
# What Every Business Leader Should Know About Cyber Risk

*As a nonprofit professional association with 125,000 certified cyber, information, software and infrastructure security professionals, (ISC)² and its members are working to raise awareness of what occurs on the front-lines of cybersecurity practice to ensure a safer and more secure cyber world. This paper shares their perspective on five fundamental areas that will help businesses take back control of cyber risk and be better prepared for the unknown.*

## Introduction: Cyber Risk is a Business Risk

Rapid adoption of technologies is transforming the business landscape at a relentless pace. The pressure is on to reap the benefits of connecting every system, however sophisticated or simple, from the high-profile innovations such as driverless cars, and remotely connected medical devices to the tasks that allow product fulfilment and inventory management across a vast and distributed network of retailers. It's a transformation that reaches far beyond the systems themselves to enhance what people can achieve and their levels of independence, delivering huge productivity gains and new opportunities for organisations.

Unfortunately, the transformation comes with new risks as hostile individuals and groups have also exploited the changing landscape for nefarious purpose. Such threat actors have the skill, the motivation and the time to research targets, craft and launch attacks, and are contributing to an evolving and proliferating threat landscape that has become both increasingly sophisticated and easy to access by those that would do harm. Businesses and organisations have as a result found themselves dependent on new capabilities long before they have developed a clear understanding for how they are leaving them vulnerable.

For most organisations, whatever their size, cybersecurity has been a consideration. Preparations, however, are not standing up to the test of a real-world cyber-attack or reflecting the impact being felt. This is because information and cyber risk remains poorly understood outside of the information security profession, limiting the commitment and ability to robustly quantify the risks. High-profile examples of incidences demonstrate this daily, while companies are increasingly exposed to harsh press and regulatory scrutiny: Recent attacks forced the cancellation of non-emergency treatment across many NHS Trusts; Tesco Bank customers were defrauded of £2.5 million[1]; Chrysler was forced to recall 1.4 million hackable cars[2] and there are many other examples that can be cited. In all these cases, customer service, reputation and operations were severely disrupted. Smaller companies too, are targeted as part of the supply chain of larger

[1] https://www.theguardian.com/technology/2016/dec/02/tesco-bank-cyber-attack-involved-simply-guessing-details-study-claims
[2] http://money.cnn.com/2015/07/24/technology/chrysler-hack-recall/index.html

organisations or for having less sophisticated defences, and often the attacks are not targeted, just aimed at those that can be penetrated.

Reported breaches are now 60 times what they were a decade ago[3], while Lloyds of London[4] estimates a serious cyberattack poses a financial risk to the global economy equivalent to that of a superstorm such as Hurricane Katrina. Cybersecurity cannot remain the concern of the Chief Information Security Officer (CISO) alone. Business leaders must rather move to work with their CISO and overall security resources to actively gauge their new dependencies, and the investment in risk treatments that are warranted.

To begin the process, we offer five action points to follow:

1. **Accept cyber risk is a business risk**
2. **Align cyber spend to your risk**
3. **Create a culture that prevents vulnerability**
4. **Get control of data**
5. **Ensure security and privacy are 'baked in' to processes**

## 1 Accept Cyber is a Business Risk

Traditional business risks, such as failed product launches and physical damage to assets are typically believed to be far more potent and tangible than cyber risk. What organisations fail to see is that a cyber event can have a similar impact. For example, TalkTalk did not devote the same attention to cyber risk as to other business risks and failed to notice a critical vulnerability in its systems for which a patch was publicly available. This oversight led to a criminal cyber-attack, a record-breaking £400,000 fine, the loss of 95,000 customers and ultimately cost TalkTalk over £60 million[5] as its share price tumbled.

On average, organisations suffer over 100 targeted cyberattacks a year. One in three of these attacks — an average of 2–3 every month — are successful.[6] The lessons being learned from current breaches are that cyber risks do not just affect IT systems, but are also a contributory factor, and even enhance the likelihood of business or physical risk. One incident from the steel industry resulted in significant damage to a factory and blast furnace in Germany, when hackers successfully breached office systems that opened a window to production systems.

