Client Alert

15 August 2013

Beware the Botnets: Cyber-Security is a Board Level Issue

By Sue McLean

Today, you would be hard pressed to find an organisation that does not use IT systems and the internet to conduct its business. While technology offers great benefits, it also brings risk. As technology becomes ever more complex, the scope and scale of cyber-risks is increasing at an unprecedented rate. Because responsibility to manage cyber-risks rests with each organisation, it needs to be high on each board's agenda. It's clear that this is no longer just an issue for the IT department.

Governments around the world are trying to educate businesses about the risk of cyber-crime, while at the same time equipping law enforcement authorities with the tools to prosecute offenders. The EU in particular is seeking to take a lead in efforts to raise the bar in cyber-crime prevention and enforcement and the UK has identified cyber-crime as a 'Tier 1' threat to national security alongside terrorism.

Although it will never be possible for cyber-risks to be eradicated entirely, there are many steps that companies can take to address and mitigate cyber-risks and to respond appropriately when an attack occurs. But evidence suggests that many companies are still not putting in place adequate measures to address cyber-security. According to the UK government, "*about 80% of known attacks would be defeated by embedding basic information security practices for your people, processes and technology*". Indeed, KPMG recently announced that it had been able to collect employee user names, email addresses and sensitive internal file location information about every UK FTSE 350 company using data publicly available on the internet. This kind of data could be used to carry out fraud or obtain companies' intellectual property. The research also indicated that more than half of the FTSE 350 companies demonstrated potential vulnerabilities to attack because they did not have up-to-date security patches and/or were using old server software. As the Director of GCHQ (the UK's communications intelligence agency) said in guidance published last year, "*Value, Revenue and Credibility are at stake. Don't let cyber security become the agenda – put it on the agenda.*"

BACKGROUND

Cyber-attacks can be conducted using a variety of different methods and technologies, including botnets, denial of service attacks, spamming, pharming, spoofing, malware (*e.g.*, viruses, worms, Trojan horses, *etc.*), phishing, and ID theft.

Such attacks may be instigated by a wide variety of players for different reasons (*e.g.,* employees accidentally, through negligence or maliciously, competitors conducting industrial espionage, sabotage or intellectual property theft, state sponsored actors such as foreign intelligence services, organized crime gangs, terrorists, cyber criminals intent on fraud and hackers and hacktivists, *etc.*).

Cyber incidents can be caused by a variety of factors including vulnerable IT systems and networks, insecure email, lost and stolen devices, social engineering, *etc*. The inside factor cannot be underestimated. According to Symantec's recent annual Cost of a Data Breach Report, employee actions and system errors were the cause of nearly two thirds of all data security breaches.

Cyber incidents can result in damage to infrastructure, downtime and business interruption, loss of commercially sensitive data, theft of intellectual property, fraud and liability to third parties. Accordingly, the potential harm that can be caused to businesses by cyber incidents is substantial and may include:

- financial losses (*e.g.*, loss of money, the cost of remediating and rectifying damage, impact on share value, loss of revenue, *etc.*);
- reputational damage (damage to brand, loss of trust with customers, *etc.*);
- damage to business interests (*e.g.,* loss of business/clients, impact on potential merger/corporate transaction, reduced competitive advantage, *etc.*);
- legal and regulatory penalties (*e.g.,* fines, *etc.*); and
- compensation to affected third parties.

LATEST DEVELOPMENTS: UK

Cyber-security is high on the UK government's agenda. A Cyber Security Strategy was published in November 2011 and various initiatives have since been launched to deal with the issue. Latest developments include the following.

