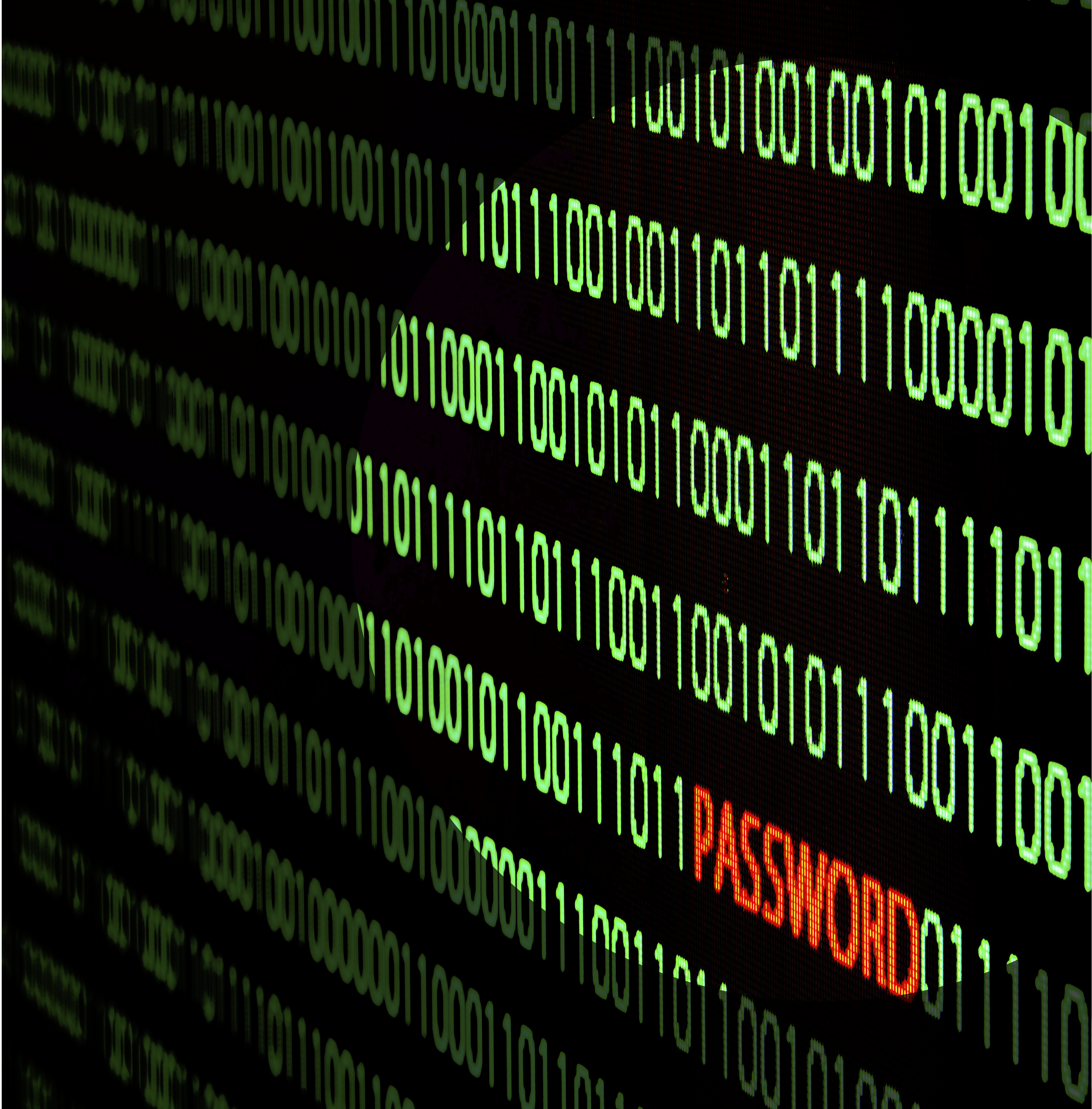
RISCAuthority

administered by

FPA | Fire Protection Association

S28: Cyber crime - overview and sources of support



Published 2015

Acknowledgements

The generous assistance in the preparation of this guide of the Cyber Risk & Insurance Forum (CRIF) and their chairman, Matthew Hogg of Liberty Specialty Markets, is gratefully acknowledged.

