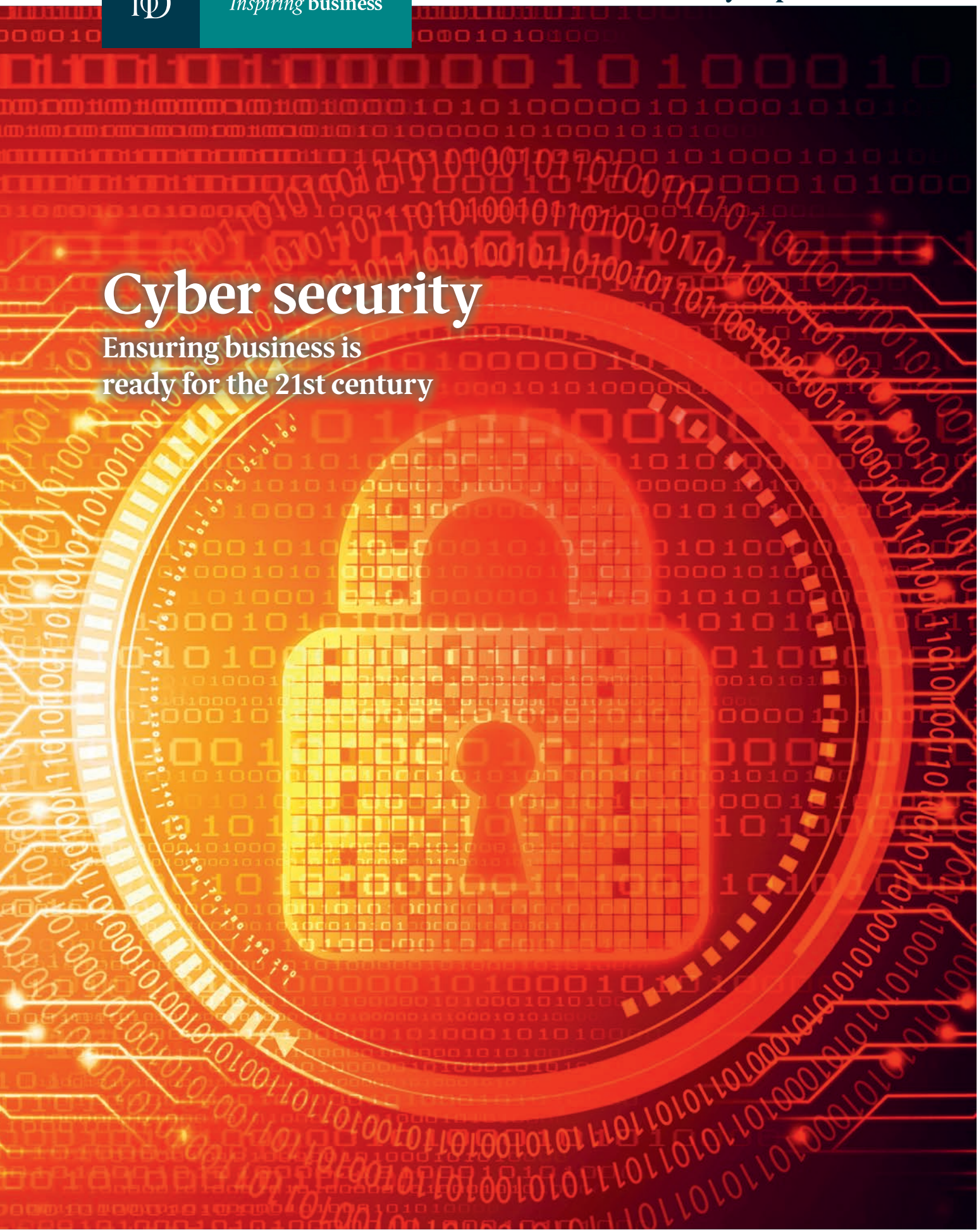
IoD Inspiring business

IoD Policy Report March 2017



Cyber security

Ensuring business is ready for the 21st century

BARCLAYS Digital Eagles

Foreword

Troels Oerting
Group chief information security officer, Barclays

@TroelsOerting

Digital technology has radically changed nearly every aspect of people's lives, and has brought untold benefits. However, the introduction of this fast moving industry has also provided us with a new and emerging threat – cyber crime.

Cyber criminals are harnessing this new digital reality, in which they can reach out across the globe, anonymously, risk-free. They attack systems, data and networks virtually without intervention and traditional defences are no longer adequate. For the financial sector in particular, the game has changed. Barclays has already implemented a strong protection for our business and we will continue to adapt to the rapid change in cyberspace.

For centuries, society and banks have steered through unprecedented events; cyber crime is another challenge, and it too can be managed by implementing a strong strategy built on resilience and intelligence.

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 cyber crime. Since 2014, Barclays has provided free training to anyone who needs help 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. Since 2016, Barclays has launched Eagle Labs across the country, a community resource available for everybody. From accelerating UK business, enabling collaborative innovation and digital empowerment for all, to supporting businesses and families to stay safe in cyberspace. Further information on cyber at Eagle Labs can be found by going to labs.uk.barclays/cyber-security-workshops

About the author

Professor Richard Benham
Cyber-security expert

@prof_benham

Professor Richard 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 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.

James Sproule
Chief economist and director of policy
james.sproule@iod.com
@jamesrsproule

Throughout our history, Britain has always been at the forefront of technological innovation – from the marine chronometer that fostered the exploration of the world, to eurobonds which underpinned globalisation, and to the digital revolution that's all around us. We should be incredibly proud of this fact – as we should be proud of the fact that more than 12 per cent of our GDP today comes from the digital economy.

The next wave of progress is perhaps the most exciting. Self-driving cars could well revolutionise the way we get around cities, taking millions of vehicles off the road and fundamentally changing the way we interact in cities and towns. Personal banking has never been easier, and will only become more a part of business life too – are we far away from the point when a physical handshake could trigger instant funds transfer? And 'the internet of things' could free up hours of our lives by automating simple but time-consuming processes. While a decade ago this may have sounded like science fiction, the next generation might find it quaint that we ever even used paper money. Progress moves, it seems, ever quicker.