- In September 2012, the UK government published cyber-security guidance for UK businesses explaining what cyber-risks are and providing a 10-step plan for the management of cyber-risks. However, according to a recent survey, although almost all of the companies surveyed thought that their company's specific exposure to cyber risk was increasing, almost 50% of company boards had not discussed this guidance and 28% of boards had not even seen it.
- In March 2013, the government launched the Cyber Security Information Sharing Partnership (CSIP) to help government and industry share information and intelligence on cyber security threats. The kind of information to be shared includes technical details of an attack, methods used in planning an attack and how to mitigate and deal with an attack. The initiative will initially involve 160 private sector organisations.
- In April 2013, the government published further guidance on cyber security specifically for small businesses.
- In April 2013, the government published its detailed 2013 Information Security Breaches Survey. The survey identified that 93% of large organisations and 87% of small businesses had experienced at least one security breach in 2012. This was an increase of roughly 50% on 2011 figures. The average worst security breach cost large organisations between £450,000 and £850,000 and small businesses £35,000 to £65,000. 81% of respondents briefed their board or senior management on cyber-risk, but the frequency of such briefings varied considerably.
- In May 2013, the government published guidance outlining the required criteria for a cyber-security standard for companies. Businesses have until 14 October 2013 to submit views.

- It has been recently reported that the UK's intelligence agencies MI5 and GCHQ have written to FTSE 350 companies urging them to carry out cyber-security health checks. The companies have been asked to complete a questionnaire identifying how they protect intellectual property and customer data. The data will then be aggregated anonymously to enable companies to see how they rank compared with their peers. The companies will then be contacted to discuss where the company may be vulnerable under a second stage of the initiative.

Other industry-specific initiatives have been launched. For example, in February 2013 it was reported in the UK parliament that the Financial Services Authority (the UK's financial regulator prior its replacement by the FCA and PRA in April 2013) is reviewing the cyber practices of 30 major financial institutions. When the review is concluded, the regulator intends to publish an updated version of its Business Continuity Management Practice Guide and a discussion paper.

LATEST DEVELOPMENTS: EUROPE

Pursuant to the EU's cyber-security strategy, in June 2013 the EU's cyber-security agency ENISA was formally granted a seven-year mandate with an expanded set of duties and in July 2013 the Cyber-Crime Directive was adopted. In addition, the draft Network and Information Security Directive and the draft Data Protection Regulation continues to make progress through the legislative process.

Cyber-Crime Directive

On July 11, 2013, the Foreign Affairs Council of the European Union and the European Parliament reached agreement on the final text of the Directive on attacks against information systems (otherwise known as the "Cybercrime Directive") and, on July 22, the Directive was formally adopted by the Council. The Directive builds on rules contained in the previous Framework Decision 2005/222/JHA on attacks against information systems.

The new Directive aims to tackle the increasingly sophisticated and large-scale forms of attacks on information systems (including increased use of botnets) that have emerged since the Framework Decision and is intended to enlarge the scope of criminal offences, increase the level of sanctions and provide a reinforced framework for cooperation between the relevant EU agencies and bodies, such as Eurojust, Europol, the European Cybercrime Centre, and the European Network and Information Security Agency (ENISA).

Following the Directive's publication in the Official Journal, EU member states will have two years to implement the Directive into national law (except for Denmark, which has decided to opt out of the Directive.) Although the Directive has been broadly welcomed, commentators have noted that tracking down the perpetrators of cyber-crime will remain a huge challenge for authorities.

The Directive establishes the following criminal offences, where committed intentionally and without authorization or otherwise permitted by law:

- *Illegal access to information systems*: it will be an offence to access the whole or part of any information system by infringing a security measure.
- *Illegal system interference*: it will be an offence to seriously hinder or interrupt the function of an information system inputting computer data, by transmitting, damaging, deleting, deteriorating, altering or suppressing such data, or by rendering such data inaccessible. It will also be an offence to attempt to commit this offence.

- *Illegal data interference*: it will be an offence to delete, damage, deteriorate, alter or suppress computer data on an information system, or render such data inaccessible. It will also be an offence to attempt to commit this offence.
- *Illegal interception*: it will be an offence to intercept, by technical means, non-public transmissions of computer data to, from or within an information system, including electromagnetic emissions from an information system carrying such computer data.

It will also be an offence to intentionally produce, sell, procure for use, import, distribute or otherwise make available: (i) a computer program designed or adapted primarily for the purpose of committing an offence or (ii) a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed ("prohibited tool"), without authorization or otherwise permitted by law and with the intention that such tool be used to commit one of the offences. In addition to penalizing commission of the offences, it will be an offence to incite, or aid and abet, another to commit any of the offences. The offences only apply in 'cases that are not minor'. Member States will have the freedom to define what constitutes a minor case (but could include, for example, where the damage caused, or risk to legal interests, is insignificant or is of such a nature that the imposition of a criminal penalty or liability is not necessary, *e.g.,* the activities of 'ethical hackers', *etc*.).

