Cybersecurity – Fighting Crime's *Enfant Terrible*

ACCA ima®

The Future Today

Abstract

The purpose of this report is to review the cyber-threat landscape, to discuss cybersecurity and its future trends and areas of concern, and to highlight particular areas that are likely to have direct impact on the future of accountancy.

As computers are playing an ever-increasing role in what finance professionals have to do on a daily basis, cybersecurity is becoming inextricably linked to such fundamentally important tasks as protecting the safety and continuity of the business, ensuring confidentiality of sensitive data and helping clients understand and manage a wide range of cyber-risks. Other key considerations are that cybersecurity is no longer a purely technical issue, and has become so complex that there is no single third party that a business can fully rely upon in order to stay secure.

Professional accountants and finance professionals have to step up to the challenge and learn how to survive the tidal wave of cybercrime.

About ACCA

ACCA (Association of Chartered Certified Accountants) is the global body for professional accountants. We aim to offer business-relevant, first-choice qualifications to people of application, ability and ambition around the world who seek a rewarding career in accountancy, finance and management.

Founded in 1904, ACCA has consistently held unique core values: opportunity, diversity, innovation, integrity and accountability. We believe that accountants bring value to economies in all stages of development. We aim to develop capacity in the profession and encourage the adoption of consistent global standards. Our values are aligned to the needs of employers in all sectors and we ensure that, through our qualifications, we prepare accountants for business. We work to open up the profession to people of all backgrounds and remove artificial barriers to entry, ensuring that our qualifications and their delivery meet the diverse needs of trainee professionals and their employers.

We support our 178,000 members and 455,000 students in 181 countries, helping them to develop successful careers in accounting and business with the skills needed by employers. We work through a network of 95 offices and centres and more than 7,110 Approved Employers worldwide, who provide high standards of employee learning and development.

www.accaglobal.com

About IMA

IMA® (Institute of Management Accountants), the association of accountants and financial professionals in business, is one of the largest and most respected associations focused exclusively on advancing the management accounting profession. Globally, IMA supports the profession through research, the CMA® (Certified Management Accountant) credential, continuing education, networking and advocacy of the highest ethical business practices. IMA has a global network of more than 80,000 members in 140 countries and 300 professional and student chapters. Headquartered in Montvale, N.J., USA, IMA provides localized services through its four global regions: The Americas, Asia Pacific, Europe, and Middle East/Africa.

www.imanet.org

For further information, please contact:

Faye Chua
Head of Business Insights, ACCA
+44 (0)20 7059 5975
faye.chua@accaglobal.com

Dr Raef Lawson
Vice President of Research and Policy
Institute of Management Accountants
+1 201 474 1532
rlawson@imanet.org

Table of contents

Acknowledgements

GARY★BROWN Certified Public Accountant

Gary R. Brown CPA, CMA

Managing Director at Gary R. Brown, CPA firm

Gary is managing director of a full-service boutique CPA firm based in Georgetown, Texas, specialising in tax, accounting, and business management services. Previous experience includes chief financial officer and senior finance and technical management positions with both multinational and start-up organisations located in Asia, Latin America, and the US. He holds an MBA from Texas Tech University and an accounting degree from Montana State University. Gary has held global leadership positions with the Institute of Management Accountants and is a past president of the Stuart Cameron McLeod Society.

ATKINS

Simon Cole FCCA

Group Financial Controller at WS Atkins PLC

Currently Simon is group financial controller and reporting director for WS Atkins plc, the FTSE 250 design and engineering consultancy that designs everything from roads to railways, hospitals to airports, not to mention the odd experimental nuclear fusion reactor.

Simon has held a number of roles since joining the Group and has previously been divisional FD for large parts of the Group, both in the UK and in the Far East. His roles have taken him to numerous countries as the company has grown from fewer than 2,000 to 20,000 people, located in five regions and over 30 countries.

HONG KONG COMPUTER SOCIETY

Dr Toa Charm

Founder and Chairperson, BI & Big Data SIG at Hong Kong Computer Society

Toa Charm is the vice-president of the Hong Kong Computer Society. Toa is a widely connected and reputable senior executive and information technology professional in Asia-Pacific. He has more than 25 years of management experience with leading multinational and Chinese companies in Asia-Pacific. He was an associate partner of IBM GBS Greater China, regional head of the BI Competence Centre for HSBC Asia Pacific, general manager of BI Division for Oracle Greater China and managing director of Hyperion Greater China. He specialises in strategy, business model innovation, digital transformation, business intelligence (BI) and big data, FinTech, customer experience and loyalty, and internationalisation for Chinese enterprises.

Bowden Jones solicitors

Faris Dean FCCA

Head of Business Services at Bowden Jones Solicitors

Faris heads the Business Services Department of Bowden Jones Solicitors. He advises and acts for clients on a range of matters including business sales and purchases, investment agreements, anti-bribery systems and data protection. Before joining Bowden Jones, Faris worked in law firms dealing with national and international commercial and corporate transactions. As well as practising as a solicitor for over 10 years, he is a qualified chartered certified accountant, having trained with two of the 'Big Four' international accountancy firms. His understanding of financial issues affecting business often helps provide another perspective when advising clients on corporate and commercial transactions.

Alex Erchov

Computer Technologies Consultant

Alex started his career as a software engineer and then gradually progressed towards technical management. In the early 1990s he was at the forefront of internet-orientated systems development, becoming an IT director of PeopleBank (The Employment Network) – one of the first large-scale online recruitment systems in the UK. Several management positions followed, and then eventually Alex chose a role of a consultant, helping his clients navigate the technology minefield in search of the best possible solutions for their business needs.

Matthew Harris ACA, ICAEW

Chief Financial Officer at Constain Group

Matthew was appointed finance director for the Natural Resources Division of Costain Group in November 2012. He has responsibility for the financial reporting and strategic planning of the water, power, and oil and gas sectors of Costain, as well as the integration of the recently acquired Rhead Group. Prior to joining Costain, Matthew was a director of Hanson Cement, and has previously held senior finance roles with American Water, Thames Water and BMW. Matthew qualified as a chartered accountant with Price Waterhouse, and became a fellow of the Institute of Chartered Accountants of England and Wales (ICAEW) in 2014.

Dr Darren Hayes

Director of Cybersecurity and Assistant Professor at Pace University

Darren is a leading expert in the field of digital forensics and cybersecurity. He is director of cybersecurity and an assistant professor at Pace University, New York. He is listed by Forensics Colleges as one of the Top 10 computer forensics professors. He has developed a computer forensics programme at Pace, including setting up a computer forensics research laboratory. As a forensics examiner, he has worked on numerous cases involving digital evidence in both civil and criminal investigations. For a number of years, Darren has served on the board of the High Technology Crime Investigation Association. In late 2014, he published his latest book, entitled *A Practical Guide to Computer Forensics Investigations*.

Shariq Khwaja

Information Technology and Services Consultant

Shariq is a freelance business consultant specialising in FinTech project management, who has successfully carried out initiatives for several high-profile partners, including the London Stock Exchange, Credit Suisse, Old Mutual, RBS and Lloyds Bank. He remains true to his software engineering roots and keeps his technical skills honed, continuing the development and testing of a set of algorithmic trading tools that he built as part of his MSc thesis.

Acknowledgements

Hastings Mtine FCCA, FZICA, LLB Unza

Managing Partner MPH Chartered Accountants

Hastings is the co-founder of MPH, which consists of three partners with over 80 years' experience between them. The firm was founded in 2011 and its major focus is provision of services to SMEs. Hastings sits on a number of committees, including ACCA's Global Forum for SMEs. He also sits on three local Plc boards and was last year honoured with 'The Lifetime Achievement Award for 2014' issued by the local institute and IoD for his contribution to the development of the accountancy profession. He wants SMEs to focus on ICT ingenious development while being mindful of security concerns.

Dilesh Magdani FCCA

Director of Finance Operations at Specsavers

Dilesh is the director of finance operations at Specsavers. He is an experienced senior professional and an award-winning leader. He has worked in multinational blue chip, private and VC-backed organisations and has experience across a variety of industries, including retail, utilities, manufacturing, distribution, food and beverage.

Dilesh is responsible for designing and implementing a global back-office footprint, and prior to this led the shared-service operations for Specsavers. He has previously created and led operations for Stella Travel Group and Premier Foods plc, and held various finance roles within National Grid plc, RS Components and T&N plc.

Rob Mutchell ACCA

BP Ventures' Chief Financial Officer and BP Alternative Energy Head of Finance

Rob holds two roles in BP as the chief financial officer for the Venture Capital unit and head of finance for the Biofuels division. As part of his remit, he serves as a non-executive director of two UK-based portfolio companies. Rob qualified as an accountant with ACCA in 1998, studying part-time while enjoying his first career as a professional footballer with Oxford United, Barnet FC and Stevenage Borough.

Phil Talbot

Head of Technical Services at Matrix Solutions

Phil has over 17 years' information technology experience. He is currently head of Technical Services at Matrix Solutions, a provider of business and customer intelligence solutions, bearing overall operational responsibility for all related physical assets, networks and communications, as well as systems architecture. Ensuring cybersecurity for the company to which clients entrust their data is one of Phil's topmost priorities.

