Cyber security – a real world issue

Cyber security is now a Board level issue for many companies, and one that lawyers advising the Board must understand. But what is a cyber attack? Who are the cyber criminals? And what are businesses, and the Government, doing to protect against this increasing threat?

'Industrial espionage on an industrial scale'

Cyber security has recently attracted the attention of the world's governments and media alike. High-profile security breaches at brands such as Sony and Adobe have attracted global headlines, as have the Prism revelations and rising diplomatic tensions over alleged state-backed hacking.

Closer to home, the Director of GCHQ has declared that Britain is experiencing 'industrial espionage on an industrial scale', and UK Government statistics show that 93% of large corporations reported a cyber breach last year.[1]

Organisations are therefore becoming increasingly aware of the risks associated with cyber attacks. Cyber security is now a Board level issue for many, and one those advising the Board must understand.

In this article we go back to basics: what is a cyber attack, who are the cyber criminals and when are companies most at risk? We also look at some of the steps companies can take to protect against cyber threats and focus on recent guidance issued on "Cyber Security in Corporate Finance". Finally, we highlight what the UK and EU legislators are doing to try to tackle this 'Tier One' threat.[2]

Cyber attacks: what are they and who are the perpetrators?

The term 'cyber attack' is very broad. It is currently used to describe many different types of attacks on computers and computer-based equipment and information through the use of other computers – the aim being to compromise the integrity, availability or confidentiality of those computers, equipment and/or information.

The method of attack varies greatly, as does the source of the threat and the aims of the attacker. Common attacks range from denial of service attacks which target a website or server, to phishing and spear phishing attacks which target individuals (see the *Glossary* below for more information).

Cyber criminals come in many shapes and sizes. Some are financially motivated, while others have commercial, political, ideological or personal drivers.

1 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/191671/bis-13-p184es-2013-information-security-breaches-survey-executive-summary.pdf

2 The Government has categorised cyber attacks as a 'Tier One' threat to our national security, alongside international terrorism – https://www.gov.uk/government/publications/the-national-security-strategy-a-strong-britain-in-an-age-of-uncertainty

CYBER ATTACK: WHY, WHO AND WHAT?				
Why?	**Business** Aim: to profit from the attack		**Ideological** Aim: to cause disruption and/or harm	
Who?	**Financial** Criminals	**Commercial** Unscrupulous competitors Governments	**Political** Hacktivists Terrorists Governments	**Personal** Disgruntled employees Personal grudge Hackers
What?	Anything that can be sold or otherwise used to make money, such as: (i) commercial secrets that can be sold; (ii) personal secrets that can be used to blackmail; (iii) financial details (e.g. credit card details or bank account passwords); or (iv) information affecting the share price of a company	Commercial information or trade secrets that can be used by competitors or nation-states seeking advantages for state-sponsored industries Could include cutting edge IP, business/strategy plans, confidential negotiation positions, prices, customer details	Anything that can: (i) cause damage and/or disruption to a country's critical infrastructure, security or business interests; (ii) attract publicity or obtain information to support a political agenda (e.g. animal testing); or (iii) provide information on the activities of another state (government espionage)	Anything that can: (i) cause damage, destruction or embarrassment (e.g. damage to an individual, company profits or company reputation); or (ii) increase a hacker's reputation (e.g. some hackers gain notoriety from penetrating 'secure' systems). Young hackers (sometimes called 'script jockeys') can easily access 'hacking kits' online

When are companies most at risk?

While it may be difficult to predict if/when a company will suffer a cyber attack, certain factors can increase the risk, for example:

- *Operating in a high-risk sector*
  The UK Government has identified certain sectors that relate to the provision of 'essential services' as being particularly at risk from cyber attacks. An attack on an organisation in the health, energy, transport or finance sector could cause significant disruption to the country, making them ideal targets for a politically or ideologically motivated hacker. Similarly, at an EU level, the proposed Network and Information Security Directive (see *Upcoming EU legislation* in the *Legislation Tracker* below for further detail) identifies certain sectors as 'market operators' who would need to adopt risk management practices and report major security incidents.

