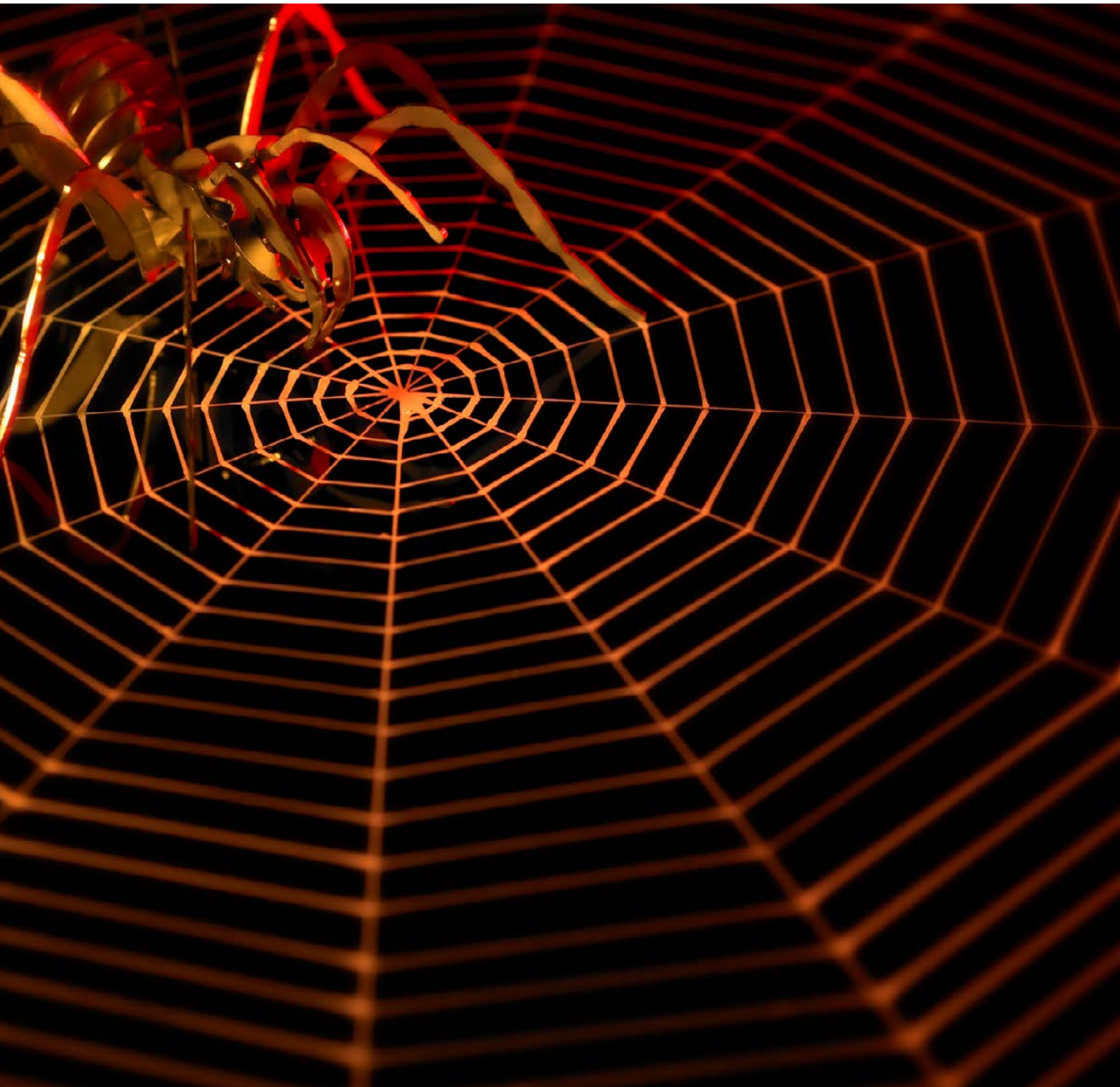
Solicitors Regulation Authority

Spiders in the web:

The risks of online crime to legal business

March 2014



Contents

Executive summary . . . 3

Introduction . . . 5

The incidence and impact of cybercrime . . . 6

Types of cybercrime and the risks it presents . . . 7

- Breach of confidentiality . . . 7
- Structural and financial Instability . . . 12
- Bogus firms . . . 14

Good and bad practices . . . 15

- The Ten Steps to Cyber Security . . . 17

Conclusion . . . 18

Signposting . . . 19

Glossary . . . 20

Index of sources . . . 24

Executive summary

As a risk-based regulator, a vital activity that we undertake is the identification of risks to the regulatory objectives, as set out in the Legal Services Act 2007[1]. As well as allocating our own resources, proportionately, in-line with these risks, we require firms to ensure that they are also managing them.

The purpose of this paper is not to alarm you, but to highlight an emerging risk and support law firms in taking appropriate actions to protect themselves, their clients and the wider public interest.

This paper sets out the risks that result from Cybercrime and practical examples of how it has affected law firms and other professional service providers. A range of measures that firms can take to protect themselves and their clients is also summarised.

Under Principle 10, regulated firms have a responsibility to *'protect client money and assets*'. Cybercrime presents a significant risk to clients and their assets, including information and money.

As a result, cybercrime also presents a risk to Outcome 4.1, which requires that law firms 'keep the affairs of clients confidential unless disclosure is required or permitted by law or the client consents'.

The impacts of cybercrime may also lead to a negative impact on the structural or financial stability of a law firm. Therefore, managing this risk effectively is in the best interest of your firm. Responsibility to manage this risk is also aligned by Principle 8, which states:

> *'run your business or carry out your role in the business effectively and in accordance with proper governance and sound financial and risk management principles'.*

Prevention

Online crime is widespread and diverse, but the greatest risks can often be overcome by taking straight forward steps. Government Communications Headquarters (GCHQ) estimated that 80 percent of all online attacks could be prevented if firms followed simple guidance on safe use of information systems.

Examples of controls that firms can adopt include:

- ending or restricting the use of datasticks and email attachments, in favour of secure direct log-ins and online collaboration tools
- keeping browsers, operating systems and anti-virus systems fully updated
- ensuring that staff can access only those files that they need, to protect against insider attacks.