IMPORTANT NOTICE

This document has been developed through the RISCAuthority and published by the Fire Protection Association (FPA). RISCAuthority membership comprises a group of UK insurers that actively support a number of expert working groups developing and promulgating best practice for the protection of people, property, business and the environment from loss due to fire and other risks. The technical expertise for this document has been provided by the Technical Directorate of the FPA, external consultants, and experts from the insurance industry who together form the various RISCAuthority Working Groups. Although produced with insurer input it does not (and is not intended to) represent a pan-insurer perspective. Individual insurance companies will have their own requirements which may be different from or not reflected in the content of this document.

The FPA has made extensive efforts to check the accuracy of the information and advice contained in this document and it is believed to be accurate at the time of printing. However, the FPA makes no guarantee, representation or warranty (express or implied) as to the accuracy or completeness of any information or advice contained in this document. All advice and recommendations are presented in good faith on the basis of information, knowledge and technology as at the date of publication of this document.

Without prejudice to the generality of the foregoing, the FPA makes no guarantee, representation or warranty (express or implied) that this document considers all systems, equipment and procedures or state-of-the-art technologies current at the date of this document.

Use of, or reliance upon, this document, or any part of its content, is voluntary and is at the user's own risk. Anyone considering using or implementing any recommendation or advice within this document should rely on his or her own personal judgement or, as appropriate, seek the advice of a competent professional and rely on that professional's advice. Nothing in this document replaces or excludes (nor is intended to replace or exclude), entirely or in part, mandatory and/or legal requirements howsoever arising (including without prejudice to the generality of the foregoing any such requirements for maintaining health and safety in the workplace).

Except to the extent that it is unlawful to exclude any liability, the FPA accepts no liability whatsoever for any direct, indirect or consequential loss or damage arising in any way from the publication of this document or any part of it, or any use of, or reliance placed on, the content of this document or any part of it.

Contents

Summary of Key Points

This document has been developed through the RISCAuthority and published by the Fire Protection Association (FPA). RISCAuthority membership comprises a group of UK insurers that actively support a number of expert working groups developing and promulgating best practice for the protection of people, property, business and the environment from loss due to fire and other risks. The table below summarises the key points of the document.

Exponential growth in cyber crime	• The incidence of criminal breach of IT resources is outpacing the roll out of IT services and growing in sophistication through more accurate targeting of victims.
Ignoring the risks is not an option	• The threat of criminal breach is pernicious —it is thought that an unprotected computer is compromised within minutes of first being connected to the internet and it has been found that security breaches remain undiscovered for an average of 229 days.
The impact can be unexpected	• The ways in which a criminal breach can damage an organisation are more varied than generally realised ranging from disruption and data loss or damage through leakage of intellectual property and denial of service to sabotage, extortion, statutory fines, damaged brand and impaired customer relations.
Comprehensive insurance protection becoming available	• Standard property and liability insurances are not designed to compensate policyholders for most types of cyber breach but specialist covers are becoming more widely available and are expected both to develop further and become more affordable as market experience is gained.
Security starts with basic precautions	• Experts are of the belief that the application of fundamental best practices on the part of IT controllers and operators would defend against in excess of 90% of the types of attack seen today.
Research and analysis required for bespoke protection	• Despite the existence of a national strategy for cyber security, users are faced with a large number of advisory documents, schemes and initiatives from a variety of official sources from which they need to put together a coherent security policy.

Symbols used in this guide

✓ Good practice

✗ Bad practice

≡ Discussion topic

FAQ Frequently asked question

1 Introduction

The fact that organisations' dependence on IT for efficiency, market advantage, or simply survival, grows every day, and that the rate and sophistication of cyber attack seems to be growing at an even faster rate, is creating widespread anxiety amongst users. Cyber security experts assert that it's only a matter of time before a given user suffers a security breach, and that users who believe they are free from infiltration 'are probably not looking in the right places'. It is known that cyber criminals can infiltrate an organisation's systems undetected for months or years.

Accounts of organisations suffering financial loss, reputational damage or heavy fines arising from their use of IT seemingly appear in the media on a daily basis. Many of these IT security breaches are caused by human or technical failure but malicious or gratuitous acts attract the most attention and cause the most alarm. Smaller organisations in particular are perplexed at the range and complexity of the issue and the fact that they can no longer assume the problem is largely one for larger targets.

