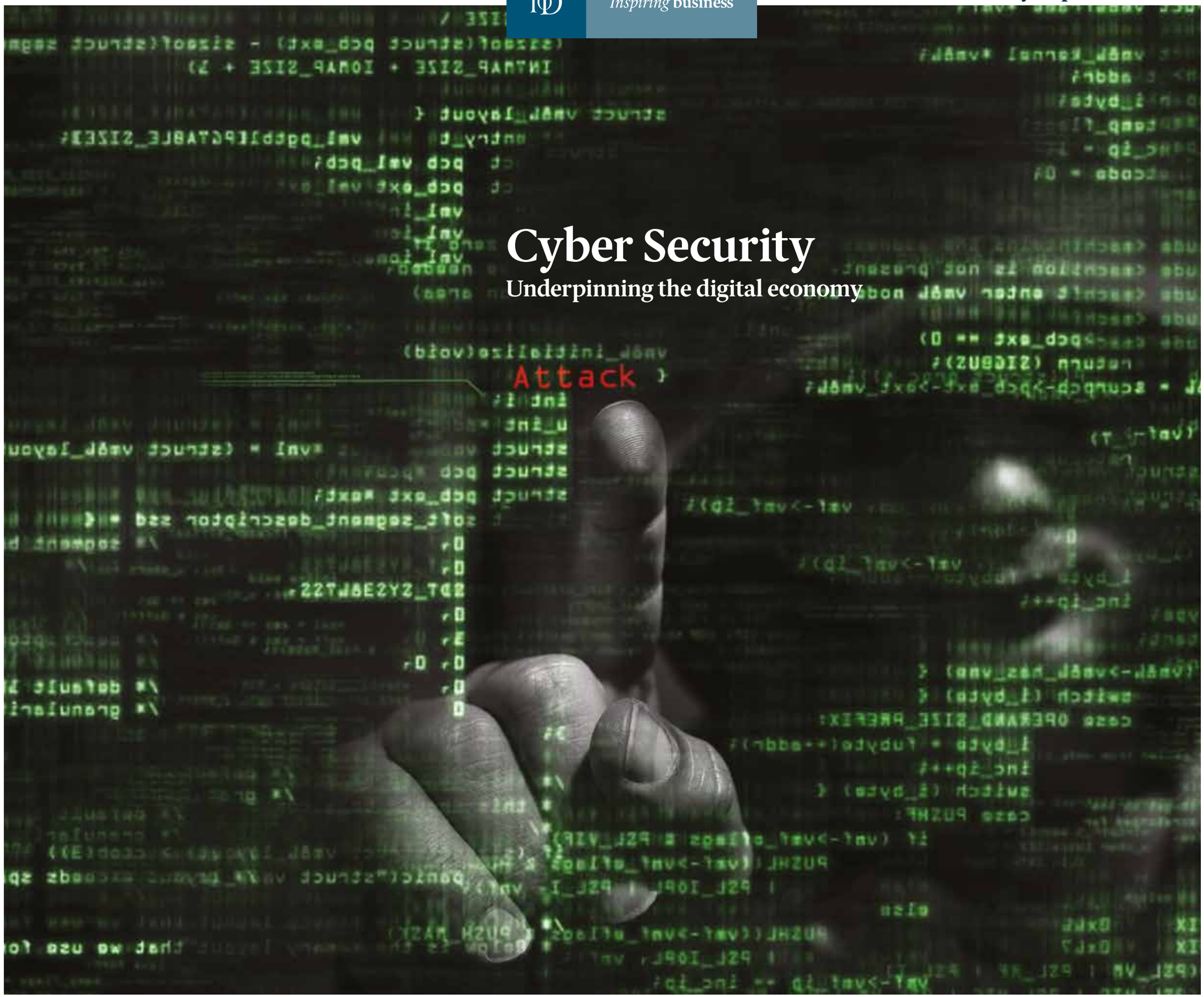
Inspiring business

Cyber Security

Underpinning the digital economy



Institute of Directors

For further information on this report, please contact:

James Sproule
Chief Economist and
Director of Policy
020 7451 3113
james.sproule@iod.com

The Institute of Directors

The IoD has been supporting businesses and the people who run them since 1903. As the UK's longest running and leading business organisation, the IoD is dedicated to supporting its members, encouraging entrepreneurial activity, and promoting responsible business practice for the benefit of the business community and society as a whole.

www.iod.com

Training
Events
Networks
Mentoring
Research
Influencing

BARCLAYS

Foreword from Barclays

Adam Rowse
Head of Business Banking

"In today's digital age, people are increasingly carrying out their daily tasks and choosing to transact online. Therefore, it is critical that businesses recognise the threat cybercrime poses and take the necessary measures to ensure the continuity of service while maintaining security and building trust with their customers.

"This requires on-going investment to ensure internal systems and processes remain robust and secure as well as a focus on supporting and educating customers to help them protect themselves from potential cyber attacks. We also recognise the shared benefits of coming together as an industry to strengthen our cyber resilience which is why we welcome this White Paper from the Institute of Directors which serves to shine a light on this important issue."

