psychology - Cyberpsychology. Thomas Holt wrote a chapter in a book on this topic, called Cybercrime and Deviance (2015). He asserts that there are two general behaviours relating to the misuse and abuse of computers and cyber technology namely cyber-deviance and cybercrime. Cyber-deviance relates to behaviours which might not necessarily be illegal in nature, but are contrary to social norms of acceptable behaviour. Cyber-deviance could be seen as a gateway behaviour into the second category, cybercrime. Cybercrime is defined as the status change from deviant into criminal behaviour when the offender's actions violate established legal statues.

Cybercriminals perform illegal behaviours in a digital/virtual environment, which Holt outlines have having three key attractions to offenders:

1. **Ease of access and user friendliness**: the tools and information needed to perform these behaviours and acts are readily available and accessible online.
2. **Anonymity:** the virtual environment allows the individuals to present whichever version of their identity (real or fabricated) that they wish, but it also allows them anonymity to hide their identity while performing illegal acts, which gives them the safety to be pro-risk with little chance of repercussions.

3. **Volume**: where real-world crime would generally have to be on a smaller scale, with victims being approached individually over a period, cyberspace allows for the targeting of, and access to, multiple victims at once. i.e. sending out mass malware or phishing emails

These enticing elements of the digital environment match the findings from the UK IPO study, which outlined that respondents indicated the aspects that would deter them from infringing include:

1. **Access and unavailability of content**: Respondents stated that if everything they wanted access too was available legally, they would be less likely to infringe or if a subscription service was available rather than large licences or initial costs.
2. **Cost**: If legitimate services were cheaper they would be less likely to infringe.
3. **Defined rules**: Respondents also cited that they would be less likely to infringe if there was clarity around what was legal and what was illegal.

The very nature of cybercrime and cyberspace make it difficult for victims to report the crimes, as there is little direction and support on how to report cybercrimes which take place on a global scale.

Thomas Holt and Adam Bossler collaborated on an article in the journal of Deviant Behaviour in 2014, which outlined predictors of digital piracy:

1. **Peer associations (social imitation)**: When infringers had peers, who engaged in digital piracy, they were more likely to engage in the behaviour themselves, due to both access to content through the peers, as well as positive reinforcement of the behaviour.
2. **Perception of a victimless crime**: Unlike hacking or deception, infringers would rationalise piracy as causing minimal to no injury to the copyright holders, as they would be none the wiser to the infringement. They perceive the act of piracy to cause no harm.
3. **Minimal Responsibility**: Infringers are more likely to pirate media when they have a sense of reduced responsibility for their downloading behaviours. This perception is created through a rationale that there are no clearly defined rules concerning digital piracy, and through the easy and immediate access to the material.

Holt and Bossler refer to the concept of low self-control as being a driving factor of these behaviours. What this means is that those who engage in digital piracy and related behaviours have little (or no) regard for user agreements associated with the media they are pirating, or the financial impacts on the copyright holder.

Dr. Mary Aiken is a world renowned Cyberpsychology, and author of the book “The Cyber Effect” (2017). The book outlines various aspects of cyber behaviour, also aligning it to deviant and criminal categories. On the topic of piracy, Aiken notes that criminologists recognise that an entry point to criminal activity is an ambivalence to the law. This real-world theory is mirrored in online criminal behaviour. Aiken also explains that the mindset behind digital IP theft is rationalised away by infringers by saying that unlike tangible theft which is a breach of law (taking something from a store), digital piracy is seen as intangible and therefore not real.

4. Attitudes towards IP cybercrime

Attitudes to IP crime vary greatly, not only between geographical locations but between cultures and generations as well. Until recently, Eastern approaches to IP rights was vastly different to that of Western nations. Where countries like China did not see copying of products or media as a criminal offence, the Western approach was to preserve and protect IP rights wherever possible. A study on the attitudes of Asian versus American students and their attitudes to digital piracy found that it is more widespread in Asia. This research by Szde Yu (2013) identified that neutralisation was more prevalent in the Asian student community than in the American student community, whereby they tended to consider it less of an offence since the wider community was doing the same thing. Alexander Bryan wrote an article in the Plymouth Law and Criminal Justice Review (2014) focused on the concept of neutralisation among British students in relation to digital piracy, and found that the common excuse of "everyone else is doing it" was at the forefront of the findings.

"intellectual property protection is one of the central public policy pillars on which the knowledge-based industries and global markets of the 21st century rest. Rapid changes in key technological, policy, and social drivers all underscore their growing importance." – OECD, Business and Industry Advisory Committee

The above quote is taken from an illicit trade course offered by the International IP Crime Investigators College, a division of Interpol. Throughout the course the importance of protecting IP rights is promoted as a key driver for innovation, production, and economic advancement on a global scale.