Andrew Vorster

Technology Foresight Consultant at AndrewVorster.com

With more than 30 years' technology experience across a broad range of industries, Andrew has spent his entire professional career helping organisations understand and exploit the opportunities, and mitigate the risks, presented by new and emerging technology. He is a member of the World Future Society and recently left the position he had held for almost seven years as vice-president of technology research for Visa Europe, in order to develop his own business.

Emmanuel Walter FCCA

Director at Winfos Capital Ltd

Emmanuel is a highly accomplished and results-driven executive with more than 20 years' international experience in Europe and Asia. He has previously held various senior financial and operational positions for large businesses (c. US$500m and 2,000 staff), such as multinationals Dialog Semiconductor, GE and ABB Power, specialising in the industrial sector (energy, manufacturing/engineering, automotive/ EV, semiconductor) as well as in the Chinese market, where he has worked 10 years as CFO for a company manufacturing power-related equipment. He is highly experienced in managing JVs.

Belinda Young FCCA

Director at Centrecourt Group of Companies, Singapore

Belinda has been an ACCA member since 1986. Currently she is an ACCA Council member and also a member of the Qualifications Board, Global Forum for Business Law and Global Forum for Taxation. She set up an accounting firm 16 years ago and now has clients from over 15 countries and more than 18 different industries.

Voluntary work is very familiar territory for Belinda, having offered her services to a myriad of non-profit organisations for the past 10 years. She has served on the boards of charities and numerous finance and audit committees.

Foreword

Cybercrime gets so much attention and coverage from the media that there is a danger of its being perceived as a kind of familiar, omnipresent and inevitable ill force that everyone simply needs to accept and learn how to live with. In fact, nothing can be further from the truth.

Ng Boon Yew,
Executive Chairman,
Raffles Campus Pte Ltd
and Chairman, ACCA
Accountancy Futures
Academy

Cybersecurity is a complex issue and it can only be ensured if businesses and individuals appreciate that they themselves have to accept a large part of the responsibility for it, because neither governments and law enforcement nor IT professionals can be relied upon to provide adequate protection.

It is now essential but no longer sufficient to understand and follow the basic rules of cyber-hygiene, as cyber-criminals constantly find new and inventive ways of perpetrating crime, at many different levels. This report by ACCA and IMA emphasises that finance professionals need to keep an eye on the changing cyber-threat landscape and be wary of knowledge gaps. A 'head in the sand' attitude is not a viable option.

Right at the heart of this is the issue of clients' trust, which finance professionals have to keep, no matter what. For as long as cybercrime remains a threat to the trust that clients and customers have in finance professionals and companies, the future of accountancy depends on cooperation across the profession to help combat, and defeat, the '*enfant terrible*' of crime.

Executive summary

Throughout history, criminals always used advances in science and technology to try and gain a cutting edge in their struggle against law enforcement. From this point of view, cybercrime is the inevitable flip side of the 'Third Industrial Revolution', also known as the Digital Revolution.

The role of computers in the modern world becomes more and more prominent, but unfortunately so does the danger that the cybercrime presents. Naturally, anything to do with finance is of particular interest to cybercriminals: thieves tend to follow the money. Therefore cybercrime presents 'clear and present danger' for the future of the finance profession.

Compared with more traditional types of crime, cybercrime is new but it is proving to be a true *enfant terrible*, causing massive disruption and financial damage to individuals, businesses and governments. Recent years have seen consistent increases in the scope, scale and technical complexity of cyberattacks, and 2014 was definitely the worst year on record to that date. Attacks were extremely wide-ranging and included destructive cyber-assaults by nation-states, successful attacks on Cloud providers, targeting of social media, new advances in 'ransomware', and more.

As much as everyone would like to have an off-the-shelf 'silver bullet' solution to the problems that cybercrime presents, such a solution simply does not exist, nor can it: the problem is too complex, too diverse and too fluid. Law enforcement around the world is desperately trying to bring cybercrime under control, but this is proving to be a very difficult thing to do. Unlike mainstream criminals, cybercriminals operate in a borderless world and their activities often leave very little, if any, physical evidence. Their tools and techniques are

widely available to those who want to use them, and are often free. This and the balance of potentially huge financial gain versus relatively low operational risk make cybercrime a very tempting proposition for technically minded people with idle hands.

Consequently, the 'good guys' have to learn how to counter these new cyber-weapons, as well as how to build powerful weapons and protection tools of their own. This, however, presents a problem of its own, as lack of transparency and adequate monitoring of the development work for such weapons and tools can potentially lead to misuse and is being currently widely questioned. A recent survey by ACCA shows that finance professionals are not overly concerned about the pervasive capturing and storage of, and access to, information, sometimes referred to as 'living in a fishbowl', so the future of these developments is far from clear. For instance, legal aspects of data encryption, and indeed its validity, have been recently questioned at the highest level (government), although such discussions seem unlikely to have an immediate impact on the development of relevant technologies.

Another cybercrime issue that has to be considered is the increasing risk related to the use of new or quickly expanding technologies: mobile devices, contactless and mobile payment systems, the Cloud in its various incarnations, the IoT (Internet of Things), advanced personal authentication technologies, and, last but not least, social networking. While all these things are convenient and useful, they often introduce new security loopholes that cybercriminals look for and exploit.

Cybersecurity is no longer a purely technical issue; the impact of a cyber-breach is typically felt across every aspect of a business and often involves operational, reputational and financial damage, as well as regulatory penalties. What is needed, but is still often lacking, is a strategic approach to mitigating cybercrime risks. Professional accountants and finance professionals can, and should, play a leading role in defining certain key areas of such an approach: creating reasonable estimates of financial impact that different types of cybersecurity breaches will cause, defining risk-management strategy, helping businesses to establish priorities for their most valuable digital resources. They can also closely follow the work of governments and various regulators, in order to have clear up-to-date information on relevant legislation and on requirements for adequate disclosure and prompt investigation of cyber breaches.

Another vitally important aspect of cybersecurity is closely linked with maintaining clients' and customers' confidence. Safeguarding clients' trust and ensuring confidentiality of sensitive data is a vital task for any accountancy practice. Therefore, as computers and electronic documents are playing an ever-increasing role in what finance professionals do on a daily basis, cybersecurity must become one of the key concerns. This is especially true because cybercriminals often use the so-called 'lateral movement' approach, whereby they might target an accountancy practice in order to use its breached IT system as a stepping-stone for subsequent attacks on the victim's clients. Specifically with this in mind, it has to be accepted that no company is too small to become a victim of a cyberattack.

While there have been attempts by some governments and their agencies to create cybercrime information-sharing services, there is a strong argument for finding shortcuts for exchanging information about recent cybercrimes. The need to monitor what cybercriminals are up to might facilitate creating a 'Neighbourhood Cybercrime Watch' for the finance profession.

Escalation of cybercrime and concerns over the safety and security of digital assets have recently led to increased interest in cyber insurance; finance professionals can play an important role in helping businesses with adopting it.

Solving cybersecurity problems is a complex technical discipline that is arguably better left to professionals; but what is very important is firm knowledge of the basics of safety. Gaps in such knowledge are a huge risk factor, as even one small gap is often enough for the enemy to get in. Therefore, observing the rules of cyber-hygiene, being aware of the cyber-threat landscape, and making constant efforts to close one's knowledge gaps, are very important.

Professional accountants and finance professionals should always be mindful of the old saying: 'a fool and his money are soon parted'. Now, and for as long as the profession heavily relies on computers, no one can afford to be a cyber-fool.

1. Introduction

One of the first notable depictions of cybercrime in popular culture was in a 1969 comic caper film called *The Italian Job*, in which a gang of charmingly inept British rogues managed to pull off a gold bullion robbery.

The key part of the plan involved a clever, if slightly weird, mathematician disrupting the traffic of central Turin by planting a virus into the mainframe computer that controlled the traffic lights; there was also an accomplice whose hardware gadgets disrupted closed-circuit television (CCTV) monitors. At the time, all this must have seemed very funny and completely improbable. Almost half a century later, crimes like this are commonplace, and no one is laughing anymore.

Crime's *Enfant Terrible*

Cybercrime is still in its infancy: if we think of law enforcement history (starting from the Law Code of Ur-Nammu, c. 2100 BC) as the lifespan of a person who has lived up to the venerable age of 100 years, cybercrime's lifespan in comparison would be merely that of a one-year old toddler! Yet this *enfant terrible* has already claimed a unique place in crime history: it is causing massive disruption and damage to individuals, businesses and governments alike. Heads of state all over the world have to make it their priority to address cybersecurity issues. Many thousands of people have to be recruited and trained in order to combat the cyber-threat. We frequently see yet another headline-grabbing cybersecurity news report, ranging from high-profile security breaches and massive toxic data leaks to stories about misbehaving gadgets, such as the one that was recently reported as secretly recording conversations and then storing them online in an unencrypted format, without the knowledge of or prior consent from an unsuspecting user (BBC Technology 2015).

What makes it worse is the fact that the *enfant terrible* is constantly growing and becoming ever more powerful and dangerous. A recent study by a reputable cybersecurity expert estimated that the likely annual cost to the global economy from cybercrime, including both the gains to criminals and the costs to companies for recovery and protection, is simply staggering: it exceeds $445bn (McAfee 2014).