Barclays' partnership with the IoD is part of the bank's commitment to protect its customers by raising awareness of the importance of cyber security and the impact of cybercrime. Since 2014, Barclays has provided free training to anyone who needs help with using technology through their Digital Eagles, in-branch staff who provide free digital support to customers and non-customers. This training includes how to stay safe online. In January 2016, Barclays ran a new TV ad to help people understand how they could protect themselves from falling victim to fraud. It has also partnered with the government by being part of the UK's new joint fraud taskforce. Later on this year Barclays will host a series of events specifically for businesses providing guidance on how they can protect themselves from cyber crime. Further information on how to be cyber-smart can be found by going to www.barclays.co.uk/fraudsmart

BARCLAYS

Overview

Cyber security was once the quintessential boring-but-important subject: no longer. Today cyber security is critically important to any business which wishes to operate online, in the cloud, or engage with social media. In other words, every company in more or less everything they do has to be aware of the threats and challenges. This report seeks to examine and highlight some of the key areas that will affect UK businesses in an ever-changing digital world over 2016 and beyond.

It is striking that when we stop and look back over the events of 2015, we only then truly realise the pace of change in technology and its increasing impact on the UK, be it in the public or private sectors. The UK is at the forefront of e-commerce, indeed it leads the world in terms of percentage of the economy that is online, 12.5%[1], all great and good, but such a leading position also leaves the country uniquely vulnerable to cyber attack.

We have grown accustomed to seeing technology changing at an ever-faster pace and for the most part people have been happy to embrace the revolution, ushering in businesses and processes which have allowed greater productivity, better customer experiences and a reduction in costs. The internet continues to allow new and existing business of all sizes to access and trade digitally at ever increasing levels in a global marketplace.

In part it is always going to be challenging countering a global threat with domestic UK law and practices, but there is also the opportunity for the UK to set the global standards and best practices in a threat that businesses and consumers will undoubtedly face as time goes on. As a consequence global distributed threats have emerged. These are not restricted by geographic boundaries and are targeted at everyone from governments and global corporations to individual citizens. The threats we see today are at an all-time high in terms of sophistication and volume and these variables will only increase as consumer demand for quicker and easier interaction comes at a price.

Traditionally a definition of cyber security would be to describe it as the protection applied to computing devices and networks including hand-held devices that cover the whole internet. By this definition there are few areas left in the world where this does not have an impact. This is also where most money has been historically spent by governments and businesses to protect themselves.

> **"The effect of a cyber attack on an organisation or individual has a destructive cascading effect on both the connecting technology and human aspects that are linked. The extent of the destruction depends on the awareness and protection levels built around the sequential points of the attack."**

[1] Boston Consulting Group; 1 May 2015 Press release; "The Internet Now Contributes 10 Percent of GDP to the UK Economy, Surpassing the Manufacturing and Retail Sectors."

This paper seeks to reinforce that the future of cyber security lies in its extension into the human behaviours when interacting with faster and contactless technologies, many of which directly impact operationally on businesses.

The Cyber Ripple Theory describes the future threat landscape for us all. It states that:

"The effect of a cyber attack on an organisation or individual has a destructive cascading effect on both the connecting technology and human aspects that are linked. The extent of the destruction depends on the awareness and protection levels built around the sequential points of the attack."

The sudden rise of Intelligent Environments[2] and the Internet of Things[3] will present life changing benefits with associated rippled risks to us all. How we as humans interact and have trust in these developments will define our vulnerability.

In short cyber security is no longer just about the protection of technology, it is also the protection of ourselves in our digital environment. This environment stretches from infrastructure, for instance energy distribution networks, to particular smartphone apps, to the broader Internet of Things. The fragility of the economy as a whole was brought home in the lorry drivers' strike of 2000, where a short disruption in supply exposed the economic fragility of much of the UK economy. Given the speed at which the UK is adopting e-commerce, this fragility is only set to increase, and as it increases the importance of an effective cyber security plan rapidly grows.