- *Developing new products/technologies or focusing on R&D (e.g. pharmaceutical or manufacturing companies)*
  Intellectual property and information on new product or technology developments are extremely valuable company assets. By compromising a computer system or targeting a key employee to steal this information, an unscrupulous competitor can beat a rival to market or undercut the developer's price. Although for confidentiality reasons many of these attacks do not reach the public domain, there have been some published examples – for example an email-based cyber attack targeting a research director led to a biotech company having its research on a new pharmaceutical product stolen. This enabled a foreign competitor to release a cheaper product onto the UK market before the UK company, damaging the company's profits and ability to secure funding for further R&D.

- *Engaging in corporate finance transactions*
  When a company engages in a corporate finance transaction, such as M&A activity or a refinancing exercise, it is common for large amounts of important and highly sensitive information to be compiled and shared between multiple parties and advisers. This increases the risk of a cyber attack for the companies involved, along with their advisers, investors and/or financiers. In addition, the transaction itself may increase the cyber risk as a company may acquire a target which has already been compromised by a cyber attack, or which has weaker systems making it more vulnerable to attack. In our Cyber Security Focus below, we look at the recent "Cyber Security in Corporate Finance" guidance published by the Institute of Chartered Accountants in England and Wales, with support from the Government, and discuss some of the practical steps a company can take when undertaking a corporate finance transaction.

- *Dealing with state-related counterparts in jurisdictions with a higher incidence of cyber attacks*
  While commentators estimate that many states around the world are involved in cyber espionage, a number of countries (for example China and Russia) have attracted particular media attention for alleged hacking of (often Western) organisations. Unscrupulous competitors and nation states wishing to steal information or support state-backed organisations may use cyber attacks to obtain confidential plans, negotiation positions, trade secrets and/or intellectual property.

What can you do to reduce your risk?

Cyber attacks are increasing in terms of both volume and sophistication. It is therefore impossible to eradicate the risks. However, many online attacks can be detected or (ideally) prevented with basic security practices.

There are a number of practical steps you can take, and guidance you can follow, to help protect against cyber crime. This includes managing cyber risk within your corporate governance structure as a business rather than a technology risk – i.e. planning and management by the Board, with senior management leading implementation of an information risk management regime and reassurance through the corporate governance process.

Plan:

- Protecting your information is a Board responsibility: Government guidance[3] confirms that proactive management of the cyber risk at Board level is critical. But does the Board have the full picture? Have they identified and agreed what are the key information assets, the likely cyber risks and the company's appetite for risk? Do they understand the impact on the company's reputation, share price or ability to survive if: (i) sensitive internal or customer information were to be stolen or compromised; or (ii) your online services were to be disrupted for a sustained period? Also, has responsibility for the cyber risk been appropriately allocated (e.g. is it on the risk register) and is the Board kept up to date with developments (for example, does the CIO provide regular intelligence updates on the latest threats and methods of attack)?

- Is your business subject to any particular legal and/or compliance issues? The data protection regime requires that adequate security measures are in place whenever an organisation is dealing with personal data, and certain sectors (for example, the financial services sector) have additional regulatory requirements. Also, different jurisdictions may have different legal requirements around key security techniques such as encryption (for example, some states prohibit encryption unless the encryption keys are provided to certain authorities). Multiple jurisdictions can also complicate matters as conflicting laws and regulations may make it difficult for multinational organisations to plan a single international strategy.

- Have you considered how you would respond to an attack? Could you continue doing business? Would you need to notify anyone or obtain the help of any third parties? While good cyber hygiene practices will go a long way to protecting vital IT systems, they can never eradicate the problem altogether. An important part of effective cyber security is considering what should be done if there is a cyber attack.

