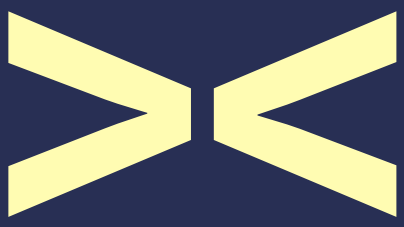
LLOYD'S

Closing the gap

Insuring your business against evolving cyber threats

June 2017

In association with KPMG and DAC Beachcroft



KPMG

DAC beachcroft

Contents

Section 1
Executive summary

1.1 Overview

Over the past few decades the internet has enabled extraordinary innovation to take place, creating new business models, giving rise to world-changing companies and generating millions of jobs.

But this progress has come at a cost. By their nature, digital systems are susceptible to cyber-attacks by malicious individuals or groups with increasingly serious repercussions for businesses around the world. The nature of the threat is evolving so fast that it is becoming more and more difficult for organisations to counter it.

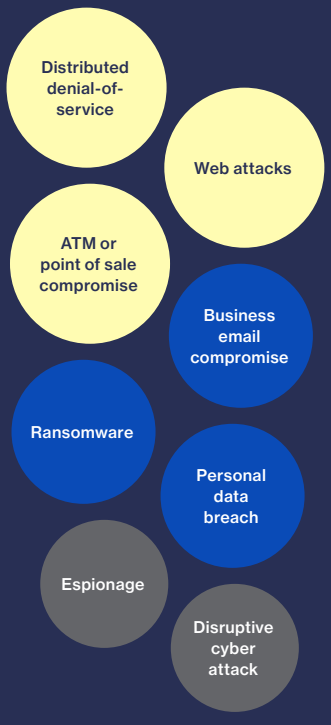
But while the threat is becoming more complex, many business leaders lack awareness about the cyber threat. A recent Lloyd's survey of more than 350 senior decision-makers across European business revealed that although 92% of businesses had experienced some form of cyber breach in the past five years, only 42% were worried that another incident could happen again in the future.

This Lloyd's report, produced in association with KPMG in the UK, international law firm DAC Beachcroft and Lloyd's insurers, helps companies understand the cyber threat better.

The first part of the report offers a unique assessment of the various cyber threats facing companies today, broken down by sector (an example for financial services is displayed here), and looks at ways to mitigate them. It also details the full financial impacts of data breaches and analyses some of the costs associated with recent high-profile cyber-attacks.

The second part looks at four reasons why companies need to raise their game when it comes to tackling cyber risk and offers expert insight from Lloyd's cyber insurers on some of the ways they can do this.

Financial services sector risks



(The order of the circles in the same category does not indicate relative frequency.)

To view the unique sector assessment of various cyber threats facing companies today, see page 15.

Sectors covered include:
- Education
- Financial services
- Healthcare
- Hospitality
- Information technology
- Manufacturing
- Media and entertainment
- Oil and gas
- Professional services
- Public Sector
- Retail
- Telecommunications
- Transportation
- Utilities

1.2 Key findings

The types of cyber-attacks against businesses vary from sector to sector and are constantly evolving. For example:

- There has been a major growth in targeting companies through CEO fraud, which is resulting in significant financial losses.
- The financial services sector finds itself at the sharp end of targeted attacks by organised cyber-crime but retail is increasingly being targeted.
- Professional services firms such as lawyers and accountants are increasingly targeted as a gateway to attacks on their clients, which are often large corporates.
- Ransomware and distributed denial-of-service attacks are increasingly used against businesses with healthcare, and media and entertainment particularly targeted.
- The public sector and telecommunications sectors are highly susceptible to espionage-focused cyber-attacks.

Businesses need to be aware of the full costs of a cyber-attack, in particular, the "slow-burn" costs (i.e. those associated with the long-term impacts of a cyber-attack, such as the loss of competitive advantage and customer churn). When added to immediate costs (i.e. legal and forensic investigation fees, and extortion pay outs), slow burn costs can dramatically increase the final bill.

There are four factors that aggravate the damage caused by cyber-attacks, making it all the more important that businesses mitigate their cyber risks and improve their cyber security:

- Higher penalties for companies that breach cyber-security rules as set out in forthcoming European legislation.
- Cyber-breach victims' greater willingness to sue companies that have lost their data.
- Increased responsibility for cyber security in the supply chain.
- Greater vulnerability through the increasing use of connected devices (the internet of things).

1.3 Next steps

Lloyd's is home to more than 70 insurers who offer cyber insurance cover. Based on unique and expert insight from the Lloyd's market, the report highlights four key ways in which businesses could prepare for and mitigate the cyber threat:

1. Understand the specific threats to your company, including both the immediate and slow-burn costs – everything from reputation as perceived by customers and the value of the data held, to supply chain vulnerabilities and business-leader profiles.

2. Evaluate both current and future threats: underwriters will evaluate both so they can offer you the insurance cover that best suits your needs.

3. Ensure all employees, including management, have a comprehensive understanding of the cyber threats your company faces and promote a cyber-risk management culture.