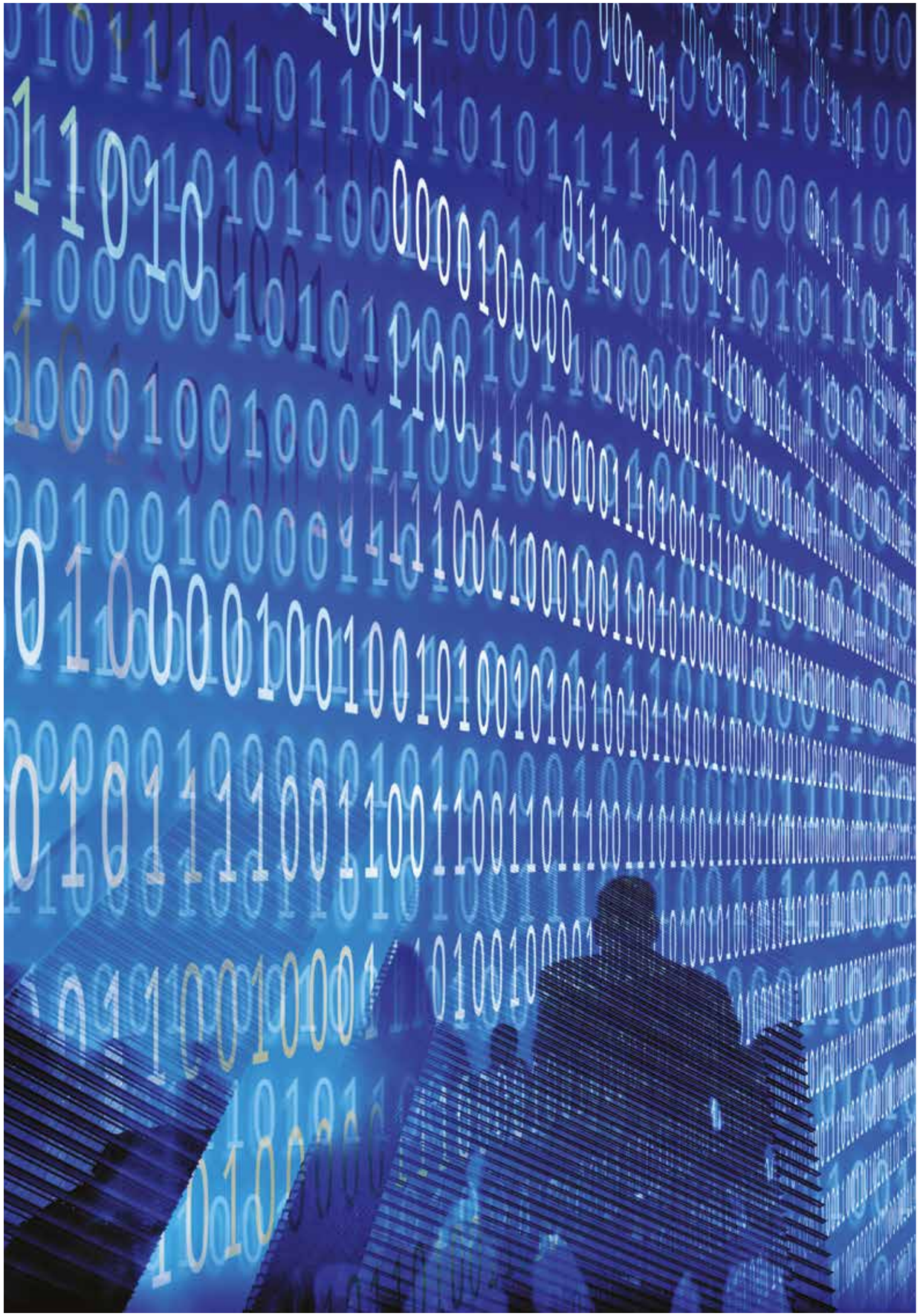
For businesses and organisations, we are also seeing the rise of "economic cyber terrorism" where an individual, organisation or state is using the fear of cyber attacks and exposure of vulnerabilities by social media to economically ruin it through loss of reputation and customer trust.

Key messages:

- **Cyber security is a hygiene issue; businesses expect other businesses to get it right, and a failure to do so will be seen as a dereliction of duty**
- **SMEs may well take the strategic decision that the cyber threat means they can access greater expertise and trading safety through the outsourcing of their IT needs.**
- **Cyber is a rapidly evolving market and with new approaches and offerings proliferating, and costs likely to fall, directors should resist locking themselves into long-term contracts.**
- **Reputational damage from cyber security lapse is likely to be uninsurable, and could potentially be fatal.**

[2] Intelligent Environments are spaces that have embedded technology and communication capabilities creating a space that is interactive with humans and enhances their experience. Commonly today this is through a mobile phone reacting to preferences held on it; however this capability is set to expand hugely over the coming year(s).

[3] The Internet of Things can be described as the emergence of a network linking everything that can collect, store and exchange data. This can include devices, computers, vehicles, buildings: in fact anything with network connectivity.



The Institute of Directors Cyber Survey 2016 – key findings

The IoD conducted a Policy Voice Survey[4] focused specifically on cyber security, investigating how fast the pace of technology is changing our members' attitudes and views on cyber security.

[4] December 2015 survey of IoD members from across the UK, based on 980 complete responses.

1% **Only 1%** of the members surveyed said their organisation was completely unreliant on the internet

This isn't a surprising statistic and makes clear that UK businesses and the economy are dependent on the internet to operate, and that the integrity of the internet is paramount.

91% **91%** said that cyber security (defined as firewalls, anti-virus, encryption, etc) was important to their organisation

It is standard for any computer or network to have these safety features built in upon purchase and the awareness of users with anti-virus protection is well marketed. What becomes interesting is how many of these features are kept up to date; an answer I suspect few would wish to admit to.

57% **Only 57%** said they had a formal cyber/information security strategy

This was an encouraging response; however the challenge is ensuring that any strategy is of a minimum common standard and that it is updated as part of a regular risk review. There is a consensus that it would be prudent for audited company accounts to include this as a specific item.

49% **49%** said they provided cyber awareness training for staff

Any cyber security strategy should include awareness training to be effective. The biggest risk as technology becomes more sophisticated is human failure.

6% **6%** said they spent nothing on cyber security over the past year

Quite often cyber security forms part of an IT budget and any distinct spending is not normally a priority outside of this unless you have been a victim of hacking. I would hope next year for this figure to be approaching nil.

49% **49%** said the biggest damage was interruption to business

In total, one in eight members experienced damage due to a cyber attack that interrupted business. The implication of this figure is that anti-virus software/firewalls are not being used effectively either by the business or their provider. While loss of reputation was significantly less, its impact can be devastating if the business concerned relies on customer trust (e.g. bank or online retailer).

11% **11%** of these suffered an actual financial loss

It is normally difficult to quantify intangibles such as loss of reputation, unknown lost sales, staff morale however this figure shows that cyber crime does hit the bottom line.