The challenge of securing organisations therefore goes beyond the resources of cybersecurity professionals and the small pockets of deeply technical experts that analyse the threats. A holistic understanding of both the nature of the cyber risk that your organisation faces and the potential impact on your business is needed to guide the necessary treatments.

The impact of breaches can include loss of revenue, intellectual property (IP) and customer data, as well as reputational damage and loss of consumer trust. Such broad and varied concerns call for a fundamental

[3] http://www.pwc.com/us/en/press-releases/2016/pwc-gsiss-2017-announcement.html

[4] https://www.lloyds.com/news-and-insight/press-centre/press-releases/2017/07/cyber-attack-report

[5] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/

[6] https://www.accenture.com/us-en/insight-building-confidence-facing-cybersecurity-conundrum

realignment in the way business risks are managed and prioritised and a comprehensive assessment right across the business.

### To make this fundamental realignment happen, business leaders should:

- **Acknowledge that cyber risk exists as a current and high-level threat to their business**
- **Debunk the perception that information and cyber risk is a technology problem to be managed by the information security and IT functions**
- **Place cyber risk on the organisation risk register**
- **Create or enhance the governance framework to include cyber risk management**
- **Bring the CISO into all risk discussions**
- **Identify the key operational dependencies and prioritise resource for protection**

## 2 Align Cyber Spend to Your Risk

(ISC)²'s Global Information Security Workforce study[7] has reported increasing security department and IT security budgets for over a decade. Hiring of security personnel is also robust with 70% of hiring managers around the world participating in the survey planning to add to their teams in the next 12 months. Despite this investment, our Workforce study shows that since 2013 there has been a declining global state of security readiness with organisations taking longer to recover from a breach and often unable to identify the cause. Even though they are armed with bigger budgets, cyber security professionals are forced into a 'fire-brigade' approach of simply addressing security incidents when they occur. Instead, business leaders at varied levels must work with security professionals to proactively assess specific risks to their organisation, project or function, not just the systems, to develop a robust understanding of the most appropriate and level of resources required to mitigate or manage them.

[7] http://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html

There is no one-size fits all solution. Organisations must develop their corporate 'cyber literacy' to reflect the context of their industry, their business and their organisational culture. This provides the framework for managing the inevitability of a breach, including assuring a consistent and desired standard of response. It provides the guiding principles to help identify, for example, key data assets, how they are processed and stored, and the controls and levels of protection that should apply along with any relevant insurance considerations.

### Business leaders should challenge their managers and the CISO to:

- **Use a consistent and robust methodology to identify, treat and manage cyber risks**
- **Highlight critical systems and data**
- **Assess regularly the vulnerability of those critical systems and data against an evolving technological landscape and threat**
- **Implement cyber risk treatments and measure their performance over time**
- **Show how risk treatments are effective at reducing risk, through metrics, KPI or KRI**
- **Demonstrate how investment is matched to risk**
- **Link cyber risk to organisational frameworks such as Enterprise Risk Management**
- **Invest in technology and expertise to assess and manage the measures taken by partnerships and suppliers to maintain a level of cyber security proportionate to the identified risk**
- **Prepare, and regularly rehearse, organisation response to cyber events in a way that reflects the value of the data or systems breached and the potential impact on their organisation.**

## 3 Create a Culture that Prevents Vulnerability

Organisations require a dialogue that ensures cybersecurity is broadly appreciated as being more than an IT or specialist concern and plugs into the business acumen that is driving its success. This dialogue should cover how the organisation, its products, services and business processes are evolving, and must be grounded in the terminology of, not just risk, but also ambition, development objectives, sector traits and so on. Business leaders should regularly and actively challenge IT and information security leaders on how organisation developments and innovations could open them up to new risks.

IT and security leaders must challenge the business to communicate not just their requirements, but also their aspirations for how systems will be used by people, employees and customers, so everyone can gauge potential risks. This is a two-way street: as much as information security leaders can push this dialogue, business leaders must make time to listen, comprehend and discuss the risks so that everyone can fully develop their understanding.