Moving away from a global divide, there is a difference of opinion in smaller community groups as well. Research indicates that the internet gives access to 'like-minded' people through online forums, social media, blogs, and peer-to-peer sites. Both hackers and digital pirates alike have various ways of justifying and normalizing their behavior in order to change their own perceptions about the criminality and illicit nature of their actions. In a research article into the subcultural evolution of deviant behavior (2007), Thomas Holt recounted an interview with a hacker he interviewed who explained that he and other hackers would spend time in forums sharing pirated software or tips on accessing it. The hacker went on to say that it was through these interactions that his lack of respect for software copyright emerged. Again, the theme of anonymity and ease of access are prevalent, which was the precursor to the follow up article by Hold and Bossler mentioned previously. Infringers have a sense of 'protection' due to the nature of the environment in which they operate. The inability to be easily identified, the difficulty in cross-border enforcement in the unlikely event that they were identified, the perceived lack of a victim, and the vast scope of cyberspace itself, creates a level of comfort and invisibility which makes online IP crime a difficult issue to approach.

5. Anti-piracy & licence compliance

Having understood the complexity of the challenges being faced by SMEs in terms of hacking and piracy, there are success stories in terms of protection and recovery.
From a digital piracy perspective, Anti-Piracy and Licence compliance techniques are fast evolving into a global solution.

Anti-Piracy refers to the approach taken by specialist firms, and in some cases software companies themselves, to identify infringers and build a case against them in order to enforce licence compliance. This is achieved through various approaches such as embedding phone-home software into their products which can notify the copyright holder when an unlicensed version of their product is being used. This approach actively seeks to address the infringer directly.

Other approaches include software which search the internet for mentions or obvious usage of the software in a pirated or cracked format.

Licence Compliance is the follow-on process to the above, which seeks to stop an infringer from continuing to use illegal versions of the product, comply with the legal licencing of the software and prevent the illegal version from being further distributed.

To date, specialist firms have recovered millions of Euros in lost revenue by enforcing licence compliance with digital media pirates.

The implications of digital piracy can often be far more serious than infringers may think. Firstly, cracked or duplicated software may not have quality controls in places to ensure that the software is fully operational or the correct version of the software. In instances such as 3D modelling software, this could result in catastrophic health and safety issues when it comes to designing machinery, buildings, medical equipment etc. Through using unofficial software packages, the end user is put in danger of unstable products.

Secondly, pirated media is often used to disseminate malware and viruses. When digital pirates replicate the media, they embed additional code which carries malware and viruses with it, and are installed on the user's device once downloaded. Malware can remain dormant on a system for extended periods of time and then be activated to gather personal and sensitive data, or allow hackers access to the user's system.

(Cracking down on digital piracy report 2017: https://www.fact-uk.org.uk/files/2017/09/Cracking-Down-on-Digital-Piracy-Report-Sept-2017.pdf)

(Example of work being performed in Wales: https://businessnewswales.com/cardiff-consultancy-recovers-20million-international-ip-theft/)

6. Implications for 3D printing

3D printing is still an emerging technology which is advancing continuously. Although more in-depth research still needs to be conducted into this topic, 3D printing has the potential of seeing a hybrid infringement of both physical counterfeiting and digital piracy come together.

Through digital platforms, hackers can gain access to and copy digital IP such as blueprints and instructions, transfer them via cyberspace from one country to the next, and use 3D printers to print out the product or item without any controls, regulations or border/customs oversight. Once printed, this unregulated product is then ready to be distributed to an unsuspecting consumer.

With the existing 3D printing technology currently available, scientists are able to print organs and medicines with molecular 3D printing, manufacturers able to print motorcar and aeroplane parts, weapons, and children's toys. All of which run the risk of going to market via pirated media and without the proper controls in place if appropriate measures are not taken.

Information and Resources

1. IP Wales: https://www.ipcybersecurity.com/
    a. SME Guide to Cyber Security: https://docs.wixstatic.com/ugd/67d7d9_493b309ebced48608ceede4563031a4b.pdf
2. UK IPO: https://www.gov.uk/government/organisations/intellectual-property-office
    a. Online Copyright Infringement Tracker Survey (7th wave): https://www.gov.uk/government/publications/online-copyright-infringement-tracker-survey-7th-wave
3. UK National Cyber Security Centre (NCSC): https://www.ncsc.gov.uk/
    a. The Cyber Threat to UK businesses 2017-2018 report: https://www.ncsc.gov.uk/cyberthreat
4. BSA – Software Alliance: http://www.bsa.org/
    a. 2016 Global Software Survey: http://www.bsa.org/~/media/Files/StudiesDownload/BSA_GSS_A4.pdf
5. Alliance for Intellectual Property: https://www.allianceforip.co.uk/
6. Federation Against Software Theft (FAST): https://www.fast.org/
7. Federation Against Copyright Theft (FACT): https://www.fact-uk.org.uk/

For additonal support and community engagement:

1. South Wales Cyber Cluster: https://southwalescyber.net/
2. The Global epic: https://globalepic.org/ece/index.php

Further Reading

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

Aiken, M (2017), *The Cyber Effect*

Bryan, A (2014), *Digital Piracy: Neutralising Piracy on the Digital Waves* in Plymouth Law and Criminal Justice Review

Holt, T (2001), *Cyber Crime and Deviance*, in *Cyberpsychology*, Attrill, A (2015)

Report of *The Commission on the Theft of American Intellectual Property* published May 2013 by The National Bureau of Asian Research.

UK Government *National Cybersecurity Strategy 2016-2021*

UK IPO *Online Copyright Infringement Tracker* 2017

Yu, S (2013), *Digital Piracy Justification* in International Criminal Justice Review