28% **28%** of these attacks were reported to the police

Many police forces have dedicated cyber crime units. However, it is recognised that as a global crime committed anywhere in the world the challenge of tracking and punishing criminals is huge. The use of analytics and the role of GCHQ in catching international cyber criminals mean that every crime as a minimum should be reported to Action Fraud Aware.

68% **68%** of members were unaware of Action Fraud Aware

Action Fraud Aware[5] is the UK's national reporting centre for fraud and internet crime which people should report to if they have been defrauded, scammed or experienced cyber crime.

[5] Its telephone number is 0300-123-2040 or visit www.actionfraud.police.uk

59% **59%** said they outsourced their data storage

The model of outsourcing data storage is only set to increase due to its financial advantages for organisations. This makes perfect sense; however the need to ask certain questions is vital and is covered as one of the topics of this paper.

43% **43%** didn't know where the data was physically stored

This is a truly frightening statistic. It effectively means businesses are losing control of their organisation's data which may well be the biggest asset of a business.

20% **20%** hold cyber insurance with **21%** unsure

With the threat of cyber attacks becoming more frequent and some household names providing credible case studies, it is no surprise that many are predicting that cyber insurance cover will become a 'must have' for businesses. The next survey will, I predict, show a figure nearer 90%.

21% **Only 21%** are considering cyber insurance within the next 12 months

Over the coming years, it is likely we will see IT and cloud providers introducing cyber insurance as standard. Any organisation is taking an unnecessary risk by avoiding this step, but even then cyber insurance is no silver bullet.

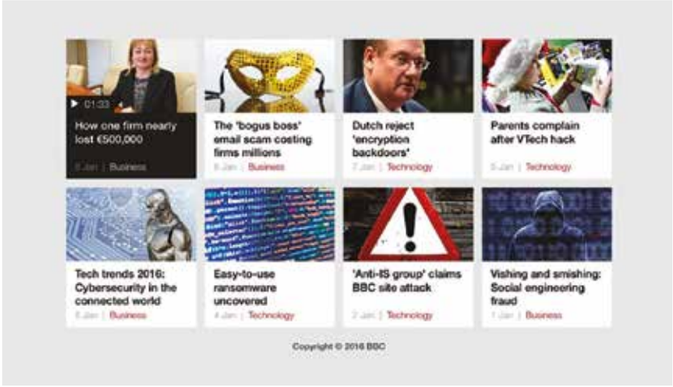
72% **72%** had received bogus invoices

This shows the extent of social engineering and how the internet can be used to defraud businesses. Along with false house purchase completion requests for solicitors this is truly alarming. This is why human interaction with technology needs to be failsafe and why cyber is becoming a largely human problem.

The threat landscape

Cyber attacks do come in many guises and their impact can be far reaching. The picture below was taken from the BBC News website for the first week of January 2016 and illustrates this point perfectly.

It is noted that half the stories were generated from the BBC business pages, confirming that cyber security is very much a business as well as a technology issue.



So how big is this problem and how serious is the threat to business?

The Office for National Statistics issued figures for the year ending June 2015 that make disturbing reading about the size of cybercrime and fraud leading directly to a debate about how policing resources should be allocated in the future. It should be noted that these are only cases reported to the authorities; the real figure is almost undoubtedly higher.

Computer misuse	2,460,000 cases
Unauthorised access to personal information (incl hacking)	404,000 cases
Computer Virus	2,057,000 cases

Source; National Office for Statistics, year ending June 2015

While this threat landscape sounds depressing, it has presented the UK with an opportunity to use its expertise to take advantage of this and lead the world. For Cheltenham, the home of GCHQ, there is an excitement in the growth of a cyber hub there, best described by the Member of Parliament for the town.

"I was delighted when the chancellor announced last year that Cheltenham would be the home of the new national Cyber Innovation Centre – a digital ecosystem in which our best people move in and out of GCHQ, bringing the finest minds and deepest expertise into the private sector, and the latest innovation back into government. It will help cyber start-ups proliferate, get the investment and support they need, and help them win business around the world. It is a fantastic opportunity for Cheltenham, and UK plc more generally."

Alex Chalk MP
Member of Parliament for Cheltenham

Some key cyber moments of 2015

"2015 has proved to be yet another fast-paced year for all of us in cyber security and the number of emerging threats and successful attacks puts us all, again, on notice. However it is not all gloom; the innovation and benefits that come from faster and different ways of using technology are exciting and should be embraced to help us all."

Sir Kevin Tebbit
Former Director GCHQ and Chairman, Ascot Barclay Group

A pivotal moment came in January 2015 when, following the Sony cyber hack, the UK prime minister, David Cameron met with the US president, Barack Obama specifically to agree the sharing of intelligence and conducting of cyber security war games.

With a global media spotlight on this event cyber security suddenly rocketed upwards as a priority for the western world and was propelled into the public eye from relative obscurity.

The Sony cyber hack changed the way that attacks were viewed, from disrupting Sony's ability to operate through to threatening cinemas who showed a movie called *The Interview*[6]. Further leaking of company emails, exposing unequal salaries and using social media to destroy its reputation, made this a campaign of attack.

The notion of a cyber attack being a simple "hack and attack" were over. A sophisticated joined-up model using social media and the power of inflicting reputational damage were of such concern that an executive order from the US president was necessary.

