CGI

Experience the Commitment®

The Cyber-Value Connection

Revealing the link between cyber vulnerability
and company value

Contents

Page

Appendices

Foreword

The digital revolution creates unprecedented opportunities for UK companies, enabling them to transform and grow in ways that seemed impossible just a few years ago. But alongside these opportunities come new and unfamiliar cyber security risks which could prevent companies from fulfilling their digital potential, and may even threaten the profitability and survival of the company.

At CGI we have a mission to help business leaders understand and manage these cyber risks, allowing their companies to thrive in the digital economy. Towards this end we have developed The Cyber-Value Connection to put cyber security in a context that will resonate with business leaders.

The Cyber-Value Connection looks at the reduction in company value that arises from a cyber breach, vividly demonstrating how a severe incident leads to a decline in share price. To ensure rigour and independence, CGI commissioned Oxford Economics to develop a robust econometric model using a ‘difference in differences’ technique to isolate the damage caused to company value by a cyber breach from other movements in the market.

The evidence of the connection between cyber breach and company value identified by this method is powerful and, I hope, will contribute towards building more mature cyber security business cases.

At CGI, cyber security is part of everything we do.

We actively encourage other organisations to take the same attitude, especially as our economy becomes increasingly dependent on digital businesses.

Although we deliver security services to many of our clients, the story is not yet complete as companies remain in denial about the necessity to get security right. We hope this study helps your organisation further understand the risks, the impact and the importance of taking action.

Dr Andrew Rogoyski
Vice President Cyber Security Services,
CGI UK

Executive summary: The Cyber-Value Connection

Cyber risk has risen to the top of the corporate agenda but few company leaders are aware of the full extent of damage caused by a cyber breach — or the full costs. CGI has worked with Oxford Economics to create a rigorous model that captures the damage done by cyber breach to a company's share price.

The Cyber-Value Connection reveals that share prices fall by an average of 1.8 per cent on a permanent basis following a severe breach. To put that in context, investors in a typical FTSE 100 firm would be worse off by an average of £120 million.

However, in some extreme cases, breaches have wiped as much as 15 per cent off affected companies' valuations, substantially more than this sum.

The damage to shareholder value is significant today — but The Cyber-Value Connection analysis suggests severe cyber breach will become even more costly in the future as industry analysts include cyber as a factor affecting valuation and new regulation demands that companies disclose incidents.

Clearly, the CEO has responsibility for increasing company value. With the link between cyber breach and company value established in this report, it is clear the CEO's responsibility must also include direction and governance of cyber security. The Cyber-Value Connection concludes with advice on how they can challenge their organisation and put in place effective governance.

Setting the scene

Cyber security is now a leading item on the global agenda: the World Economic Forum[i] recently identified 'massive cyber breach' as one of the top technological risks to continued global growth.

There can be no doubt that the world is now awake to the risks posed by cyber security. The last few years have seen a gathering succession of stories about leaks, hacks and cyber attacks affecting governments, political parties, private individuals and companies across every sector. High profile cyber incidents such as those suffered by Yahoo! and SWIFT have made people uncomfortably aware of their cyber vulnerabilities.

Cyber security was also identified in the top five business priorities in CGI's Global 1000 Outlook report, where over 1,000 senior IT and business clients were interviewed on their business and industry challenges[ii]. Business leaders certainly understand that cyber is something they need to be on top of: in a February 2017 survey of FTSE 100 companies[iii], 87 per cent stated that cyber is a principal risk to their organisation.

However, in many cases, business leaders may struggle to articulate the extent of these risks within their own organisation and, as revealed by CGI's 2016 study, Cyber security in the boardroom: UK plc at risk[iv], company boards are often not equipped with a clear understanding of the many and diverse issues presented by a cyber breach.

Getting a handle on cyber

It is not surprising that board members, like many employees in non IT roles, struggle to get to grips with the totality of cyber risk. Cyber risk is a big issue: one that extends across the enterprise, from customer facing functions to the back office and beyond through the supply chain. It is a deeply technical problem, shrouded in arcane language and difficult concepts. Cyber risk is multifaceted, representing the different kinds of value lost or damaged by a breach. A cyber incident can mean a company's trusted reputation is lost when customer data is hacked. Or commercially sensitive information, critical to the company's future, is leaked to competitors. Sometimes the nature and extent of damage quickly becomes apparent. In other cases, it can take years for the full scale of the damage to emerge.

Given this inherent complexity, rooted in the use of technology, it has been difficult to highlight the problem to company leaders in a way that guarantees attention. In this report, CGI and Oxford Economics have demonstrated a clear link between cyber incidents and company valuation, as expressed in the share price. This may be the simplest and most powerful method yet to illustrate the damage inflicted by a cyber incident.

The cost of The Cyber-Value Connection

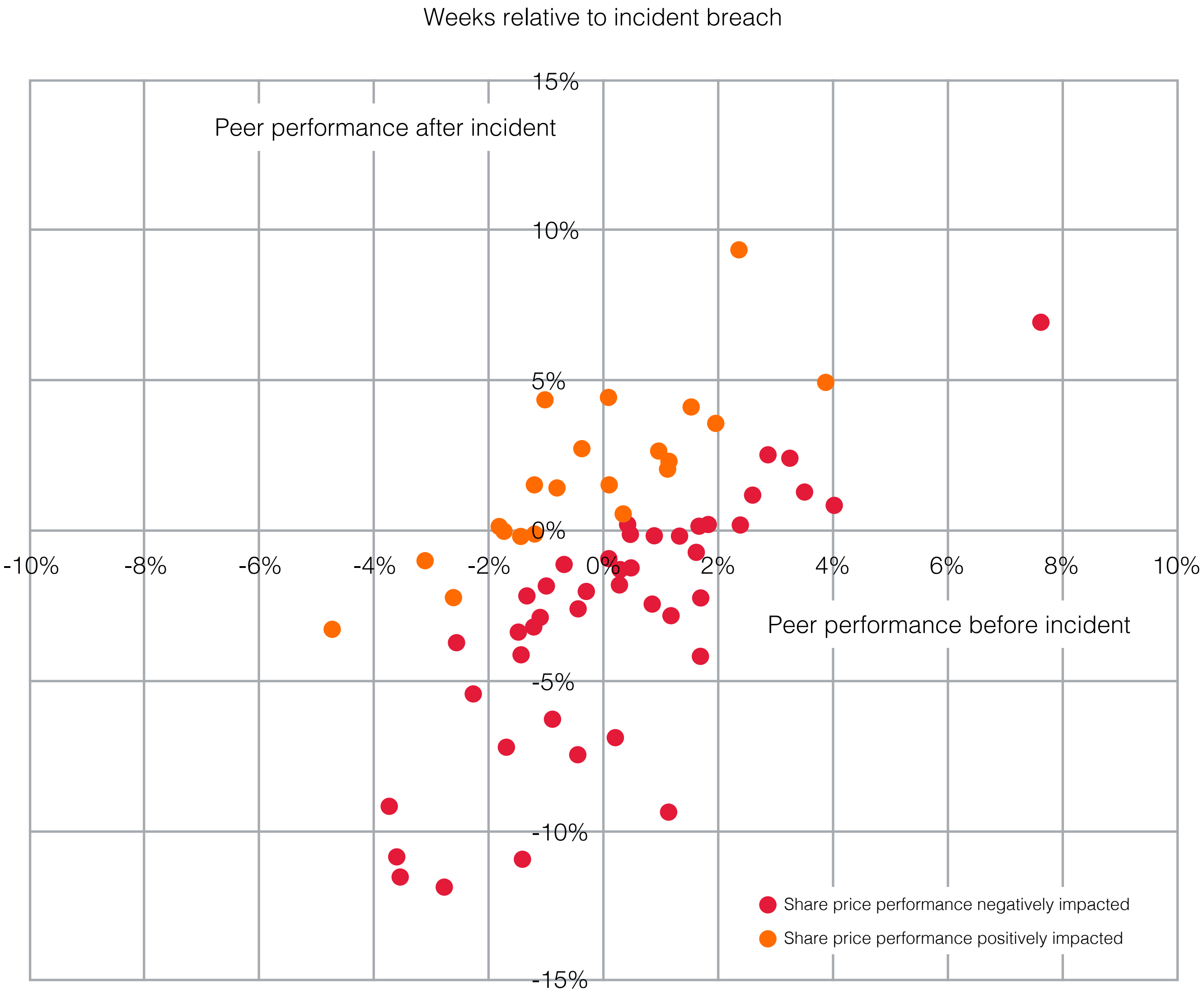
Companies that experience a severe cyber breach see their share value fall by, on average, 1.8 per cent on a permanent basis. What's worse, the analysis undertaken for The Cyber-Value Connection suggests the negative impact on share value is getting more severe, year-on-year.