4. Seek expert help when it comes to arranging cyber insurance to ensure that your risks are adequately covered.

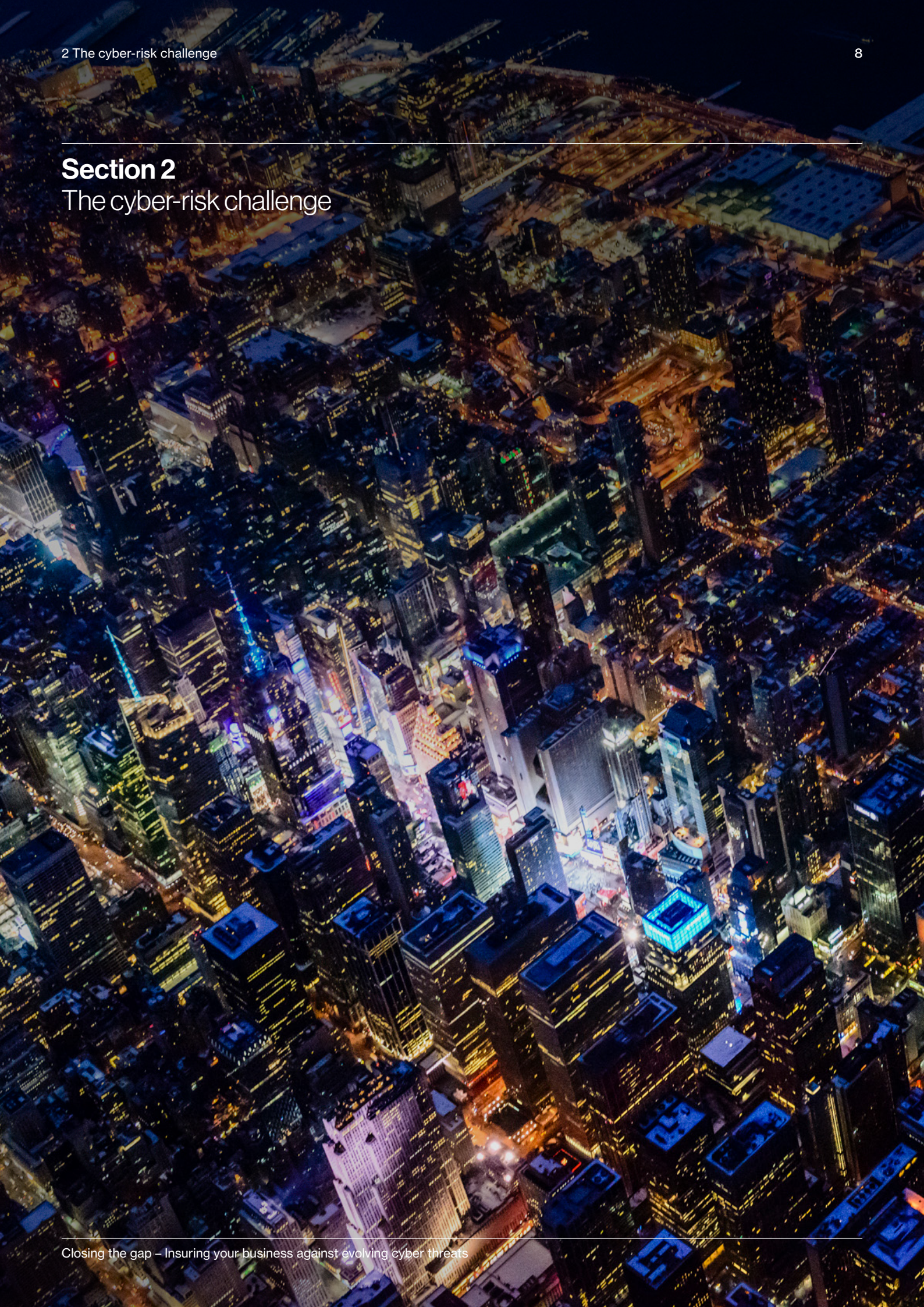
1.4 Conclusion

The cyber threat is evolving daily so companies must be better prepared for the consequences of a cyber breach. Not only are the costs likely to increase with the introduction of new European legislation but the number of ways companies can be targeted is increasing.

While it is not possible to be 100% secure from a cyber-attack, there are a number of measures companies can take to reduce the risk of it happening, and to ensure they minimise the consequences and recover more quickly should a breach occur.

Insurance is part of this solution. Every day, Lloyd's specialist cyber underwriters work with thousands of companies, from multinationals to SMEs, across the world to understand their risks better and to provide them with the expert advice and insurance cover they need.

Section 2
The cyber-risk challenge



2.1 The cyber-risk challenge

Over the past few decades technology, and particularly the internet, has provided a remarkable platform for business growth and innovation.

The impact of this technology cannot be underestimated. From Amazon to Uber, technology has given rise to companies that could not have existed without it. In less than a generation, it has disrupted long-standing industries, killed off established brands, allowed new brand Titans to emerge and transformed the way business is conducted.

But while this change has created huge opportunities for new ideas and fresh thinking, it has brought with it many risks as well.

Globally, cybercrime is now estimated to cost businesses $400bn[1] a year, meaning cyber risks are among the top issues businesses[2] have to consider when it comes to their resilience and continuity planning. The same study also suggests that cybercrime is comparable in scale to narcotics and counterfeiting or the piracy of goods in terms of economic impact.

What makes cyber risks so challenging to deal with is the rapid pace of change in the digital space. Because new cyber threats are emerging all the time, businesses have to monitor developments constantly and ensure their security systems are up to date to protect themselves more effectively from cyber-attacks.