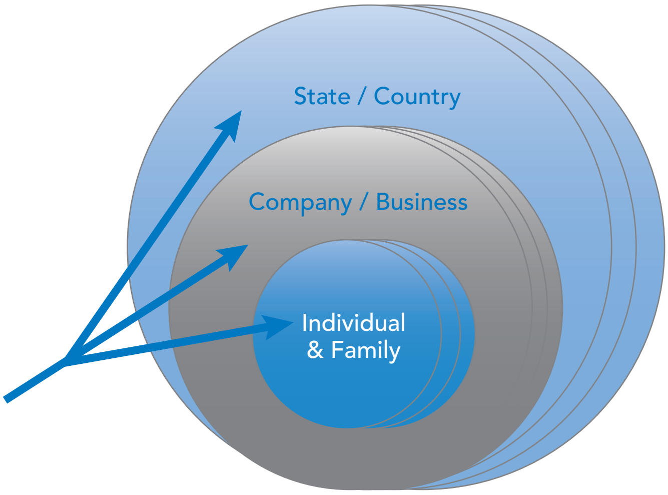


Figure 1.1: Target levels of cybercrime

Directions of cyberattacks are extremely diverse, with targets ranging from individuals and their families to companies and businesses and further up to state/country level, as shown in Figure 1.1.

For individuals and their families, within either their home environment or a public space, threat types include spam emails with malicious links or attachments, fake websites, unsecure wireless hotspots, a plethora of viruses, spyware and malware, removable media (USB drives and media players), social networking, all kinds of mobile devices and the apps that they run – the list is seemingly endless.

For companies, ranging from small and medium-sized enterprises (SMEs) to large corporations, one significant type of threat is the exploitation of different types of cybersecurity 'holes' within their IT infrastructure. Perpetrators include rogue nation states and terrorists, competitors engaging in industrial espionage, orchestrated crime, and individual hackers and 'hacktivists'. Another notable type of threat is action by dishonest or disgruntled employees who can steal valuable electronic data. Most types of threat for individuals (listed above) also apply in a business environment.

Finally, governments and their agencies and officials are also targeted. State-run services, ranging from Web-based information to critical infrastructure, are targeted too; infrastructure attacks might involve highly sophisticated malicious software, and attacks on Web-based information can be achieved by any of the threat types mentioned above.

Cybersecurity has become so important that it is being discussed at the highest levels of power and at the world's most prominent forums. For instance, it was addressed at the 2015 annual State of the Union Address in the US, during which President Obama categorically stated: 'No foreign nation, no hacker, should be able to shut down our networks, steal our trade secrets, or invade the privacy of American families, especially our kids. We are making sure our government integrates intelligence to combat cyber threats, just as we have done to combat terrorism...If we don't act, we'll leave our nation and our economy vulnerable. If we do, we can continue to protect the technologies that have unleashed untold opportunities for people around the globe' (The White House 2015).

These concerns are clearly echoed in many countries all around the world, as governments are trying to strengthen their cyber-defences by creating relevant agencies and introducing new legislation and regulatory mechanisms. The Cybersecurity Framework in the US (NIST 2014) and the National Cyber Security Strategies that are currently being developed by the European Union Agency for Network and Information Security (ENISA 2014a) are among the examples.

How does it affect the profession?

Cybercrime presents a number of threats for the finance profession. According to a recent study, the theft of financial assets through cyber-intrusions is the second largest source of direct loss from cybercrime (McAfee 2014). This is hardly surprising: as the saying goes, 'thieves always follow the money'.

A key consideration is that cybersecurity is no longer a purely technical issue; the impact of a cyber-breach is typically felt across every aspect of a business. What is needed, but is still often lacking, is a strategic approach to mitigating cybercrime risks. Professional accountants and finance professionals can, and should, play a leading role in defining certain key areas of such an approach. These include:

+ creating reasonable estimates of financial impact that different types of cybersecurity breaches will cause, so that a business can be realistic about its ability to respond to an attack and/or recover from it

+ defining risk management strategy (Table 1.1 below highlights different types of risk from cybercrime, depending on the nature of the attack targets)

+ helping businesses to establish priorities for their most valuable digital resources, in order to implement a 'layered' approach to cybersecurity

+ closely following the work of governments and various regulators, in order to have clear up-to-date information on relevant legislation and on requirements for adequate disclosure and prompt investigation of cybersecurity breaches.

Table 1.1: Impact of cybercrime: Types of risk according to targets of attacks

TARGETS FOR ATTACKS	TYPES OF RISK			
	Operational	Reputational	Financial	Regulatory
Business itself	•	•	•	•
Customers and their data	•	•	•	•
Clients and their data	•	•	•	•

Another vitally important aspect of cybersecurity is closely linked with an issue that is right at the heart of the accountancy profession: it is the vital task of maintaining clients' confidence. Since computers and electronic documents are playing an ever-increasing role in what finance professionals do on a daily basis, cybersecurity must become one of the key concerns. Note that cybercriminals often use the so-called 'lateral movement' approach, whereby they will target a company's IT system (for instance, that of an accountancy practice) not merely to get into that particular system, but in order to use the breached system as a stepping-stone for subsequent attacks on the victim's clients.

A 2015 survey by ACCA and IMA showed that professional accountants and other finance professionals clearly understand just how important this issue is: 85% of respondents said that management at their respective companies is sufficiently concerned about risks related to cybercrime (ACCA / IMA 2015). The same survey showed that 48% of the respondents are more concerned about cybercrime than they were 12 months previously (see Figure 1.2 for scores by region).

This report presents an overview of current and future cybersecurity threats and their impact on the accountancy and other finance professions.

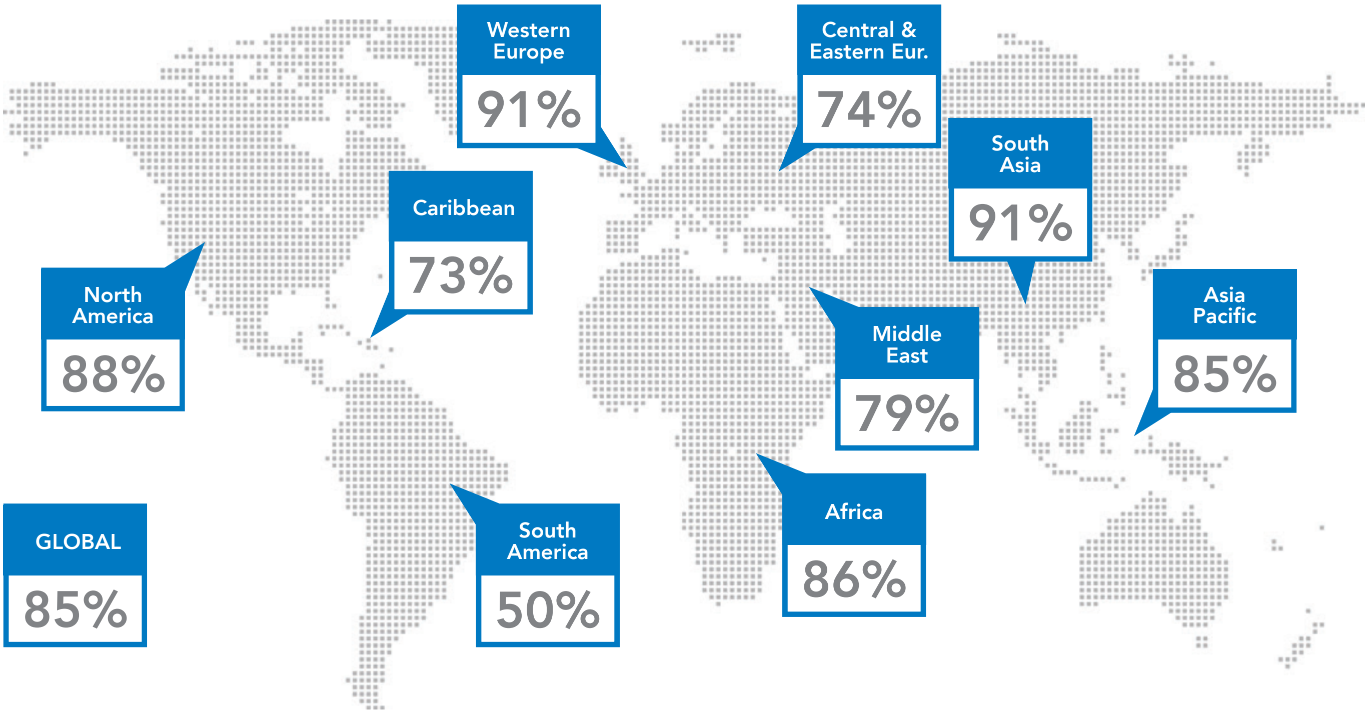


Figure 1.2: Percentage of respondents expressing concern about cybercrime (ACCA-IMA Survey 2015)

2. Review of the cybersecurity landscape

Notable cybersecurity breaches of 2014–15

The role of computers in the modern world, the amount and complexity of data, as well as the degree of interconnectivity of people and businesses that computers enable, all keep growing at such a great rate that the available technology is often not ready to meet the demand. Rushed technical solutions inevitably introduce new vulnerabilities within hardware and software, which criminals of all kinds are keen to exploit. Recent years have seen consistent increases in the scope, scale and technical complexity of cyberattacks, and 2014 was the worst year on record, up to that time. A recent survey suggested that in 2014 the annual estimated reported average financial loss attributed to cybersecurity incidents grew by 34% over the previous year; the total number of detected security incidents climbed to 42.8m, an increase of 48% over 2013; it was the equivalent of 117,339 incoming attacks every day (PWC 2015).