This new world comes with new threats – and cyber crime is rapidly climbing to the top of that list. As data and intellectual property become ever more the currency of business, their value to criminal minds grows ever higher.

That's why, for the second year in a row, the IoD is delighted to put this issue at the top of the business agenda. For more than 110 years we've been delivering on our Royal Charter obligations to support our members, to promote good governance, and to lobby for a climate more amenable to entrepreneurs and businesses. Ensuring Britain remains a safe and secure place to do business in a digital world ticks each of those boxes and then some.

Table of contents

Introduction

The digital world presents many opportunities for business, not least the reduction of costs, a better customer experience, and an ability to trade globally.

This reliance on technology comes alongside a trust that it will be secure, safe and robust. This is vital in an environment where goods and services are traded in real time, where funds are transferred and stored electronically, and where huge amounts of personal data – with strict legislation affecting their storage – are at risk from sophisticated hackers and human error alike.

Nobody should be scared of the 21st century and the digital revolution, but that does not mean going into it blind. Despite the headlines focused on our global position or geopolitical machinations, there is a very strong chance that the defining business challenge of the 21st century will be ensuring that data, bank accounts and intellectual property remain secure. Such is the scale of the cyber crime challenge.

This report builds off IoD survey research of almost a thousand business leaders.[1]

- **95 per cent** consider cyber security to be very or quite important to their business, and yet **45 per cent** do not have a formal cyber security strategy.
- IoD members are aware of the threat presented by cyber crime, particularly on mobile and tablets. But just over half have protected all of their devices, and less than a third use virtual private networks (VPNs).
- If the victim of an attack, almost half of IoD members – some 40 per cent – would not know who to contact, an issue which will become all the more relevant with new European General Data Protection Regulation (GDPR).
- Two-thirds have taken government advice to use a variety of different passwords and a similar number use cloud software.
- Only 44 per cent have laid on cyber awareness training, and many leave gaps of more than a year between their training programmes.
- 73 per cent have a process in place when receiving invoices and requests for electronic payments to verify their legitimacy.

Over the last 12 months, the number of cyber security incidents has continued to increase, and more and more it is being demonstrated that it isn't just 'the usual suspects' being attacked. From Lincolnshire County Council to Tesco Bank, it's clear that cyber security is an issue for just about every organisation. With new legislation in the form of the EU's GDPR on the way, firms must ensure that they're equipped for the 21st century.

There are no signs that such threats are going to decrease. Take internet fraud, for instance, relevant not just to personal consumers but to businesses whose banking accounts and credit cards are often very similar in nature; a 64 per cent increase from 2014 to 2015 alone, to a scale of some £133.5m.[2]

Small, medium and large firms need to consider the best way to protect themselves against what might be the defining challenge for business in the

[1] Survey of 844 IoD members via online "Policy Voice" panel software, 9-23 December, 2016

21st century. Government, too, needs to do more to point busy business leaders towards existing schemes and advice, and making schemes more relevant. They might also consider encouraging training through 'nudges' on the business community. Ultimately, however, this is a matter for business – in a digital economy, it's the equivalent of installing a burglar alarm.

[2] HM Government, *National Cyber Security Strategy,* 2016-2021

The context

The past year has seen a continued increase in the number of cyber attacks hitting British and international companies – but it's no longer just corporate organisations that are in the crosshairs. From councils to presidential elections, cyber crime has never been far from the headlines.

January 2016

Ukraine: In what is believed to be the first successful attack on a power grid, hackers were reportedly able to remotely switch off substations, disable IT components and launch a denial of service attack on a call centre. More than 200,000 people were left without power for over eight hours.

Lincolnshire County Council: Council systems were bought to a standstill in a ransomware attack, with hackers reportedly asking for a £1m payment to reinstate them. The malware was believed to have been introduced via an email with a bogus invoice.

February 2016

Central Bank of Bangladesh: Weaknesses in Bangladesh Bank's cyber security allowed hackers to issue instructions to steal $951m from the Central Bank of Bangladesh via the international Swift network, which banks use to share secure data and finance across international borders. Some $101m-worth of transactions were successful, though much of the money has been recovered. Dridex malware was used for the attack.

April 2016

Morrisons: After the leaking of a spreadsheet containing bank details, salaries and national insurance numbers in 2014 by an employee – since prosecuted – some 6,000 current and former employers have undertaken a group legal action against Morrisons. Claims were cut off in April 2016, and the outcome of the case is awaited.

General Data Protection Regulation adopted: The new EU data protection laws seeking to unify data regulation across the European Union were formally adopted in April 2016. The rules will come into force in April 2018, with Britain expected to transfer the regulations to British law via the Great Continuity Bill once the UK has left the European Union.

August 2016

World Anti-Doping Agency: The "Fancy Bear" hacking collective – believed to be linked to Russian intelligence – were responsible for hacking the medical records of hundreds of prominent athletes. The attack was believed to be in retaliation against the whistleblowing Russian athlete Yuliya Stepanova, whose records were released in the hack.

October 2016

Launch of the National Cyber Security Centre: The Centre, which is intended to bring together the UK's cyber security efforts, is jointly based in Cheltenham and London. Its role is to advise and support both the public and private sectors to beef up cyber security protection.

North Lincolnshire NHS attack: The Hospital Trust was forced to cancel as many as 35 operations after a virus disrupted electronic data operations

November 2016

Yahoo: Thought to be the biggest cyber attack ever involving customer data, Yahoo announced in 2016 that millions of passwords had been stolen in 2013.

Tesco Bank: Up to 40,000 customer accounts were hacked, with nearly half seeing a direct financial loss as a result. The seriousness of the breach led to a fall in the Tesco share price.