Estimated global cost of cyber crime a year

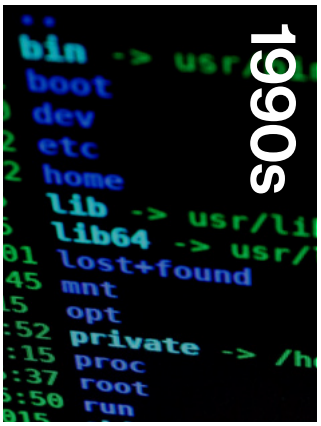
$400bn

1 Net Losses - Estimating the Global Impact of Cyber Crime, Center for Strategic and International Studies, June 2014
2 http://www.forbes.com/sites/elenakvochko/2015/11/14/cyber-risk-as-a-top-10-global-risk-for-businesses/#611f38436a90

2.2 A brief history of cyber threats (1980s to present day)

The timeline below explores how cyber risk has grown in just a few decades to become one of today's most pressing issues on the boardroom agenda.

The internet is a closed-off world, dominated by academics and hobbyists. Curious hackers develop a reputation for both good and bad behaviours becoming known as "white-hats" and "black-hats", respectively. "Hacking" has recreational and educational purposes but, inevitably, other motivations prevail and over time the internet loses some of its early innocence.



By the mid-1990s the internet starts to reach mainstream consumers who are often easy prey for criminal attacks. As more businesses come online, computerised systems are regularly attacked, sensitive and financial data becomes a criminal commodity and denial-of-service techniques become weaponised. By the late 1990s the first incident of cyber espionage is reported.

The internet is now a regular part of life for most people and an accepted field of business and government activity. More sophisticated cyber threats emerge, such as financial Trojan malware (see section 2.3) and the hijacking of millions of online banking sessions, coupled with a dramatic increase in the number of data breaches. The rise of smartphones makes mobile the new frontier of cyber risks. This decade also sees the first allegations of military cyberattacks, in Estonia (2007) and Georgia (2008).

The battle between cyber criminals and cyber security firms reaches maturity, each developing their own tools and reverse-engineering each other's to gain an advantage. While cyber security is a $75 billion marketplace[3], front-line cybercriminals thrive in a black market where high-end exploitation tools can reportedly change hands for up to a million dollars. Cybercrime costs business an estimated $400 billion annually, and mirrors the legitimate growth of the digital economy, now estimated to be worth $4.2 trillion[4]. The internet of things is likely to become the new cyber battleground.

3 http://www.gartner.com/newsroom/id/3135617
4 https://www.bcg.com/documents/file100409.pdf

2.3 Cyber risk today

Businesses today are confronted by a bewildering variety of cyber-attacks. This often makes cyber risks feel overwhelming.

Analysis completed by KPMG in the UK[5] shows that attackers tend to be clustered into three main groups, using either "commoditised", "targeted" or "high-end" approaches to victim selection and exploitation, as set out below.

Commoditised attacks

Hundreds of millions of victims
$300–$10,000
High impact

Targeted attacks

Tens of thousands of victims
$10,000–$1 million
High impact

High-end attacks

Dozens of victims
$1 million –$100 million
Extreme impact

5 https://home.kpmg.com/uk/en/home/insights/2016/07/taking-the-offensive-working-together-to-disrupt-digital-crime.html

2.3 Cyber risk today

Commoditised attacks

Attackers: Organised crime groups operating internationally. Smaller-scale criminals. Hacktivists.

Victims: Wide range of individuals and businesses, often via their customers.

Victim numbers: Hundreds of millions.

Financial cost: $300-$10,000.

Technical ability: Generally low. Attackers rely on an assortment of specialist tools designed by others and available in the online cybercriminal marketplace.

Overall impact: High. Although returns may be relatively low, these economy-of-scale attackers monetise millions of victims and damage many more.

Method of attack: "Spray and pray" techniques, using spam emails, malicious website "watering holes" that target a group of people from a certain organisation or geography, and criminal infrastructure to leverage vulnerabilities in often out-of-date software.

Common tactics

Financial Trojans Malicious software that's often delivered by email attachment or web link to a victim's computer, allowing an attacker to hijack and modify a customer's online banking transactions. Other versions target corporate accounts to steal larger sums.

Commodity ransomware Malware that locks a victim's computer or mobile device, and then demands a ransom payment to regain access. Today's strains often use encryption to lock files forever if the user declines. Osterman's recent survey[6] found that 39% of the organisations it surveyed had been impacted by a ransomware attack in the past year, and Kaspersky reports[7] a major growth in ransomware during the latter part of 2016, with over one million infected users being reported in Q3 2016, an increase of over 190% on the previous quarter.

Denial-of-service attacks These cause disruption to online services by overloading networks and servers with attack traffic. Extortion-based, distributed denial-of-service attacks are considered business as usual by some companies: in the financial sector they account for 44% of all attacks[8], costing as little as $15 per hour to deploy but an average of $40,000 per hour to mitigate.

SQL injection Web software that has a bug within it which allows SQL injection, meaning an attacker can smuggle commands into databases to destroy or modify company data or passwords.

6 Understanding the depth of the global ransomware problem, Osterman Research, August 2016
7 Kaspersky Security Bulletin, Overall Statistics for 2016
8 Verizon, 2017 Data Breech Investigations Report

2.3 Cyber risk today

Targeted attacks

Attackers: Organised crime groups operating internationally.

Victims: High-net-worth individuals and businesses, often targeted through their supply chains and customers.

Victim numbers: Tens of thousands.

Financial cost: $10,000-$1 million.

Technical ability: Generally high. Attackers will deploy customised and targeted attack tools against commercial systems.

Overall impact: High.

Attack methods: Demonstrate an understanding of the industry they are attacking, including its systems and communications, and often causing significant business disruption by tailoring the attack to the victim, thus ensuring greater impact and financial rewards.

Common tactics

Repurposed banking Trojans Often used to harvest and index victim data and install remote access tools, which allows targeted access to ultra high-net-worth individuals' online devices and, subsequently, their accounts. Criminals are now diversifying to target less mature sectors, including online retail customer accounts.