Implement:

- Many organisations will already have some form of risk management regime. The first step is often therefore to ensure that this now also covers information and cyber risk. Once you have established an information risk management regime and defined your attitude and approach to risk management, it is important to communicate this throughout your organisation.

- Do you have appropriate security policies and controls in place to protect your IT systems, equipment and information? The Government has produced guidance ("10 Steps to Cyber Security"[4]) on some of the measures organisations should take into account, from home and mobile working, to network security and user education and awareness. Educating staff is particularly important: users are often the weakest link in the security chain and targeting an employee (for example, encouraging them to open an email with malicious content) can be cheaper and more effective than mounting a technical attack.

- As many organisations now have complex technology supply chains, or outsource their IT arrangements, any policies and controls should also cover these supply arrangements. You may also want to review these contracts to see what contractual obligations and security provisions the suppliers have in place, and whether any amendments are required.

- Are you engaging in regular information sharing with other companies in your sector, regulators and (where appropriate) the relevant authorities? By encouraging technical staff to share information with other companies in your sector, you can learn from others, benchmark and help identify emerging threats. Also, one

[3] See our List of Useful Resources section of the Focus (below) for more information on guidance for Boards and small businesses
[4] See our List of Useful Resources section of the Focus (below) for more information

of the central elements of Government guidance and upcoming EU legislation is to encourage greater co-operation and information sharing between companies (particularly the essential services), their regulators and the relevant authorities.

- Do you follow best practice when disposing of IT assets? Basic IT security and data protection compliance recognises that it can be hard to completely remove information from IT assets that are no longer required, and the Information Commissioner (the UK's data protection regulator) has published guidance on this from a data protection angle.

- Does your incident management plan include provisions on what to do if you do suffer an attack? For example, it should consider issues such as containment of the attack (e.g. through network isolation), your PR response if the attack enters the public domain, your communications protocol (knowing your systems may be compromised, how will you communicate internally regarding any investigation?), notification of enforcement authorities and interested parties, protection of intellectual property and the appropriate steps to resume business as usual (including how disaster recovery plans can provide emergency IT provisions where necessary). You should not only consider the immediate impact that a cyber attack will have on your ability to run your business, but also the effect on your share price and longer-term reputation.

- Given that some cyber attacks may lead to litigation or regulatory investigations, any plans should also consider how to maintain privilege in relation to appropriate documentation when carrying out an investigation into the attack.

Review:

- It is important to review and test the effectiveness of your controls. Many companies engage in regular penetration testing of their IT systems. Technical staff should also regularly monitor and review network and system logs for indicators of suspicious activity. Larger companies in key sectors have engaged in sector wide cyber security war games. Recently, the financial sector organised a day-long simulated attack on its systems in London (dubbed 'Waking Shark II') following a similar test undertaken in 2012 to assess vulnerabilities to cyber attacks during the Olympics. The findings were published earlier this year (5 February 2014) and highlight a number of areas for improvement.[5] The Government, in a recent communiqué from an event entitled 'Strengthening the cyber security of our essential services', has indicated that it intends to work with partners to deliver and participate in similar programmes for companies who are in the essential services sector.[6]

- Are you keeping abreast of the latest developments? More importantly, are you acting on any information you receive, whether on emerging threats or weaknesses in your controls? Cyber security is a developing area of law and a burgeoning industry in its own right. New tools are continually becoming available and new guidance is regularly published. For example, last November the Government concluded a consultation on organisational standards in cyber security, which led to them working with industry to create a new standard on basic cyber hygiene and publishing the Cyber Essentials Scheme on 7 April 2014[7]. At a European level, the proposed Network and Information Security Directive will particularly affect organisations operating in certain critical sectors (see *Upcoming EU legislation* in the *Legislation Tracker* below for further detail) and so it is important that organisations in those sectors prepare for this additional regulation.