Advice from the Department of Business, Innovation and Skills recommends that firms should see managing the risks of cybercrime as a board-level or senior management responsibility. They point out that treating this risk only as a technical area for IT specialists can lead to many important preventative measures being missed.

Firms that have reason to believe they may be the targets of more deliberate attacks, for instance for the purposes of commercial espionage against major clients, should consider taking expert advice.

Nature of the risks

The major risks presented by cybercrime are set out in more detail below:

Breach of Confidentiality

Criminals may seek to obtain confidential client material, either for the purposes of espionage or for financial gain. This can be done via harmful computer programs designed to record information, often referred to as 'malware'. Alternatively the threat may come from direct hacking of a system, for instance by breaking a password and other security systems.

The notable threats to confidentiality can come from human factors, such as employees selecting guessable passwords, or from the attempts to deceive employees into giving cyber criminals access to IT systems or privileged information (sometimes referred to as 'phishing').

Firms whose clients' work involves confidential materials, such as high-tech patents, may be seen as 'weak links' that can be exploited by more sophisticated espionage.

Structural and financial instability

The effects of some forms of cyber-attack may actively destabilise a firm by rendering key systems unavailable.

The most notable threats to the operations of a firm come from online activists and hackers. There has also been an emerging risk from programs that encrypt data, effectively taking it 'hostage' - with a demand for payment for its de-encryption.

The financial losses caused by online crime may cause or contribute to financial difficulty in a firm. This is another operational risk that law firms must manage.

Bogus firms

In addition, bogus firms represent a specific case of online crime, posing risks on clients who are tricked into sharing information or paying over money. Often, the perpetrators behind these scams use data from law firms to make their activities look more genuine.

By taking basic identity theft precautions, firms can reduce risks presented to the public and to their own reputations.

Introduction

Crime acts like a business and, like any other business, constantly seeks new opportunities for profit. Given the importance of the internet to commercial life, criminal activity online has become an increasing concern.

Much online criminality is aimed at naive individuals. The omnipresent 'spam' junk emails, for instance, are in the main offers to sell illegal or counterfeit goods or efforts to induce people to invest in scams. The consequences for those that fall for these may be severe, but their main impact on business is the time and server space wasted by them. With recent law enforcement successes in cracking down on spam distributors[1], coupled with increasingly sophisticated spam filtering by email providers, the volume of this nuisance has reduced recently[2].

Of greater significance is more serious online criminality targeted at business. This has, in recent years, become a larger proportion of crime on the Internet[3]. The distributors of harmful software – known as 'malware' – are increasingly serious criminal enterprises interested in profit. Malware encountered now is more likely to be unobtrusive and aimed at gathering access information. These systems are professionally produced and distributed by sophisticated networks of criminals[4].

The subtlety of much cybercrime can be seen from the fact that, in 2012, nearly two thirds of firms that became aware that they had been the subject of a cyberattack took over 90 days to discover the breach, with nearly a fifth taking over a year to discover the attack[5]. Many firms will never become aware that they have been a victim of cybercrime.

In distributing this paper, we do not intend to cause alarm. There are simple steps that law firms can take to help protect themselves from criminals. These help to turn businesses from soft to hard targets. This paper sets out some recommendations on best practice that have come from the computer security community and from organisations such as GCHQ and the Department for Business, Innovation and Skills.

Our previous paper on 'cloud computing' risks, *Silver Linings,* discussed a range of issues involving information security online[6]. Although this paper is intended to stand alone, many of the risk controls relevant to decisions concerning the adoption of cloud infrastructure are also relevant to protecting a firm from online criminality.

1 Solon, O World's Third Largest Spam Botnet Shut Down By Security Researchers, Wired, 20 July 2012.
2 Krieger, S, 2012 and 2013 Email Security Trends: Increased Threat Levels Despite Spam Decline, Eleven, 8 January 2013.
3 Microsoft, Evolution of Malware: Malware and Potentially Unwanted Software Trends, Microsoft Security Intelligence Reports, 2011.
4 Lyne, J, Everday Cybercrime And What You Can Do About It, TED (Video), 13 February 2013.
5 McCullen, R, Trustwave 2013 Global Security Report, Trustwave-Osterman, 2013.
6 SRA, Silver Linings: Cloud Computing, Law Firms and Risk, SRA, November 2013.

The incidence and impact of cybercrime

Estimates of the impact of cybercrime on business vary. It is possible for firms to be targeted, successfully or otherwise, without ever becoming aware of the attack. Businesses that have incurred loss from online crime often do not publicise the fact. For these reasons, most figures that circulate concerning the level of online criminality are highly speculative and should not be uncritically accepted. We detail some of them here for illustrative purposes.

- Norton estimate the global cost of all forms of **online crime at $388bn** (£237.6bn) in 2012, a figure comparable to the global value of drug trafficking[7].
- The Federation of Small Businesses estimates the **average annual cost to small businesses of online crime as £4,000 per firm**, and state that a third of their members reported having been the victim of some form of online crime in 2012[8].
- **12 percent of partners and IT directors in legal firms believe that they have been subject to an online attack**, 80 percent believe that they are likely to be the subject of cyberattack, whereas only a third believe that their systems could withstand an attack, according to a survey of 370 partners and IT directors in legal firms in 2013[9].
- **8% of large organisations and 63% of small businesses were attacked by an unauthorised outsider** in 2013, according to a PwC survey[10].
- Of the small businesses responding to the survey, **57% had suffered staff-related security breaches[11].**
- Unwanted 'spam' is estimated as making up **over three quarters of all email** received by a typical organisation[12]. This can still lead to direct costs even though this may have declined in recent years as more effective means of detecting it have become available and as high level producers are identified and shut down. Around a tenth of this will be linked to malware, the remainder is made up of various online scams and efforts to sell illegal or counterfeit products.

7 Norton (2012), 2012 Cybercrime Report, Norton Security.
8 Federation of Small Businesses, Cybersecurity and Fraud: The Impact on Small Businesses, FSB, 2012.
9 Reynolds, A, Fears of Cyber Crime Rise As Nearly 80% Believe Their Firm Could Be Hit By Web Hack, Legal Week, 3 May 2013.
10 PwC / BiS, 2013 Information Security Breaches Survey: Technical Report, PwC, 2013.
11 PwC / BiS, 2013 Information Security Breaches Survey: Technical Report, PwC, 2013.
12 McCullen, R, Trustwave 2013 Global Security Report, Trustwave-Osterman, 2013.