A company's share price tells you a lot about a company and its prospects: it is the sum of the market's expectations for a company. Broadly speaking, the share price rises when the market has a positive view on the company's future profitability and falls when that assessment turns negative. Could changes in the share price in the wake of a publicly disclosed cyber incident tell us something important about the costs of cyber attacks?

CGI set out to test the hypothesis that there is a link between cyber breach and company value. To ensure independence and rigour, CGI asked Oxford Economics to develop an analytical methodology to examine share price movements in companies that had experienced cyber breaches[1]. At the heart of this method was a comparison of each affected company's share price against a cohort of similar companies operating in the same markets, isolating the impact of the cyber breach from other market movements. Details of this approach are provided in the appendix.

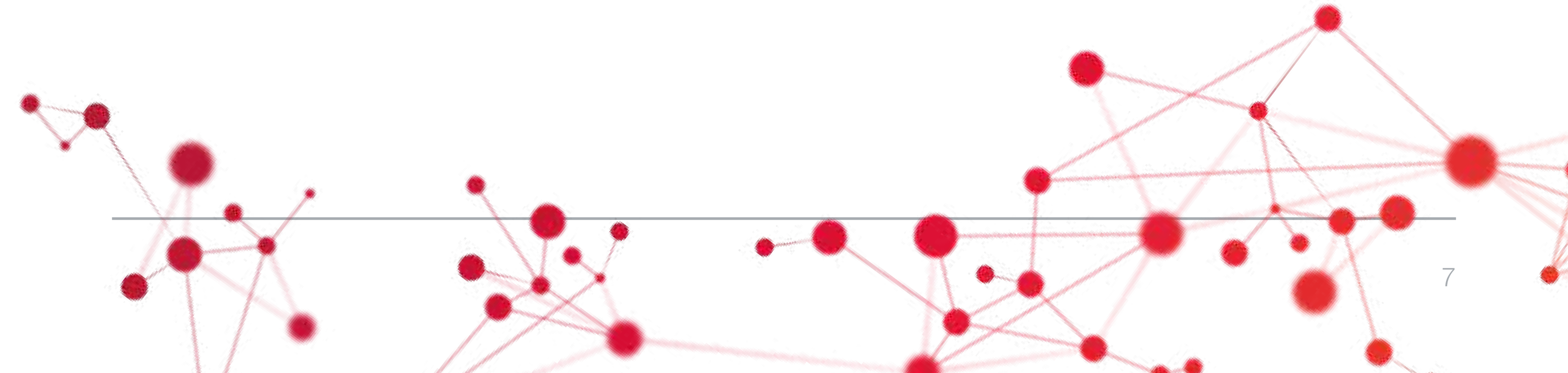
According to Cyber-Value analysis, a severe cyber security breach represents a permanent cost of 1.8 per cent of company value. Two thirds of companies had their share price adversely impacted, in comparison with their peer group, after suffering a cyber breach.

[1] In this study, the term 'breach' is used to describe any form of major cyber incident.



Source: Oxford Economics / Gemalto / Bloomberg

There is some indication that companies that were already underperforming in comparison with their peer group may find that their share price is impacted harder — a reduction of 2.3 per cent in comparison with an average of 1.1 per cent for companies performing ahead of their peer group, although the size of the sample means that is not possible to establish a difference at the usual statistical confidence levels.



Counting the cost

For a typical FTSE 100 firm the impact of 1.8 per cent equates to a permanent loss of market capitalisation of £120 million. Applying the analysis methodology to the 65 companies whose severe breaches were used to compile this study, the cost to shareholders of these companies would be in excess of £42 billion.

In the case of firms that experience a catastrophic cyber breach, where a very large amount of sensitive information is lost or compromised, the impact on company value can be even more dramatic.

Looking at those companies that suffered the ten largest share price impacts reveals just how serious cyber breaches can be in terms of company value. In many cases, these incidents continue to be a topic that affects their on-going business performance, with markets, investors and customers seeking reassurance that business operations are fully restored and that the security vulnerabilities have been removed.

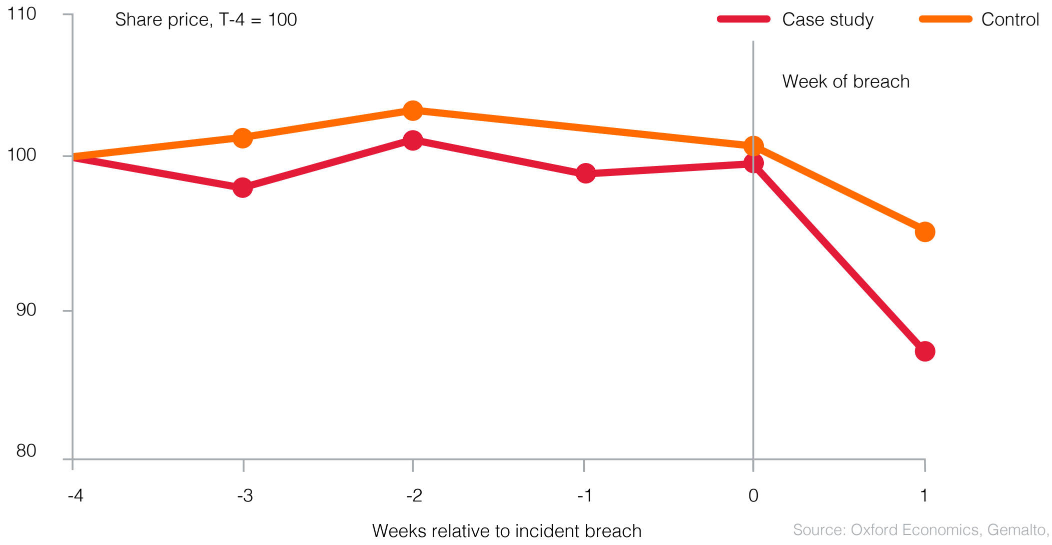
Company sector	Country of listing	Incident year	Share price fall (%)*
Media and communications	UK	2015	-15.0%
Retail	UK	2014	-12.9%
Media and communications	USA	2015	-9.3%
Technology	USA	2013	-8.5%
Technology	Japan	2016	-8.3%
Media and communications	Japan	2015	-7.2%
B2B industrial	Japan	2014	-5.9%
B2C industrial	Japan	2016	-5.5%
Financial	USA	2014	-5.0%
Media and communications	USA	2015	-4.8%

*represents the % change in the firm's share price on the Friday following the attack

Source: Oxford Economics / Gemalto / Bloomberg

Looking deeper at case study examples demonstrates how the organisation's value is impacted in the wake of a breach. One of the firms involved in the Cyber-Value analysis was a UK supermarket chain that had suffered a major cyber attack. This involved significant exposure to the business where sensitive information was lost and the breach rapidly became a mainstream news story.