The US election: Hacking groups played a starring role in the build-up to the US election, with significant leaks of personal emails from figures close to Hillary Clinton making the headlines

Legislative changes

"Today, many personal data breaches in the UK go unreported by businesses. In jurisdictions that already have mandatory breach reporting requirements, such as the US, unprepared directors have found themselves losing their job after a breach for failing to give adequate attention to the issue, and therefore letting down their stakeholders, damaging their business's reputation, and exposing it to regulatory and legal sanctions. The mandatory requirement to report security breaches will bring an increased risk of quasi 'class action' lawsuits in the UK. Furthermore, negative publicity tends to drive regulators to use their powers in a more robust way: under General Data Protection Regulation they will have power to award substantial fines to UK businesses."

Marc Dautlich, data legislation partner, Pinsent Masons LLP

General Data Protection Regulation

So what *is* GDPR and why does it matter? Simply put, it's a new data protection framework that will apply across all 28 – soon to be 27 – EU states. GDPR comes into force in May 2018, replacing the Data Protection Act of 1998 in UK law. The UK government has confirmed that the decision to leave the EU will not affect either the commencement of the regulations or their standing once we have exited, with the regulations transferred over to UK law through the Great Repeal Bill and secondary legislation. Such equivalence will be crucial to ensure digitally minded UK firms can operate across the EU, their biggest trading partner.

The GDPR significantly expands the level of accountability of data processors and controllers – which is to say, the vast majority of business leaders. In particular, the GDPR will mandate that business leaders 'show their working' to prove that they are following the principles of the GDPR.

From an individual perspective, the GDPR radically expands the rights of a subject to information about their data, from the right to erasure to the right to object. From a business perspective, most interesting are changes to accountability and new provisions on breach notifications.

The accountability principle

The new accountability principles mean that business leaders must demonstrate that they are complying with data protection rules elsewhere in the GDPR. The Information Commissioner's Office, for instance, recommends that business leaders should:

- Implement appropriate technical and organisational measures that ensure and demonstrate that you comply. This may include internal data protection policies such as staff training, internal audits of processing activities, and reviews of internal HR policies.
- Maintain relevant documentation on processing activities.
- Where appropriate, appoint a data protection officer.
- Implement measures that meet the principles of data protection by design and data protection by default. Measures could include:
    - Data minimisation
    - Pseudonymisation
    - Transparency
    - Allowing individuals to monitor processing
    - Creating and improving security features on an ongoing basis
    - Use data protection impact assessments where appropriate

Furthermore, the GDPR will bring in a host of documentation procedures – some similar to those in the Data Protection Order, some of a more stringent order. If an organisation has more than 250 employees, significant new obligations to maintain additional internal records of your processing activities are on the way; even small- to medium-sized enterprises of less than 250 employees will be required to maintain records of activities related to 'higher risk' processing, such as CRB checks or those where a leak could risk the 'freedom' of an individual concerned.

Breach notification

The GDPR will introduce an obligation on all organisations to report data breaches to a supervisory authority and, in the case of personal data breaches, to the individuals concerned.

Failing to do so could see fines of anything up to €10m or two per cent of your global turnover.

Implications

Unsurprisingly, these new regulations present a challenge to British businesses. While large firms have been alive to the coming changes for a while, small- to medium-sized companies are only beginning to assess what changes they might need to introduce in order to comply. The British government will have, of course, a degree of flexibility in how the regulations are transferred over. There are derogations built into the GDPR language that might allow UK firms to process consumer data without specific consent; financial services firms, for instance, are keen to ensure that they remain able to conduct CRB checks for financial crime on potential employees, as they would be in breach of other regulations if they weren't aware of a fraud conviction.

It's also unclear whether existing 'consents' from data subjects will be grandfathered through. The alternative would be an overwhelming barrage of emails and communication to consumers seeking to ensure that they remain 'opted in' to data processing by an individual firm; and firms, frankly, do not need the regulatory nightmare of attempting to wipe their data, re-establishing consent, and then re-gathering their data. Serious thought needs to be given as to how to transfer to the new regime and how it integrates with other regulatory regimes – around money laundering or modern slavery, for instance.

Government programmes and activities

The government has been keen to expand the knowledge base on cyber security beyond the world of spooks and compliance officers. The past year, in particular, has seen a number of announcements looking to do just that.

Cyber Schools

A new £20m programme, Cyber Schools will "support and encourage students to develop key skills to help defend the nation's businesses". The intention is to identify around 5,000 teenagers by 2021 who will be taught a cyber security curriculum both in the classroom and on placements.

Cyber Security Regulation and Incentives Review

Across 2016, government consulted with business groups, cyber security experts and academics to review whether there was a need for additional regulation or incentives to boost cyber risk management across the wider economy.

The Review, not without controversy, concluded that there is no need for further regulation over and above the coming GDPR, a conclusion business broadly supports. There is of course always the risk that any such regulation would produce tick-box compliance as opposed to genuinely putting cyber security higher up the agenda. Instead, the government is minded to expand its non-regulatory interventions, many of which will be delivered through the National Cyber Security Centre.

The National Cyber Security Strategy

Backed by £1.9 bn of taxpayers' money, November saw the government's updated National Cyber Security Strategy outline a range of government initiatives and interventions which, over the next five years, are designed to ensure Britain becomes the most secure data economy in the world, as well as giving firms the space and room they need to innovate in a fast-moving business environment.[3]

The Strategy's centrepiece is the National Cyber Security Centre. For the first time, it was recognised that the numerous agencies involved in cyber security – 12 of sufficient size and influence – would be a more effective force if bought together under one roof. As the chancellor at the time said, the Cyber Security Centre was a response to the need to "address the alphabet soup of agencies involving in protecting Britain in cyber space". Opened in November, the NCSC will "analyse, detect and understand cyber threats" and by sitting under GCHQ it will have access to the expertise of that organisation, too.

"Given the industrial-scale theft of intellectual property from our companies and universities, as well as the numerous phishing and malware scams that waste time and money, the National Cyber Security Centre shows that the UK is focusing its efforts to combat the threats that exist online."
Robert Hannigan, former GCHQ director

Cyber First

The Cyber First programme sponsors undergraduates through university education to take part in cyber-focused courses. Judged a success, the minister for cyber security, Matt Hancock MP, announced further funding to support the programme in March 2016.