Types of cybercrime and the risks it presents

Despite the diversity of crime and the wide range of specific attacks that firms may experience, the impact on legal businesses can be broken down into a short list of risks.

The most serious threat is to confidential client information. Other risks are presented to the structural and financial stability of firms. In other cases, consumers can be targeted directly by bogus firms, these sometimes operate using the 'stolen identities' of real law firms. This is a risk to the interests of consumers, as well as the reputations of the real law firms that become associated with it.

Breach of confidentiality

Protecting client confidential information is one of the most essential requirements of any legal business, and firms must ensure confidentiality to comply with Principle 10 and Outcome 4.1.

Confidential material that may be of interest to criminals ranges from personal data, to trade secrets, through to the financial details and personal dealings of prominent clients. Simple payment information such as credit card details may be of interest for criminals intent on straightforward theft or identity fraud.

Law firms acting for corporate clients, especially those dealing with patent information or in high-tech industries, are at increased risk of being targeted in this manner. Commercial espionage is an increased concern, including overseas state-sponsored efforts to obtain business and technological secrets. Some law firms acting in these cases may be viewed by some as a 'weak link'[13] to accessing this information.

Espionage is not the only motive for these attacks. Online activists may also seek to obtain confidential information from law firms as part of a campaign. A spokesperson from the 'Anti-sec' hacking group stated in 2011 that:

> "*Generally we target government systems, police systems and evil corporations. But law firms do usually contain a wealth of private information, and when they are representing people who are already in our crosshairs, it's fair game.*"[14]

Human factors

The simplest threat comes from 'phishing': criminals obtaining information or passwords by deceiving staff into giving it to them.

Phishing tactics can range from the simple, such as e-mailing people in a firm claiming to be from IT or HR and asking for password details, through to complex and targeted 'spear-phishing' attacks using social media information to pose as a contact of a specific individual. This can be highly effective. As with most IT issues, the human element is the most likely area to fail.

Such attacks can give a data thief access to an account ID and password, and accordingly the potential for a significant loss of data. They can also be used by criminals as a means of installing harmful computer programs, which is discussed on the following page.

13 Ames, J Cyber Security: Lawyers Are The Weakest Link, The Lawyer, 28 October 2013.
14 Gallagher, R, Anonymous Splinter Group Anti-Sec Wages War on 'Profiteering Gluttons', Guardian, 27 February 2012.

Case Study:

Commercial espionage by ‘spear phishing’

In 2011, a Toronto law firm working on a proposed acquisition of a Chinese company was targeted by data thieves. Lawyers working on the deal received emails that appeared to be from a partner in the firm who was involved in the transaction. The emails were actually a targeted phishing operation, and contained an attachment which installed a computer program on to the firm’s IT systems. This programme was used to record data and information and allow the third party to access it.

The attack involved three other Toronto law firms, and was eventually traced to computers in China. Commercial espionage was the presumed motive for the attack[15].

Case Study:

The bogus applicant

One tactic used to persuade a target to install malware on to their system has been the use of fake job applicants. This can involve an emailed job application, with an attachment that purports to be a CV or application form but that is actually a disguised malware program.

This is usually detectable by antivirus systems, but is a route that has seen successful use in several cases as the attachment’s existence makes sense in the context of a job application email. As this type of email is one that firms will expect to receive from people that they do not know, it is more likely to be opened[16].

A more novel approach on record involved an ‘applicant’ arriving late for an interview, wet from rain, and holding a collapsing folder full of soaked documents that were no longer readable. The aim was to enlist sympathy from reception staff and to persuade them to allow the ‘applicant’ to print out fresh copies of their CV and portfolio, which the ‘applicant’ had saved on a datastick[17]. Once the datastick was inserted it installed malware to the firms systems.

15 Mintz, M Cyberattacks on Law Firms: A Growing Threat, Martindale.com, 19 March 2012.
16 Spamfighter, Beware of Fake Job Application Emails, Spamfighter Blog 21 January 2013.
17 Lyne, J, Everday Cybercrime: And What You Can Do About It, TED (Video), 13 February 2013.

Harmful software

‘Malware’ comes in many forms. The main threat to confidentiality comes from the form known as ‘Trojan horses’. These programs hide on a system and can remain undetected for long periods: many are designed to survive straightforward removal techniques and to neutralise antivirus software. They can only reach a system either by being deliberately installed or if a user is tricked into installing them.

The functions of these systems vary. Some actively steal information such as banking information while others form networks with other hijacked computer systems. This may be used by cyber criminals to distribute spam email or to provide computing power for password cracking.

Most malware targets Windows machines, as these are the most popular systems around the world. No system, however, is truly immune, and malware has been discovered for all operating systems in wide use. If other operating systems become more popular, then malware creators will increasingly target them as well.

Anti-virus systems can only protect against malware that has already been identified and analysed by the anti-virus company, and the defences built into operating systems can only protect against known weaknesses. As such, they should not be relied upon exclusively for protection against attack. The best defence is to reduce the opportunity for infection by closing common routes. Criminals use varying methods to induce a target to install their malware, including datasticks and deceptive emails.

Case Study:

Trojan horses and the Iranian nuclear programme

The Stuxnet worm, discovered in June 2010, was a reportedly US-devised malware system intended to infiltrate and damage the Iranian nuclear program. Although the degree of sophistication demonstrated in the software was unusual, the means by which it was first introduced to the target was a conventional method that is also used by criminals.

The agents delivering the malware are reported to have dropped a number of USB sticks in the car parks of facilities linked to the targeted programme. Once an employee picked one up and later used it, the malware was programmed to run automatically.

Although the attack was specifically targeted, the infiltration systems in the worm were highly effective and it spread further than the designers had presumably intended. The worm spread beyond Iran and infected systems in countries from Israel to Belarus.

Two years later, another Trojan horse was discovered infiltrating Iranian systems. Using similar systems to Stuxnet, this was an espionage tool designed to quietly occupy systems and steal information. Analysis revealed that it was an older tool, that had remained undetected for years[18].