A visually striking way of presenting the scale of recent data breaches has been devised by Informationisbeautiful.net (see Figure 2.1); the size of the circle indicates the number of stolen records, and the Y-axis is ordered by time. Black market prices for hacked data are shown in Figure 2.2.

Directions of attacks were extremely wide ranging; they included:

+ destructive cyber-assaults on the US by nation-states; in February 2014 there was an attack on the Las Vegas Sands Corp, the world's largest gambling company – according to James Clapper, director of US National Intelligence, it was later established that Iran was behind the attack (Bloomberg 2015); this was followed by attacks on Sony Pictures Entertainment

+ successful attacks on Cloud providers (including celebrity photographs allegedly leaking from Apple's iCloud)

+ targeting of social media; for instance, hackers claiming to back Islamic State reportedly hacked Twitter and YouTube accounts of the US military command (BBC News 2015a)

+ further use of botnets, such as Zeus, Citadel and Asprox

+ the theft of around 14m current and former civilian US government employees' personal infomation

+ new advances in ransomware (such as Cryptolocker and Cryptowall), which can enter a computer system by stealth, gradually encrypt files using a genuinely unbreakable algorithm, and then demand a ransom in order for files to be decrypted.

The year 2015 is now thought to have been even worse than 2014. For instance, a circle high up on Figure 2.1 refers to Anthem, a health insurance company that suffered a loss of possibly as many as 80m records through a cybersecurity breach (the exact scope of damage is still unknown, as the investigation is in progress). The fact that cybercriminals are targeting health records is understandable, bearing in mind that the estimated black market price for a health record is twice as high as that of a bank record (see 2.2).

The most recent disaster, which was coming to light during the preparation of this report, involves mSpy, a company that develops software allowing parents to monitor their children and employers to track their employees. The exact scale of the breach is yet unknown but a security expert reported that hundreds of gigabytes of data had leaked, which he was able to verify by contacting some of the victims (Krebs 2015). The company later admitted to BBC news that 'it had been the victim of a "predatory attack" by blackmailers' (BBC News 2015b).

World's Biggest Data Breaches

Selected losses greater than 30,000 records
(updated 7th February 2016)

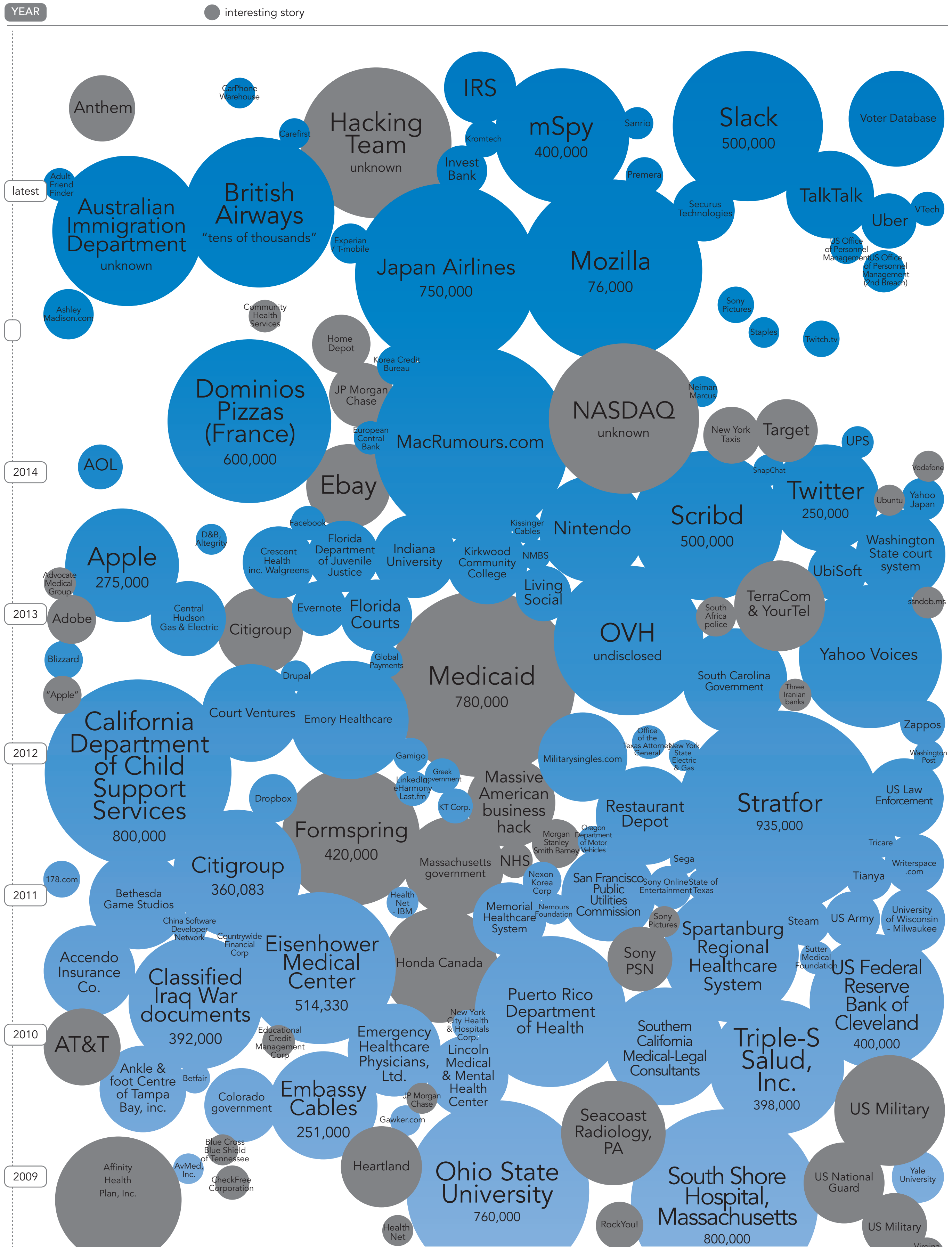


Figure 2.1: Recent data breaches. Source: Informationisbeautiful.net

How much is your hacked data worth?

Black market $ prices

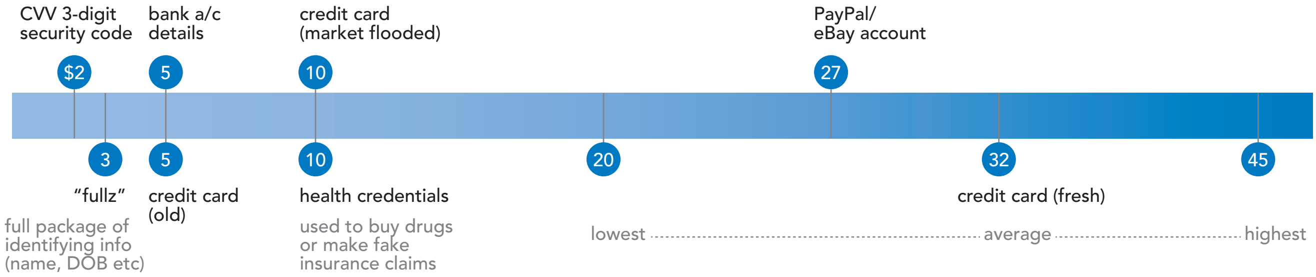


Figure 2.2: Prices for hacked data. Source: Informationisbeautiful.net

Crime and punishment – the cyber arms race

Advances in science and technology have always played an important role in the evolution of crime. This is perfectly understandable: technology makes crime more efficient and often gives criminals a cutting edge. For instance, the so-called 'Second Industrial Revolution' of the late 19th century introduced many inventions and new technologies that criminals quickly learnt to use to their advantage. As the quality of steel grew so did the power and reliability of personal firearms, allowing criminals to threaten their victims more effectively. As trains became more popular, so did train robberies, especially when banks started using trains to move large amounts of cash around. Development of automobiles meant that getaways became simpler; in addition, many new types of car-related crimes sprang to life.

Naturally, those who had to defend against crime had no choice but to rise to the challenge; law enforcement had to learn how to counter powerful new weapons, as well as how to build powerful weapons and protection tools of its own.

The Digital Revolution, also known as the Third Industrial Revolution, brought to life remarkable achievements in computing and electronic communications that are having profound effects both on society and on individuals. Unfortunately, the impact of this wonderful new technology on crime is equally profound, and so it is the old technology-driven 'crime and punishment' arms race all over again; but this time around the rules of the game have changed quite dramatically. Here are some of the changes worth noting.

+ Owing to the nature of the internet, we are living in an increasingly borderless world, and this means that many traditional barriers to crime, such as physical borders between countries, can be easily bypassed by cybercriminals. Furthermore, this often makes it difficult to tie a criminal to a specific location, creating jurisdictional headaches for law enforcement.

+ Cybercrime often leaves no 'traditional' physical evidence: in a 21st-century cyber-robbery, a crime scene does not offer such clues as skid marks, fingerprints or DNA samples. Consequently, cybercrimes can be very difficult to investigate; in fact, they often go completely unnoticed for days, weeks or even months. Therefore, in order to be able to find and trace the origins of the crime, a vast new discipline called 'computer forensics' is having to be developed.

+ A significant aspect of modern technology is the way it combines computing power and wide availability, benefiting everyone including criminals. Never before could the 'bad guys' do so much damage to so many, so quickly, and so cheaply. This certainly makes the development of serious planned profit-driven cybercrime very appealing; much cybercrime is a 'low risk, high reward' business.