[3] National Cyber Security Strategy, 2016-2021

The state of play

IoD members are aware of the threat posed by cyber crime, but their views on where they are most vulnerable changes significantly depending on what device is being used. The results below and over the following pages are taken from an extensive survey of IoD members carried out at the end of 2016.[4]

Understanding

We can, at least, take heart from one thing: IoD members 'get it' on cyber crime. Fewer than one in 10 are ignorant of the importance of putting the right systems in place.

It's worth interrogating therefore where business leaders feel most vulnerable.

Members feel less secure when they are out and about on mobiles or tablet devices than they do when they are safely installed in the office. But in a world in which our mobile phones, tablets and indeed home PCs are so closely integrated – with work emails and personal phones often intertwining – such confidence could well be misplaced. A hack on a mobile could be just as damaging as somebody breaking into a company mainframe. That might explain why members feel at risk when using public WiFi.

Unfortunately, while business leaders have recognised the importance of cyber security and identified where they feel most vulnerable, there is still much work to be done to instil the cultural change that is required across the business landscape as a whole.

How important or unimportant is cyber security to your primary organisation?

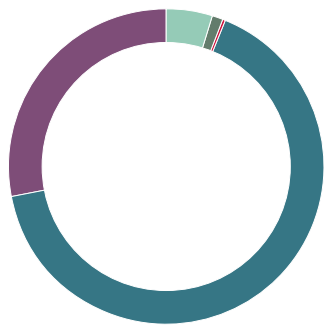
66% Very important

28% Quite important

5% Neither important nor unimportant

1% Quite important

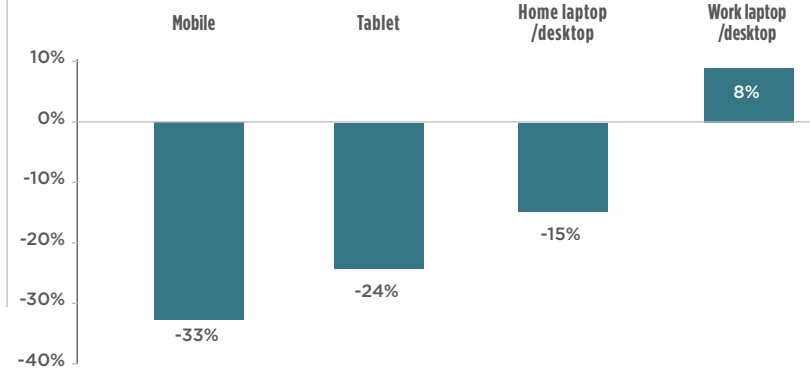
0% Unimportant



How vulnerable or secure do you feel to the threat of cyber crime on the following devices?

	Mobile	Tablet	Home laptop/ desktop	Work laptop/ desktop
Very vulnerable	14%	9%	13%	9%
Somewhat vulnerable	43%	39%	36%	30%
Sum VULNERABLE	57%	48%	49%	39%
Neither vulnerable nor secure	19%	16%	13%	11%
Somewhat secure	18%	19%	25%	27%
Very secure	5%	5%	10%	20%
Sum SECURE	24%	24%	35%	47%
Net	-33%	-24%	-15%	8%

Net confidence rating across different devices



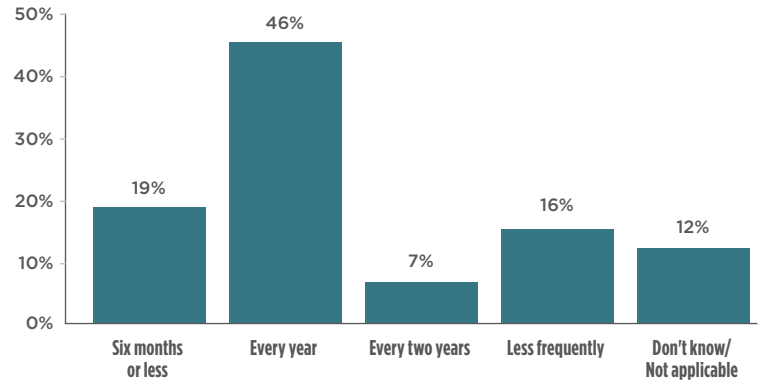
[4] Survey of 844 IoD members via online "Policy Voice" software, 9-23 December 2016

Governance and training

"From the boardroom downwards in any business, your employees and your business remain susceptible to cyber or data hacks. This can range from clicking on links within emails through to paying false invoices and taking data home. Creating a culture of personal responsibility in which your directors and employees become your first line of defence requires consistent and enduring cyber awareness training. This is now a must for all businesses in our battle against both cyber crime and employee negligence."
Angela Edwards, chief executive officer, The Cyber Club

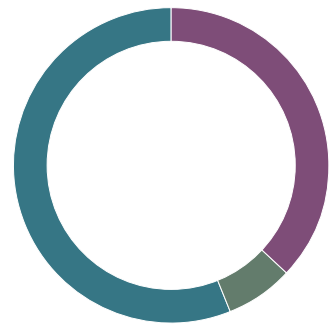
More than a third of IoD members lead or work in organisations without a formal cyber security strategy, and almost half have no cyber awareness training integrated across their primary organisation. This is, of course, a significant problem. Much has been written that the key vulnerability on cyber security is human error. Those human errors become far more likely without training or clear guidelines on appropriate good practice, led from the top.

How often do you require staff to undertake training?



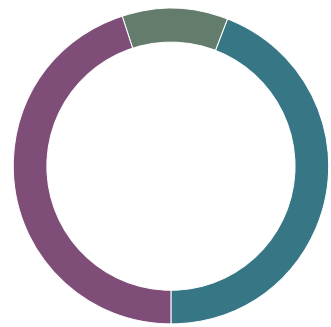
Does your organisation have a formal cyber security strategy?

56% Yes
37% No
7% Don't know/ Not applicable



Does your organisation provide cyber awareness training for staff?