The threat of military cyberweapons such as this may seem exotic, but recorded efforts to steal information from law firms have shown the signs of state sponsorship and there was little sophistication in Stuxnet's initial delivery. Preventing malware from getting onto a system is a better defence than relying on antivirus software to defeat software that is already at work[19].

Case Study:

Windows XP

From 8 April 2014, Windows XP will no longer be supported by Microsoft, and the company will no longer provide updates for security on that operating system[20]. As a result, any security vulnerabilities that have not been identified before that date will never receive a remedy.

Although the operating system itself will no longer be maintained, Microsoft have confirmed that they will continue to provide malware updates for existing XP users of their Security Essentials system for another year. This provides twelve months of limited security for those still using XP.

This represents a significant risk to the IT security of remaining users. Software producers continually identify vulnerabilities in their products, especially those that criminals are known to be exploiting, and issue regular updates to remedy them.

Vulnerabilities that have not yet been remedied by the computer companies are highly valuable criminal commodities. They represent attack routes that antivirus systems will not spot and which computers are not equipped to prevent.

Windows XP remains in use by a high proportion of businesses. More than a quarter of all desktop computers in the world[21] still have XP as their operating system. These users will all face increased security risk.

18 Kushner, D, The Real Story of Stuxnet, IEEE Spectrum 26 February 2013.
19 Edge, J, The Power to Destroy: How Malware Works, Symantec, 14 November 2013.
20 SRA, Confidentiality of Client Data: Are You At Risk?, SRA, 14 January 2014.
21 Bright, P, Windows 8.x Breaks 10 Percent, Ars Technica 3 January 2014.

Hacking

Attempts by cybercriminals to break directly into a sensitive computer system also pose a confidentiality risk. The simplest form of attack involves efforts to gain unauthorised access by means of guessing log-in passwords. Hackers can also use search engines and common website referencing practices to seek access to otherwise hidden areas of a website such as client case information or staff private areas. As many people use guessable passwords, such attacks are often highly effective.

Unsecured wi-fi provides an opportunity for hackers. It is possible to copy large amounts of data transmitted through a wi-fi network from outside the owner's premises without a high chance of this being identified. Even if the data is encrycted, the hacker will then have time to try and break this encryption[22]. Depending on the system being used, work from home on an unsecured wi-fi may enable hackers to gain direct access to otherwise secure corporate systems.

More serious efforts to crack password details involve the application of significant computing power, and can be ingenious. Firms that believe they may be the target of highly organised intrusion should take professional advice on the best way to secure their network.

Case Study:

Exposure of client information following online attack

In February 2012, the 'Anti-sec' online activist group hacked into the servers of a Washington law firm that was acting for a US soldier convicted of war crimes in Iraq. They obtained tens of thousands of emails, and posted them online. Their stated objective was to expose "rich and powerful oppressors", presumably referring to the political lobbying that had been alleged in the case.

The emails released included confidential information relating to the case. They also included confidential details of unrelated cases including witness statements from victims of sexual assault.

A spokesman for the group stated that they may attack further law firms "If law firms stick their necks out in defence of notoriously corrupt corporations – especially if it is shown that wrongdoing was involved..."[23]

22 Delany, P, The Five Deadly Dangers of Unsecured Wi-Fi, South Jersey Technology Blog, 31 March 2013.
23 Gallagher, R, Anonymous Splinter Group Anti-Sec Wages War on 'Profiteering Gluttons', Guardian, 27 February 2012.

Structural and financial Instability

Although confidentiality breaches are the likeliest risk from cybercrime, firm structural and financial stability can be at risk as well.

As Principle 8 requires firms to 'run their business effectively and to apply proper risk management', it is important that firms be aware that online crime can pose structural and financial threats.

On-line activism

One method of on-line activism involves large numbers of individuals repeatedly accessing a website, aiming to overload its servers and cause downtime (these are referred to as 'distributed denial of service (DDoS) attacks').

Such campaigns can be organised by campaigning groups, or can be co-ordinated through networks of computers that have been hijacked by malware.

The downtime caused has direct consequences for firms, especially those dependent on cloud computing for their entire IT infrastructure. Indirect harm can include reputational damage from an unavailable site.

Indirect exposure to these attacks may also cause problems for law firms. If one firm using cloud provision becomes a target, then the overload may affect other users of the same cloud service.

Case Study:

Denial of service attack on a trade body

In September 2010, the 'Anonymous Collective' organised a DDoS attack on the website of the Australian Federation Against Copyright Theft ("AFACT"), rendering AFACT's site inaccessible for several hours. AFACT's website was hosted on a remote computing provider, whose servers were also overloaded by the attack. Over 8,000 websites hosted by the provider experienced a loss of connection as a result. Many were small businesses, and none were connected to AFACT[24].

There are steps that can be taken to protect servers from overload, such as using parallel backup servers. Firms that suspect they may become the targets of such action may wish to investigate ways to protect themselves ahead of time.

It is likely that cloud providers are better equipped to defend against DDoS attacks now than they were in 2010. Firms intending to use cloud systems, however, may still wish to ask prospective providers about the potential for disruption in the event of a DDoS against them or another user. Such queries form a key part of standard due diligence.

24 Winterford, B, Operation Payback Directs DDoS Attack at AFACT, IT News, 28 September 2010. Accessed on 06 January 2014.

Data being held hostage

A relatively new threat from cybercrime is data being 'taken hostage' by harmful computer programs. These programs are termed 'ransomware' and literally hold a target's data hostage in return for ransom money. They generally work by encrypting data and demanding payment for the codes to release it.

The best defence against this threat is to maintain reliable backup systems, ideally using removable media that are not routinely connected to live servers. This is a standard recommendation for all computer users in case of system failure, so should not represent a significant additional burden for business users.

Case Study:

Cryptolocker[25]

First detected in Autumn 2013, Cryptolocker has been described as the first really effective example of a concept that criminals have attempted to implement many times previously – 'ransomware'.

Currently spread by means of falsified email attachments, Cryptolocker has little ability to distribute itself across a wider network, though it can access cloud storage files and actively connected backup systems to which the targeted user has live access privileges. Newer versions may have added code enabling them to spread by infecting USB datasticks[26].