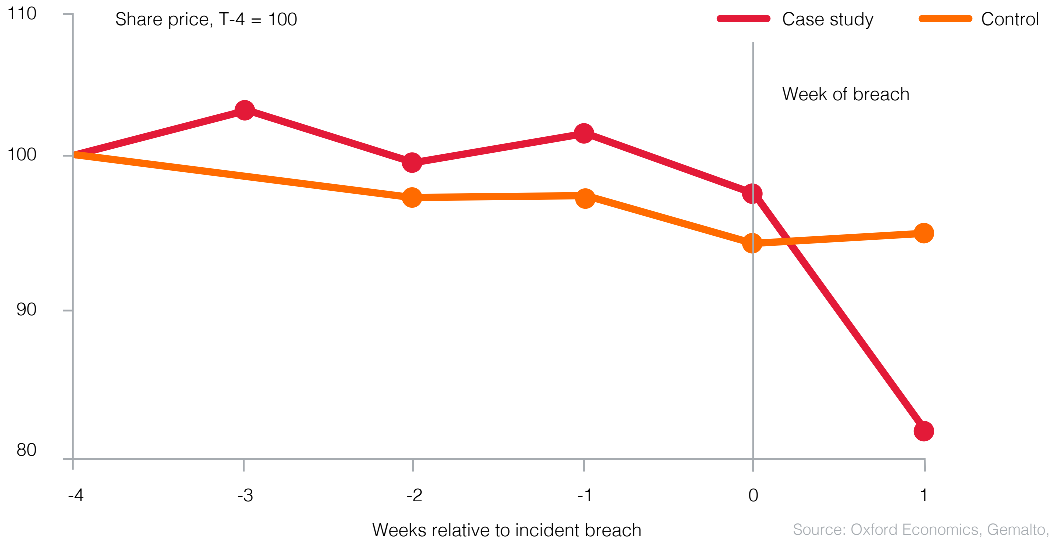
Over the week following the attack the company's share price fell by seven percentage points, compared to the average share price movement in the sector. The situation then worsened when it was announced that the breach had led to legal proceedings against the supermarket. This saw the share value fall a further one per cent.



Source: Oxford Economics, Gemalto, Bloomberg

Another case gave an even more dramatic demonstration of the impact of cyber breach on company value. Here a UK communications firm suffered two separate attacks during 2015. The first attack (shown as occurring in week -2 in the graph below) had little discernible impact on the company's share price.

A second attack (shown in week 0) led to a sharp divergence in the share price versus the control group. While the company estimated that the hack resulted in between £30-35 million in one-off costs, its value fell by over £430 million in the week following the incident.



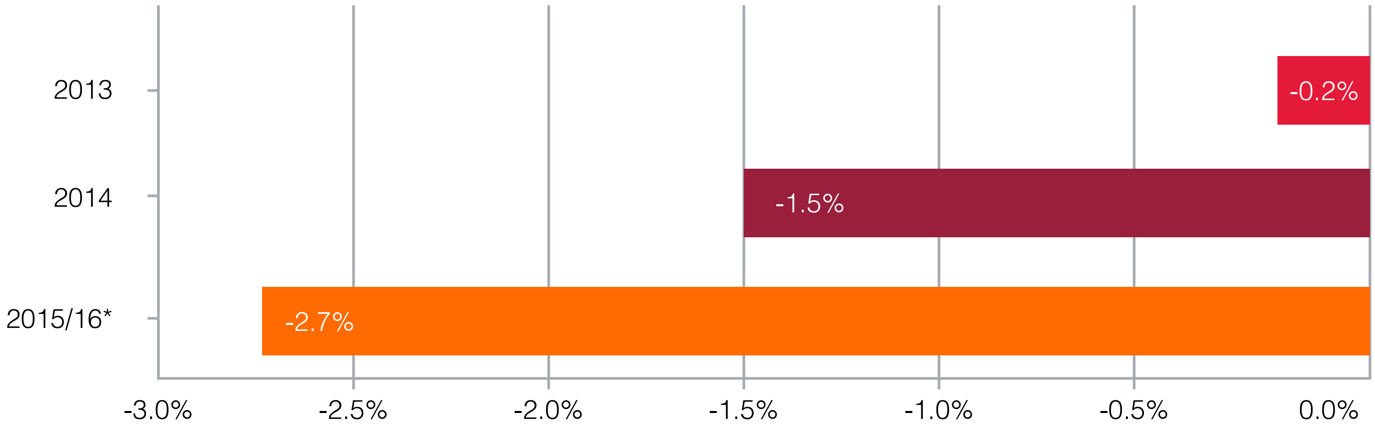
Source: Oxford Economics, Gemalto, Bloomberg

Impact worsens year-on-year

There is evidence that the impact of cyber attacks on share price has become more pronounced over recent years. Analysis of the companies included in The Cyber-Value Connection reveals that breaches that occurred over the past 18 months led to a much more severe negative impact – particularly in comparison to 2013.

The sample size is small, but the trend is clear, also explaining earlier work which found little impact on share price by cyber breaches[v].

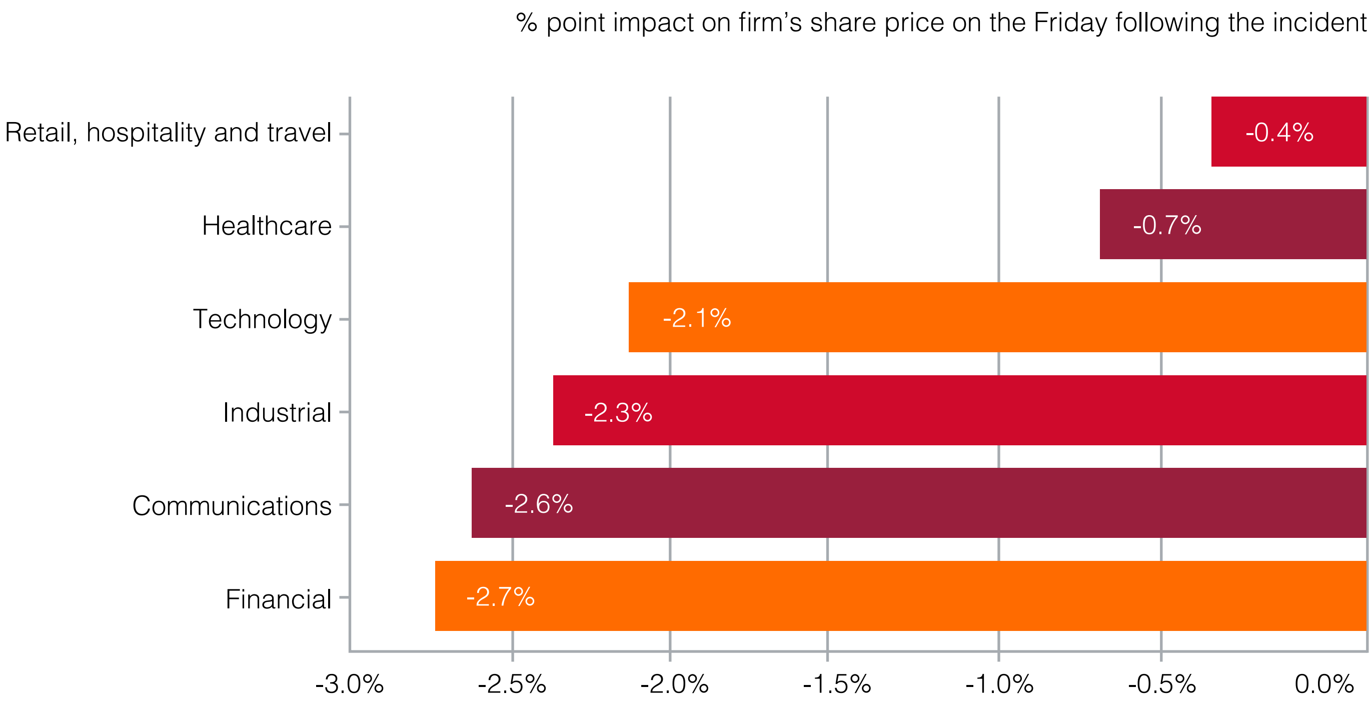
% point impact on firm’s share price on the Friday following the incident