Business email compromise fraud / CEO fraud Searches for ways to mislead financial controllers, treasurers and payment clerks, and trigger fraudulent payments, often by pretending to be CEOs or other senior executives. Their methods rely on social engineering and open-source research of the victims, together with poor email integrity. The FBI reports that more than $5.3 billion was lost to such fraud between October 2013 and December 2016, up from $3.1 billion reported to May 2016.

Targeted ransomware Bespoke ransomware is now targeting particular business-critical systems and data stores. Using knowledge of commercial system vulnerabilities, this software aims for maximum impact and disruption to ensure large ransom payments from businesses. Vulnerabilities exist across government and other sectors, but education and healthcare are currently the targets of choice in part because of legacy IT and decentralised management. The May 2017 WannaCry malware incident impacted more than 200,000 systems worldwide causing major disruption to the National Health Service in the UK, as well as forcing emergency patching of ageing and unsupportable IT systems.

2.3 Cyber risk today

High-end attacks

Attackers: Often smaller-scale, highly covert, organised crime groups operating internationally.

Victims: Financial systems and infrastructure, through inside and specialist knowledge.

Victim numbers: Dozens.

Financial cost: $1 million-$100 million.

Technical ability: Generally high. Attackers will understand the vulnerabilities and design a customised attack methodology.

Overall impact: Extreme – the damage to reputation and financial costs will permanently affect a business.

Attack methods: Conceived from a specialist viewpoint with insider knowledge and understanding. These attackers develop their own custom toolkits to target software vulnerabilities. While their attacks can sometimes be easily recognised as the work of a particular group, in many cases the true motivation remains unknown.

Common tactics

Breaking into banks and financial systems Highly lucrative attacks, often aimed at "weak links" such as smaller banks or those in less developed countries. Recent examples include the 2016 attack on the SWIFT transfer system at South Asian banks (insiders are suspected to have enabled an attempted $951m heist), and unlimited cash-out operations on ATMs between 2011 and 2013, following hacks on credit and debit card payment processors.

Disrupting critical infrastructure These types of attack have all the hallmarks of an Advanced Persistent Threat (APT), a common euphemism for state-sponsored cyber espionage techniques. Often aimed at critical national infrastructure, recent examples include activity in Ukraine in December 2015, when 225,000 people were plunged into darkness by a cyber-attack on power stations and, in Germany in December 2014, when "booby-trapped emails" were used in a cyber-attack on control systems at a steel works, causing massive damage.

The cyber-attacks that frequently dominate the headlines can distort how businesses perceive the risks associated with cyber. There is a natural tendency to focus on the unusual or memorable, but this doesn't always reflect the reality of the cyber risks facing companies every day.

2.4 The changing threat

The threat landscape continues to evolve. Organised crime groups continuously develop tools, tactics and targets. Denial-of-service attacks now exploit compromised networks by using CCTV cameras, digital video recorders and home routers to create attack traffic. Mobile devices have become a new battleground as mobile phone operators and vendors fight to counter new cyber-attack strategies.

Criminals look to repurpose attacks used against banks to target new institutions such as e-retailers and the healthcare sector. Industrialisation of cyber-crime continues, with criminals scaling their operations, and looking to automate the targeting and exploitation of business networks. At the same time, nation states continue to invest in cyber-espionage and military cyber-attack capabilities. Geopolitics will drive the use of these cyber weapons.

The infographic over the page shows the different types of attacks that various organisations are subject to. As a result, the sector descriptions demonstrate the complex set of circumstances that businesses need to adapt to in order to keep themselves and their customers safe. This data also points to the sophistication of today's hackers. Organisations are not, by and large, dealing with scattergun attacks. Instead, they are facing a world in which their security measures are tested time and time again by highly informed, well prepared individuals and groups that target specific sectors.

Financial services

Banks are locked in a battle with cyber criminals to secure digital banking channels and counter fraud. The roll out of two-factor authentication has reduced online fraud levels. Chip-and-pin has limited the ability to exploit stolen card data, but card-not-present frauds are increasing. Criminals are becoming more financially savvy, and have started to target bank systems and financial infrastructure.

Information technology

Cloud-service providers can find themselves targeted for distributed denial-of-service attacks aimed at hosted services, which cause collateral damage and disruption to other clients.

Professional services

Lawyers and accountants are being increasingly targeted as the trusted route into major firms. They often hold sensitive client data, and criminals have used their email systems to send highly targeted phishing emails to clients as part of business email compromise fraud. This sector also encounters ransomware frequently.

Healthcare

As personal data breaches target those firms that handle our most sensitive data, healthcare companies are often the victims. Data is sold on in the black market, enabling fraud and other attacks. Ransomware has also become a particular problem in the healthcare sector. Disruption to systems can have both real and reputational impact.

2.4 The changing threat

Public sector
Espionage is the major threat. This is often state-sponsored focusing on sensitive information on politically exposed persons, sensitive intellectual property, strategic investments and key infrastructure.

Retail
Web attacks are the biggest risk for retailers, as they target firms that offer rich digital services to clients. Their complex websites can be breached to collect customer data or provide a route into their core systems, and point-of-sale terminals are also targeted.

Education
There are particular challenges in imposing strict security controls and a security culture in the education sector. Personal data, dissertations, intellectual property and exam results can all be targeted. A culture of software downloads can make the sector a target for malware infections, with education establishments seeing some of the highest ransomware infection rates.

Manufacturing
The biggest threat to manufacturers is ransomware. This hits firms whose reputation depends on them being able to provide vital services to their clients which are in turn dependent on IT systems and data availability.