5 http://www.bankofengland.co.uk/financialstability/fsc/Documents/wakingshark2report.pdf
6 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/277525/Communique_-_SoR_FINAL_v1_FEB_2014.pdf
7 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/262114/bis-13-1308-call-for-evidence-on-preferred-standard-in-cyber-security-response.pdf and https://www.gov.uk/government/publications/cyber-essentials-scheme-overview – see also Upcoming UK legislation in the Legislation Tracker below for further detail

- If you do suffer a cyber attack, will you learn from the experience? For example, will you ensure your response includes the removal of any ongoing threat (e.g. removing malware), addressing any security gaps identified by the attack and understanding the cause?

'Put cyber crime on the agenda, before it becomes the agenda'[8]

A successful cyber attack could destroy a company's reputation or financial standing. While the majority of cyber attacks will not make the headlines, and some go completely undetected, the threat is growing in terms of both size and sophistication. Lawyers, and the Boards they advise, should therefore take the cyber threats facing them seriously and ensure that their organisations adopt a corporate governance framework that prioritises cyber security and can be modified to meet the ever-changing threat. On a more personal note, many cyber attacks target key people within an organisation and it is therefore equally important that senior executives and the in-house legal teams who advise them understand that, as guardians of the most sensitive corporate information, they themselves are often the focus of the cyber criminal. Ultimately, both corporate and personal vigilance is required to combat the growing cyber threat.

This article was written by Rob Sumroy, Natalie Donovan and Richard McDonnell. Rob is a partner, and Natalie and Richard are lawyers, in the Technology Group at Slaughter and May.

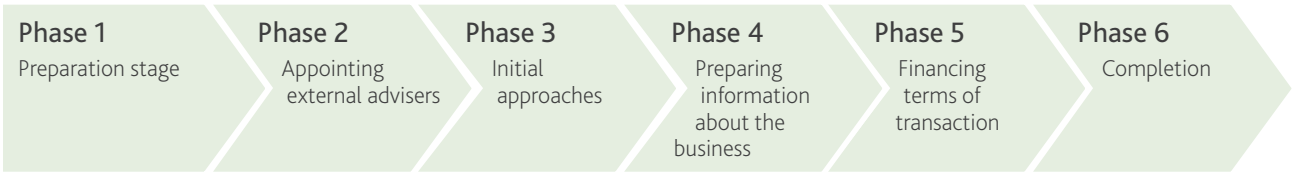
[8] 10 Steps to Cyber Security – page 5

FOCUS: CYBER SECURITY IN CORPORATE FINANCE

Corporate finance transactions are a key part of the business world, and are vital to the wider economy. However, engaging in a corporate finance transaction, whether you are refinancing an existing facility, or acquiring a new company, could make your business more susceptible to a cyber attack. In this *Focus* section we look at the risks involved in the different stages of a corporate finance transaction, and some of the actions that can be taken to help mitigate those risks. In particular, we look at the recent guidance published by the Institute of Chartered Accountants in England and Wales together with the Government and a number of other business organisations on "Cyber Security in Corporate Finance"[9] (the 'Guidance'). The Guidance aims to raise awareness of the issues involved and help organisations take the appropriate steps to manage cyber risk as a strategic business, rather than a purely technology, issue.

Why the increased risk?

Corporate finance activity involves multiple parties and the collection and sharing of large volumes of commercially sensitive information. This creates a heightened cyber risk at each phase of the transaction and the Guidance identifies six phases:



For example, at the preparation stage of a business sale/purchase (Phase 1 of the six phases identified above) there is the risk of alerting outsiders to the fact that a transaction may be imminent, while in the latter stages the confidential information compiled and shared as part of the planning and due diligence stages may become the target, along with the negotiation strategies or bid prices of competing bidders. The completion stage itself may also attract attention, as funds are transferred (with the risk of interception) and confidential plans about future strategies are likely to be in place (e.g. potential synergies with the newly acquired business, plans to expand into new markets, or details of how the business will be separated from its previous group). Even following completion, the transaction may still introduce new risks into an organisation, for example newly acquired IT assets may have already been compromised, introducing a weakness into a previously secure system.