The concern is well founded. PricewaterhouseCoopers claims that the number of cyber security incidents globally soared 48% to 42.8 million in 2014. The 2013 **Information security breaches survey** here in the UK found that security breaches had reached their highest ever levels and that the rise had been most notable for small businesses.

In some quarters it is said that the consequent damage to the confidence of users is putting their continued business use of the technology at risk. Similarly there could well be a risk that end users will start to think twice before dealing with banks, retailers etc online.

Estimates of the cost to the economy are unreliable but the cost to the UK alone has been estimated at £27 billion pa. The Ponemon Institute estimates that each data breach costs US companies approximately $5.4 million on average.

It is common for small businesses to just assume they are too small to be of interest to cyber criminals or that the information they hold would be of no interest. This is a dangerous assumption as small and medium-size enterprises (SMEs) are increasingly targeted and criminal motivations are frequently more sophisticated or complex than mere theft.

2 What are the impacts?

The following table shows how organisations are impacted by security breaches with examples of the types of intervention that are typically found to be the cause. These are restricted to breaches arising from the acts of those with wilfully negligent, vandalistic or malevolent motivations, whether within or outside the organisation.

Examples of impacts	Typical cyber security breach
Loss, degradation or unauthorised modification of digital assets and/or personal, customer and intellectual property, resulting in uncontrolled release of proprietary information and consequential erosion of competitive advantage, regulatory fines, civil litigation awards and costs, related costs eg customer notification expenses, credit agency fees, investigation and remediation, data restoration or recreation.	• physical theft of/damage to hardware/ software/data; • malware eg virus, trojan, backdoor, spyware, worm; • exposure of third party to malicious code under enterprise control; • hacking/hacktivism • fake, malevolent (eg anti-virus) software; • phishing; • exploitation of social media users to gain access; and • malicious act or omission of suppliers and service providers.
Espionage, allowing (eg) a competitor to gain competitive advantage.	• penetration of the organisation's stored data or communications channels; • phishing, trick etc;

FAQ

What exactly is a denial of service (DoS) attack?

In a successful DoS attack, a targeted computer server is saturated with incoming data or requests for a response such that it cannot respond properly, or at all, to legitimate traffic. Where the perpetrator has arranged for the attack to be mounted simultaneously from a number (usually a very large number) of surrogate computers (or 'bots' – internet robots performing repetitive instructions, usually forming the elements of a 'botnet') the attack is termed a 'distributed denial of service (DDoS) attack'.

Examples of impacts	Typical cyber security breach
Direct pecuniary loss	• phishing and similar cyber frauds; • extortion; • hacking/hacktivism; and • malicious act or omission of suppliers and service providers.
Theft/misappropriation of IT resources	• Trojan, worm, hacking, fake, malevolent (eg anti-virus) software.
Sabotage of IT assets and services	• denial of service (DoS) and distributed denial of service (DDoS) attacks; • hacking/hacktivism; • cyber terrorism; • cyber war/state sponsored aggressive act; • malware and fake software; and • website destruction, damage, defacement or unauthorised modification.
Third party bodily injury/property damage, litigation awards and costs.	• degradation/adulteration of cyber-based goods/services.
As above but extending also to staff on the organisation's premises.	• malicious intervention in the correct functioning of support services eg building services, through cyber vandalism, cyber terrorism, extortion bid.
Failure to perform to contract, litigation awards and costs.	• malicious cyber breach impacting customer supplied goods and services.
Malicious undermining of the activities of the organisation.	• theft (and subsequent wilful circulation) of sensitive information and communications eg concerning staff/associates; • injection of spurious email etc traffic, social media data; and • website defacement or modification.
Damage to reputation through revelation of organisation's vulnerability to, or inadequate measures against, cyber attack.	• any one or more of the above.

FAQ

What is a hactivism?

A 'hacker' in the context of cyber security is someone skilled at a keyboard in gaining access to a computer or network for an illicit or illegal purpose, or just for mischief, whereas, more specifically, 'hactivism' denotes hacking motivated by a political agenda.