Media and entertainment
Media, gambling and gaming websites are targeted by criminals using high-volume, distributed denial-of-service attacks. Extortion is often the motive but politically motivated media attacks also occur. Online advertising can also be a target for fraud.

Oil and gas
Oil and gas firms can find themselves caught up in national politics and can be the subject of espionage as well as occasional high-end disruptive attacks; they essentially become political cyber footballs. They are also open to all types of fraud, even point of sale attacks on petrol stations.

Telecommunications
As the heart of our networked world, telecom firms attract criminal attention as a route to compromise mobile devices. They also find themselves a target for state espionage and, occasionally, infrastructure attacks.

Transportation
As a sector transportation tends to be less heavily targeted, although public websites can be subject to web application and denial-of-service attacks. There have been isolated cases of payment-card compromise.

Hospitality
Personal data and credit-card information are being targeted by organised crime, with frequent examples of point-of-sale terminals being exploited. Criminals also see loyalty card schemes as a potential target for exploitation.

Utilities
A less frequently targeted sector by organised crime, although occasionally the subject of denial-of-service attacks. Concerns over attacks by nation states and political activists, linked to increasing dependency on industrial control systems, have led to growing government pressure to improve security.

2.4 The changing threat

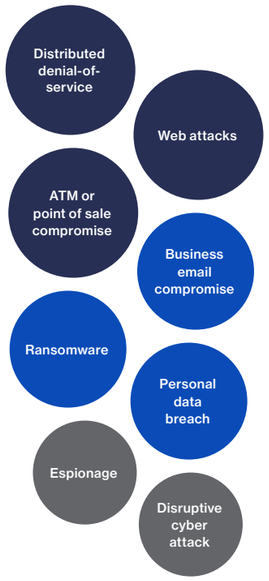
The infographic is based on KPMG's analysis of publicly available references[9] and KPMG's industry insights.

Key

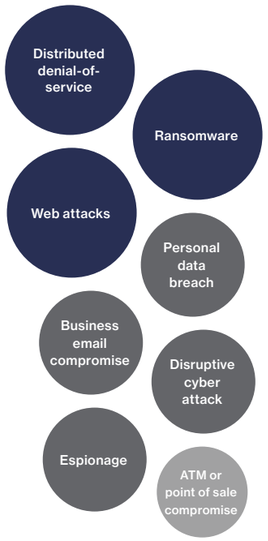
- Primarily targeted
- Frequently targeted
- Occasionally targeted
- Rarely targeted

The order of the circles in the same category does not indicate relative frequency.