Cryptolocker's limited ability to replicate itself has not prevented rapid spread. First distributed to the internet in September 2013, by December 2013 it was recorded as having infected 250,000 known targets[27].

When Cryptolocker infects a target, it encrypts a wide range of data files. It then places a warning on the target's desktop wallpaper stating what has happened and that they have 72 hours to pay $300 to the controllers. If the deadline expires without payment, the controllers delete the private key that is the only means of breaking the encryption.

The scale of payments and distribution tactic suggest an intent to target individual consumers and small businesses, as does the lack of a system for propagation across corporate networks[28].

25 For a full discussion of Cryptolocker, see Goodin, D, You're Infected - If You Want To See Your Data Again, Pay Us $300 In Bitcoins, Ars Technica 17 October 2013.
26 This may have been a copycat rather than an upgrade, as it was in other ways less sophisticated than the original strain. Pichel, A New Cryptolocker Spreads Via Removable Drives, Trendlabs Security Intelligence Blog 25 December 2013.
27 Kelion, L, Cryptolocker Ransomware Has Infected 'Around 250,000' PCs, BBC, 24 December 2013.
28 Raising fears of the release of an "enterprise edition" of the Trojan seeking higher costs from hijacking networks. Goodin, D, Researchers Warn of New, Meaner Ransomware with Unbreakable Crypto, Ars Technica, 6 January 2014.

Case Study:

Cybercrime and direct financial loss

In April 2013, a criminal gang stole £1.3m from a branch of a major bank in London. A member of the gang had posed as an IT engineer in order to gain access to the branch's computer systems, and had installed a monitoring device to enable the gang to transfer money remotely[29]. Banks may seem the obvious targets for this form of financial crime, but other businesses may be seen by criminals as easier targets.

Bogus firms

We are seeing increasing reports of fake law firms, many of which advertise online and operate by stealing the identity of an existing, real law firm. This can be used as a method of stealing money from clients that are tricked into thinking they are dealing with a genuine law firm.

Reports of this activity have significantly increased. We received 549 reports of these fake firms in 2013, a 57 percent increase on the number in 2012[30].

This form of commercial identity theft can be guarded against with many of the same concepts as used against personal identity theft, such as ensuring the secure destruction of documents that carry sensitive information about the firm.

Firms should also at least occasionally monitor references to themselves online and on sites such as 'Find a Solicitor'. This may help detect fake branches. If dealing with a suspected criminal, they should be cautious in sending documents that carry their letterhead.

Our warning notice on bogus firms and identity theft sets out a range of guidance for avoiding and detecting this type of crime[31].

29 Ring, S, Barclays Cybercrime Suspects Arrested Over $2.1m Theft, Bloomberg, 20 September 2013.
30 SRA data.
31 SRA, Warning Notice: Bogus Firms and Identity Theft, SRA, 26 March 2012.

Good and bad practices

Advice from the Department of Business, Innovation and Skills recommends that firms make managing the risks of cybercrime a board-level or senior management responsibility. They point out that treating this risk purely as a technical area for IT specialists can lead to many important preventative measures not being implemented[32].

GCHQ estimate that 80 percent of online attacks could be prevented by simple compliance with best practice[33].

The following is a synthesis of the advice from multiple sources.

Good practices:

National surveys of UK businesses have been carried out to establish common and best practices concerning cyber security[34]. Reviewing these in line with the GCHQ 'Ten Steps' guidance on security[35] should place firms in a strong position to protect themselves.

Examples of best practice in risk management policies for cybercrime, include:

- including information risks as a discrete category in their risk registers
- regularly reviewing the effectiveness of online security controls, including password policies, and the degree to which staff are adhering to them
- planning for worst-case scenarios
- developing a mobile working policy and training staff to comply with it
- treating violations of information security policies as serious disciplinary matters
- ensuring that computer security policies cover safe use of organisational systems and that staff understand them
- establishing detailed computer account management systems, including ensuring that staff only have access to needed files and limiting the number of highly privileged accounts
- controlling and limiting the use of removable media
- maintaining ongoing monitoring of organisational systems and investigating anomalies
- monitoring mentions of their name online to detect fake branches.

32 HM Government, FTSE350 Cyber Governance Health Check, BiS, November 2013.
33 Lobban, I, Ten Steps To Cyber Security: Executive Companion, CESG, 2012.
34 HM Government, FTSE350 Cyber Governance Health Check, BiS, November 2013.
35 Lobban, I, Ten Steps To Cyber Security: Executive Companion, CESG/GCHQ, 2012.