*Statistically significant at the 10% level

Source: Oxford Economics estimates

The value impact varies across sectors



Severe or catastrophic cyber breaches appear to produce markedly different impacts across different market sectors. Understandably, financial services experience the greatest burden in terms of impact, reflecting the high levels of regulation, the importance of customer confidence in these organisations and the potential for financial fraud to be a facet of the breach. Industrial and technology companies that depend on their intellectual property – product designs, processes and tools – are also seen to be severely impacted by a cyber incident.

The relatively low impact on retail, hospitality and travel is perhaps unexpected as companies in these sectors increasingly rely on online sales channels.

When examining the type of incident suffered by companies in the sample, it was revealed that B2C firms (retail and media & communications) seem to suffer proportionately more incidents due to identity theft and account access, whereas B2B sectors, such as technology and industrial, suffered proportionately more incidents of financial access. Understanding the prevalence of certain types of attack allows organisations in these sectors to make better judgements about their risk and their necessary responses.

Factors for the future

Companies are facing a greater degree of cyber scrutiny from investors and regulators alike as the worlds of finance and government become ever more sensitive to the risks of cyber breach.

Today, most cyber incidents occur behind the scenes: CGI estimates that less than ten per cent of major cyber breaches in Europe come to be known about. However, undisclosed breaches will become rare as regulators force cyber incidents into the open with legislation such as the General Data Protection Regulation and the Network and Information Security Directive, both coming into force in 2018 across Europe, including the UK.

Investors demand the full picture

The financial community is becoming more vigilant about cyber security as an issue that can be shown to affect the value of their investments. One recent survey of buy side investors and sell side analysts across the UK, US, Asia and Europe[vi] found most investors would lower post close valuations if either party in the merger had suffered a breach. Verizon's recent offer to acquire Yahoo! was reduced by nearly eight per cent following Yahoo!'s very public cyber breach[vii]. The survey also found that the number of investors that took an investment decision based on the level of security in place has more than doubled since 2014, rising to over a quarter of all investors.

Growing awareness of cyber risk is also influencing credit ratings. In 2015 Moody's confirmed that cyber risk is of increasing importance to its credit analysts when assigning credit ratings to corporations. In the report Cross Sector - Global: Cyber Risk of Growing Importance to Credit Analysis[viii], Moody's identifies several key factors to examine when determining a credit impact associated with a cyber event. These include the nature and scope of the targeted assets or businesses, the duration of potential service disruptions and the expected time to restore operations.

Mitigating risk through insurance

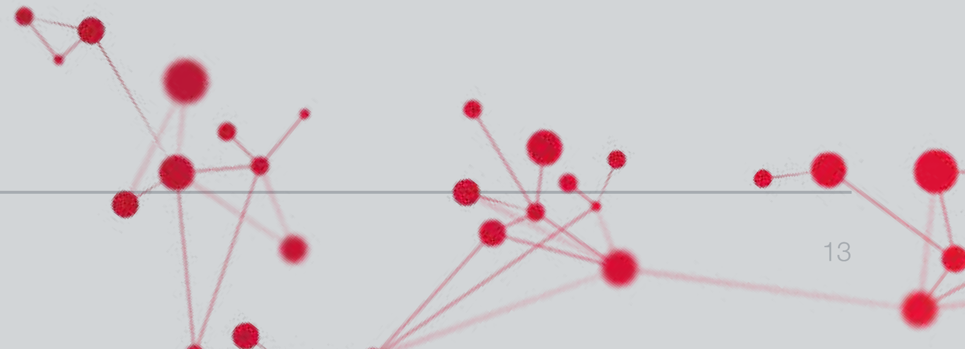
As the level of cyber scrutiny increases, there are a growing number of ways companies can act to mitigate cyber impact. Raf Sanchez, International Breach Response Manager at insurer and CGI partner Beazley looks at the role insurance can play:

“Organisations are collecting more, and more detailed, data about their customers and seeking to monetise this data. The rapid evolution of the regulatory landscape for this data, especially in Europe, means that many organisations are subject to increasingly onerous compliance regimes at a time when the number and nature of cyber risks is growing exponentially.

Beazley sees data security as more than just a compliance issue – it is an ethical, reputational and financial challenge that is the key to maintaining customer loyalty and trust. This challenge can be met through a combination of tailored insurance cover, integrated risk management and third party protection. That is why Beazley provides, as an integral part of our coverage, access to a range of expert services designed to mitigate reputational risk to the insured and diminish the risk of legal action being brought.

Additionally, these services will likely reduce the administrative burden that organisations commonly encounter when handling a breach on their own.”

Raf Sanchez,
International Breach Response Manager, Beazley



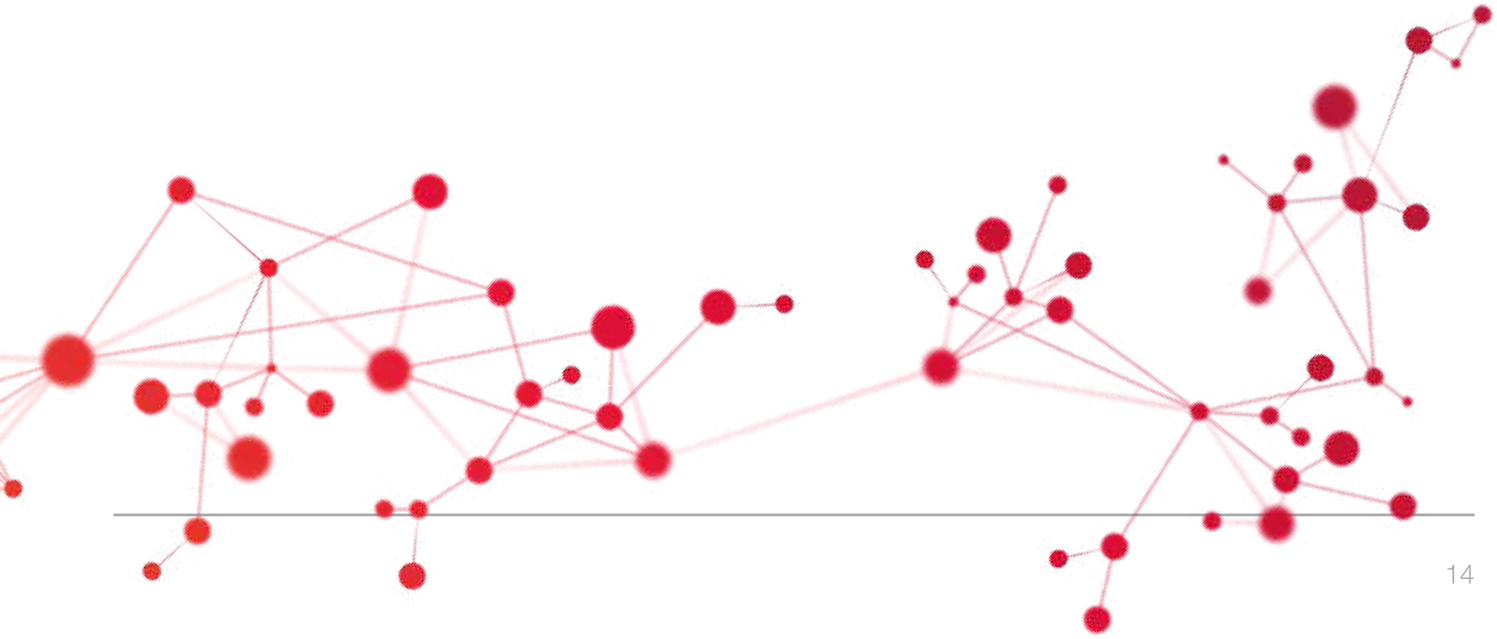
Regulation and cyber disclosure

Many governments are moving towards mandatory breach notification to encourage greater action from businesses to address and mitigate cyber risk. In the US, mandatory breach notification has been a reality in most states for several years. In Europe, it will become compulsory from May 2018 as the General Data Protection Regulation (GDPR) comes into full force.