The attack on Sony showed that the age of economic cyber terrorism had arrived.

[6] *The Interview* was a 2014 American political satire comedy produced by Columbia Pictures who were owned by Sony Pictures Entertainment. Its storyline about the North Korean leader led to Sony being hacked by "The Guardians of Peace" who it was claimed had links to North Korea.

[7] Apple Pay – is a mobile payment service offered by Apple Inc that allows payment to be made via Apple device (iPad / iPhone / Apple Watch)

[8] Cyber Essentials – is a scheme launched by the UK government in 2014 with the aim of reducing cyber risk across all UK organisations.

Other key cyber moments for business

1 **June 2015** Ashley Madison: the mass hack and theft from a dating site used for adultery was followed by the demand that either the site was closed or the data would be published.

Ashley Madison refused, with catastrophic effects on the people identified, including alleged suicides and cash extortions from third parties. The original motivation wasn't even money motivated. It was claimed at the time of the leak that 1.2 million people were signed up in the UK, but whatever the truth its impact was real and highlighted the consequences of losing sensitive customer data.

2 **July 2015** The UK launch of Apple Pay[7], which is building on the introduction of contactless point-of-sale payment mechanisms by banks. Apple products can facilitate payments from a far larger customer base than any single bank and the risk and consequence of a single point of failure from an attack has to be higher. The question is whether Apple or a similar provider would be liable, can underwrite such a risk to the supplier, and if so become a virtual bank in its own right. It would not be a surprise to see Amazon, Google and others following suit this year.

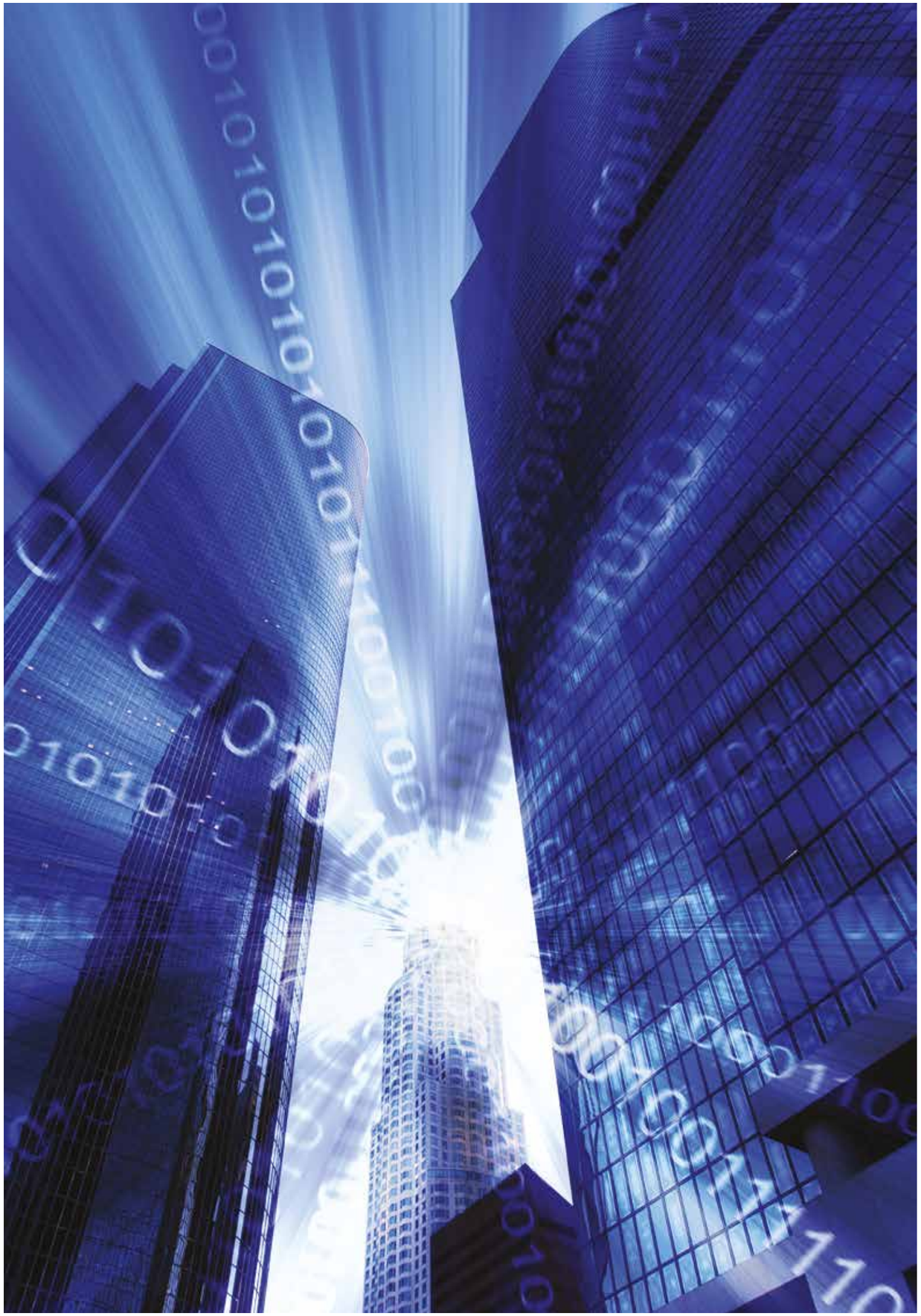
3 **Sept 2015** The launch of The National Cyber Awareness Course at the House of Commons supported by the prime minister and three UK universities. It is designed simply to deliver an increased awareness of the risk and benefits of the digital world and aimed at all employees, students and members of the public. It is predicted that this, alongside Cyber Essentials[8], will form the mandatory UK training minimum for organisations seeking cyber insurance.