- In order to build successful defences, an organisation has to defend all possible vulnerabilities, but mounting a successful attack needs only one place for a break-in. From this point of view, criminals always have an edge over those who safeguard. This is proving to be a vital factor because, owing to the nature of IT, where innovations are constantly introduced, any kind of system may often be riddled with security holes that no one knows or even thinks about – until criminals find and exploit them.

- Finally, the latest trends in cybercrime clearly show an escalation of advanced persistent threats (APTs) from terrorists and rogue nation-states, which target critical infrastructure providers and suppliers, as well as trying to steal trade secrets and intellectual property for political and economic advantage. This brings cybercrime to levels beyond what 'traditional' crime could reach before.

As a consequence of factors listed above, law enforcement is facing an increasingly difficult task, and there seems to be no clear winner in the arms race between cybercriminals and guardians of the peace. For as long as this is the case, every reasonable person and every responsible business cannot fully rely on the 'powers that be' to provide complete and adequate protection, and needs to understand what the dangers are and what needs to be done in order to build up successful cyber self-defence.

3. Future trends and areas of concern for cybersecurity

Raising the stakes

It is very likely that targeted attacks by terrorists and nation states aimed at governments and key infrastructure will continue in the near future. A recent report on the cyber-threat landscape confidently suggests that: 'taking into account resources and budget availability, hostile cyber-activities of nation states are a severe threat that can cause high defence costs, while creating severe impact both at governmental and corporate levels. Main targets of this threat agent group are state secrets, military secrets, data on intelligence, as well as threatening the availability of critical infrastructures. The degree to which performed attacks are successful can be considered as rather high' (ENISA 2014b). The same report suggests that cyber physical systems (CPS) – engineered systems that interact with computing equipment in a variety of areas such as power supply, medical systems or health care, industrial systems and manufacturing, transportation, telecommunication and others – will emerge as a target, especially within the scope of critical infrastructure protection (CIP).

In February 2015, the director of US National Intelligence placed cyberattacks from foreign governments and criminals at the top of the list of threats to the US. He identified computer system attacks by Russian, Chinese, Iranian and North Korean operatives as representing the biggest threat. He said that he no longer believed that the US faced 'cyber Armageddon', but he warned: 'We foresee an ongoing series of low-to-moderate level cyberattacks from a variety of sources over time, which will impose cumulative costs on US economic competitiveness and national security' (Taylor 2015).

In a noteworthy recent development, Russia and China signed a cybersecurity deal, agreeing not to conduct cyber-attacks against each other, as well as to exchange technologies and information between law enforcement agencies (Razumovskaya 2015). This might signify an effort by both Russia and China to challenge the dominant role of the West in internet governance. In addition to that, the agreement, according to an expert, 'will undoubtedly see the two nations strengthen their defences significantly, while freeing up offensive resources for deployment elsewhere' (Munson 2015).

Living in a fishbowl

A recent survey by ACCA showed that accountants and finance professionals are not overly concerned at present about the pervasive capturing, storage and access to information, sometimes referred to as 'living in a fishbowl'. Only 16% of all respondents selected it as one of the six factors that might have the largest impact on the profession in the medium term (3–10 years). This view may, however, be affected in the near future by the outcome of several current debates on the issues of privacy in the cyber-world.

The revelations of the former National Security Agency (NSA) contractor Edward Snowden made in 2013 for ever changed the way in which the world perceives the role that law enforcement agencies play in safeguarding cyberspace. Numerous highly classified documents stolen by Snowden and then released into the public domain with the help of the *Guardian* newspaper indicate the extraordinary levels of global technical surveillance conducted by the NSA and its allies. It purportedly involves tracking, each and every day, hundreds of millions, possibly billions of e-mails, phone messages and other types of electronic communication, which is achieved by tapping into the very backboneof internet infrastructure and having direct unrestricted access to the bulk of the world's internet traffic via data streams flowing through the largest internet service providers.

The true scale of the NSA's data monitoring capabilities is still hard to comprehend, and opinions about its legitimacy are sharply divided: some argue that 'living in a fishbowl' is safer and therefore pervasive surveillance is justified, while others insist that civil liberties have to be protected at all costs.

Some of these discussions go back to the 'technology arms race' between criminals and guardians of the peace that was mentioned earlier. If law enforcement is expected to provide adequate protection, then surely its agents need to have tools in their arsenal that are equal to the task? The answer to this question is not as straightforward as it might seem. There is, for instance, the issue of data encryption.

To encrypt or not encrypt?

In the wake of the aforementioned revelations by Edward Snowden, an average computer user would be forgiven for thinking that governments and secret services can now crack any data encryption. For instance, following increasing concerns over security of data flowing through internet, many popular service providers, including Google and Facebook, made a point of enabling data-encryption technology known as Secure Sockets Layer (SSL) for all their users. According to Snowden, however, the NSA already has the ability to either crack or circumvent this protection.

This certainly does not mean that all data protection is now pointless. For instance, PGP (Pretty Good Privacy) encryption still has a reputation for being unbreakable; it is the defacto industry standard and an encryption of choice for sensitive commercial and private communications. PGP is an open-source public-key cryptography software algorithm and has been in use for over 20 years. Its author, Phil Zimmermann, currently leads development of the enterprise privacy platform called Silent Circle, which promises fully secured encrypted voice and video calls, as well as text communication; also on offer is Blackphone, a fully secured encrypted smartphone hardware device.

+

> 'Governments around the world are facing a difficult task. On the one hand, they have to bring forward legislation to support the fight against cyberterrorism. But on the other hand, too much red tape will inevitably stifle innovation.'
>
> Dr. Toa Charm, Vice-President, Hong Kong Computer Society

In a notable recent development, a plan has been announced by the US government to mandate a type of data lock for which law enforcement agencies will hold a universal key. This would be not unlike the TSA-approved luggage locks that everyone travelling in the US is familiar with. The UK government seems to back this approach, which, according to Zimmerman, is 'absurd' (the *Guardian* 2015). Debates on this issue continue, with many arguments for and against, and with an outcome that is impossible to predict.

In the meantime, data encryption should always be considered when working with sensitive data; a stolen laptop is not going to be a security headache if all the data on it is securely encrypted. Encryption mechanisms such as BitLocker for Windows and FileVault for Macs are reliable, reasonably easy to implement and free to use; another option is to use self-encrypting hard drives (although this has to be done with caution).

Further risks from the development of new technologies

New emerging technologies will no doubt play an important role in, and therefore shape, the cybersecurity landscape.

+

> 'We are so reliant on connected devices that cybercrime now affects the whole of society – not just IT departments. It is of fundamental importance to all industries that individuals and organisations are aware of the threats and know how to defend against them.'
>
> Shariq Zahir, FinTech Consultant

Mobile devices continue to grow in numbers and ubiquity, which inevitably makes them appealing to cybercriminals. Personal data contained on mobile devices will continue to be targeted for identity theft, but the range of expected threats will widen to include new areas in which mobile devices will be increasingly used, such as access to Cloud data vaults, various business applications facilitated by flexible 'bring your own device' (BYOD) business policies, online banking and payment services, etc. This presents IT departments with new challenges, as they can no longer contain valuable data and hardware within a rigid perimeter that is easier for them to monitor and protect.

New and existing **mobile payment** systems, as well as **contactless payment** systems that use radio-frequency identification (RFID) or near-field communication (NFC), are also attractive to cybercriminals. One such system that is likely to be actively targeted is ApplePay, which is being energetically pushed to the market following the release of the iWatch.

Cloud is expected to play a key role in the future development of IT; consequently, Cloud data breaches, along with surveillance, will remain a major concern. New advisory and regulatory frameworks, as well as methodologies for due diligence checks and testing of performance and resilience are being developed to mitigate the risks.

Big data is going to present new opportunities for cybercrime because it potentially allows the so-called 'salami slicing' technique, whereby a large number of seemingly unrelated small data items can be tied together to reconstruct an overall picture and identify patterns that can be used for identity fraud, with devastating effect. There are also concerns over protection of sensitive information stored within big data.

The Internet of Things (IoT) is also likely to introduce quite a few surprises. For instance, someone with access to IoT data can get a very detailed view of a life in a so-called 'smart home', which could turn into a big privacy issue. Another potential issue is that poorly conceived hardware and firmware security can present hackers with gateways leading right into the hearts of private networks, with potentially disastrous results.

Social engineering, although not technical in itself, will be getting more prominent, feeding on the increasing availability and power of modern technologies. The scope of this type of threat is massive, ranging from identity fraud to getting access to highly sensitive corporate assets. For example, security of systems and data increasingly relies on people using their electronic passwords; while it might be difficult for a hacker to break into a well-protected system, it might be easy to identify a password-holder and use various social engineering techniques to trick them into giving a password away.

Another relatively new phenomenon that is being increasingly exploited by cybercriminals is our so-called '**online presence**'; someone can collect massive amounts of information about an individual or a company by tracking them online, and then use it to fabricate what is known as 'pretext' – an invented scenario that increases the chance that the victim will unwillingly divulge sensitive information or do something that they would never normally do.