Building on the long standing 1995 EU Data Protection Directive, GDPR establishes one set of data protection rules across all 28 European states.

GDPR dramatically increases maximum penalties for mishandling data: these now amount to four per cent of global revenue or €20 million, whichever is greater. For many organisations in the UK this represents a huge increase in the ICO's (Information Commissioner's Office) current maximum penalty of £500,000.

Even with the Brexit process gathering momentum, UK companies will, alongside every company operating in Europe, have to adhere to the requirements and suffer the penalties of GDPR. The UK government has made clear with its recent National Cyber Security Strategy[ix] and Cyber Security Regulation and Incentives Reviews[x] that GDPR is here to stay.



A legal perspective

What does GDPR mean for UK companies? Andrew Gilchrist of cyber legal specialist and CGI partner K&L Gates LLP outlines some of the key implications:

“ Many UK companies have still not come to grips with existing UK data protection legislation, let alone the new and even more prescriptive requirements of the GDPR. Their preparation will need to be both operational and legal. There is much emphasis in GDPR of ‘privacy by design’: the idea that businesses should design their business models and data processes around data privacy considerations, rather than trying to retro-fit data protection compliance into their existing systems.

GDPR emphasises the need for upfront impact assessments which should be undertaken by businesses prior to engaging in personal data processing likely to result in a high risk to the rights and freedoms of natural persons. These impact assessments should be ongoing and well-documented, and are likely to be important in the event of a regulatory investigation or complaint. Compliance with GDPR is not simply a tick-box exercise for lawyers: it requires a detailed understanding of what each particular business does, what personal data it collects and for what purposes, who it is sent to, where it resides geographically and how it is protected. Knowing this information will be a key starting point for any effective compliance programme.

The next key step is to have in place systems and processes that can monitor the security of your data processing operations, and enable you to react quickly and decisively in the event a breach occurs. This is not just an issue for your IT managers. In practice, businesses will need to consider and implement insurance, PR, crisis management and business continuity and risk mitigation strategies upfront, and not simply react to a breach when it occurs.

In our view, the response to a cyber breach can only be as good as a company’s preparation for it. Once a breach has occurred, the clock is ticking and a business will only have a short period of time to instruct cyber specialists, lawyers, PR managers and insurers, while at the same time react to fulfil its regulatory obligations and position itself in the best way possible to respond to, and mitigate, any potential regulatory investigation and media scrutiny. Experience shows us that the real threat to UK businesses is not necessarily a fine from the ICO. This is a drop in the ocean compared to the bad press and loss of customer confidence that often follows a cyber-hack. ”

Andrew Gilchrist,
Senior Associate, K&L Gates LLP

Setting the leadership agenda

The Cyber-Value analysis reveals the connection between severe cyber breach and permanent damage to company value. Adverse publicity surrounding recent public breaches means that cyber risk is increasingly on the radar for investors and regulators alike. Combined, this means cyber is a critical issue for the board and, specifically, the CEO.

It is no longer possible to regard cyber risk as a peripheral issue: it is increasingly clear that cyber security is a key factor in a business's performance, reputation and, as we see in this report, its valuation. This makes cyber security a critical issue for the board.

Yet, as revealed in CGI's 2016 study, Cyber security in the boardroom: UK plc at risk, few company boards or CEOs possess the expertise or have access to the necessary advice to implement plans to protect their organisations.

This situation will change. Board members will find themselves under increasing pressure to consider cyber risk and it will become a growing influence on how their personal performance is assessed. Expectations will fall most heavily on the CEO: in the event of a cyber incident, the CEO will find him or herself facing questions from the media, customers, employees and irate investors. Indeed, it is very likely that 2017 will see a marked increase in the number of CEOs forced to resign as a result of a cyber security breach.

Challenging your Organisation — Questions the CEO needs to ask

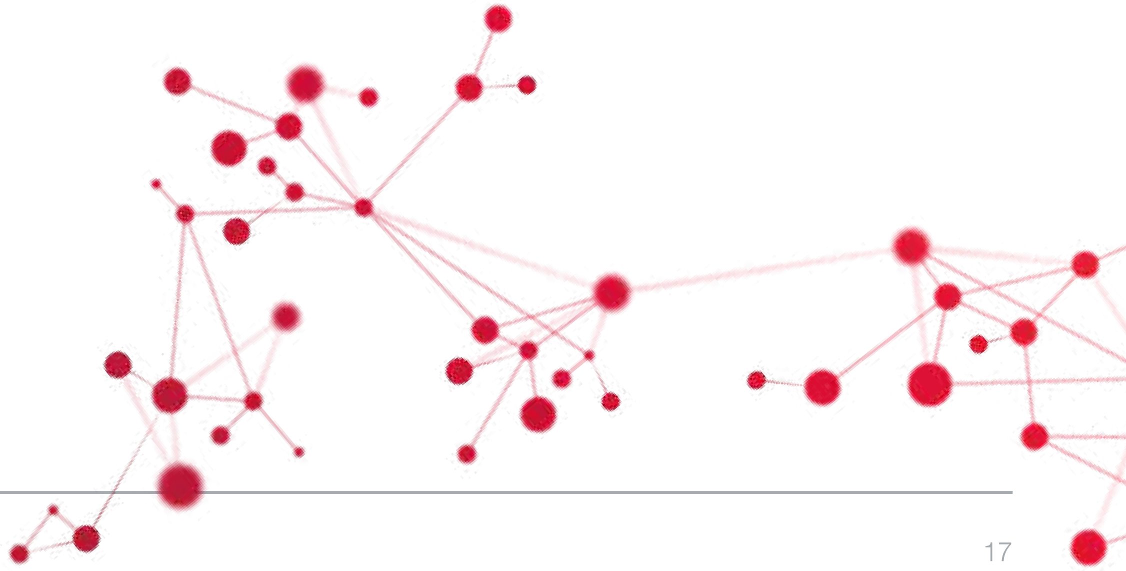
The case for introducing robust cyber governance is undeniable and urgent. The first step towards doing this is for board members to challenge their organisation on cyber issues. Only by asking the right questions can senior executives understand what they know and what they do not know, where there is confidence and where there is not, where plans are prepared and where plans rest on hope. Upon these foundations, senior leaders can begin to build the expertise, personnel and governance for anticipating and managing breaches.

Dr Andrew Rogoyski, CGI UK’s Vice President Cyber Security Services, proposes some areas of challenge across three key themes – questions that CEOs can ask their organisation. These questions are non technical – it is the confidence of the response that will reveal the real state of preparedness within their organisation.