3 Case studies

3.1 High profile hacks (and other breaches):

A recent notorious malware attack was the cause of an intergovernmental confrontation. Sony Corporation suffered its second major embarrassment when a significant cyber attack led to intellectual property and personal employee details being leaked online.

Numerous other household names have had their networks hacked for prodigious quantities of customer data. They include AOL, Adobe, J P Morgan Chase, Ebay, TJ Maxx, Staples, the NHS and HM Revenue & Customs. Often the infiltration is enabled through the use of illicitly obtained employee credentials.

Another common vulnerability in the US has been shown to be the information captured in retailer tills or the devices used by customers to swipe their cards (Point of Sale (PoS) skimming or malware attack). More prosaic causes include theft of physical media, as when the NHS lost the records of 8 million patients which were on a single laptop ‘found to be missing’. Similarly, there was a case of an AOL breach involving the theft of 92 million screen names and email addresses by a software engineer. Over 100 million US customers have been affected by cyber breaches in the past 12 months.

✗

A significant number of headline grabbing security breaches have been linked to the entrusting of IT assets to a third party service provider. It is all too easy to be focussed on in-house security and overlook the need to investigate, and set control conditions for, business partners.

3.2 Failure of physical security

Imposters, probably posing as computer technicians, attached a device to a Barclays Bank branch PC enabling them to control the PC and extract operator credentials etc, allowing the gang to transfer the money to their own account. The loss to Barclays was reported as £1.3 million. An example of how a cyber security breach can occur through a failure of physical and procedural security rather than network infiltration.

Similarly, the well known attack by (it’s alleged) US/Israeli agents on the Iranian nuclear project was said to involve no more than the insertion of a USB memory stick carrying the ‘Stuxnet’ virus into a PC under Iranian control. Then again, a current spate of a certain type of theft from ATMs is said to involve a physical, not telecommunications, breach of the ATM shell allowing insertion of a USB device that reprograms the machine. These are examples of how sophisticated IT can be compromised through the most unsophisticated of intrusion techniques.

✓

Robust physical security and access control are as important for IT assets as they are for physical assets.

3.3 Less conventional, unforeseen vulnerabilities

Numerous victims have lost sensitive information through the ‘Heartbleed’ attack method. This attack does not conveniently fit within one of the popular cyber attack categorisations. Rather than malware as such or a conventional hack of the victim network, an attack exploits one small element of code in popular software used by web designers to extract data that, until April 2014, had been considered encrypted and therefore secure. As of the date of this document, the total number of companies disclosing data breaches as a result of this security flaw is not known with confidence.

Similarly novel has been the ‘Game over Zeus’ (GO Zeus) attack, which steals online banking customers’ credentials and then takes control of the banking software, taking the place of the customer in transactions that lead to the transfer of funds to the attacker.

If, for any reason, the attack hits a problem, the perpetrator can change the attack so as to extort cash from the victim in a ‘Ransomware’ style attack eg ‘Cryptolocker’. Ransomware is malware that (usually) encrypts the files on the user’s hard drive and demands a ransom in return for which the attacker undertakes to remove the encryption.

The feature that marks out Game over Zeus as particularly sophisticated and challenging, and for which the IT business was not prepared, is that the malware is propagated and controlled via botnets rather than directly by the attackers. Botnets are networks of thousands of computers that, unbeknown to their owners, have been infected and compromised.

✓

It has become all too clear in recent times that cyber criminals find access easiest when using social media to trick staff – a clear cyber security policy that all staff can readily understand and apply is vital.

4 The role of insurance

Insurers classify risk as either 'first party' ie the exposure to risk of the insured's own assets, or 'third party', ie the exposure of the insured to the risk of incurring liability for its acts or omissions. Standard property and liability insurance policies provide cover that would include certain consequences of the security breaches described in this document but the extent of that cover is limited. Typically, the following would be included in one form or another in standard policies:

4.1 'First party' insurance

- Malicious damage to or theft of IT equipment of all kinds, usually with, sometimes without, a forcible and violent entry upon the insured's premises but excluding cover for any data lost or damaged along with the physical property.
- Replacement or restoration of computer systems records that are lost or damaged but not if a virus or unauthorised access to systems was involved. In practice, for most policies, the cause of the loss is restricted to fire and explosion and the condition that is typically applied by mainstream insurers allows for the cost of repair, replacement or restoration of such lost or damaged media to be reimbursed. There is no cover for loss consequent upon any of the high profile infiltration attacks such as computer virus, hacking, denial of service, theft of data etc and no compensation for interruption, loss of trade secrets, damage to reputation etc that such cyber attacks may cause. Indeed, outside the mainstream insurance market, ie in the Lloyds market and energy insurance sector, a clause (CL380) quite simply excludes cover for losses involving the use or operation of a computer for 'inflicting harm'.