New areas of **advanced personal authentication** will be of equal interest to cybercriminals. Computer users are slowly learning how to cope with complex and varied passwords, hardware security dongles, two-step authentication and other cybersecurity necessities. These are perceived by many as nuisance, so any solution that can promise simple and yet reliable personal authentication will always meet with enthusiasm. Fingerprints are already being widely used, with varying degrees of success. Other biometrics, such as iris scans, facial or voice recognition are also being tried. A Swiss company called Biometry is developing a method of biometric authentication based on simultaneous recognition of four concurrent factors: face, voice and lip movement, and random word recognition, while Halifax, a UK bank is trying out yet another new recognition technology, giving a customer access to the mobile banking application by checking their unique heartbeat pattern. There is, however, a serious inherent risk in biometric authentication when biometric data falls into the wrong hands.

4. Cybersecurity and the future of accountancy

Mitigating cybercrime risks

Professional accountants are well placed within business to help in dealing with the issues of risk management:

- they know how to quantify the costs and comparative cost-effectiveness of different security measures
- they typically possess required industry knowledge and understanding of the overarching strategy and end-to-end operation of the business(es) for which they work
- they have a well-deserved reputation for always being concerned with safety for their clients and employers; subsequently they tend to be cautious in dealing with innovations that have a potential to put safety at risk.

As cybersecurity is no longer a purely technical issue, and the impact of a cyber-breach is often felt across every aspect of a business, CFOs and finance professionals have an excellent opportunity to help their business mitigate various risks related to issues of cybersecurity.

> ‘Traditionally, companies have seen security as a binary thing – you either have it or you do not, and if you do the same highest level of security has to be applied to absolutely everything. However, there is a distinct trend towards ‘good enough’ security winning through.’
>
> Andrew Vorster, Technology Foresight Consultant

Historically, a typical approach to cybersecurity was to aim at providing equally comprehensive airtight protection to all available hardware and data assets. This has, however, become increasingly difficult and often impossible to achieve owing to several factors, including:

- a massive increase in volumes of data
- a demand for user mobility, and a corresponding mobility and agility of both hardware and data
- an unprecedented number and diversity of security threats, with new directions of attacks continuing to emerge at an alarming rate.

All this means that a different approach to cybersecurity is required that will involve a process of identifying, researching and assigning priorities to relevant risks. Questions that need to be answered include the following:

- What are the key assets that are under threat and therefore need protection?
- Where and how are they stored?
- Who has access and how are different levels of such access defined?
- What are the known directions of attacks and threat agents?
- What is the potential financial, operational and/or reputational damage?
- What are the possible regulatory penalties?

Another risk-related issue worth noting is the increasing importance of regulatory compliance in matters such as data retention and data disposal. Data offers great opportunities for generating revenue but it may also present a massive liability from a legal point of view, as development of data protection regulation around the world begins to make a significant impact on the way in which global businesses are required to approach the security of personal information. Professional accountants have to play an increasing role here, especially because data-related legislation is still far from being firmly established in any given country, and huge discrepancies in the implementation of such legislation and its enforcement exist all across the world.

Cyber insurance

Escalation of cybercrime and concerns over safety and security of digital assets have triggered increased interest in cyber insurance, and this is definitely an area for finance professionals to consider.

Cyber insurance is not a new concept. Cybercrime has been a business risk for quite some time now, and a common way of mitigating a risk is to transfer it, which can be done by taking insurance against it.

One of the key drivers for cyber insurance is legislation that requires mandatory notification of breaches, but such legislation is not yet implemented widely across the world. In addition, several other factors are slowing down the development and adoption of cyber insurance:

- company executives are often unaware that cyber risk is insurable, or they overestimate the coverage that their 'typical' business insurance would provide in the event of a cyber-breach

- the true level of cover that would be required for any given cyber-risk scenario is often very difficult to ascertain, owing to the number, complexity and interdependency of the relevant issues

- cyber insurance is not yet being widely used, and this means that there is not a great deal of reliable data within the insurance sector on which to base models; the technical complexity of cyber-crime issues and the speed with which new types of threat appear complicate things even further for insurers.

Professional accountants and finance professionals can play an important role in helping businesses adopt cyber insurance, by:

- establishing the types of incident for which cover should be provided, and estimating the costs that need to be covered

- researching the market and choosing the policy that is:
  - a good fit for the needs of the business
  - clearly defined and does not leave cover gaps, and
  - cost-effective

- making sure that the business fully understands the requirements of the policy and complies with them

- monitoring the policy to ensure that it remains current and keeping up with all the relevant compliance issues.

'I am a CFO and we have been hacked...'

To fight cybercriminals, we must know as much as possible about our enemies: their motives, tactics and technical means. In the ideal world this would involve getting detailed up-to-date information about crimes that have recently been committed. Unfortunately, such information is seldom available; this is understandable, as such information would often be of an extremely sensitive nature. Businesses would be reluctant to admit lapses in their security because of potential advantages that such admissions might give to competitors, and for fear of reputational damage. The sentence 'I am a CFO and we have been hacked...' was used when the problem was being discussed in the course of preparing this report.

Government regulators, such as the US Securities and Exchange Commission (SEC), are now paying increasing attention to the question of adequate disclosures in the event of a cybersecurity breaches. This does not mean, however, that information will be quickly made available in order to help other potential victims. There have been attempts by some governments and their agencies to create information-sharing services: for instance, Cybersecurity Information Sharing Partnership (CiSP) in the UK or InfraGard in the US. The NCSA (National Cyber Security Alliance) in the US is also worth mentioning here. The Protecting Cyber Networks Act that the US House of Representatives passed on 22 April 2015 (US Congress 2015) aims to remove some further legal barriers, so that American companies can share threat information with one another.

> 'Sharing information on cybersecurity is still rare, possibly because being better prepared is perceived as somewhat of a business advantage.'
>
> Faris Dean, Head of Business Services Department of Bowden Jones Solicitors

While all this good work is slowly building up momentum, there is a strong argument for finding shortcuts for exchanging information about recent cybercrimes across the finance profession: a Professional Neighbourhood Cybercrime Watch of sorts. A chance to exchange fresh information about current and new emerging trends in cybercrime and to issue crime alerts could be extremely useful for accountants and other finance professionals; it could help companies, especially SMEs, and potentially save hours of work and massive amounts of money. One possible way of doing it would involve an intermediary: an independent body that could collect such information, investigate where necessary, and then present its findings and recommendations in a strictly anonymous way.

No company is too small to become a victim

The plight of SMEs in fighting cybercrime deserves a special mention. From the technical point of view, small companies are exposed to many of the same types of attack as larger ones, and, despite their size, they may present a more tempting target for cybercriminals. They have fewer resources to build proper defence systems and therefore are likely to be an easier target, while the spoils of an attack may be enticing enough for criminals to take an interest.

A common scenario of a cyberattack is when criminals are not actually targeting the company whose IT network is being breached: the main objective is getting access to its clients. For instance, imagine someone in a finance department getting an email from their accountants, urging them to click on an enclosed link in order to view an urgent piece of new legislation – but in fact the email was sent by a criminal who had penetrated the accountants' individual computer or computer network in order to launch a devastating attack on their clients.

Unfortunately, it appears that no company is too small or too insignificant to become a victim.

As the resources of small companies are usually limited, covering all the minutiae of cybersecurity is often a practical impossibility; sometimes this has disastrous consequences. According to a recent UK study, becoming a victim of cybercrime costs smaller firms between £65,000 and £115,000, and those worst hit suffered up to six breaches a year, pushing the total cost even higher (BIS 2014). Having to pay such sums of money might easily push an affected small company out of business. Equally, maintaining the required level of trust among their clients is essential for a small accountancy practice; reputational loss due to cybersecurity breach can be truly catastrophic.

> ‘In this day and age, if you work as a tax agent, you usually have to file online on behalf of hundreds of clients, and each of them has a right to ask you: ‘How do you know that my data would be safe online?’
>
> Belinda Young, Director at Centrecourt Group of Companies

There is also another thing to consider. The changing nature of accountancy work, such as having to deal with digital data and to submit documents online, means that clients are starting to ask just how secure their personal data is, now that it travelling across cyberspace in electronic format. Professional accountants simply cannot find themselves in a position of not knowing how to provide a meaningful, detailed answer to questions like this, as this will undermine their clients’ trust.

Another thing to remember is that there is more to cyber-defence than keeping the IT infrastructure secure. Members of staff need to be fully aware of the dangers that cybercrime presents and of the relevant company policies and procedures. Such policies need to be clear on internet use (including access to personal email, social media and social networking websites) and on use of mobile devices. If the BYOD practice is in place, security needs to be facilitated by adequate hardware and software checks. Disaster recovery testing is definitely required; periodic security checks against the latest vulnerabilities, including external penetration testing, are also a good idea.

Finally, the rising profile of cybersecurity means that more and more help is being offered by governments and law enforcement agencies, so SMEs should be on the lookout for suitable opportunities to enhance their own security.

Minding the knowledge gap

In order to boost their products’ appeal to consumers, technology vendors often try to make it appear simpler than it actually is. When this succeeds (as it often does), a gap appears between consumers’ perception of technology and the reality of it. There is nothing wrong with that, in fact this is how it should be – for as long as someone ‘minds the gap’.