Over time, an appreciation of the motives for attack, the known habits and design flaws that introduce vulnerability, the trends prevalent within their sector and the like, add to the organisation's overall resilience. This goes further than the need to develop user awareness: engineers and department managers must develop the instincts to ask the right questions, identify requirements and provision solutions when and where relevant. For example, software engineers must anticipate security requirements, including the potential for misuse, not just usability, as part of the design and understand how to commission relevant 'stress tests.' Risk managers must be able to calculate costs against anticipated impact within the right context: A data breach at a healthcare organisation will likely produce a different cost equation than one at a chocolate factory. Eventually, every business unit

should proactively build up a specific understanding of how their organisation, or their latest innovation, might be vulnerable.

A good place to start this dialogue is with the human vulnerabilities, as this affects all employees. A common and fast-growing technique, 'phishing' attacks, most often in the form of fraudulent emails, lure employees to click on a link that could launch a malicious piece of software, share sensitive information, or even transfer money. In 2016, the CEO of Austrian aerospace parts manufacturer FACC, lost his job when he failed to spot an email scam that cost his organisation $47 million[8]. The development of digital profiles across social networks means everyone can be effectively targeted. Training should be designed around the relevant concepts that apply to an individual's job. Finance can be tested on their ability to identify fraudulent attempts to transfer money, and all staff can learn to recognise a genuine email from their HR department. As everyone is effected, the effort to raise awareness around phishing attacks opens the door to broader conversations about cyber risks.

## Building a culture does not happen overnight. However, business leaders can:

- **Emphasise cyber risk in all their discussions**
- **Encourage cross-departmental cyber security collaboration**
- **Build awareness and education about cyber risks into all the training materials of the organisation**
- **Link objectives, bonuses and pay to the identification and management of cyber risk**
- **Set expectations that all projects, business cases and initiatives address cyber risk and have consulted with the CISO**
- **Question and require regular reporting and updating from direct reports, the CISO and other stakeholders on the cyber risk status of the organisation**
- **Mandate the creation or use of a cyber risk governance framework, management standards and methodologies.**


[8] http://www.reuters.com/article/us-facc-ceo-idUSKCN0YG0ZF[3] https://www.lloyds.com/news-and-insight/press-centre/press-releases/2017/07/cyber-attack-report

## 4 Get Control of Data

Due to the ease of collection and the cheap cost of storage, many organisations harvest as much information as possible without properly defining its value or how they intend to exploit it. Harvesting, storing and sharing information has to date been both technically easy and low-risk. Yet the task of tracking and protecting it is increasingly difficult. According to the Veritas Global Databerg report[9], 85% of data held by European organisations is either redundant or has no known value, leaving only 15% considered as business critical. Against this background, data exfiltration — the copying and theft of data — has become the number one concern for 2017[10] within security professional communities around the world. If an organisation is ever to manage its cyber risk, it must understand what information it collects, processes, transmits, stores and destroys by assessing its information risk.

Governments are increasingly coming to this conclusion and mandating the responsible use, management and protection of data that is housed on an organisation's systems and within their products. Penalties are set to escalate in May 2018 when the European Union's new General Data Protection Regulation (GDPR) comes into force with fines set at up to 4% of worldwide turnover and new rights for individuals leading to further costs and penalties. GDPR not only requires organisations to know about a significant sub-set of their data — that which has personally identifiable attributes for any EU citizens — but also demonstrate that they have a legal basis to store it, use it, and are both managing and securing it properly.

This presents a clear need – and opportunity – to identify information that is of value to a given business unit or process and eliminate the rest. It sets out principles and rules that will form the expectations of the future for doing business responsibly, and competitively, while also creating a pathway for expressing clearly the harm to a business, customer, or society should a malicious or accidental incident occur. Customers rightly expect that organisations will take good care of any information they share and any organisation that can demonstrate that good care may be able to convert it into competitive advantage or into new products and services.

### To get control of data, business leaders can:

- **Use legislation and regulation to 'clean house', i.e. challenge why data is being retained and push for old or out-of-date data to be deleted**
- **Identify information that is critical to the business and discover where it is stored**
- **Identify information that may be subject to legislation or regulation**
- **Instigate projects to improve data quality**
- **Ensure that relevant risk treatments are aligned to the value of data**

## 5 Design in Security, 'and Privacy'

The lack of understanding of cyber risk means that too many businesses continue to build, buy or use their IT without security in mind, thereby increasing their risk. Security must be designed into products and services, the strategic direction taken with IT systems, employee policies and more. The consequences of not doing so were aptly demonstrated when an attack exploited idle computing capacity to be found in internet-connected toasters, refrigerators and other appliances, to bring down much of America's internet[11] and the big

[9] https://www.veritas.com/news-releases/2016-03-15-veritas-global-databerg-report-finds-85-percent-of-stored-data

[10] https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf

[11] https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet

companies that relied on it, including Amazon, Spotify, Netflix and the New York Times.