4 **Oct 2015** The compromise of TalkTalk became a high-profile media event that caused organisations across the UK to seriously examine their own cyber security and the financial and reputational effect a simple breach can have.

5 **Nov 2015** The chancellor of the exchequer, in a speech at GCHQ, as well as pledging monies for new cyber start-ups and greater ties with industry, announced the setting-up of two Cyber Security Centres of expertise in London and Cheltenham.

6 **Dec 2015** An attack on the JD Wetherspoon chain took place in June 2015 but was only uncovered in December. While the actual customer data hacked was significantly larger in number than TalkTalk it was limited in its content.

7 **Dec 2015** The announcement that the European Parliament would be seeking to enshrine into EU law a common set of minimum cyber security standards across its members. In particular the mandatory reporting of breaches within key critical sectors such as banks, energy and water companies.



A view from the author

Professor Benham is one of the pioneers of the study of Cyber Security Management having founded The National MBA in Cyber Security and The National Cyber Awareness Course.

As well as being an author and international speaker, he is recognised as a leading authority in the areas of cyber banking and cyber crime having worked for numerous financial institutions and law enforcement bodies. Professor Benham lectures both at Coventry Business School, the University of Gloucestershire and the National Cyber Skills Centre. He also continues to act as an adviser to several large organisations including government and is Professor in Residence at The National Cyber Skills Centre and a Visiting Professor of Policing at Staffordshire University.

Richard Benham
Professor of Cyber Security Management

prof.benham@outlook.com
07810 831 546

The current threat is real enough, but what about the future? What trends are developing? In the following essay, Professor Richard Benham outlines four key trends that he believes will become ever more important over the coming years - with significant impacts for British businesses.

Cyber in the boardroom

There is a growing awareness in the boardroom and at the top of businesses that cyber is now a board level issue affecting not just the IT department but all areas of the business as part of its operational and strategic risk models.

Cyber education

The increase in the need for cyber education at all levels to help businesses protect themselves particularly from social engineering attacks[9], staff negligence or malicious insider attacks.

The cloud

The significant increase of cloud-based solutions providers in the UK offering more competitive priced solutions and allowing data protection to be outsourced for a defined monthly fee.

Cyber insurance

The introduction of a visible UK cyber insurance marketplace with standalone policies now actively being marketed.

The thoughts on this page and in the rest of this report are those of the author and not necessarily the views of the sponsor

[9] Social engineering is a term used to describe a non-technical method that hackers use to obtain or change information. It involves tricking people into breaking normal security procedures and is the biggest emerging cyber risk for organisations.

Cyber in the boardroom

The dependence on technology and the internet in most businesses is now critical, be it the storing of financial and regulatory information, employee, supplier and customer details or just a business bank account. Indeed it is hard to envisage most businesses surviving without real-time access to electronic data of one sort or another.

This presents directors of UK companies with an evolving set of opportunities and challenges which require new skillsets and awareness. In short the corporate landscape is shifting but at a faster rate than previously seen due to the speed of technological advancement.

Traditionally in larger companies computer or IT security was the responsibility of the IT director or a chief information officer. What we are now seeing is that cyber security (which includes IT security) is the responsibility of the whole board as its definition crosses into all parts of a business. Indeed the emergence of a new "chief information security officer" role to bridge departments illustrates this change well.

For SMEs that do not have the budget to create new specific roles, and where many directors have multiple hats, the urgency to understand and deal with the risk of cyber attacks is equally as critical. Regardless of size, every board or business owner has a responsibility to manage its own risk profile and act accordingly. Cyber security is becoming a critical and larger risk and should be treated accordingly.

It is important that directors and owners realise they do not need to be cyber experts to understand the risk but do have policies and processes to deal with any situation; in short, a plan B.

Given that many IoD members are directors of SMEs, they will naturally look to outsource cyber security. Indeed sophisticated cyber abilities are likely to become one of the key determinants in selecting an outsourced IT supplier.

"The importance of cyber security continues to grow as businesses increasingly transform their operations and engage with stakeholders on the basis of digital technology. Most companies are still struggling to join up IT and information risks with a wider understanding and management of business risks. This therefore increases the challenge of good decision making about cyber security and undermines meaningful board accountability."

Mark Brown
Executive Director,
Cybersecurity and Resilience,
Ernst and Young LLP

Cyber education

It is fair to say that the UK government has been proactive in recent years and has led the way on cyber education through the Education and Information Assurance wing of GCHQ known as CESG (Communications-Electronics Security Group).

Notably, it has established a number of centres of excellence within UK universities to allow up-to-date research into cyber-related topics. In addition, it also provides accreditation to individuals, companies, universities and training providers in the cyber sector. Historically these have been focused on the technical elements of cyber security. Examples are digital forensics, ethical hacking, coding, penetration testing and drawing together common standards.