Note that the Directive does not impose criminal liability where the acts are committed without criminal intent (*e.g.,* where the person does not know that access is unauthorized or where a person is engaged by an organisation to carry out penetration testing, *etc*.). Also, if a user breaches Terms of Use or an employee breaches a user security policy although this may be considered unauthorized access, this would not attract criminal liability under the Directive (although may be caught by other national law).

The Directive increases the level of criminal penalties to a maximum term of imprisonment of at least two years.

In addition, when committed intentionally, the illegal system and illegal data interference offences will be subject to a maximum term of imprisonment of: (i) at least three years, where a significant number of information systems have been affected through the use of a prohibited tool that was designed or adapted primarily for that purpose; or (ii) at least five years, where the offence is committed within the framework of a criminal organisation, causes serious damage, or is committed against critical infrastructure. Also, where these offences are committed using an innocent party's personal data this may be regarded as aggravating circumstances.

As we mentioned above, companies may perpetrate cyber-attacks for the purpose of corporate espionage or sabotage or intellectual property theft and the Directive addresses this issue by introducing liability for legal persons. Organisations can be criminally held liable for a cyber-crime offence if: (a) the offence is committed for the organisation's benefit by any person having a leading position within the organisation; and/or (ii) the lack of supervision or control of a person allows the commission, by a person under the organisation's authority, of the offence for the benefit of that organisation.

The Directive requires that sanctions for organisations should include fines and may include other sanctions, such as: (i) exclusion from entitlement to public benefits or aid, (ii) temporary or permanent disqualification from the practice of commercial activities; (iii) placing under judicial supervision, (iv) judicial winding-up; and (v) temporary

or permanent closure of establishments which have been used for committing the offence.

Update on the Network and Information Security Directive

As we reported in February, a draft EU Directive on network and information security has been introduced that would require a range of organisations that provide critical infrastructure (including key internet enablers and financial institutions) to meet certain security measures in relation to their IT systems and notify regulators of any significant cyber breaches. The draft Directive is currently being scrutinised by EU Member States. The UK government ran a consultation on the draft Directive between 22 May 2013 and 21 June 2013 and will publish its report on the consultation in due course. On 4 July 2013, the UK's privacy regulator, the ICO, published its response to the Directive. The ICO broadly welcomes the objectives of the Directive, but raises a number of concerns. In particular, the ICO makes clear that: (i) it does not wish to take on responsibility for security breaches which do not involve personal data, (ii) it would like to see the removal or minimisation of any personal data disclosed as part of a breach notification, and (iii) it considers the proposals relating to sharing information on risks and incidents to be too vague. The European Parliament is expected to begin consideration of the draft Directive in February 2014.

Update on the Data Protection Regulation

Data breaches remain a key cyber-security risk. In the UK, for example, data security breaches account for the vast majority of all enforcement actions brought by the ICO, the UK's privacy regulator. Currently, within the EU, except for personal data breaches involving telcos and ISPs, personal data breach reporting is not generally mandatory[1]. However, with the introduction of the Data Protection Regulation, that is set to change. As we have reported previously, the draft Data Protection Regulation, which is intended to replace the existing Data Protection Directive (95/46/EC), introduces broad personal data breach notification requirements. Authorities must be notified without undue delay within 24 hours of the controller becoming aware of the breach. In addition, following notification to the authorities, affected individuals must be notified without undue delay (unless the controller can demonstrate that it applied appropriate measures to protect the data).

Since its publication the draft Regulation has been the subject of extensive negotiations and on 31 May 2013, the Council of the European Union released a draft compromise text. The compromise outlines a more relaxed data breach notification regime, increasing the time period from 24 to 72 hours and requiring only significant breaches resulting in severe material or moral harm to be notified. The European Parliament and Council of the European Union are expected to begin negotiations on the final text of the Regulation in September 2013.