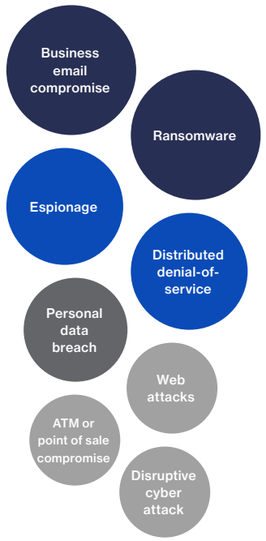
Financial services



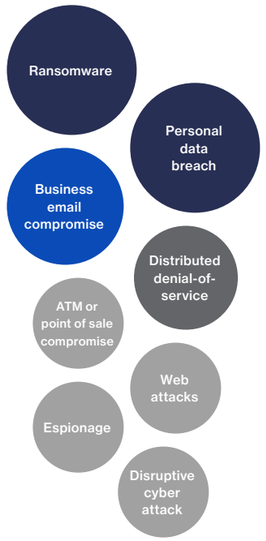
Information technology



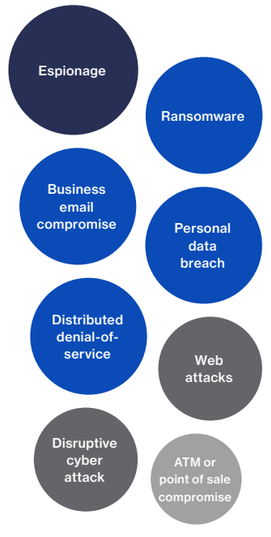
Professional services



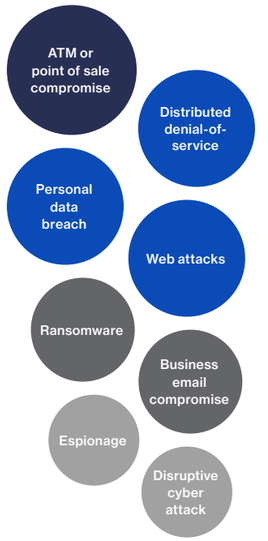
Healthcare



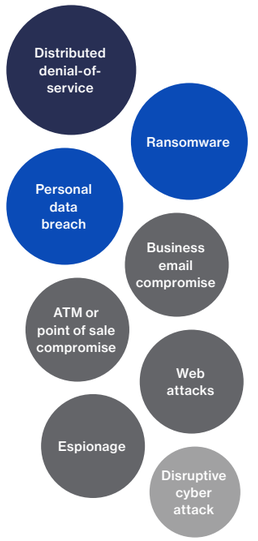
Public sector



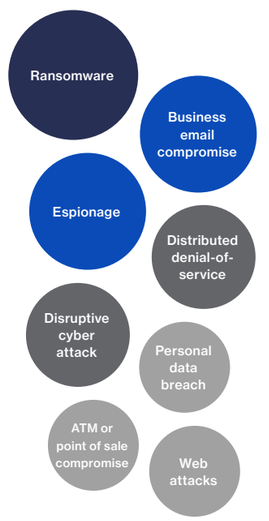
Retail



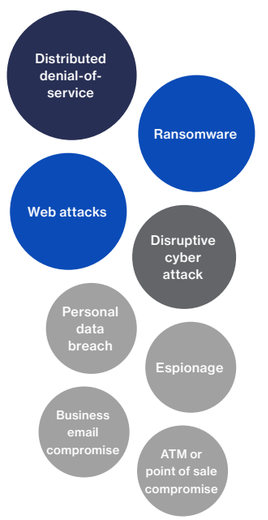
Education



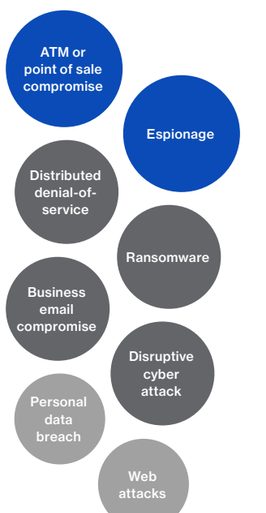
Manufacturing



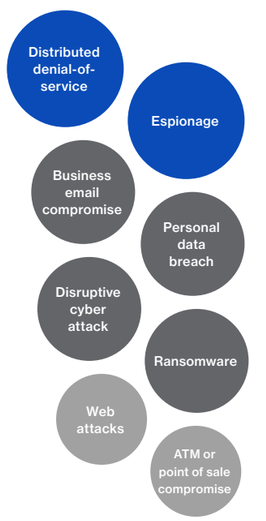
Media & entertainment



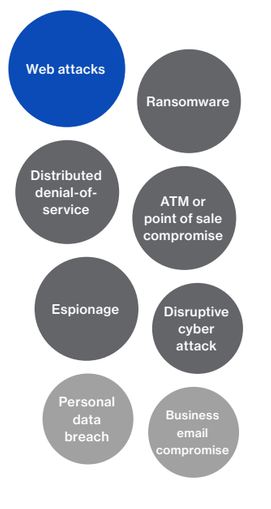
Oil & gas



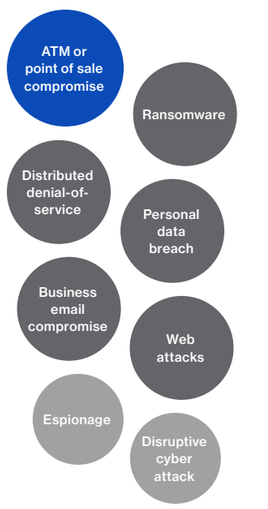
Telecommunications



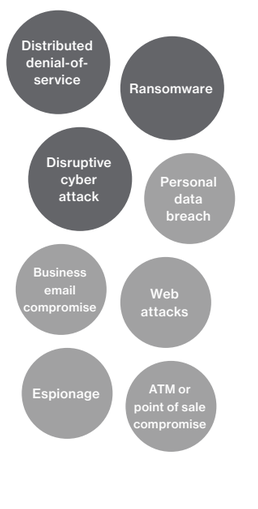
Transportation



Hospitality



Utilities



9 CERT-UK, DoS A Rising Tide, 2016; Akamai, State of the Internet Report, Q1 2016; Verizon, Data Breach Report, 2016; Symantec, Ransomware and Businesses 2016, Ransomware Infections by Organization Sector, Jan 2015-Apr 2016; Bitsight Insights Report, The Rising Face of Cyber Crime: Ransomware, September 2016; Trend, Following the data, analysing breaches by industry, 2005-2015 data breach records; Ponemon, Cost of Data Breach Survey, 2015, Per capita cost by industry classification; Mandiant, M-TRENDS 2016

2.4 The changing threat

Looking in more depth at some of the higher risk areas, the infographic shows the extent to which today's hackers are prepared to customise their attacks to reap the greatest rewards from a victim.

Professional advisers, such as lawyers and accountants, while rarely the subject of web or distributed denial-of-service attacks, often find themselves the targets of business email scams. With the valuable customer data and access they obtain, the hackers can then mount targeted phishing attacks on the professional advisers' clients.

By comparison, distributed denial-of-service attacks may not be employed regularly against professional services firms but do come into play for a wide variety of organisations that depend on customer access via online channels such as gaming, media and financial services. By attacking key IT infrastructure such as internet exchanges, domain-name servers and registries, the costs of denial-of-service attacks can be substantial and can include lost revenue and long-term brand damage.

The 21 October 2016 attack on cloud-provider Dyn disrupted access from the US east coast to Twitter, GitHub, PayPal, Amazon, Reddit, Netflix and Spotify over a three hour period. The attack took place through compromised CCTV cameras and digital video recorders.

These attacks are not limited to internet websites. Many healthcare sites in the US have found their telephone systems overwhelmed by fake calls, followed by extortion demands from attackers.

Revolving as it does around the theft of information from a network, cyber espionage has clear relevance for public bodies, defence organisations, as well as the IT and telecommunications companies through which hackers gain access. But cyber espionage techniques are also evolving, with traditional tactics now being repurposed by criminals to attack banks and financial infrastructure via Advanced Persistent Threats (APT). APT - such as the infamous Stuxnet worm, a cyber weapon that damaged Iranian nuclear facilities - persistently target a specific objective at a low level over a longer period of time.

Ransomware, which locks organisations out of their own systems, focuses on healthcare and services firms where service disruption can have an immediate impact on clients, and where reputational damage can also be significant. Unfortunately, ransomware can also be indiscriminate, hitting every sector of the economy including utilities and transport companies.