Regarding cyber education for business specifically, there are three notable national products that have emerged during 2015:

The National MBA in Cyber Security The first of its kind, an MBA designed specifically to look at the management and business issues faced in a digital world and help executives and leaders to understand them. Currently offered through Coventry University Business School, this course is being adopted both by large corporates to train its cyber consultants and by individuals who wish to be the key digital decision makers within their organisations.

The timeliness of this qualification for business was illustrated by its cross-party launch at the House of Commons, supported by the prime minister and many of the UK's leading companies. It was in fact the first UK degree to be supported by a prime minister upon its launch, showing the critical importance attached to cyber education at this moment by the UK government.

Cyber Essentials A government-backed industry-supported scheme to help organisations protect themselves against common cyber attacks. There are two levels of assurance which allow a snapshot of an organisation's technical cyber robustness to be reviewed internally or externally. Certification is awarded and a badge may be displayed to provide assurance for customers and suppliers.

The National Cyber Awareness Course A low-cost basic cyber awareness course written in a non-technical format backed by three UK universities designed for all employees, students and citizens of the UK to raise awareness both at work and home. It effectively sits in the marketplace alongside Cyber Essentials to address the human and real-life work and home threats of cyber security.

"I am again pleased to show my support for the launch of the National Cyber Awareness Course which, following the successful launch of the National MBA in Cyber Security last year, is welcome in increasing cyber knowledge in this digital age."

Rt Hon David Cameron MP
Prime Minister

The cloud

"The cloud" is a storage solution which allows firms and individuals to store data, including applications and files remotely, on server space leased from a third-party provider. Files can be accessed from multiple computers 'on-demand' through an internet connection. The main advantages for businesses are that cloud services are often cheaper than dedicated servers, and are easier to scale up and down depending on business needs.

Despite these advantages, there remain some key questions that any organisation should ask before outsourcing its data to a third party.

1. Never forget that the cloud is someone else's computer
Good marketing has diluted the fact that any cloud solution is really someone else's server. Apple, as a trusted provider, led the way for our personal storage and back-up issues and this trust has generally remained for all cloud providers, but it may be time for a more rigorous challenge to be applied.

2. Where is my data actually being stored?
All data is being stored somewhere, possibly over multiple sites in different countries, or with back-up in different locations. If a business owner or the key senior management team don't know where it is, and there is no guarantee of its location other than a supplier's word, then a business may be at risk. Differing jurisdictions may well have differing legal requirements about data disclosure, and business leaders need to be aware of this.

3. Can the cloud provider be trusted?
With many players offering cloud services and more set to join it's a bit like choosing a bank, but without deposit insurance. Household names known for their stability and reputation may well top the list for many businesses, but they and all other providers should be asked for their insurance details. If a company is large enough, circumstances may warrant having two cloud providers, a primary and a less frequently updated deep storage.

4. What is their track record on 24/7 help desk availability?
If something goes wrong on a Friday evening and a business owner cannot rebuild or restore systems, including payment systems, then the potential for lost business or indeed reputation is obvious. Many businesses will consider a 24/7 help desk a mark of a quality cyber provider.

5. Has the cloud provider ever been hacked itself?
Cloud providers like to sell themselves as "digital fortresses" but they face the same risks of being hacked, neglected or compromised by staff as other businesses.

> **"Moving your IT function to a cloud provider often makes sense for any organisation as it provides greater flexibility and reduces the risk of having to recruit and pay for teams who are a scarce and expensive resource. However the provider must be trusted with their record, size and stability absolutely key. It is easy enough to think your data is secure; it is essential you know it is."**
>
> **Richard Archdeacon**
> *CTO IS Strategy – Hewlett Packard Security Services*

6. How tied in to a cloud provider is a business?
Once a cloud provider has been selected, the degree of integration and detailed knowledge of a business's operating systems can be considerable. Therefore, moving from one supplier to another can be protracted and in practice too difficult to seriously contemplate, certainly on a regular basis. If a change is to be undertaken, it may well involve running parallel systems for a time and incurring the doubling of any expense.

7. What happens if the cost becomes challenging?
Most current providers are reasonable and responsible but ultimately they are businesses too and will not tolerate long periods of non-payment. As with any utility that is essential to the running of a business, payment will need to be treated as a priority.

More broadly businesses should be aware that cyber is an industry experiencing a good deal of creative turmoil. In such circumstances it is normal to expect new offerings to be developed and prices of existing services may well fall. Providers may well try to insist on long-term contracts, effectively locking businesses into an expensive, or not fully up-to-date offering.

An interesting development in this sector is the emergence of nation island states offering both virtual and physical security of data. Guernsey and the Isle of Man are just two examples of jurisdictions which are politically stable and have a track record of secure data provision and expertise with their banking and gaming communities.

Cyber insurance

The UK government has said that cyber and terror attacks must be viewed as similar threats. One thing is certainly clear – cyber attacks occur an awful lot more often.

Virtually all businesses rely on technology that includes networks and contact to third parties. Because of this it can be subject to the risks that lead to interruption of service, income loss, damage to IT infrastructure and reputation. The examples given earlier in this paper during 2015 provide case studies of the reality of this risk.

Is it overstated or isolated? A UK government survey in 2015 estimated that 90% of large corporations and 74% of small businesses suffered a breach. The average cost of a breach was estimated at £1.46m-£3.14m for large business and £75,000 - £311,000 for SMEs.[10]

As a result of this increased risk a single policy cyber insurance market has emerged to cover both first-party and third-party protection. The challenge to the insurance market is designing a model that gives realistic cover at an affordable premium. This is difficult where third-party consequential loss cannot be accurately predicted or controlled.