4.2 Third party insurance

Standard liability policies only entertain bodily injury and property damage and usually exclude any form of loss or damage involving data or cyber infiltration, not least virus infection.

Third party insurance in the form of 'professional indemnity' cover protects the insured against claims arising from civil liability in the 'ordinary course of your professional services'. However the scope of standard cover is narrow:

- While cover may extend to cyber losses caused to third parties arising from loss of, or mishandling, data, allowing hacker attacks, spreading a virus, breach of privacy or copyright and defamation, frequently such breaches cannot be shown to have arisen as part of the 'professional services' and the cover fails.
- There may be a variety of ways the third party can demonstrate cyber loss through the act or omission of the insured but actual negligence must be shown as well. In many cases, negligence, as such, will not have been a factor.
- As recognised third parties are limited to the clients receiving 'the services', claims made by others, such as employees (eg for negligent handling of their personal data), payment card partners (eg for inadequate control of transactions), contractors (eg for allowing malicious access to their operation), are inadmissible.
- Certain causes such as virus transmission may well be excluded altogether.

4.3 Specialist cyber insurance

A widening of standard policy cover may be available in return for additional premium by way of endorsement of the standard wording. However, the wide spectrum of potential sources of risk is stimulating demand for much wider specialist insurance protection against cyber security breaches of all kinds, and a number of large 'composite' insurers, as well as small specialists and Lloyds operations, can now offer tailored cover.

The mosaic of cover wordings and policy conditions, varying substantially or subtlety, may seem a 'minefield' to the prospective policyholder so research and/or the services of a trusted advisor (eg a specialist insurance broker) is advised.

Computer systems that control plant, machinery and industrial processes, sometimes referred to as SCADA (supervisory control and data acquisition) systems, have enjoyed relative immunity from hacking and viruses, being traditionally separate from an organisation's main business IT. But this is changing as increasingly such systems are connected to the internet, frequently with inadequate cyber defences. It remains to be seen how big a problem this is seen to be and what implications there may be for personal injury.

Typically, the core covers of these specialist insurance products include:

First party risks:

- business interruption from network downtime;
- cyber extortion under threat of damage or release of data;
- reputational damage from loss of data leading to loss of business or customers;
- theft of, loss or damage to, equipment or digital assets; and
- forensic and recovery costs.

Third party risks

- security and privacy breaches, investigation and defence costs, civil damages;
- customer notification costs where there is a legal or regulatory obligation to notify them of a privacy breach;
- media issues involving defamation, breach of privacy or negligent publication leading to investigation and defence costs and civil damages; and
- loss of third party data including compensation for denial of access, failure of software or systems.

The above are typical core covers but coverage is by no means limited to these – there is no 'standard' cyber policy. Indeed, policies generally also provide assistance with, if not management of, incidents.

4.3.1 Data protection law penalties

In addition to the business risk from the types of cyber breach already mentioned, an insured party may be culpable in law if they infringe data protection (DP) legislation and might incur a fine as a result. In this connection it is significant that a new European General Data Protection Regulation is to be introduced that, unlike the situation currently in the UK, will oblige those in control of breached systems to report each incident to the DP authorities. The regulation is intended to fully harmonise data protection rules and enforcement throughout the EU and is expected to feature fines of €100 million or up to 5% of global corporate turnover, which would be a crippling amount for many companies.

The new legislation will have the benefit of vastly enlarging the present body of intelligence on attacks and shine a spotlight on system owners that fail to deal with their vulnerabilities. The Regulation could be finalised as early as the first quarter of 2015 but it seems more likely that it will be delayed to late 2015 or 2016, and then two years will be allowed for the transition from the current patchwork of national DP legislation.

At present in the UK there is uncertainty as to whether the availability of insurance protection for fines arising from DP legislation would automatically be open to challenge from the responsible authority and, if not, in what circumstances an insured may be able to recover. The situation should become clearer as legal precedents are set in the courts.