While ransomware attacks do target manufacturers, they rarely target industrial control systems. There is, however, a risk of accidental disruption of such systems from the infection of a company's broader network, which may cause substantial permanent damage.

In future organised crime groups may exploit this access for extortion purposes. Beazley, an insurer that works in the Lloyd's market, has seen an increase in ransomware attacks on its customers grow from under 50 in 2014[10] to more than 200 last year. It predicts this will double to more than 400 this year.

10 https://www.beazley.com/news/2017/beazley_breach_insights_january_2017.html

2.4 The changing threat

Financial Trojans are increasingly being adapted to counter bank security (such as defeating the use of SMS text messages to authenticate transactions). Organised crime groups are using Trojans in this way to attack a wider range of targets (such as e-retail) as well as linking the use of Trojans to other attack methods (such as SIM swap frauds) aimed at defeating bank security.

Retailers and banks also face a wide range of attacks aimed at payment systems. These include malware targeting electronic funds transfer point-of-sale (EFTPOS) terminals, as well as an increasingly creative range of attacks on ATMs which exploit the computers controlling the terminals rather than more traditional card-skimming methods

In summary, cyber attackers target companies that:

- Possess information that can be monetised and exploited.
- Are most open to extortion from system disruption due to service criticality and reputational impact.
- Are vulnerable to fraud because they handle substantial volumes of financial transactions or have high levels of liquidity.

Case study

An employee from a chain of opticians received an email to say she had been caught speeding and clicked on a link which offered to show her a photograph of her being caught in the act. Shortly afterwards the client received an email to say their systems had been infected with the Cryptolocker virus and that all the files on its servers were encrypted.

The encrypted files included sensitive patient records and the software used to run the business. The criminals requested Bitcoins for the decryption key. The company's insurer Hiscox approved the company's payment for the key, providing reimbursement for the costs. But it didn't end there: unfortunately the decryption key only recovered 90% of the files and the company needed an IT contractor to help them recover the remainder.

The company's cyber and data risks insurance policy covered them for business interruption as well as the costs of being unable to trade for a couple of days and not being fully up-to-speed for a couple of weeks.

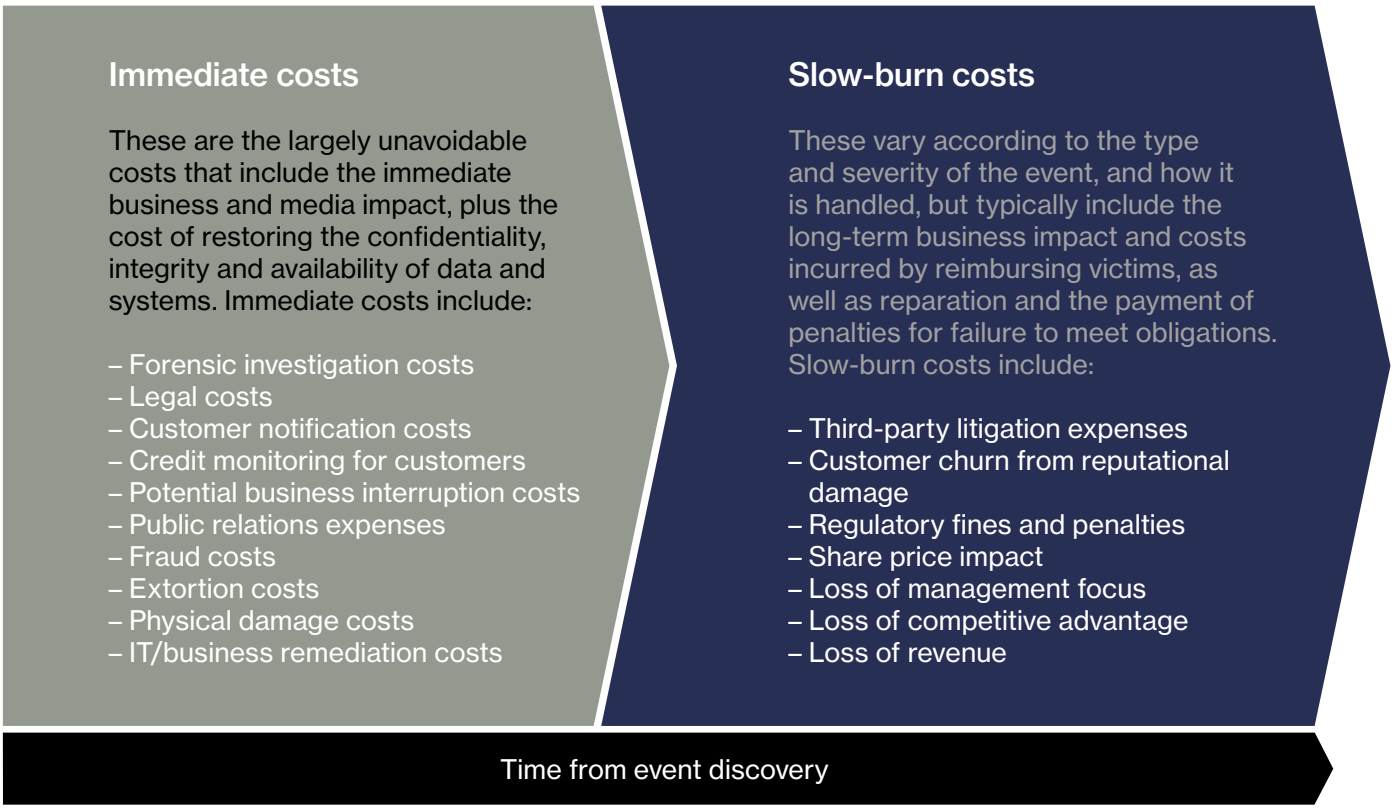
Section 3
The true cost of cyber crime

3 The true cost of cyber crime

The costs of a cyber incident typically occur in two distinct phases – immediate and slow burn (see diagram below). The extent of these costs can vary considerably by sector, and can be affected by a range of factors. These include the type of company targeted, the data the company handles, and the regulatory and legal implications of any incident. This means that cyber-attacks with similar impacts can have vastly different costs.