Consider the automobile industry, for instance – cars are highly complex and sophisticated products of design and engineering work; yet, many drivers do not know what is under the bonnet. The key reason for this is that, when it comes to driving a car, we are surrounded by safety nets. There are detailed well-written instruction manuals, dashboard indicators, service and petrol stations, emergency rescue services, mandatory insurance, government rules and regulations forcing regular check-ups. All this helps to keep us safe on the road, while reducing the required level of knowledge about cars to a number of simple procedures that are easy enough to follow. It has not always been like that; in fact, some 60 to 70 years ago the motor industry had a rather poor safety record. Things have changed since then.

Information technology provides nowhere near the ideal combination of safety and comfort for its customers, and cybersecurity is a prime example of that. Rapid development of new technologies means that new knowledge gaps appear all the time. One common way in which cybercriminals exploit this is via the so-called ‘scareware’, which tries to fool a user into thinking that their computer system or their data is in danger and suggests a clean-up service, for which a user has to pay.

> ‘I agree with “hybrid”. A person of the future should be able to be on both sides of the fence.’
>
> Gary Brown, Managing Director at Gary R. Brown, CPA firm

Existence of such knowledge gaps becomes a huge risk factor, which is why basic understanding of where the gaps might be, and timely risk analysis, become crucial: a 'head in the sand' attitude is not a viable option. Professional accountants and finance professionals should be well prepared to deal with this suite of problems, thanks to the logical and analytical skills that they have acquired through the very nature of their training and their work. Very often, all that is needed is making the first step by starting to ask the right questions and identifying the right people to ask for the answers. For those accountants who have a knack for information technology, there is a distinct opportunity to take on 'hybrid' roles that, in addition to core financial skills, would require understanding and hands-on experience with IT technologies.

Observing the rules of cyber hygiene

Computers have become an integral part of modern life to such an extent that the well-being of various computer-based echo-systems directly affects our ability to function properly. From this point of view, health-related comparisons are no longer merely a figure of speech; they are a statement of fact.

Importance of health and hygiene issues in the physical world is something that modern society understands well. Children are taught from an early age that they need to wash their hands and brush their teeth, whether they like it or not. Observing a healthy diet and dressing warmly when it is cold also do not require any convincing. A bout of flu means that physical contact with others needs to be reduced to a minimum, and tissues have to be promptly and safely discarded. There are painkillers available, and hospital emergency units will help if things are getting serious. Furthermore, there is clear understanding that health issues are by no means limited to individuals: viruses and harmful bacteria can spread, so public health is everyone's responsibility; failure to understand this is deemed antisocial, and in some cases even illegal.

When it comes to cyber hygiene, things are far from being quite so clear-cut. Unfortunately, people typically exhibit one or more of the following attitudes.

+ I do not care.
+ It is all too complicated.
+ The way I have always done it is the right way.
+ This is not my problem, other people are supposed to do it for me.

+ Regardless of what I do and how hard I try, bad things will happen.
+ There simply is not enough time to worry about all this. (This excuse is very common, owing to the ever-increasing pressures of modern life).

An 'acid test' that should always be used when any of the excuses listed above comes to mind is simple: try to apply the same excuse to issues of physical health and hygiene. Most of the time, it would seem ridiculous and so it should. In the cyber-world, all these excuses will become equally ridiculous as best practices become a de facto standard – that is simply a question of time but waiting could have serious consequences.

Two key considerations should be always considered by every accountant and other finance professional.

1. The cybersecurity of your own business and of your clients' affairs is inextricably linked to your personal cyber-safety and cyber-hygiene, and is therefore one of your professional, rather than merely personal, responsibilities.

2. Making even a small effort in the right direction can, and will, go a long way; a majority of security breaches attempted by unsophisticated actors (estimates vary between 80% and 90%) can be prevented by strictly observing basic rules of cyber hygiene.

Conclusion

Cybercrime has become a persistent business risk and its impact is now reaching across business and up to C-suite and boardroom levels. Despite its relatively tender age, it is potentially the most devastating form of crime; defending against it is by no means easy and is no longer limited to solving purely technical issues.

A chain is only as strong as its weakest link

Cybercriminals probe for all kinds of weakness: as the saying goes, 'a chain is only as strong as its weakest link'. Therefore, solutions would usually involve a mix of approaches covering technology, people and business processes. It is important to note the dangers of over-reliance on paper-based security policies. When such policies are not enforced they will be completely ineffective.

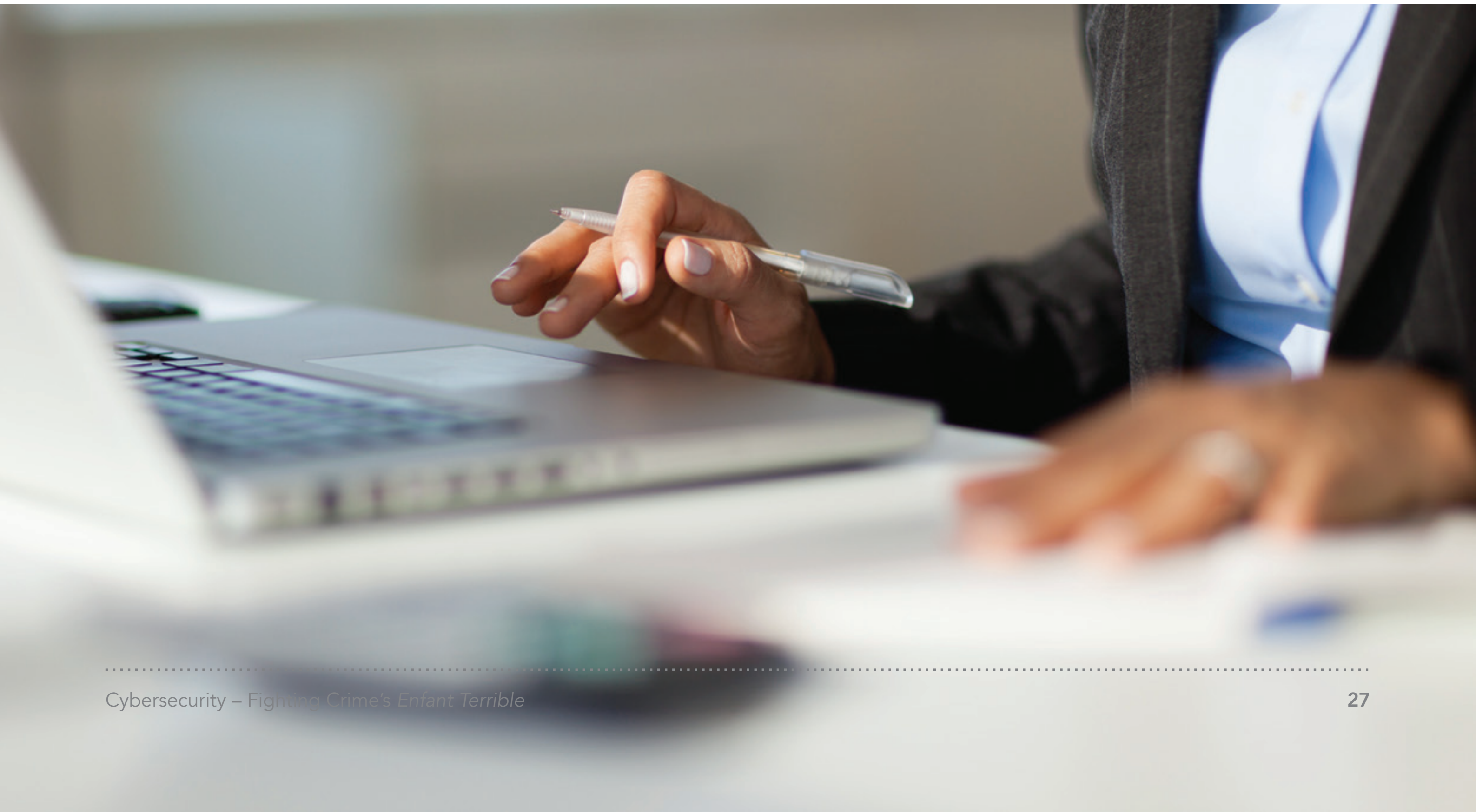
Accountants and finance professionals can, and should, play an active role in ensuring that their own businesses, as well as affairs of their clients, remain safe and sound. In order to do this, they need to be fully aware of the cyber-threat landscape and 'mind the knowledge gap'. Observing the rules of cyber-hygiene becomes extremely important, particularly because, with work and home life getting increasingly intertwined, the cyber-health of individuals in now inextricably linked to public and business cyber-health. Another key area is helping the business walk the minefield of cybercrime-related risk management, whether the risks are operational, reputational, financial or regulatory. A close collaboration across the business, and in particular between finance and information technology professionals, will naturally be required for that.

No 'silver bullet' solution

The benefits that the Digital Revolution has brought us are truly remarkable, but these benefits do not come free. The price that society has to pay includes the need to combat crime, whose perpetrators try, as they have always done, to use the benefits of new technology to their advantage and to the detriment of law-abiding folk.

As much as everyone would like to have an off-the-shelf solution to the problems that cybercrime presents, such a solution simply does not exist, nor can it: the problem area is too complex, too diverse and too fluid.

Professional accountants and other finance professionals should always be mindful of the saying: 'a fool and his money are soon parted'. Now, and for as long as the profession heavily relies on computers, no one can afford to be a cyber-fool.



Appendix A. A brief history of cybercrime – how it all began

Cybercrime, the *Enfant Terrible* in crime history, showed first signs of life in the early 1970s. As it happens, one of the first computer-related crimes ever recorded was finance-related: it was committed by an employee of the Park Avenue branch of New York's Union Dime Savings Bank, who used a computer to syphon over $1.5m from hundreds of customers' bank accounts.