Relevant considerations for your organisation include: business processes; new technologies you plan to embed within your environment; their connection to legacy systems; how suppliers work with and contribute to this environment; connections to other environments such as inventory; design criteria for contributed components, who is involved at every step and how you will protect your customers' information at every point in the customer journey.

Many organisations simply do not understand cybersecurity well enough to engineer their business practices, systems and products so comprehensively, leaving them heavily reliant on testing at the point of release of a new product or service. This not only limits the scope of security assessment but also sets delivery teams up to resist implementing whatever results the testing turns up, as they introduce delay and often unanticipated cost as deadlines loom. The majority of reported attacks exploit often well-known, but missed or ignored vulnerabilities.

Organisations should bring security expertise into the beginning stages of any development to deliver robust risk assessments and treatments. Building security in, just like creating a culture, takes time.

## Business leaders can take positive action, using the following steps:

- **Mandate a cyber risk assessment for all new IT-related projects**
- **Require all project managers to build in regular cyber risk reviews and include cyber risk in major project review milestones**
- **Adopt, where relevant, standards for secure software design**
- **Build in time for security testing throughout the development process**
- **Halt projects where cyber risk has not been adequately considered and remediate**
- **Buy in tested, secure products where development is not considered viable or is outside the organisation's remit.**

## In Conclusion… Leadership is key

The pace of change in today's business landscape is increasing complexity and introducing new risks that challenge our understanding of what good business practice means in a connected world. It is time to set our organisations on a journey to becoming a resilient thriving concern in this world. CEOs and Boards can look to the cybersecurity profession as advisors, managers and fonts of front-line knowledge — but not as the front-line of accountability. Business leaders themselves must grasp the challenge, set the dialogue and motivate the robust understanding and response required to stand the test of real-world cyberattack.

Cyber risk is a business issue and responsibility, not just the domain of the experts.

## About (ISC)²

(ISC)² is an international nonprofit membership association focused on inspiring a safe and secure cyber world. Best known for the acclaimed Certified Information Systems Security Professional (CISSP®) certification, (ISC)² offers a portfolio of credentials that are part of a holistic, programmatic approach to security. Our membership, over 125,000 strong, is made up of certified cyber, information, software and infrastructure security professionals who are making a difference and helping to advance the industry. Our vision is supported by our commitment to educate and reach the public through our charitable foundation — The Center for Cyber Safety and Education™. For more information about (ISC)² visit www.isc2.org, follow us on Twitter or connect with us on Facebook.

### References


(1) https://www.theguardian.com/technology/2016/dec/02/tesco-bank-cyber-attack-involved-simply-guessing-details-study-claims
(2) http://money.cnn.com/2015/07/24/technology/chrysler-hack-recall/index.html
(3) http://www.pwc.com/us/en/press-releases/2016/pwc-gsiss-2017-announcement.html
(4) https://www.lloyds.com/news-and-insight/press-centre/press-releases/2017/07/cyber-attack-report
(5) https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/10/talktalk-gets-record-400-000-fine-for-failing-to-prevent-october-2015-attack/
(6) https://www.accenture.com/us-en/insight-building-confidence-facing-cybersecurity-conundrum
(7) http://blog.isc2.org/isc2_blog/2017/02/cybersecurity-workforce-gap.html
(8) http://www.reuters.com/article/us-facc-ceo-idUSKCN0YG0ZF
(9) https://www.veritas.com/news-releases/2016-03-15-veritas-global-databerg-report-finds-85-percent-of-stored-data
(10) https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf
(11) https://www.theguardian.com/technology/2016/oct/26/ddos-attack-dyn-mirai-botnet


(ISC)² CISSP SSCP CAP CSSLP HCISPP CCSP