Loss of reputational damage is always hard to quantify and it is unlikely to be covered specifically in a policy. What will be covered, should an incident occur, is the cost of a public relations specialist and damage limitation, and possibly, for an additional premium, any loss of profits. But just as home insurers expect their customers to take precautions to prevent burglars (or they reserve the right to not pay out on a premium), so too do insurers increasingly expect businesses to take basic measures to protect themselves against cyber crime.

[10] HM Government, 2015 Information Security Breaches Survey, 2015

While immediate financial loss can be insured and perhaps recovered, reputational damage is much more serious and generally uninsurable. Businesses which depend upon customer trust can expect harsh reactions if they violate or are careless with that trust, and it can potentially be fatal. This was neatly summed recently by Bronwyn Boyle of Solis Solutions Limited

"With cyber crime now the most prevalent crime in the UK and corporate attacks on the increase, cyber insurance is becoming a must-have for businesses. The challenge for companies is that they must be capable of evidencing appropriate controls and due care to guarantee a payout. Given the changing environment and what constitutes due care this is no mean feat. However, it is certain that cyber insurance will mature as a market significantly."

"The need to be able to respond quickly and correctly to a cyber attack is critical for the reputation and possible survival of any business. I would urge all businesses not only to hold cyber insurance but to know what is actually offered should the worst happen."

Wendy Cheshire
Director – Control Risks Group

Conclusions for UK business

The challenge of cyber security is that it is a quintessentially international threat and most of the proposed solutions are more often than not primarily national. Effective solutions are, as a result, difficult. Moreover the more dramatic the cyber attacks, the more danger there is of an over-reaction focused on a single set of circumstances either from politicians or business executives themselves. The solution is to get a credible plan that looks at a wide range of threats and responses and outlines what would be done in varying circumstances.

What can UK businesses do now to protect themselves further against? It has to be remembered that this is a new, rapidly evolving problem that just gets bigger. Unfortunately, government guidelines, joined-up national cyber policy, legal precedents and education are all developing behind the threat, but failing even to contain it, let alone anticipate tomorrow's cyber threats.

1. Having a cyber insurance policy makes good sense, but it is important that it is the right one for a business and that those taking out the policy appreciate it is by no means a silver bullet. Reputational damage is the most obvious element of a cyber attack that may not be covered.

2. Boards should discuss how they would react to different scenarios and have a mitigation plan for when they are hacked or compromised. It is important that all departments are involved in this; cyber security is as much an HR issue as a technology one.

3. Senior managers should spell out a basic checklist for cyber security for all staff, ensuring they are all cyber aware and alert to scams and social engineering, not sharing passwords or memory sticks and are aware of public WiFi risks.

4. Cloud and IT providers must be challenged to demonstrate the security protocols they have in place and their disaster recovery plans.

5. Conduct a data audit to classify your most sensitive data.

6. Always have up-to-date antivirus software.

7. Check that all mobile phones and tablets have antivirus software installed.

"Business has to stop thinking of cyber security as an IT issue; it is a matter of corporate governance and industry reputation. Leadership must therefore start at the top, with cyber expertise in the boardroom, so the right actions are embedded in strategy and best practice percolates down to each and every employee. For a board, the subject should be as routine as audit."

Ashling O'Connor
Head of the Media, Technology & Entertainment Practice, The Inzito Partnership

What should we anticipate in 2016?

1. More contactless payment methods and non-brand-name providers of financial services.

2. The customer experience is about to become more sophisticated with intelligent environments providing relevant personal and timely data to individuals through their mobile devices.

3. More high-profile attacks, with social media used to inflict economic and reputational damage to companies.

4. Cyber insurance may become a legal requirement for many organisations.

5. More legal action from individuals and companies seeking damages caused by cyber breaches. We expect markets to evolve quickly and set defining standards more rapidly than any legislation.

6. More sharing of cyber-attack information between government, industry and the police. Cyber security is a critically important national infrastructure requirement and the role of GCHQ, working with and protecting businesses from international threats, will increase.

What is the forecast for cyber security and our digital environment in the coming years?

1. A secure UK business intranet will emerge for all approved UK businesses, government departments and banks to transact and trade with each other securely, "outside" of the internet and hosted by GCHQ or similar.

2. A cyber paradox will emerge in which the internet (even with encryption) will start to carry an unacceptable level of risk for the most sensitive data. Reversion to old-fashioned methods of information transfer is predicted to return in some ways.

3. As banking evolves into an increasingly digital business, the importance of cyber security increases. Banks will need to continue their efforts to create systems to protect their customers and raise awareness of how to stay cyber safe to control these new risks.

4. The heightened risk of cyber attacks raises the possibility that the Bank of England and regulators will impose minimum cyber standards on banks and financial institutions, further to the demands they already place on the banking industry.

5. Having witnessed the evolution of the iPhone/iWatch how long before a chip is embedded (voluntarily) in a hand or ear to enable access to the internet or similar?

6. The legal system will experience some defining cases in the next five years that will ask serious questions both ethically and legally to governments, business and citizens.

7. The MoD will spend at least 10 per cent of its annual budget on a cyber warfare capability.

8. A global cyber security centre will be established to police the internet and come under the umbrella of the United Nations as a military peacekeeping capability.