44% Yes
45% No
11% Don't know/ Not applicable



Practical steps

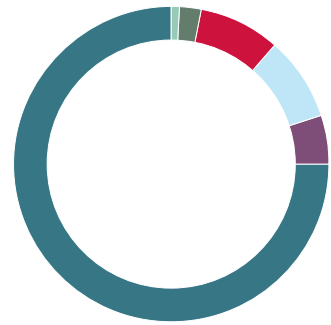
If we've established then that business leaders are aware of the threats but not necessarily putting the governance and training in place around cyber security, are they taking practical steps?

There are signs that some are. For instance, more than seven out of 10 have more than five passwords across different accounts, creating a system of checks and balances across accounts. If one is hacked, in essence, it is unlikely that the other 'dominoes' will fall.

The story is not quite so good when it comes to the use of VPNs – virtual private networks – when using public WiFi. In layman's terms, a VPN is essentially a 'private' network that spreads across shared or public networks as if their devices were directly connected to the private network. Laden down with security features, they are significantly safer when using public internet connections than simply logging on independently, and then using work email or downloading files to a tablet. Perhaps most alarming is the nearly one in five members who don't know whether they use one or not. Furthermore, only 47 per cent of members are familiar with two-factor authentication.

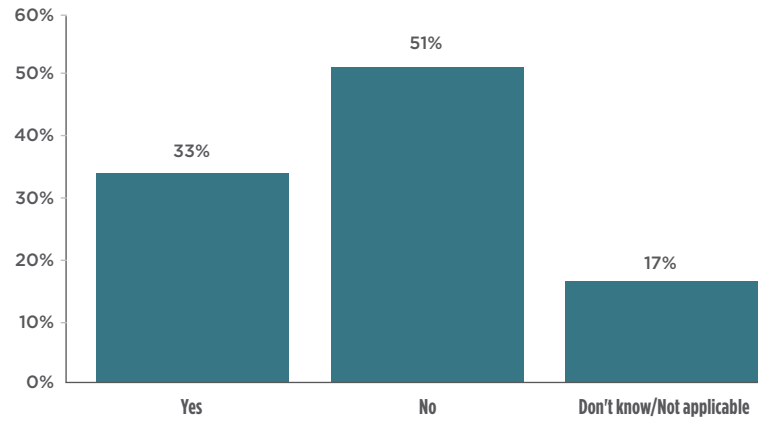
There are bright spots, however. Almost three-quarters of businesses now have processes in place when receiving electronic invoices or payment requests to verify their veracity. With bogus invoices on the rise, this is a sign that business leaders *are* listening.

How many passwords do you use across different accounts?



1%	1 password
2%	2 passwords
8%	3 passwords
8%	4 passwords
5%	5 passwords
71%	More than five passwords

Do you use a VPN app for protection when sending emails or confidential information over public wi-fi?



The overall picture, in short, is of a business community that, while aware of threats, remains underprepared to deal with them, with even basic cyber security steps still far from omnipresent across the British business landscape. It is no surprise, then, that policing data suggests threats are on the rise.

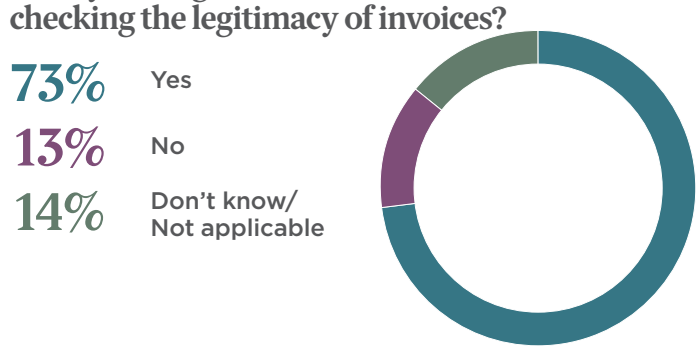
"The fast-changing digital world presents challenges to us all in both a positive and a negative way. The crime figures show how cyber-related incidents are now the majority of all reported crime, and the help of business to combat this is vital to the United Kingdom."
Richard Berry, deputy chief constable and cyber security lead, National Police Chiefs' Council

The National Crime Agency's Cyber Crime Assessment, released in 2016, makes clear the scale of the threat to British business.

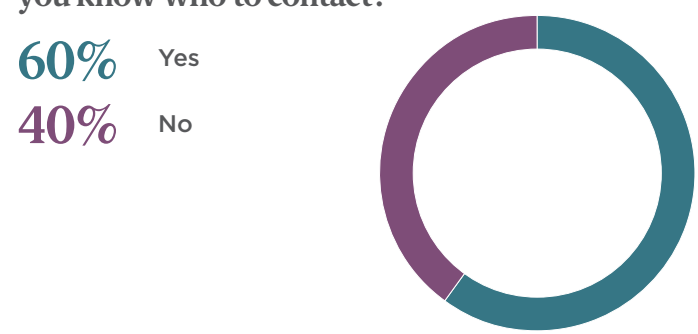
"A cyber attack that poses an existential threat to one or more major UK businesses is a realistic possibility. The long-term impact of such a cyber attack could include substantial loss of revenue and margin, of valuable data, and of other company assets. The impact of litigation costs (and, with the arrival of new regulations, potential fines), the loss of confidence from reputational damage and possible executive-level dismissals could also result in immediate and material loss of shareholder value. The NCA estimates that the cost of cyber crime to the UK economy is billions of pounds per annum – and growing." [5]

In 2015, the Office of National Statistics (ONS) included cyber crime in the annual crime survey for the first time – and the results were astounding. The ONS estimated that there were some 2.5 million cyber incidents, with 2.1 million victims. Despite these figures, just over 700,000 incidents were reported to Action Fraud, the police agency which should be notified of any cyber attack.

Does your organisation have a mechanism for checking the legitimacy of invoices?



If you were a victim of online fraud, would you know who to contact?