MANAGING CYBER-RISKS

In order to deal with cyber-risks, organisations need to put in place a multi-layered strategy that covers prevention, mitigation and reaction and that takes a holistic approach, focusing on people, processes and systems. Organisations should consider the following best practice steps.

[1] See our article Dealing with Data Breaches in Europe and Beyond for more details.

- Treat cyber-risks as strategic business risks as opposed to purely IT risks and consider what level of risk the organisation is prepared to accept.
- Ensure that you have board and senior stakeholder ownership of the cyber-security strategy. To help non-technical management understand the extent and nature of the potential cyber-security risks, create cyber-security risk metrics and communications that can be easily understood (*i.e.,* avoid technical jargon wherever possible).
- Carry out a thorough risk assessment across the whole business (don't just focus on the IT department) - identify the company's key information assets and services, assess their vulnerability to attack and from whom and consider the potential impact if an incident took place. People are often the weakest link, so consider the risks posed by suppliers, employees and other users, in addition to technical risks.
- Ensure that you understand your legal and regulatory obligations (and recourse) with respect to cyber-attacks. Become familiar with any available government, regulatory and industry guidance.
- Establish a governance framework that enables and supports cyber-security management across the organisation.
- Allocate responsibility for cyber-risks appropriately. Use risk registers and other tools to document and monitor risks.
- Consider working with third parties (including other companies in your sector) in order to benchmark, learn from others and help identify emerging threats.
- In terms of employees and other users:
    - implement clear security policies and procedures (including in respect of new technologies and practices which can compound security risks *e.g.*, BYOD[2], social media, *etc.*);
    - promote a risk management and incident reporting culture and carry out regularly training to educate users as to the possible security risks and the importance of compliance with your security policies and procedures;
    - carry out appropriate background checks and ensure that third party providers do the same;
    - carry out effective privilege management to ensure that users only have access to the files, systems and data that they need; and
    - monitor compliance with security policies and procedures and investigate and consider disciplinary action in respect of abuse.
- In terms of users of websites, mobile apps and social media networks, *etc.*, put in place appropriate terms of use, security policies, takedown procedures, *etc.*
- Ensure that security is carefully considered when designing, developing and implementing all IT systems. Implement appropriate malware protection software, ensure that security patches are implemented, ensure secure configurations for all IT equipment and disable unnecessary devices and removable media access. (With systems becoming increasingly complex vulnerabilities are becoming more difficult to identify. New

[2] See our previous Alert on Bring Your Own Device Challenges for more details.

technology leads to new types of risks. For example, companies must not overlook mobile apps – it has been reported that many apps are currently unprotected against reverse engineering and tampering attacks. And commentators have also acknowledged the potential for security risks posed by disruptive technologies such as the 'Internet of things' and 'Big Data').

- Keep up-to-date and meet good industry practice and recognized standards in terms of security management (*e.g.*, BSI's PASS 555:2013 which was published in May 2013, ISO/IEC 27001, *etc*. Note that ISO/IEC 27001 is currently being revised and is due to be formally published in November 2013. It is expected to include a requirement for senior management commitment).
- Put in place appropriate disaster recovery and business continuity procedures and test those procedures regularly. Ensure that those procedures include clear cyber-security incident response plans covering all appropriate steps (including notification to regulators where required, managing media and communications, *etc*.).
- Carry out regular monitoring and conduct regular security audits, risk assessments and testing (including penetration testing).
- Check insurance cover and, where appropriate, put in place specific insurance to cover cyber-risks. (Earlier this year, Marsh reported that the number of clients purchasing cyber insurance policies increased by 33% from 2011 to 2012 and also that those companies buying cyber insurance are buying higher limits of cover.)
- Put in place appropriate security measures with all relevant third party providers of goods and services, including appropriate contractual provisions dealing with all relevant aspects of security. Check existing contracts and amend where appropriate to ensure that it is clear what your rights and remedies will be if security requirements are breached (including in terms of notification, indemnification and liability, audit, step-in rights, termination, *etc*.). Note that certain types of services (*e.g.*, cloud computing) may raise particular security concerns that will need to be addressed.

Contact:

Sue McLean
44 20 7920 4045
smclean@mofo.com

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 10 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.