The picture in the US differs with mandatory reporting of breaches varying state to state. At present the Americans seem some way from agreeing consistent US-wide legislation on reporting. UK firms with a US business need to tap into the expertise of specialist insurers to ensure they have the protection necessary for their type of operation.

4.3.2 Future of specialist cyber insurance

Before leaving the subject of specialist cyber insurance it is important to recognise that this sector is writing insurance covers that are at the frontier of the market, pushing as they are against traditional underwriting methods based on 'classes' of cover that reflected the needs of commerce when insurance first became available. The assumption is that the developers of specialist cyber insurance products will continue to widen the range of contingencies for which protection is available. Those close to the subject think that cover for property damage and bodily injury arising from cyber attack (imagine, for example, the potential impact of the corruption of an aviation or marine navigation system) will not be long in coming.

It can also be expected that the purchasers of specialist cyber insurance products will refine their awareness of the risks and their particular needs. As a result they are likely to discriminate more knowledgably between insurance offerings which at present vary from one provider to another to the extent that significant differences exist between the range of terms and conditions, causation types covered and available compensation. Underwriting skill, risk appetite and available capacity also vary considerably in this market sector at present.

Looking forward, the specialist cyber insurance market will doubtless continue to expand and it is significant that government and the insurance industry are collaborating to promote the growth of the cyber insurance market as a means of improving cyber security risk management, with the side effect, through better actuarial data, of more accurate and affordable pricing.

5 Where to go for help

To be clear, this paper does not attempt to address security breaches arising from causes that cannot be said to follow from vandalistic or malicious types of act. Specifically, it does not discuss human neglect, carelessness or error, except in the context of such weaknesses being exploited by wrongdoers. Nevertheless most of the materials and sources that follow do tackle such issues and contain sound advice on such problems as:

- operational error;
- data corruption due to design or management issues;
- loss of portable devices and data storage;
- unsuitable software architecture, coding failures;
- careless or negligent act or omission of a supplier/contractor;
- failure to deliver cyber-based goods/services;
- careless or negligent management of custody of electronic media in the public domain;
- operational risks due to poor system design;
- inappropriate configuration settings and permissions;
- power and/or network problems due to inadequate specification; or
- skills or training deficits.

Understandably, most of the help available concerns attack prevention but experts point to the fact that, despite precautions, there is an inevitability that criminal penetration will occur given the evolution of criminal methods and their constant development. That being so, there has been a move by sophisticated users from investing mostly in prevention to focussing instead on detection and mitigation of the effects of intrusion. Will this thesis be more readily accepted by the security authorities and reflected in their advice to commerce?

It is likely that the continuous news of increasing cyber threat engenders a feeling of helplessness and inevitability amongst, particularly, the SME community. However, stakeholders such as customers, investors, regulators and the government itself are putting pressure on users to take responsibility for their IT security. Naturally, help is available from security businesses and consultancies but it is believed that by simply seeking out and implementing basic controls and countermeasures a barrier against a high percentage of likely attack scenarios for the average business can be created. However businesses in more exposed operations such as e-commerce have no choice but to ensure they receive the best possible bespoke advice.

There follows a selection from a wide range of freely available sources of guidance and information. Most contain pointers and internet links to various other documents and services that will be of interest, according to the searchers' needs. The sheer amount of, and variation in, available advice can be bewildering to a user anxious to pin down the action that needs to be taken but the absolute fundamentals are covered concisely in the first two publications listed and priority attention to these is recommended.

Cyber Essentials scheme

https://www.gov.uk/government/publications/cyber-essentials-scheme-overview

This high profile government scheme sets the minimum level of cyber risk controls for small business. It is also adopted by larger firms as a basic platform of good practice across the whole business. The scheme is designed for SMEs and identifies five basic and cost effective cyber controls which could, it is said, prevent up to 80% of computer security breaches. Users can self assess against the scheme or engage an external certifying body. The government requires suppliers bidding for higher risk contracts to be Cyber Essentials certified. Funding is available through the Innovation Voucher for Cyber Security scheme, albeit subject to budgetary constraints.

Ten steps to cyber security

https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility

This document also suggests the basic controls – in this case ten measures – that are judged as core precautions and supports each with scenarios.