One recent report suggested that as many as 45 per cent of firms had experienced a cyber attack in the past year, and that same report suggested that the average estimated cost of a cyber attack was as much as £25,000 for a firm with fewer than 100 employees, rising to £53,000 for large firms with more than 2,250 employees.[6]

This is unsurprising. An IoD report in March 2016 revealed that some 68 per cent of members were unaware of Action Fraud, and only 28 per cent of those hit with cyber attacks even reported the incidents to the police. This needs to change if we are to tackle the scourge of cyber crime. Even today, 40 per cent of IoD members would not know who to contact if they were a victim of online fraud. The second foot to fall, of course, would be an increase in resources available to Action Fraud and police forces across the country.

[5] National Crime Agency, *Cyber Crime Assessment 2016: Need for a stronger law enforcement and business partnership to fight cyber crime*, July 2016

[6] Hiscox, The Cyber Readiness Report 2017

The language of cyber attacks

One reason individuals perhaps don't report cyber attacks is that they fear the reputational risk. Another might be a lack of understanding of what's happened, and confusion over the terms used by those 'in the know'.

So what kind of attacks should business be on the lookout for – and what language should business leaders be embedding throughout their training?

Phishing

Phishing is the attempt to obtain sensitive information such as usernames, passwords and credit card details usually by clicking on a link that is disguised as trustworthy or genuine. Company spam filters are becoming more effective at stopping these emails getting to the intended recipients' inbox.

Ransomware

Ransomware is a type of malicious software designed to block access to a computer system or to release data, usually gradually, accompanied with a ransom demand.

False email instructions

Also known as the bogus boss, this is a simple bogus email asking for funds to be transferred urgently to a fraudster's bank account. While the account name may be the same as a colleague or a departmental head, the account number is invariably different.

Bogus invoices

Bogus invoices are exactly that – a request for funds, often for licences, that is simply signed off unchecked. Smaller amounts appear to be more successful, emphasising how important it is that cyber security awareness is embedded not just throughout the IT department but across an entire organisation.

Theft of IP

The stealing of intellectual property is not new, but the storing of valuable company information in online databases gives criminals a far easier way to steal it. IP has been stolen by everybody from competitor businesses to nation states.

Disruption of service

Many of the more well-known hacks have involved a distributed denial of service attack (DDoS) in which a company's IT infrastructure is simply bombarded with information until it refuses to cope. Quite often malicious in nature, these attacks are typically conducted by individuals as opposed to the larger organised crime gangs.

Practical steps for your business

The great irony of cyber security is that these machine-based crimes often rely on human error: clicking on the wrong link, signing off an invoice as you dart out the door on a Friday afternoon, even sending an Excel spreadsheet to a personal email account so that you might be able to work on it at the weekend.

We have already revealed the lack of cyber awareness training throughout the workplace – but then, as we have also seen, too many business leaders fail to install proper procedures, from using VPNs to two-factor authentication.

Evidence from elsewhere suggests in particular that small- and medium-sized businesses are particularly behind the curve when it comes to cyber awareness training. This isn't necessarily a surprise. Perhaps because of the language or a lack of knowledge regarding training providers, cyber security has too often been placed in the 'too hard' box.

Large organisations that have a clear interest in delivering better cyber security across Britain are pushing forward with schemes to enhance understanding across the business landscape. The government and universities, too, have chipped in with schemes ranging from the introduction to the intensive.

Cyber Essentials

This is a government-backed, industry-supported scheme to help organisations protect themselves against common cyber attacks. There are two levels of assurance – Cyber Essentials Plus is the more advanced version – which offer a snapshot of an organisation's technical cyber robustness. Certification is awarded and a kitemark may be displayed by businesses to assure customers and suppliers. Crucially, since October 2014, government has required all suppliers bidding for certain sensitive and personal information-handling contracts to be certified against the scheme. We expect more red and blue tape of this nature in the coming years. It is important that government work with businesses and cyber experts to ensure Cyber Essentials is for for purpose.

• Barclays Digital Eagles

Cyber security awareness and education by the Digital Eagles is run through a range of community events covering every age demographic for Barclays' personal, business customers and clients and always welcomes the general public.

Barclays has adapted its Code Playground and Tea and Teach initiatives to explore and educate on cyber security. They have DigiSafe Cadets brought to you by Code Playground, a fun and interactive workshop for seven–11 year-olds. The Digital Eagles introduce the basics of coding and game building with a cyber security twist. During each DigiSafe Cadet session, the Digital Eagles also run a mission control workshop with the parents and guardians to increase their awareness and educate them with current themes of online activity for children aged between seven–17 and how to keep them safe.

Barclays also offers DigiSafe in Cyber Space, which is a new addition to the Tea and Teach programme and includes everything an attendee needs to master their digital world, while giving tips and guidance along the way to keep themselves and their devices safe, ranging from fun and interactive activity, support with social media privacy settings and advice on pop-ups to tips on recognising fraudulent emails.

Barclays Digital Eagles are dedicated to helping people protect their businesses, and employee education and awareness is the key to becoming cyber secure. Cyber @Eagle Labs are workshops that Barclays offers across our Eagle Lab sites that give businesses an introduction to cyber security and the opportunity to learn how to protect themselves and their employees from cyber attacks.

Our Digital Eagles work with industry experts to bring to customers and attendees to all sessions the latest intelligence in real time and real language to help them combat cyber threats and stay safe. For further information please contact your local Eagle Lab at labs.uk.barclays

• Barclays Chief Security Office

Barclays Chief Security Office provides comprehensive training and education to embed a security culture, aligned to the security goals of Barclays and driven from the board to every colleague. Together, we deliver a multi-faceted programme to engage colleagues, empowering them to become the strongest link in defending against cyber and physical security threats. This will be achieved through a range of education courses, products and solutions, themed awareness campaigns and events.

• Barclays Business Banking Regional Digital Eagles

The Regional Digital Eagles are currently educating businesses at local events and via national webinars on the subject of cyber security and fraud. If you would like to learn more about the current threats and some generic guidance on what you can do to mitigate risk, please contact your local business manager for more details.