[9] http://www.icaew.com/~/media/Files/Technical/Corporate-finance/Corporate-finance-faculty/tecpln12526-cyber-web.pdf

FOCUS: CYBER SECURITY IN CORPORATE FINANCE

What can you do to manage the risk?

The Guidance discusses the risks, questions to ask and possible actions an organisation can take at each phase of the corporate finance transaction. Some common themes which emerge include:

Information controls	Risk analysis and information gathering	Additional protections
Share information on a need--to-know basis only – do not provide more information than is necessary to more people than is necessary (operate 'need to know' lists) Keep teams small – for example only a limited number of people need to be involved at Phase 1 Implement procedures to track information flows Hold back particularly sensitive information until later in the transaction Appoint someone to be responsible for looking after information flows/information security in your organisation	Understand your risk profile at each phase – is there anything about the deal that increases the risk (sector, jurisdiction, additional regulatory obligations etc.)? Has the risk profile changed? Identify which information is particularly sensitive If receiving information, ask the party providing it to identify which information is particularly sensitive Use any expertise you have within the organisation – e.g. do you have a security expert who could provide additional help? Ask other parties involved to divulge any increased risks of which they may be aware Include cyber security questions (such as asking what standards the other parties comply with) in the due diligence process Consider/plan what would happen at each stage if a cyber attack were to occur	Ensure people within your team are cyber aware (e.g. do they know to use social media carefully) and understand any deal-specific risks Check you have sufficient measures and procedures in place Consider whether separate IT systems and people may be required where the transaction is particularly sensitive, and check the security credentials of the parties involved (including advisers and data room providers) Monitor access to information and treat particularly sensitive information differently (e.g. more restrictive access, keep information off-line) Ensure appropriate confidentiality and information sharing/use contracts are in place Seek cyber security assurances as part of the due diligence and warranty process Check any systems/assets acquired during the transaction are not already compromised and update your policies and procedures if required

While it is important that both parties keep information secure, each party will also have its own particular priorities. Buyers will want to carry out sufficient due diligence on the cyber threat of any potential target, while sellers will want to ensure that the value of that target is not compromised by any cyber threat or incident. The Guidance therefore highlights how important it is for all organisations involved to build the issue of 'cyber security' into their transaction processes. It is also an indication of how the 'cyber risk' is moving up the UK's corporate finance risk agenda, following countries like the US where the SEC's Division of Corporation Finance published guidance in October 2011 indicating the importance, in its view, of disclosure obligations relating to cyber security risks and cyber incidents.[10] Finally, it is a reminder more generally that "all businesses involved in corporate finance need therefore to be aware of these cyber risks, and of what they can do to help protect their data, their clients and their reputation."[11]

LIST OF USEFUL RESOURCES

Resource Title and Date	Aim
Guidance: Cyber Risk Management – a Board Level Responsibility https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/34593/12-1119-cyber-risk-management-board-responsibility.pdf 5 September 2012	Contains key questions for CEOs and Boards as well as those advising them
Guidance: 10 Steps to Cyber Security https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility 5 September 2012	Contains cyber security information and advice for 10 critical areas (including home and mobile working, network security and incident management), covering both technical and process/cultural areas
Guidance: Small Business Cyber Security Guidance https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/34593/12-1119-cyber-risk-management-board-responsibility.pdf 23 April 2013	Straightforward guidance for small businesses to improve their cyber hygiene
Guidance: Cyber Streetwise Campaign https://www.cyberstreetwise.com/ 13 January 2014	Campaign aimed at individuals that encourages the following cyber behaviours: (i) using strong, memorable passwords; (ii) installing anti-virus software; (iii) downloading patches when prompted; (iv) using privacy settings on social media; and (v) shopping safely online
Guidance: Cyber Security in Corporate Finance http://www.icaew.com/~/media/Files/Technical/Corporate-finance/Corporate-finance-faculty/tecpln12526-cyber-web.pdf 16 January 2014	Aims to raise awareness of the cyber risks and issues involved in the different phases of various corporate finance transactions, and help organisations take the appropriate steps to manage the cyber risk

[10] see http://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm

[11] David Willetts, Minister of State for Universities and Science: Cyber Security in Corporate Finance foreword.