Cyber security: what small businesses need to know

https://www.gov.uk/government/publications/cyber-security-what-small-businesses-need-to-know

This is a practical guide for small businesses on how to put simple and sensible cyber security measures in place.

Cyber Streetwise

https://www.cyberstreetwise.com/

Another government body aimed at the smaller business but also at individual users.

Get Safe Online

https://www.getsafeonline.org

Also providing practical advice for individuals on how to protect their computers, mobiles devices and their business against fraud, identity theft, viruses other online risks.

National Fraud Intelligence Bureau

https://www.cityoflondon.police.uk/advice-and-support/fraud-and-economic-crime/nfib/Pages/default.aspx

A City of London Police operation which harvests fraud data to provide actionable intelligence to the UK counter fraud community; embodies Action Fraud.

Action Fraud

http://www.actionfraud.police.uk/

A central point of contact for information about fraud and financially motivated internet crime.

Cyber Security Skills: a guide for business

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/290049/bis-14-649-cyber-security-skills-a-guide-for-business.pdf

A Department for Business, Innovation and Skills guide to the key opportunities for businesses to engage with cyber security skills and capability initiatives.

UK National Computer Emergency Response Team (CERT-UK)

https://www.cert.gov.uk/

Provides regular advice and guidance on a range of cyber issues to CiSP members (see below) with the aim of sharing information and encouraging best practice. News, alerts, best practice guidance and useful links are also freely available on their website.

Cyber-security Information Sharing Partnership (CiSP)

https://www.cert.gov.uk/cisp/

A joint industry government initiative to share cyber threat and vulnerability information in order to increase overall situational awareness of the cyber threat and therefore reduce the impact on UK business. Members receive a weekly Situational Awareness report which provides a summary of threats discussed on the site. The service has considerable potential but attracts few cyber crime victims at present. The London Chamber of Commerce is campaigning to have this service more widely promoted to the business community.

Information Security Forum (ISF)

https://www.securityforum.org

A member organisation which proffers opinion and guidance on all aspects of information security, particularly to the larger, more complex user.

Communications-Electronics Security Group (CESG, the information security arm of GCHQ)

www.cesg.gov.uk

Inter alia this body promotes a cyber Incident Response Scheme which enables victims of cyber-attack – SMEs, national and multinational industry, to source an appropriate incident response service tailored to their particular needs.

Business Resilience Centre

Launched in January 2015, this Mayor of London initiative, will help smaller businesses protect their assets using crime prevention advice, business-to-business alerts and through the creation of cyber security standards.

BS ISO/IEC 27001:2013 Information technology. Security techniques. Information security management systems

http://shop.bsigroup.com/

This is arguably the international 'Gold Standard' for current best practice providing specific recommendations to help establish an Information Security Management System (ISMS), monitor its performance and implement improvements where necessary. A number of reputable organisations offer recognised certification against the standard but the costs and complexity deter small businesses. These however have the option of certification against the government's Cyber Essentials scheme via, for example, an IASME (Information Assurance for Small and Medium Enterprises) accredited certification organisation. UK Government and EU grants ('Innovation Vouchers') are available via Innovate UK (previously the Technology Strategy Board) for organisations involved in projects with a high level of innovation.

Insurance industry sites

International Underwriting Association (IUA)

IUA members only: Cyber Underwriting Group (for carriers) and Cyber Interest Group (principally for market technicians). Contact: Scott Farley, director of communications, International Underwriting Association email: scott.farley@iua.co.uk

Cyber Risk & Insurance Forum (CRIF)

http://www.cyberriskinsuranceforum.com/

This cyber risk support forum is maintained by a number of providers operating in the Cyber risks insurance market. Recommended as an excellent source of news, advice and information.

RISCAuthority

administered by

FPA Fire Protection Association

Fire Protection Association
London Road
Moreton in Marsh
Gloucestershire GL56 0RH, UK
Tel: +44 (0)1608 812500
Fax: +44 (0)1608 812501
Email: administrator@riscauthority.co.uk
Website: www.riscauthority.co.uk

2015 © The Fire Protection Association
on behalf of RISCAuthority

S28 First published 2015 Version 01

Printed by: Quorum 0.75/02.15