Cyber insurance

Virtually all businesses rely on technology that includes networks with and contacts to third parties – and because of this it can be subject to the risks that lead to interruption of service, income loss, damage to IT infrastructure and of course reputational damage. The examples given earlier in this paper – and those splashed across the front pages – demonstrate the reality of the risk.

Like all risks, a cyber insurance market has developed to cover both first- and third-party protection.

Reputational damage is always hard to quantify. Often, insurance policies might cover the fees for a public relations specialist or – usually for an extra premium – a loss of profits payment. But just as home insurers expect you to take precautions to prevent burglars, so insurers expect businesses to take basic measures to protect themselves against cyber crime.

While immediate financial loss can be insured and perhaps recovered, much more serious and generally uninsurable is reputational damage. Businesses which depend upon consumer trust can expect harsh reactions if they violate or are seen to be careless with that trust, and could have far more lasting and significant impact than simply a bad headline or two.

A check list for business

Prepare for GDPR – understand what it means for your business and how you can prepare.

Ensure your **directors and board members** are trained on the business risks of cyber security.

Run an **attack simulation** with senior management to ensure your processes are suitably robust in the case of an attack.

Ensure all your staff have **regular cyber awareness training**, building it into induction processes and ensure your people are a robust and secure first line of defence.

Regularly **scrutinise** your cloud and server suppliers to ensure their processes are up to date.

Investigate whether you need cyber insurance, and whether it is already covered by any IT disruption policy.

Incentivise employees to spot false invoices or emails, and encourage honesty when human error has been made

Case study

From the top: boardrooms and cyber security

James Jarvis, corporate governance analyst, Institute of Directors

It is increasingly hard to imagine a business operating in the UK without some form of digital interaction. Be it consumer sales, company accounts or customer reference management systems, utilising the opportunities presented by the cyber revolution can lead to increased profit and efficiency. However, with this opportunity comes risk, both to revenue and to reputation. Cyber security is no longer a case of protecting against viruses; it now requires an evolving strategy to protect the business and its customers from cyber criminals. Cyber crime is increasing at a massive rate (the ONS estimates that there were 5.6 million fraud and computer misuse crimes in the 12 months up to the end of June 2016). Moreover, the fallout for a company from a breach, especially smaller businesses, can be catastrophic. It is hard to picture an SME being able to survive the impact of a security breach the size of those at TalkTalk or Sony.

These notable and public breaches of a company's data have highlighted the risks of not having a proper plan in place, and the PR damage that can result from poor crisis management. Where ultimate responsibility lies for security can be a bone of contention. A recent survey conducted by a FTSE company showed that while a large proportion of IT professionals think that responsibility falls to boards, directors themselves believe it is the responsibility of IT teams. With an issue as complex as cyber security, the reality is not as black and white: the solution lies in both knowing their separate roles.

Cyber security is of such critical importance to modern companies that it should clearly be viewed as a principal risk to business. Responsibility therefore for outlining a prevention strategy should fall to the board. While a company's tech team is clearly best equipped to deal with an issue should it arise, the strategy guiding them falls to the board to dictate. This can and should be done with the support of senior IT staff so that the board is fully equipped to set such strategy. Executive directors should realise the importance of having tech-savvy NEDs on their boards not just to ensure that there is a degree of expertise informing strategy in relation to cyber security but to also allow the organisation to capitalise on the constantly developing opportunities presented by the digital revolution.

Directors, especially in SME companies which perhaps do not have the capacity to hire an IT specialist or chief information officer, will need to ensure they are equipping themselves as best as possible with the information to inform strategic decisions. While a director's responsibility to the health of a company is nothing new, the rapidly evolving nature of digital – and the threats that come with it – add a new demand to their duties. Risk in business is also nothing new and, indeed, it will never be possible to completely remove it. It is for directors to assess the potential risks a business faces and to use this to inform the company's strategy, including an action plan for a worst case scenario attack. If a board is not able to fully understand a company's digital strategy, and the risks involved, shareholders would be right to question whether they are fulfilling their role correctly.

The cloud – is it right for you?

As ever in the cyber security field, language and terminology can sometimes obscure the truth. The cloud is a storage solution which allows firms and individuals to remotely store data, including applications and files, on server space leased from a third-party provider. But that is the point – rather than your data sitting in some kind of ethereal, other-worldly cloud, your data is in fact simply stored on someone else's server.

Now while the cloud has retained a degree of trust, in large part due to the success of organisations like Apple and Google, no new technology should ever go without challenge and questioning. A full two-thirds of IoD members now use cloud-based storage services to back up their files and data. With new regulations increasing the fines and responsibilities of business on cyber security, it's important to ask the right questions.

The benefits of cloud solutions are as you might expect – because larger cloud providers can exploit economies of scale, server space tends to be cheaper than dedicated internal servers, and "flexing" space as your business grows or consolidates is unsurprisingly much easier. In theory, it makes your life much easier.

Cloud providers should be challenged on their ability to turn round support when something goes wrong, and what their own track record is when it comes to cyber security. It's also important that firms ensure they have a degree of data portability that might allow them to move cloud providers without disentangling complicated and interconnected networks.

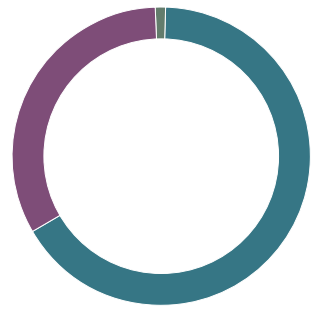
In short, cloud provision is no panacea for security. As more business leaders move data to the cloud, it stands to reason that cloud providers could become the mother lode for cyber criminals. Both cloud providers and their clients must put cyber security at the top of their agenda.

Do you use a cloud-based storage service/account to back up your files or data?

66% Yes

33% No

1% Don't know/ Not applicable



Future threats on the horizon

In the words of Marc Goodman, author of *Future Crimes: Everything is Connected, Everyone is Vulnerable and What We Can Do About It*: "We are in the first seconds of the first minutes of the first hours of the internet revolution." It's not a surprise, therefore, that as the fourth industrial revolution takes hold, the threats from cyber criminals continue to evolve.