Governance and planning

- **Who is responsible for cyber security?**
  The real answer is that you, as the CEO, are personally responsible for driving security governance, investment, planning and fronting up the organisation at the time of an incident. You may delegate the day-to-day activities to a head of security in whom you must have the utmost confidence but you cannot delegate accountability for a major cyber incident. An accompanying response is that every employee is responsible: everyone needs to play their part in keeping the company’s systems and sensitive information secure.

- **Can you show me our current cyber incident response plan?**
  All organisations that rely on IT systems should have a cyber incident response plan. It describes who is in charge of an incident, who else is involved in the response (the cyber incident response team), external organisations involved (e.g. lawyers, forensic specialists, media handlers and crisis management experts), the processes and procedures to follow, the contact details of key individuals and other essential material. A good plan should be current. It should be exercised regularly to ensure that it is workable, effective and adaptable to change.



Situational awareness

- **Who can brief me on our cyber risk profile *today*?**
  The purpose of this question is to see who has an accurate and current view of the risks that cyber attacks present to your organisation. If your organisation cannot give you this answer today, it may be that no one has thought about cyber risk recently.

- **How many attacks did we see last week?**
  There are many different types of cyber attack: the numbers often aren't meaningful. The key to a good response is that someone is aware of the status. This means being able to tell you how many of the attacks were successful, their impact, the status on fixing any arising problems and even the source of the attack.

- **What did we learn from our last cyber incident?**
  Just to admit that the organisation has suffered an incident is a sign of maturity. All organisations have incidents of one form or another: "we haven't had any" either means that attacks haven't been detected or that someone is covering up. Either of these scenarios is a problem. Treat incidents as an opportunity to learn.

- **What independent tests have we done?**
  Independent assessment of your security measures, from policy and training, through to penetration tests of active systems, is essential if you want confidence that your teams are putting the right measures in place and that they work. Evidence of independent testing is essential if your company has to defend itself against legal or regulatory challenge following a major cyber breach – it is important to show that all reasonable measures were taken to protect your sensitive data.

Business context

- **Is cyber security one of our corporate business risks?**
  Cyber security issues need to receive regular attention by senior leadership. It should therefore be raised out of the IT domain, where it is treated as a purely technical set of challenges, into the corporate risk register where it can be considered alongside all the other business risks that boards regularly review and act to mitigate.

- **How much would it cost us if we lost all our IT systems for a week?**
  This question focuses minds on the degree to which the organisation depends on its IT systems. As companies and economies become digital, the impact grows. The true cost of an IT outage can shock senior leaders who are perhaps unaware of their organisation's dependency on its computer systems.

- **What is the most valuable information that this company has?**
  How the organisation answers this question will give you a good indication of whether information security has been thought about seriously. Many organisations struggle to understand what their most valuable information is. It's not just about customer records and other personal data the company may hold. Data is often at the heart of what gives a company its competitive advantage. It might be the designs for your latest product, your customer database or the details of your next major deal.

- **How much do we spend on cyber security every year?**
  This question is often hard to answer but a well defined approach to cyber security is likely to have well understood budgets. Historically, an organisation might expect to spend five per cent of its IT budget on cyber security. Today, this number is often seen as nearer ten per cent of the IT budget.

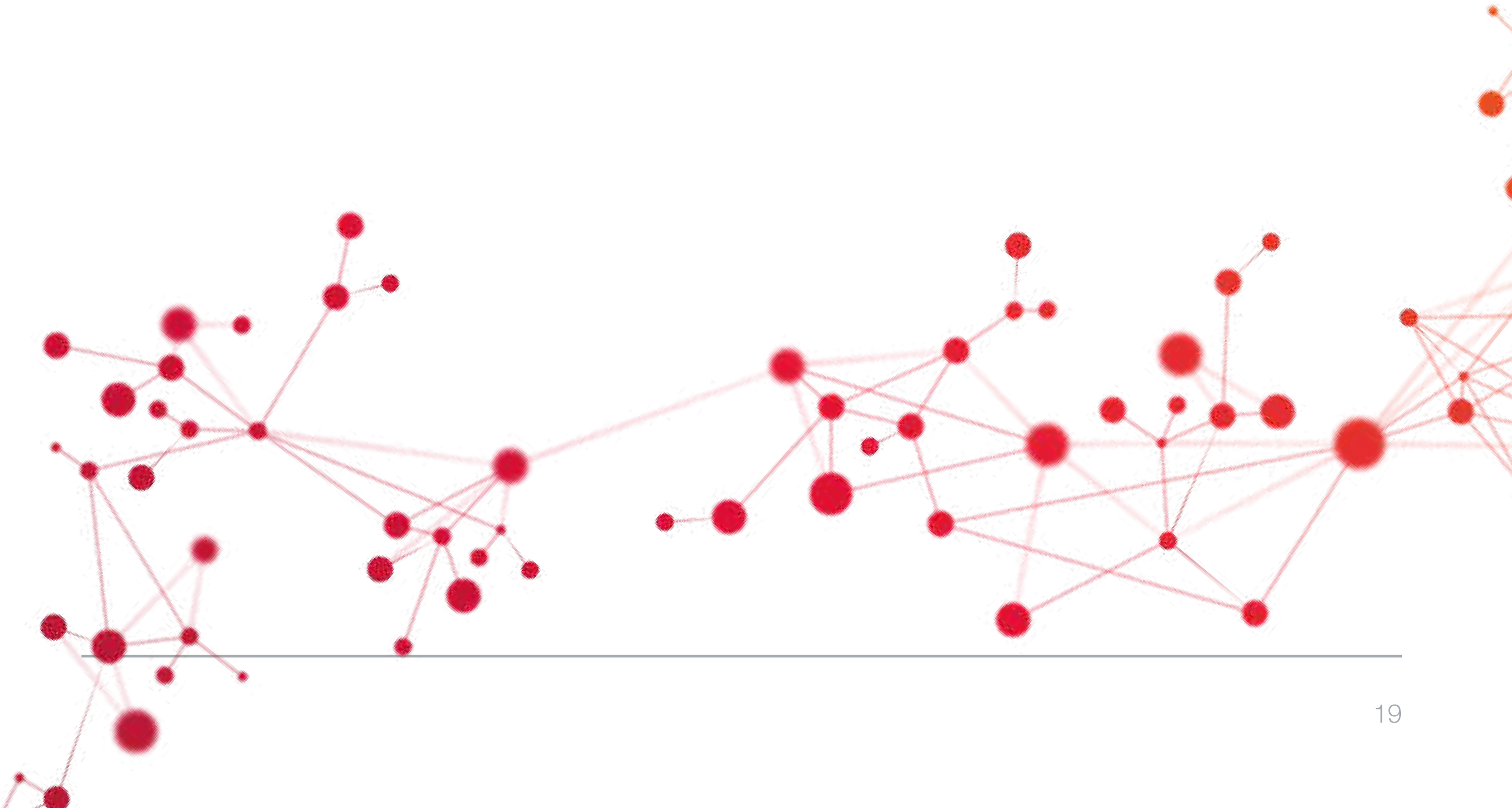
- **Are we prepared for GDPR?**
  The new data protection regulation coming into full force in May 2018 makes new demands such as having a Data Protection Officer in place, meeting a 72 hour breach notification period, delivering increased data accuracy, active consent and the right to be forgotten for user data. Organisations need to understand what sensitive personal information they hold, how it is used and how it is protected. Any company operating in the EU will have to comply and will face major fines if sensitive personal data is mishandled.

These questions are not exclusive or definitive but they give leaders a starting point in their journey towards effective cyber leadership in their organisation.

This starts at the top

The cyber risk issue has expanded in the consciousness of business, the investment community, regulators and indeed the wider public at a bewildering rate. In less than a decade something that once seemed confined to the IT department has been recognised as an enterprise wide risk and a threat to whole economies.