During the 1970s and the early 1980s, computing work was mostly performed by mainframes, colloquially referred to as 'big iron' and dominated by IBM hardware. Computer networks were rare, and those that did exist were either extremely local or highly specific. The cybercrime of this era was mostly about tampering with billing and payment software within individual systems and typically involved banks and phone companies.

PCs (personal computers) began to spread widely in the early 1980s, and PC-related crimes quickly followed. Self-replicating software programs appeared and became known as computer viruses. At first, such viruses were being created as harmless (or rather, mostly harmless) fun 'toys' for geeks who were rather proud of their technical prowess; for instance, the first known PC virus, called 'Brain', was written by two brothers from Lahore and displayed their actual postal address and phone number! Soon, however, the so-called 'ransomware' appeared, where viruses and similar malicious software techniques were used for extortion; the first known ransomware was the 1989 'AIDS' Trojan, also known as 'PC Cyborg'.

The early 1990s notably saw yet another high-profile banking fraud, but this time the perpetrator was physically nowhere near the computer that had to be breached: Vladimir Levin, a Russian scientist, managed to access accounts of several large corporate Citibank customers via a dial-up service and transferred $10.7m to overseas accounts set up by his accomplices.

It was during the mid-1990s that the nature of computing, and consequently the nature of cybercrime, changed for ever. The internet was born, and its use spread like bushfire. Businesses and individuals around the world all rushed to take advantage of the new technology; as always throughout history, so did the criminals. The innovative nature of the internet, extremely rapid adoption of new technologies and the sheer excitement of new possibilities unfortunately often meant that security considerations were either completely forgotten, or simply put aside. Criminals quickly learnt how to use the internet to their advantage.

A flurry of internet-related criminal activities followed throughout late 1990s and early 2000s, now operating in the so-called 'cyberspace'. DDoS (Distributed Denial of Service) attacks were invented; they started as a nuisance pastime for rebellious teenagers looking for thrills (the list of companies that suffered included Yahoo, eBay, CNN.com, Amazon.com, Buy.com), but quickly turned into a powerful weapon for those who want to extort money or cause major disruption to Web-based services. Governments and military were also targeted by DDoS attacks launched by hacktivists, terrorists and rogue states.

As ISPs (internet service providers) grew, they naturally presented a tempting target. In 2005, Jason Smathers, a 25-year old America Online (AOL) software engineer, stole 92m screen names and e-mail addresses and sold them to spammers, who used the data to send out up to 7bn unsolicited e-mails. According to AOL, this cost the company at least $400,000, but possibly much more, up to millions of dollars. Smathers was sentenced to a year and three months in prison. 'Cyberspace is a new and strange place', he wrote in his letter to the court, 'I was good at navigating in that frontier and I became an outlaw' (NBC 2005).

Cyberspace did not remain a 'new and strange place' for criminals for much longer; its vulnerabilities were there to explore and exploit. During the breach of the TJX retail company in 2007, hackers managed to break into a WiFi network that was protected by WEP, one of the weakest forms of security for such networks. Over the course of several months, they stole data from the credit and debit cards of shoppers, allegedly 94m records in total. The ringleader, Albert Gonzalez, initially escaped undetected. Gonzalez became one of the most notorious cybercriminals; he was later sentenced to 20 years in prison for attacking another high-profile victim, Heartland Payment Systems. This was the biggest credit card scam in history to date, for which Heartland eventually paid more than US$110m to Visa, MasterCard, American Express and other card associations to settle claims related to the breach.

Security breaches have continued to escalate steadily throughout the late 2000s. New computer technologies driven by the ubiquitous social media and proliferation of mobile devices have brought exciting new opportunities for consumers but, to the same extent, they have given criminals new areas to conquer and new tools for doing so.

Appendix B. Basic safety practices

It is not the purpose of this report to give detailed descriptions of safety practices; however, a brief reminder of basics will be useful.

- Patches for operating systems, anti-viruses and trusted security software products on all computers and mobile devices need to be applied automatically, or at least promptly after they become available; there should not be an 'I will do it when I feel like it' option.

- The issue of passwords has to be treated very seriously; passwords should not be simple and should not be reused across many systems and websites, especially sensitive ones; password-managing software can help here.

- Two-factor authentication should be used wherever it is available; while sometimes being somewhat inconvenient, it provides an excellent safety net.

- Unfamiliar software should not be automatically presumed safe, regardless of where it claims to have appeared from and what its alleged benefits are; a little homework can go a long way. Equally, invitations to download anything from unfamiliar sources should be treated with the utmost caution.

- Access rights to hardware, systems and sensitive data need to be limited wherever possible.

- Removable media, such as USB drives and media players that have been in contact with unfamiliar computers should be considered unsafe until proven otherwise.

- Data encryption, which is becoming common for most computer systems, should be used wherever working with sensitive data is involved.

References

BBC News (2015a)
'US Centcom Twitter Account Hacked by Pro-IS Group' <http://www.bbc.co.uk/news/world-us-canada-30785232>, accessed on 2 October 2015.

BBC News (2015b)
'Child Spy Firm Hit by Blackmailers' <http://www.bbc.co.uk/news/technology-32800238>, accessed on 2 October 2015.

BBC Technology (2015)
'Not in Front of the Telly: Warning Over "Listening" TV' <http://www.bbc.co.uk/news/technology-31296188>, accessed on 2 October 2015.

BIS (Department for Business, Innovation and Skills) (2014)
2014 Information Security Breaches Survey: Technical Report <https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/307296/bis-14-767-information-security-breaches-survey-2014-technical-report-revision1.pdf>, accessed on 2 October 2015.

Bloomberg (2015)
'Iran Behind Cyber-Attack on Adelson's Sands Corp., Clapper Says' <http://www.bloomberg.com/news/articles/2015-02-26/iran-behind-cyber-attack-on-adelson-s-sands-corp-clapper-says>, accessed on 2 October 2015.

ENISA (2014a)
An Evaluation Framework for Cyber Security Strategies <http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/an-evaluation-framework-for-cyber-security-strategies-1/an-evaluation-framework-for-cyber-security-strategies/at_download/fullReport>, accessed on 2 October 2015.

ENISA (2014b)
ENISA Threat Landscape <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014/at_download/fullReport>, accessed on 2 October 2015.

Guardian (2015, Feb 2)
'Tech Pioneer Phil Zimmermann Calls Cameron's Anti-Encryption Plans "Absurd"', *Guardian* (2 February) <http://www.theguardian.com/technology/2015/feb/02/encryption-phil-zimmermann-david-cameron?CMP=share_btn_tw>, accessed on 2 October 2015.

Informationisbeautiful.net
World's Biggest Data Breaches, <http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/>, accessed 15 Febrauary 2016.

Krebs, B. (2015)
'mSpy Denies Breach, Even as Customers Confirm It' <http://krebsonsecurity.com/2015/05/mspy-denies-breach-even-as-customers-confirm-it/>, accessed on 2 October 2015.

McAfee (2014)
Net Losses: Estimating the Global Cost of Cybercrime <http://www.mcafee.com/uk/resources/reports/rp-economic-impact-cybercrime2.pdf>, accessed on 2 October 2015.

Munson, L. (2015)
'Russia and China Sign Cyber Security Pact, Vow Not to Hack Each Other', *Naked Security* (11 May) <https://nakedsecurity.sophos.com/2015/05/11/russia-and-china-sign-cyber-security-pact-vow-not-to-hack-each-other/>, accessed on 2 October 2015.

NBC (2005)
'Ex-AOL Worker Who Stole E-mail List Sentenced' <http://www.nbcnews.com/id/8985989/#.VV93w0acHud>, accessed on 2 October 2015.

NIST (2014)
Cybersecurity Framework <http://www.nist.gov/cyberframework/>, accessed on 2 October 2015.

PWC (2015)
The Global State of Information Security Survey 2015 <http://www.pwc.com/gsiss2015>, accessed on 2 October 2015.

Razumovskaya, O. (2015)
'Russia and China Pledge Not to Hack Each Other', *Wall Street Journal* (8 May) <http://blogs.wsj.com/digits/2015/05/08/russia-china-pledge-to-not-hack-each-other/>, accessed on 2 October 2015.

Taylor, G. (2015)
'James Clapper, Intel Chief: Cyber Ranks Highest on Worldwide Threats to U.S.', *Washington Post* (26 February) <http://www.washingtontimes.com/news/2015/feb/26/james-clapper-intel-chief-cyber-ranks-highest-worl/?page=all>, accessed on 2 October 2015.

US Congress (2015)
H.R.1560 – Protecting Cyber Networks Act <https://www.congress.gov/bill/114th-congress/house-bill/1560>, accessed on 2 October 2015.

White House, The (2015)
State of the Union Address, 2015, <https://www.whitehouse.gov/the-press-office/2015/01/20/remarks-president-state-union-address-january-20-2015>, accessed on 2 October 2015.

ACCA ima®

The Future Today

ACCA

29 Lincoln's Inn
Fields London
WC2A 3EE
United Kingdom
+44 (0)20 7059 5000
www.accaglobal.com

IMA

10 Paragon Drive, #1
Montvale, NJ
07645
USA
+1 201 573 9000
www.imanet.org