Now, this has some perverse consequences. Bank robberies in the US are down 60 per cent since their peak in 1991 – criminals are evidently moving online.[7]

So if nobody is putting balaclavas on and robbing banks anymore, what are they doing? One cyber expert, Jason Glassberg, has identified what he sees as the major coming threats.[8]

Cyber extortion is a particular concern – ransomware is expected to become a far greater threat in the decades to come than it is now. And, as some commentators have noted, attacks on national governments or large financial institutions could become the norm, with obvious knock-on effects for business leaders and companies. The excitement of 'smart cities' – which use data to deliver a better lived experience for individuals living within connected and intelligent urban areas – and the machine learning alongside this could well be sullied if hackers are able to hold mayors to ransom by stopping the traffic, *Italian Job*-style.

Another concern on the rise is the so-called "brick attack" – so named because your PC, bank account or mobile phone can be turned into something *entirely* useless. While there's no obvious criminal victory from doing so, could this be the future of business-on-business cyber crime? Or could foreign governments use such attacks as a way to give state-owned enterprises or firms friendly to unfriendly regimes a boost against the competition?

And of course, it would be remiss not to mention the coming internet of things. As we connect ever more of our lives to the internet and connected devices, so we become more vulnerable. It may seem impossibly far-fetched, but ransomware that affects a temperature gauge in a house could leave individuals so cold (or so hot) that they simply give in – these are loosely badged as cyber assaults, in which cyber criminals use their access to connected devices to impact the physical environment rather than just the virtual.

What's more, there are other 'future trends' to look out for. With the arrival of the catchily-named Payment Systems Directive 2, banks will be obliged to offer access to their customers' accounts through open application program interfaces (APIs). In layman's terms, this means that websites, apps and any third party will be able to build financial services software using the data and infrastructure that underpins bank accounts. This will increase competition across established industries; no bad thing – but it has a significant cyber security impact.

As one report has noted, this means banks will have to "open up a significantly greater attack surface to potential cyber adversaries, and can no longer hide critical applications behind perimeter firewalls".[9] Along with the GDPR, this leaves financial institutions at real risk of significant fines if their secure data is accessed by third-party players; it is entirely possible, for instance, that a customer could log in to their bank account through their Facebook account – or indeed a fake Facebook account. Fraud teams in large financial institutions are going to be earning their money in the years to come as they attempt to put enough checks and balances into place to avoid being caught out through no fault of their own.

[7] American Bankers Association Journal, *Old-fashioned bank robberies are declining*, March 2014

[8] Fox Business, *The Future of Crime*, May 2014

[9] Accenture, *PSD2 & Open Banking*, January 2017

Further support from government

The interaction between private and public sectors is an often contentious one, and where government support should start and end is a matter of debate. That is not usually the case when it becomes issues of national security – and cyber security is certainly that. The government must therefore nudge businesses towards greater cyber security awareness and readiness.

Clearer guidance on GDPR

Through the Information Commissioner's Office, businesses have access to a sizable amount of information regarding the impact of GDPR on their internal processes, but it relies on businesses going to the ICO and proactively seeking out the information.

This is, regrettably, not always the case. Business leaders are busy people – and often while building their firms, delivering wealth creation and jobs growth, issues such as new regulation slip off the agenda.

As such, the government must make more of an effort to advertise guidance on GDPR and how it will affect small businesses, offering advice to business leaders about how to comply without jumping through onerous hoops and what questions to ask the myriad cyber security consultants who may be looking to capitalise on uncertainty. In particular, it may look to expand the amount of information sent to private businesses via joining up HMRC, BEIS and other government departments who have more regular contact with the business community with those government agencies tasked with cyber security protection.

Furthermore, the government should outline how it will use its derogations within the GDPR to ensure that innovation and new technologies are not unwittingly held back. The UK is a remarkably fast-moving digital economy and we must ensure that regulations are applied in a way that does not detract from this vibrant ecosystem.

Encourage board directors to take up training courses

In recent years, central government efforts to change behaviour in corporate boardrooms has been broadly effective, despite the relative lack of legislation in the area. Rather, a combination of public pressure and private lobbying has seen serious changes with regards to transparency, diversity and public awareness of company structures and director responsibilities.

This model could be adopted in a campaign attempting to 'future proof' today's boardrooms. Encouraging firms to adopt cyber security as standing discussion points may encourage a more honest discussion of the threats facing a particular firm around the boardroom, and lead to the cultural change across organisations that is required to ensure cyber crime readiness.

Consult on ways to incentivise cyber training and cyber insurance

The government's Cyber Essentials scheme has achieved its success in large part due to the potential for a certified business to use a kitemark on its website and marketing materials.

Whitehall should look at other inventive ways to encourage businesses to adopt cyber security awareness training or secure cyber insurance. This might go as far as creating tax reliefs to encourage, in particular, the former. Beginning the conversation would be a wise first step.

Conclusion

If there is one lesson from history, it's that technological progress rarely reverses course. And it's in that context that we must view cyber security.

Britain's economic success in the years to come will boil down to our ability to build on existing strengths in the digital economy and capitalise on new technologies. Regardless of the threats on the horizon, we must not be scared of this future – for, whether we like it or not, it is the future.

But we should not go in blind. This report has revealed that business leaders are still putting cyber security on the back burner – and the results, even for small- to medium-sized businesses, could be catastrophic.

The good news is that there are already numerous schemes and support bodies in the field who have produced high-quality work and offer welcome and rigorous advice. The business community must seek them out.

The digital world presents many opportunities for business, not least reduced costs, often a better customer experience, and an ability to trade globally. These are exciting times, but we must ensure we are secure while we push forward into the 21st century.

Institute of Directors

For further information on this report, please contact:

Andy Silvester
Head of campaigns and deputy director of policy
+44 (0)20 7451 3263
andrew.silvester@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.

iod.com

Training
Events
Networks
Mentoring
Research
Influencing