The scale, suddenness and extent of cyber risk may prove intimidating but the risks of cyber threat can be mitigated like any other, through strong leadership and sound governance, with adequate preparation and planning. It all starts at the top – and the CEO sets it in motion. Over to you.



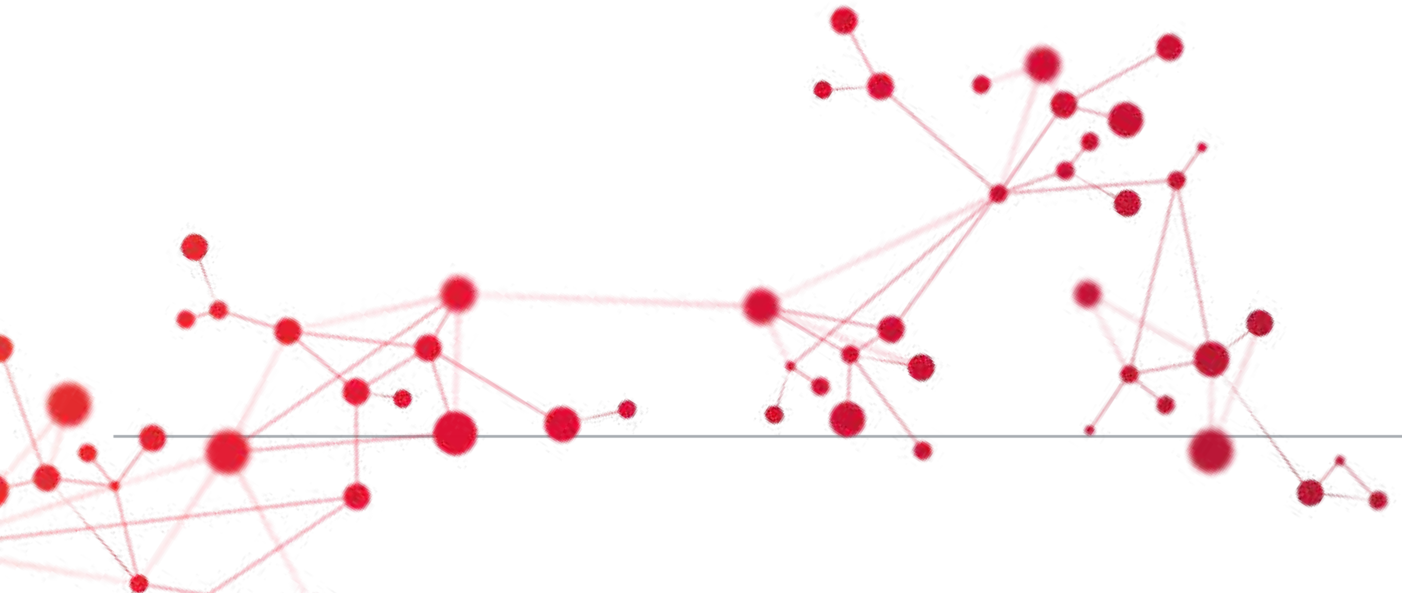
Getting specialist support on cyber security

It can be confusing to deal with the myriad of companies positioning themselves as specialists in cyber security. In broad terms, cyber security specialists will provide one or more of the following seven capabilities:

1. **Governance, risk and compliance.** Cyber specialists will act as advisors on the creation of your security strategies, policies and processes that your organisation should have in place. They will take a risk management approach: risk, combined with risk appetite, drives the measures to be put in place. Understanding the level of threat your organisation is exposed to, what the impact might look like, and the legal and regulatory obligations you might have to consider within your industry sector are all factors in assessing your risk.

2. **Secure design and architecture.** Technical specialists who design your IT infrastructure, applications and business processes to ensure that they are built as securely as possible, often to meet formal compliance schemes or mitigate specific risks identified by the governance, risk and compliance activities.

3. **Specialist security equipment.** The most common type of cyber specialist is the producer of cyber security technology — security software and hardware products that can be used to strengthen your organisation's defences. These range from network appliances like firewalls and intrusion detection systems to 'endpoint' systems that help secure user devices like mobile phones and laptops.



4. **Test and evaluation.** The most common form is 'penetration testing' where experts will attempt to breach your organisation's systems or devices in order to highlight vulnerabilities and assess whether your systems are up to standard. More advanced teams may include social engineering tests to see whether they can 'con' your employees into giving them access to vital IT systems. Lab based evaluations of specific pieces of equipment and software have been less common but are very important in high security businesses, including some government departments.

5. **Managed security services.** Generally, these companies perform monitoring of your IT infrastructure, highlighting when networks are under attack, when information is leaked or when infrastructure is compromised. They may also provide device management of security devices such as firewalls and other network defences. They often provide formal reporting to support your compliance obligations. Other managed services are emerging such as Cloud Access Security Brokers (CASB) who will identify your organisation's unauthorised use of cloud services, so called 'shadow IT', and allow you to monitor and control its use.

6. **Managed detection and response services.** Going beyond standard monitoring, these providers manage incidents where an attacker has been successful. They may offer intelligence based 'hunting' services that look for attackers that may have eluded all your standard security measures. They aim to reduce the time taken to recognise a breach, from weeks or months to days or hours, ideally identifying an attempted breach and stopping it before harm is caused. They may work closely with specialist legal and media handling firms who can mitigate unwanted publicity surrounding a breach.

7. **Training.** Awareness raising and training is a vital part of preparing an organisation to fight off cyber attackers, so training software, courses and services are an essential part of your preparation. Some novel training services may offer to mount harmless technical attacks, like phishing and simulated ransomware, to identify users who are susceptible to such exploits, others may stage a mock attack to exercise your organisation's response plans.

At CGI, we aspire to make cyber security part of everything we do. For more than 40 years, we have helped clients manage complex security challenges with a business focused approach – protecting what is most valuable to them.

We work with leading organisations across the commercial sectors and governments in the UK, Canada, North America and Europe. As a result, we understand security from all angles – technology, business and legal – and have specialists who can build cyber security into your business strategy to drive agility, efficiency and competitive advantage.

For more information please visit **www.cgi-group.co.uk/cyber** or contact **cyber@cgi.com.**

The Cyber-Value methodology

CGI commissioned Oxford Economics to develop an analytical methodology to examine share price movements in companies that had experienced publicly disclosed cyber breaches. The methodology involves four stages, each of which contributes to providing a robust model for establishing the impact on company value arising from a cyber attack.

1. Subject companies for the study were taken from the Gemalto Breach Level Index: a register of publicly disclosed cyber security breaches. In total, 315 breach events were examined with a focus on 65 'severe' and 'catastrophic' breaches occurring since 2013 across seven global stock exchanges. All of Gemalto's breaches in this category, that affected publicly listed organisations on these major bourses, were used in the analysis.

2. To gain a realistic assessment of share price performance, the analysis tracked the subject companies' shares in the two weeks leading up to the breach. By establishing the trend in the share price in the weeks prior to the incident, this made any post-breach disruption in the share price more apparent.

3. The analysis tracked the movement in the share price for one week following the breach incident: using this short time window eliminated the influence of any 'noise' from factors unrelated to the cyber breach affecting the share price.

4. To further ensure the validity of the analysis, the share price performance of affected firms was compared to a control group. The control group for each firm was made up of firms of a similar size (based on employment), which were listed in the same market and who operated in the same sector. The control group in each case was drawn from a total sample of 990 firms. This 'difference in differences' approach enabled Oxford Economics to isolate the impact on the affected firm's share price of the cyber breach and filter out the effect of broader market movements.