LEGISLATION TRACKER

Cyber security is a hot topic for legislators in both London and Brussels. Although existing legislation on areas such as data protection and computer misuse touch on cyber security, the general consensus seems to be that more specific regulation is required. Set out below are some of the particular initiatives that are currently under way:

CURRENT POLICIES AND LEGISLATION

Name and date of legislation	Aim
UK	
Government policy: Keeping the UK safe in cyberspace 25 November 2011	To prevent cyber crime and make the UK a safer place to do business, the Government's Strategic Defence and Security Review has allocated £650 million over four years to establish a new National Cyber Security Programme to: (i) set up a National Cyber Crime Unit (bringing together the Police eCrime Unit and SOCA); (ii) provide advice to businesses; (iii) build a cyber information sharing partnership with business to allow the Government and industry to exchange information on cyber threats in a trusted environment; (iv) create a joint Cyber Growth Partnership with Intellect (the technology industry body) to increase understanding of the UK cyber security issue; and (v) introduce "Action Fraud", a single 24/7 reporting system for financially motivated cyber crime, which forms part of the police
EU	
Cyber security strategy 7 February 2013	The strategy sets out five priorities: (i) achieving cyber resilience; (ii) drastically reducing cyber crime; (iii) developing cyber defence policy and capabilities related to the Common Security and Defence Policy; (iv) developing industrial and technological resources for cyber security; and (v) establishing a coherent international cyberspace policy for the European Union and promoting core EU values
Regulation (EC) No 526/2013 concerning the European Union Agency for Network and Information Security ("ENISA") 21 May 2013	The Regulation extends the mandate of ENISA for a further seven years. ENISA oversees the promotion of network and information security and is the hub for businesses to share best practices and information on cyber threats with others in their sector across the EU
Cybercrime Directive 12 August 2013, due to be implemented into national law by 4 September 2015	The Directive establishes minimum criminal offences and sanctions for cyber attacks. Companies should make employees aware of the scope of the offences as well as considering their own liability for their employees' actions

LEGISLATION TRACKER

UPCOMING LEGISLATION

Name and date of legislation	Aim
UK	
ISO Standard Consultation The results of the consultation were released on 28 November 2013. On 7 April 2014 the Government published the Cyber Essentials scheme. The full scheme is due to be launched in summer 2014	The Government decided that as current standards did not fully meet the requirements of participants, they would draw up a new standard, based on the ISO27000-series and focusing on basic cyber hygiene. The aim was that businesses across all sectors adopt the recommendations, enabling them to deal with low-level cyber attacks The Cyber Essentials scheme includes a requirements document that organisations can implement and self assess against, and a draft assurance framework for the scheme (for which feedback has been requested). The assurance framework will enable organisations to be independently assessed and obtain a Cyber Essentials certification badge when fully launched
EU	
Network and information security Directive Proposal going through the EU legislative process with amendments currently being discussed by Parliament. The Commission hopes that the Directive will be adopted by the end of 2014	The current amended proposal of the Directive provides for: (i) national competent authorities and a single point of contact to be set up in each Member State to prevent, handle and respond to network and information security risks and incidents (the UK launched its national competent authority, CERT-UK, on 31 March 2014); (ii) a mandatory co-operation mechanism for cyber security information between Member States; (iii) private organisations in critical areas (health, energy, transport, finance, internet exchange points and food supply chains) to adopt risk management practices (which can differ depending on the significance of the organisation) and report major security incidents where the disruption is to network information systems related to that organisation's core services and such disruption would have a significant impact in a Member State as a result of the failure of that organisation to maintain its functions; and (iv) Member States to encourage the use of certain European and international interoperable standards and specifications relevant to network and information security, to be determined by a European standardisation body (see the UK *ISO Standard Consultation* above)

GLOSSARY

Below is a glossary of some of the terms used when describing the more common methods of attack.