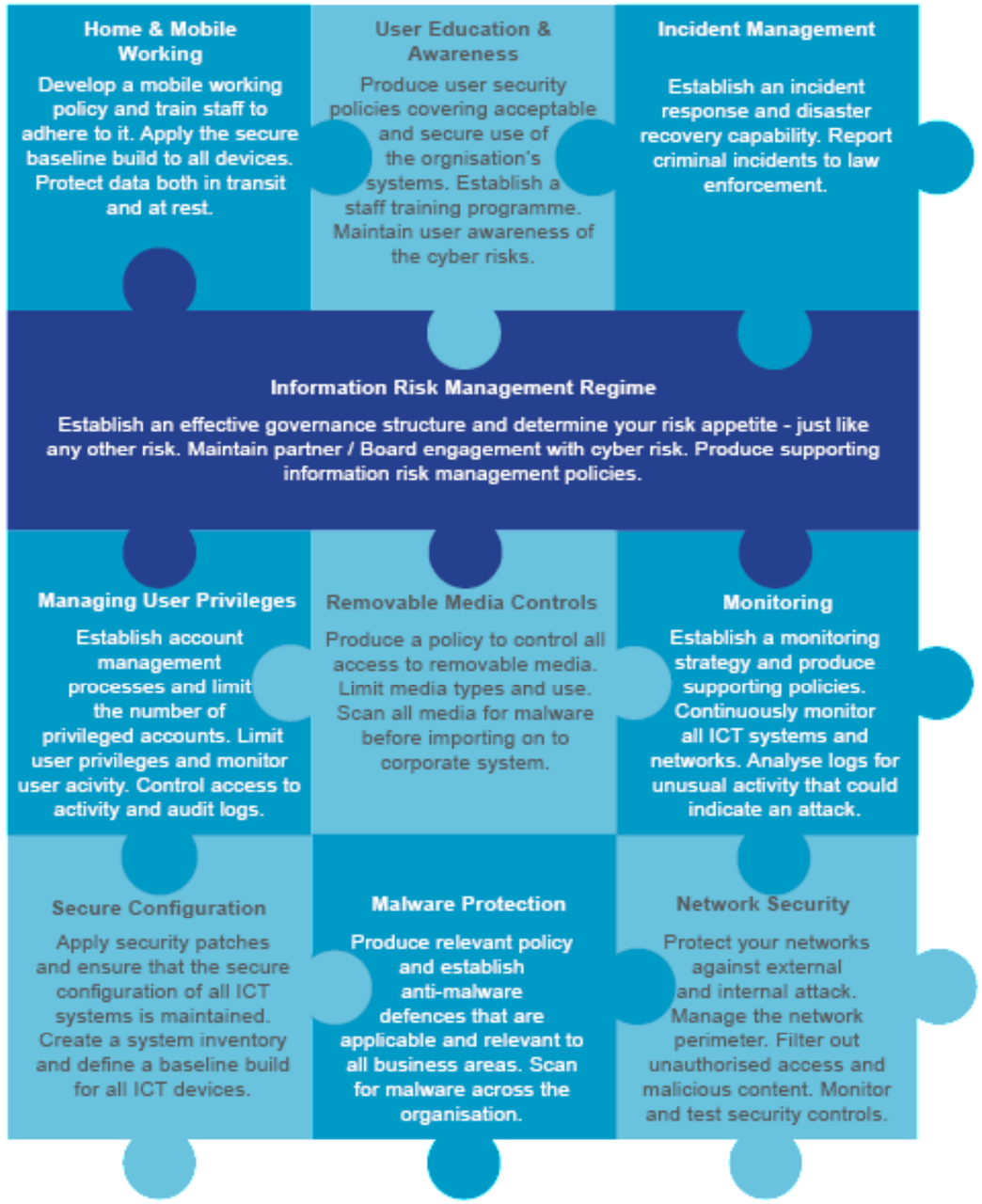
Best practice examples of practical steps firms could consider, include:

- ensuring up to date malware protection
- ensuring access control such that staff have access only to files which they need
- adopting systems that eliminate the need for datasticks and minimise the need for email attachments
- at the least encrypting any information stored on removable media or portable devices, and considering the use of systems that eliminate the need for any files to be stored on portable devices
- considering encrypting any information stored on a remote provider;
- ensuring that office systems scan any removable media for viruses and other malware
- backing up key data in multiple places, including at least one form of discrete dated archive
- ensuring that unapproved devices are not connected to the system
- ensuring that inappropriate sites cannot be accessed from work systems
- keeping operating systems, browsers and antivirus systems fully updated
- ensuring that any device connected to organisational systems, including by remote networking, is vetted for security
- ensuring that data transmission within and beyond the firm is secure at all ends
- ensuring that access rights for staff who have left the firm are revoked, and that unused accounts are closed
- conducting background checks on applicants, especially those who will have access to highly sensitive data
- reporting to the SRA if a successful cyberattack affects the firm's ability to meet the outcomes in the Code of Conduct.

The diagram on the next page is based on the original Ten Steps from CESG illustrates measures that firms can take.

Firms with specific reasons to believe that they are or may be directly targeted by serious attackers or who act for clients who may be subject to highly sophisticated espionage should take specific advice from counterintelligence professionals on securing their systems. Such subjects as the creation of air-gapped systems to significantly beyond the scope of this paper.

The Ten Steps to Cyber Security



Bad practices

Bad practices in IT security are numerous. Those listed below relate to specific vulnerabilities:

- use of unsecured webmail or unapproved devices to transfer files
- guessable passwords and locally stored files
- staff not trained to protect data
- internal use of insecure communications methods (for instance significant information sent and received as email attachments, or unsecured office wi-fi)
- failing to keep operating systems, browsers and security systems updated
- mobile working policies that do not make clear the obligation on staff to use only secure wi-fi and access routes into firm systems from home or elsewhere
- 'Bring Your Own Device' systems where mobile devices are not vetted prior to connection to firm systems or cannot be managed by the firm
- lack of access controls, such that any staff member can access any files on the network
- critical files stored online without backups.

Conclusion

The prevalence and wide variety of cybercrime means that it does pose risks for law firms and the wider public interest. As the importance of the internet to all forms of business will only increase, so will the issues relating to criminal use of the internet.

Much cybercrime, however, involves straightforward attack routes that rely for success on naive systems and absent controls.

The best remedy, as with criminality in general, comes from taking simple, common sense steps to protect yourself. This is greatly assisted by reading good practice guidelines such as those from GCHQ, BiS and the Federation of Small Businesses.

Signposting

Firms need to assess their own risks at a level that is appropriate to their needs. As such, we do not require that firms adhere to any specific set of principles for managing online security risks. There are, however, multiple sources of guidance on IT standards and risk management.

The international standard for cyber security management is ISO 27032:2012[36]. This represents a fairly maximal level of detail in this area.

The Department of Business Innovation and Skills will be releasing an information security standard on 31 March 2014, intended to provide a usable guide for businesses of all sizes. Once released, it will be accessible online.There are numerous additional sources for approachable guidance. The following recommended sources are a good place to start.

- The Be Cyber Streetwise programme aims at improving the online security of citizens and small businesses, and is a joint project of the Home Office and the Department of Business Innovation and Skills[37].
- The CESG / GCHQ "Ten Steps To Reduce Your Cyber Risk"[38] guidance and advice sheets[39] give straightforward advice on controlling the risk from cyber crime, focusing on larger firms.
- The Department of Business Innovation and Skills has produced tailored guidance for small firms on dealing with cyber risk[40].
- Microsoft has released a Security Guide for small businesses, providing clear guidance on issues including security planning and choosing a suitable IT consultant[41].
- The Information Commissioner's Office has also produced guidance on IT security, emphasising Data Protection compliance[42].

For more detailed information and explicit guidance on setting up information security systems, firms may wish to consult a suitable professional.