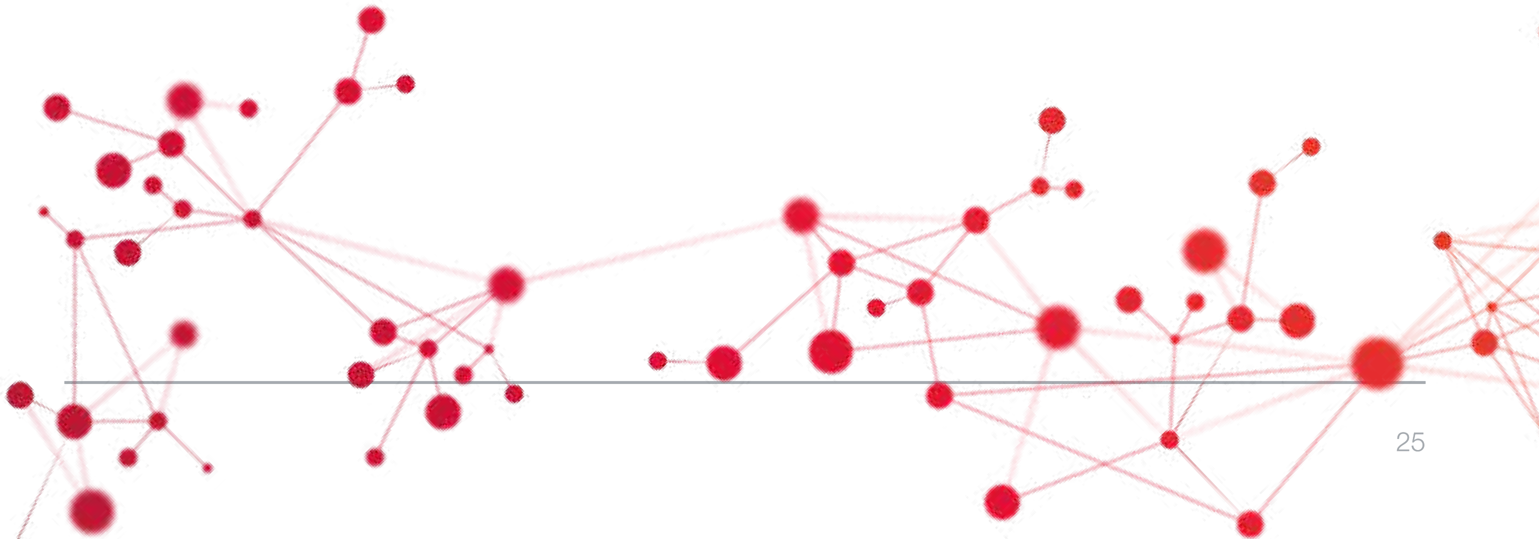
Applying the analysis revealed a significant connection between a number of cyber breaches and company value. Overall, share values in affected companies were seen to perform less well than shares in companies that had not been affected. Furthermore, this damage is permanent: an affected company's shares do not recover their pre-breach performance relative to the control group.

Gemalto Breach Index

Oxford Economics used the Gemalto Breach Index — a comprehensive and publicly available database of cyber security incidents, maintained by security specialist Gemalto – to source the breach incidents used in the analysis. Other breach indices are available but were not used for the purposes of this study. The index records many of the disclosed cyber security breaches to have affected listed firms between 2013 and H1 2016. Each cyber breach is scored between 0 and ten in terms of its severity. Share price data on the companies used in the analysis was sourced from Bloomberg.

The Cyber-Value analysis focused on companies that had suffered 'severe' or 'catastrophic' breaches: the table on the next page describes the classifications used in the Gemalto Breach Index. A share price impact was also observed in companies suffering from low grade breaches but the results were less statistically significant and therefore excluded from the main results.

Category	Score	Characteristics
Minimal	1.0-2.9	A breach with no material effect; usually less than a thousand records; breach notification required but little damage done.
Moderate	3.0-4.9	A breach with long term business impact; usually involves the loss of several hundreds of thousands of records of semi sensitive information; limited breach notification and financial exposure.
Critical	5.0-6.9	A breach with likely short to mid term exposure to business; legal and/or regulatory impact; usually tens of thousands of records of moderate sensitive information involved; some breach notification and financial loss.
Severe	7.0-8.9	A breach with significant exposure to business; legal and/or regulatory impact; large amounts of sensitive information lost (usually hundreds of thousands to millions of records); significant notification process costs involved and public image impact.
Catastrophic	9.0-10.0	A breach with immense long term impact on breached organisation, customers and/or partners; very large amount of highly sensitive information lost (usually ten to 100+ million records); massive notification cost; potentially existential financial loss for breached organisation in remediation and related costs; use of lost sensitive information seen.



A small selection of types of cyber attack

A small selection of types of cyber attack

+ Malware
This describes a variety of common forms of software that run on a computer with malicious intent. Viruses, Trojans and worms are all types of malware. Malware can be used to destroy, alter or steal data or make the hardware behave in unexpected ways.

+ Zero Day
A 'zero-day' attack is a type of attack that exploits previously unknown vulnerabilities in applications or operating systems making it difficult for security appliances like intrusion detection and antivirus systems to detect and stop it.

+ Phishing
Typically, an email, often sent to thousands of people at a time, that is designed to get the user to reveal sensitive information or to inadvertently install malware on their computer. Spear phishing emails are designed to target individuals or organisations by including very carefully crafted messages that lead the user to believe they are legitimate.

+ Cracking
When an attacker tries to gain access to a computer system by guessing their password, using automation tools or social engineering to narrow the search for potential passwords.

+ Ransomware
A form of malware that stops a user accessing their files by encrypting them and then demanding payment from the user to unlock the files. In many instances the victims pay but the files are never unlocked.

+ Water holing
Using a fake website to fool a user into revealing information or install malware.

+ Web application attacks
Databases are an integral part of most modern websites. One type of web application attack injects a malicious query that is then used to give the attacker access to the underlying database, such as credit card details or other personal information. Web application attacks are designed to exploit poorly written websites that do not perform proper URL and field inspection.

+ Drive-by download
Where malware is downloaded to a user's computer just by visiting a compromised website or 'malvertising'. Malvertising is where adverts on a website, which are supplied by a third party, have been compromised and download malware to the user's computer while the advert is displayed.

+ Denial of Service
The attacker disrupts a user's network access by overloading it with connection requests. A distributed denial of service attack (DDoS) uses hundreds or thousands of computers around the world, known as a botnet, to mount this attack, making it difficult to block.

+ Botnet
A user's computer may be infected with a type of malware that uses the computer to distribute malware, mount a DDoS attack, or other illicit function, all without the user's knowledge.

References

i World Economic Forum Global Risks Report 2017

ii CGI Global 1000 Outlook, 2016-2017

iii Cyber risk reporting in the UK, Deloitte. February 2017

iv Cyber security in the boardroom: UK plc at risk. CGI and Cebr, March 2016

v Harvard Business Review, Why Data Breaches Don't Hurt Stock Prices, March 2015

vi Third annual data valuation survey. Brunswick Insight, October 2016.

vii Reuters Technology News, Verizon, Yahoo! agree to lowered $4.48 billion deal following cyber attacks, 21st February 2017.

viii Cross Sector — Global: Cyber Risk of Growing Importance to Credit Analysis, Moody's, November 2015

ix National Cyber Security Strategy 2016 to 2021, Cabinet Office, National Security and Intelligence, HM Treasury, November 2016

x Cyber Security Regulation and Incentives Review, Department for Culture, Media & Sport, December 2016

CGI IT UK Ltd
250 Brook Drive
Reading
RG2 6UA

www.cgi-group.co.uk/cyber
cyber@cgi.com