See European CSIRT Network Project taxonomy and GovCertUK Incident Response Guidelines for more information.

Name	What it does
General	
Botnets (or zombie armies)	A network of infected computers, which are individually known as zombies (or bots), that can be remotely controlled to perform automated tasks over the internet. Hackers use botnets to launch synchronised attacks, such as DDOS, spam or phishing attacks
Hacking	The unauthorised access to or use of computers and networks, exploiting security vulnerabilities to do so
Availability Attack	
Denial of Service (DOS)	This type of attack aims to flood a server with excessive packets, causing the targeted system to overload and resulting in the failure of particular network services (for example email) or a loss of network functionality, which could lead to a website becoming inaccessible. This attack is normally used to degrade web-based services (whether static, dynamic or transactional) with the intention of causing reputational damage to the organisation or individual or loss of online revenue
Distributed Denial of Service (DDOS)	Instead of one computer and one internet connection, as is used in a DOS attack above, a DDOS attack relies on botnets, which can be located all around the world, to launch the attack
Information Gathering	
Pharming	Software installed in a system redirects people attempting to access a genuine website to a bogus site
Phishing	Numerous generic emails are sent to people, often posing as being from a trusted entity or promising a reward, to elicit the disclosure of that individual's personal information (e.g. financial details, passwords etc.) or to install malware
Scanning	Attacks that send requests to a system to discover weak points. This also includes some kinds of testing processes to gather information about hosts, services and accounts
Spear Phishing	A more targeted approach to phishing, where attackers may gather information about the target company/individual and will use that information to tailor the phishing email (known as social engineering) to specific individuals making it appear more legitimate

GLOSSARY

Name	What it does
Malicious Code (or Malware)	
Malicious Code (Malware)	Software that is intentionally included or inserted in a system for a harmful purpose. A user interaction is normally necessary to activate the code, e.g. clicking on a link or an attachment
Spyware	Malware that gathers an individual's sensitive or personal information without their knowledge, which can then be passed on to third parties. Examples of spyware include key-logging software and software that captures screenshots of the victim's computer
Trojan Horses	Malware that appears to be legitimate programs, but allows a computer to be accessed illegally, or may perform malicious unseen functions such as data theft. They may appear to be carrying out a routine job while actually undertaking concealed, unauthorised tasks
Viruses	Malware that can cause minor computer dysfunction, or may have more serious effects, such as damaging or deleting items on a computer. The programs self-replicate, and spread within and between computers. They need to attach themselves to an existing program in a computer that acts as a 'carrier'. They cannot infect a computer without a human action, such as running or opening the infected file
Watering Hole	A website that has been compromised with the intention to serve malicious code to specific and likely unknown IP addresses with the effect of compromising specific targets of interest
Worms	Another type of malware. Also self-replicating, worms can spread on their own, within and between computers, without needing a host or human action. Even at a minimum they can use up bandwidth, and may be used to allow the creation of a zombie for use in a botnet. They can also be used to place Trojans on the network
Fraud	
Unauthorised use of Resources	Using resources for unauthorised purposes including profit-making ventures (e.g. the use of email to participate in illegal profit chain letters or pyramid schemes)
Spoofing	Types of attacks in which one entity illegitimately assumes the identity of another in order to benefit from it

CYBER SECURITY AT SLAUGHTER AND MAY

Through the joint working of its Technology and Corporate Groups, Slaughter and May helps its clients to manage their 'cyber risks' within their corporate governance structures. This includes assisting with proactive planning, implementation of an information risk management regime and reassurance through corporate governance processes. For more information, please contact:

ROB SUMROY
T +44 (0)20 7090 4032
E rob.sumroy@slaughterandmay.com

FRANCES MURPHY
T +44 (0)20 7090 3158
E frances.murphy@slaughterandmay.com