36 ISO/IEC, ISO/IEC 27032:2012. Information Security Technology–Security Techniques–Guidance for Cyberspace, ISO 2012.
37 Home Office 2014, Be Cyber Streetwise
38 Lobban, I, Ten Steps To Cyber Security: Executive Companion, CESG, 2012.
39 Lobban, I, Ten Steps To Cyber Security: Guidance Sheets, CESG, 2012.
40 HM Government (2012), Small Businesses: What You Need To Know About Cyber Security, BIS 2013.
41 Microsoft, Security Guide for Small Businesses, Microsoft, 2006.
42 Information Commissioner's Office, A Practical Guide to IT Security, ICO, April 2012.

Glossary

The following glossary may assist you in understanding jargon and technical terms that you might encounter if you undertake further reading on this risk.

419 fraud	Named for the article of the Nigerian Criminal Code which prohibits mail fraud, these are the well-known spam emails indicating that someone with vast amounts of money needs your help in investing it in return for a large share, if only you will give them some money up front and your bank account details to deposit the sums. Run by organised crime, the consequences for those falling for these scams can be serious. As with all spam, the low rate of people falling for the scam is still high enough to make the millions of emails worth sending.
Air-gap	A means of securing extremely confidential electronic data by isolating it entirely from the Internet or, in extreme cases, even internal networks. This can involve storing such data only on specified machines that lack networking cards. Maintaining a successful air-gap is not simple, and specialist advice should be sought when such a system is needed.
Apps	Individual pieces of software for conducting specified tasks for the user. Short for either 'applications' or possibly 'applets'. This term has effectively displaced the much older term 'program' for most uses of software.
Bot-net	A large and distributed group of computers, unknowingly hijacked by Trojan horse software so as to devote processing time to work as a network at the behest of the network's controller. Bot-nets are used by criminals to gain processing power for attacks on secure systems (for instance to steal credit card details from websites), and to distribute junk email 'spam'.
Bring your own technology (BYOT)	The practice in certain businesses of having employees bring their own computers to work and connect them to their employer's network to access privileged information and systems. This has cost advantages for the employer and permits the employee to choose their own devices. It also carries risks for IT security and complicates the work of maintaining an office network.
Brute-force attack	One of the main methods for criminal penetration of secured systems. Brute-force attacks often involve using a computer network such as a bot-net to generate enormous numbers of possible passwords and test them against a targeted system or encrypted document.
Cloud Computing	Systems where data is stored on a network rather than on a specific machine, often with apps and data provided as a service. Widely used personal cloud systems include Dropbox and Google Docs.
Cookie	A small file loaded onto a user's computer by a website that they have visited, and readable by that and other websites. Cookies are used to retain log-in details, hold user information and to perform a host of other useful functions. They are fundamental to the operation of many websites. They can, however, also be used as a form of elementary spyware to monitor someone's web activity.
Datastick	Small, portable flash memory devices used for transferring files from one computer to another as well as for elementary backup storage. The portability of these devices poses security risks: data can leak or simply be lost if the device is lost or stolen. Data sticks are also used to spread Trojan horses and other malware. Encryption, included at a hardware level on some datasticks, can help counter the risk of data leaking in the event of loss. Note that flash memory has a limited lifespan due to the means of altering its contents: all datasticks will cease working at some point after purchase. They should not in any event be used for long term storage.
Digital Signature	A means of unequivocally verifying the identity of the sender of an electronic document. Many systems exist to accomplish this. Some rely on a network of trusted websites that can verify identity, others on the use of public key encryption to produce text that can provably have come only from the purported sender.
DDOS / Distributed Denial of Service	A systematic attack on a firm's computer systems using mass log-in attempts to overwhelm server capacity. Often co-ordinated through a bot-net of externally controlled computers.
Encryption	Concealing the content of a document from unauthorised reading by applying a cipher. Encryption systems used online are highly complex, but depend for security on a suitable passphrase or key.
Hacktivism	Online activism. Hacktivists seek to use IT skills to advance political causes. In addition to the usual tools of campaigning groups, hacktivists have been known to use Distributed Denial of Service (DDOS) attacks to interfere with the operations of organisations with which they disagree, and occasionally more direct hacking.
Malware	Computer apps intended to run on someone's computer without the owner's consent or knowledge. The purpose can be to gain information as spyware or to cause damage, or both.

Phishing	Gaining access to accounts by deception: for instance sending faked emails to employees of a company, claiming to be from the IT department and to need to compile a list of usernames and passwords for a system reset. A targeted phishing attack known as ‘spear-phishing’ involves using highly tailored falsified emails to seek information from a specific high-value individual. Information for such emails is often derived from the target’s social networking information.
Public key encryption	A system of encryption requiring different information to encrypt a message from that needed to decrypt it. The user disseminates a ‘public key’ for others to use in encrypting and sending messages to the user, and can then use their own ‘private key’ to decrypt the messages. As the public key offers no clues to the nature of the private key, this provides good security without requiring the parties to exchange keys.
Social engineering	Any means of breaking into the security arrangements of a target by inducing the target to reveal passwords or identity details. For examples, see phishing and spear-phishing.
Spam	Mass junk email, often marketing a wide range of illegal, counterfeit and undesirable products and scams. Spam is a significant problem, with a very large proportion of the email messages sent each year being spam. There are high costs associated with detection and elimination of the problem as well as a huge loss of time due to processor overload across the Internet. Although the number of people who ever act on the contents of spam email low, the cost of sending spam is sufficiently negligible that this is a highly profitable enterprise.
Spyware	A common form of malware, these are apps designed to monitor an individual’s computer use for someone else’s gain. Sophistication varies from a simple tracking cookie through to a more advanced Trojan horse such as a ‘keylogger’ that captures and records everything typed on an infected machine. Commercial use includes targeted advertising, which has been controversial due to consent and privacy issues. Criminal use includes the acquisition of bank details and passwords.
Trojan horse	Malware which either conceals itself entirely or masquerades as performing some useful function to gain access to a system. Trojan horses steal information, hijack control or simply damage the system on which they are installed.

Virtual machine	Also known as a ‘sandbox’, a virtual machine is a protected area in a computer’s memory. These are commonly created by Internet browsers and by systems intended to run on any type of computer, as with Internet games. This restricts the power available to apps using the virtual machine, but also enables the app to run on any system. Importantly, it reduces the potential for harm from malware as any malware should only have access to the virtual machine.
Virtual Private Network (“VPN”)	A system for connecting a computer to a remote secure network through secure channels, using encryption and keeping data isolated from other traffic on the networks. Users should have the impression of a direct connection to the network that they are accessing. One major use is to allow remote workers to connect to an office network whilst at home or on the move without risking data being intercepted.
Zero Day Exploit	A flaw in an operating system or internet browser that provides a weakness that malware or hackers could exploit, but which has not yet been identified or remedied by the software producer or by the major antivirus vendors. Zero day exploits are highly valuable criminal goods, as they enable attacks that antivirus systems and operating system security cannot stop. Due to their value and rarity, they rarely appear in malware, being usually held in reserve for direct attacks on high-value targets.

Index of sources

Ames, J (2013), “Cyber Security: Lawyers Are The Weakest Link”, The Lawyer, 28 October 2013. Online at: http://www.thelawyer.com/analysis/cyber-security-lawyers-are-the-weakest-link/3011315.article

Bright, P (2014), “Windows 8.x Breaks 10 Percent”, Ars Technica 3 January 2014. Online at: http://arstechnica.com/information-technology/2014/01/windows-8-x-breaks-10-percent-internet-explorer-11-makes-a-splash/

Delany, P (2013), “The Five Deadly Dangers of Unsecured Wi-Fi”, South Jersey Technology Blog, 31 March 2013. Online at: http://southjerseycomputerblog.com/dangers-of-unsecured-wifi/

Farivar, C (2013), “LOVEINT: On His First Day Of Work, NSA Employee Spied on Ex Girlfriend”, Ars Technica 27 September 2013. Online at: http://arstechnica.com/tech-policy/2013/09/loveint-on-his-first-day-of-work-nsa-employee-spied-on-ex-girlfriend/

Federal Bureau of Investigation (Undated), “The Insider Threat: An Introduction to Detecting and Deterring An Insider Spy”, FBI. Online at: http://www.fbi.gov/about-us/investigate/counterintelligence/the-insider-threat

Federation of Small Businesses (2012), “Cybersecurity and Fraud: The Impact on Small Businesses”, FSB, 2012. Online at: http://www.getsafeonline.org/media/pdf/FSBCyber_FraudDoc.pdf

Gallagher, R (2012), “Anonymous Splinter Group Anti-Sec Wages War on ‘Profiteering Gluttons’”, Guardian, 27 February 2012. Online at: http://www.theguardian.com/technology/2012/feb/27/anonymous-splinter-group-antisec-waging-war

Goodin, D (2013), “You’re Infected - If You Want To See Your Data Again, Pay Us $300 In Bitcoins”, Ars Technica 17 October 2013. Online at: http://arstechnica.com/security/2013/10/youre-infected-if-you-want-to-see-your-data-again-pay-us-300-in-bitcoins/

Goodin, D (2014), “Researchers Warn of New, Meaner Ransomware with Unbreakable Crypto”, Ars Technica, 6 January 2014. Online at: http://arstechnica.com/security/2014/01/researchers-warn-of-new-meaner-ransomware-with-unbreakable-crypto/

HM Government (2013), “FTSE350 Cyber Governance Health Check”, BiS, November 2013. Online at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/268643/bis-13-1293-ftse-350-cyber-governance-health-check-tracker-report.pdf

Kelion, L (2013), “Cryptolocker Ransomware Has Infected ‘Around 250,000’ PCs”, BBC, 24 December 2013. Online at: http://www.bbc.co.uk/news/technology-25506020

Kushner, D (2013), “The Real Story of Stuxnet”, IEEE Spectrum 26 February 2013. Online at: http://spectrum.ieee.org/telecom/security/the-real-story-of-stuxnet

Lobban, I (2012), “Ten Steps To Cyber Security: Executive Companion”, CESG / GCHQ, 2012. Online at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/73128/12-1120-10-steps-to-cyber-security-executive.pdf

Lyne, J (2013), “Everday Cybercrime And What You Can Do About It”, TED (Video), 13 February 2013. Online at: http://www.ted.com/talks/james_lyne_everyday_cybercrime_and_what_you_can_do_about_it.html

McCullen, R (2013), “Trustwave 2013 Global Security Report”, Trustwave-Osterman, 2013. Online at: http://www2.trustwave.com/rs/trustwave/images/2013-Global-Security-Report.pdf

Mintz, M (2012), “Cyberattacks on Law Firms: A Growing Threat”, Martindale.com, 19 March 2012.. Online at: http://blog.martindale.com/cyberattacks-on-law-firms-a-growing-threat.

Norton (2012), “2012 Cybercrime Report”, Norton Security. Online at: http://uk.norton.com/cybercrimereport

Osterman Research (2013), “The Global Malware Problem: Complacency Can Be Costly”, Trustwave-Osterman, January 2013. Online at: https://www.trustwave.com/downloads/Trustwave-Osterman-Research-2011-The-Global-Malware-Problem-Complacency-Can-Be-Costly.pdf

Pichel, A (2013), “New Cryptolocker Spreads Via Removable Drives”, Trendlabs Security Intelligence Blog 25 December 2013. Online at: http://blog.trendmicro.com/trendlabs-security-intelligence/new-cryptolocker-spreads-via-removable-drives/

Ring, S (2013), “Barclays Cybercrime Suspects Arrested Over $2.1m Theft”, Bloomberg, 20 September 2013. Online at: http://www.bloomberg.com/news/2013-09-20/barclays-cybercrime-suspects-arrested-over-2-1-million-theft.html

Schwartz, M (2012), “Zeus Botnet Eurograbber Steals $47 Million”, Information Week, 12 May 2012. Online at: http://www.informationweek.com/attacks/zeus-botnet-eurograbber-steals-$47-million/d/d-id/1107673

Spamfighter (2013), “Beware of Fake Job Application Emails”, Spamfighter Blog 21 January 2013. Online at: http://blog.spamfighter.com/malware-2/beware-job-application-emails.html

Winterford, B (2010), “Operation Payback Directs DDoS Attack at AFACT”, IT News, 28 September 2010. Accessed on 06 January 2014. http://www.itnews.com.au/News/233573,operation-payback-directs-ddos-attack-at-afact.aspx