Research undertaken by BT and KPMG in the UK[11] suggests businesses also have very different concerns regarding breach costs depending on which sector they are in, with litigation and regulatory enforcement concerns dominating in financial services.

Financial-loss concerns dominate in the retail sector, while tech firms are the most concerned about reputational impacts.



11 https://home.kpmg.com/uk/en/home/insights/2016/07/taking-the-offensive-working-together-to-disrupt-digital-crime.html

3 The true cost of cyber crime

To bring this to life, the breakdown between immediate and slow-burn costs is demonstrated in the analysis of two recent high profile cyber-attacks, drawing upon publicly available information.

Case study: Retail – Target

At a glance:
The theft and sale of more than 40m credit card details from Target's point-of-sale terminals cost the large retailer almost $100m in litigation, with a similar amount spent upgrading the company's retail systems.

Type of attack: Malware

Total immediate cost: $60m

Total slow-burn cost: more than $219m

Total gross cost: more than $279m

What happened?
Between 27 November and 15 December, 2013 more than 40m credit card details and 70m pieces of personal information were stolen from Target, a major US retailer. An organised crime cyber-attack on its point-of-sale terminals resulted in stolen card details being sold on the black market, with prices varying from a median of $18-$35.70 per card. Similar attacks followed on a number of other major US retailers[12].

Immediate costs: High
Target reported some $60m of fourth-quarter expenses related to the cyber-attack for 2013. This figure included immediate incident response, forensics, action to secure systems, increased call-centre staffing and the provision of a year of free credit-monitoring services to customers. It also included an initial accrual against claims by payment card networks that had to reissue compromised credit cards.

Slow-burn costs: High
Following the attack Target committed to more than $100m of system upgrades to install chip-and-pin readers at its stores[13], and invested $5m in customer education and awareness activities.[14] More than 140 legal actions were filed in various courts.[15] Since that time Target has settled with a group of banks, credit unions and MasterCard issuers for $19m[16], with Visa for $67m and shoppers for $10m[17]. Target was unable to quantify the impact on its customer base due to other factors shaping the retail environment, but did regard the breach as having an adverse effect when reporting a 5.3% drop in sales for that quarter.[18] The company incurred more than $201m of costs in the financial year following the breach, bringing the total cost to more than $261m.[19] A May 2017 settlement with US States and the District of Columbia has since added a further $18m to this figure[20]. The CEO and CIO have both since resigned.

12 http://krebsonsecurity.com/2014/05/the-target-breach-by-the-numbers/
13 http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=2019880
14 http://articles.latimes.com/2014/feb/26/business/la-fi-target-earnings-hack-20140227
15 http://www.lexology.com/library/detail.aspx?g=74d6d66d-de52-4cfc-825b-5d481fd52cbe
16 https://corporate.target.com/press/releases/2015/04/target-announces-settlement-agreement-with-masterc
17 http://investors.target.com/phoenix.zhtml?c=65828&p=irol-SECText&TEXT=aHR0cDovL2FwaS50ZW5rd2lJkLmNvbS9maWxpbmueG1sP2lwYWdlPTEwNDU1MzEyJkRTRVE9MSZTRVE9MTImU1FERVNDPVNFQ1RJT05fUEFHRSZleHA9JnN1YnNpZD01Nw%3D%3D
18 http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=1903678
19 https://corporate.target.com/annual-reports/2014/10-k/10-K-Part-II/Item-8-Financial-Statements-and-Supplementary-Data
20 http://www.cnbc.com/2017/05/24/target-in-18-point-5-million-multi-state-settlement-over-data-breach.html

3 The true cost of cyber crime

Case study: Telecoms – TalkTalk

At a glance:
The theft of more than 150,000 customer details resulted in one-off costs in excess of $52m and a 10% share price decline for one of the UK's largest telcos.

Type of attack: DDoS, followed by SQL injection

Total immediate cost: $52m

Total slow-burn cost: more than $44m (including estimate for lost revenue)

Total gross cost: more than $96m

What happened?
In October 2015, TalkTalk was the victim of a major cyber breach, leading to the theft of 156,959 customers' personal details, 15,656 bank account numbers and sort codes, and some 28,000 credit and debit cards that were obscured[21]. The police arrested two teenage suspects shortly after the attack[22], and one 17-year-old subsequently admitted hacking offences linked to the TalkTalk data breach[23].

Immediate costs: High
TalkTalk reported that the one-off exceptional costs associated with this attack were $52m – some 30% of annual profits, including direct incident response costs, forensic costs and customer management costs such as the provision of additional call-centre agents, communication and marketing costs[24]. These costs also included restoring its online portal with enhanced security features. The cyber breach dominated TalkTalk's third-quarter trading in 2015, and also led to major changes in governance including the appointment of a chief information security officer, customer-awareness campaigns and a fundamental security review.

Slow-burn costs: Medium
TalkTalk shares dropped by more than 10% when the breach was announced, but have since recovered. The company also encountered increased customer churn, losing some 95,000 broadband customers, while offering free upgrades to customers and some $4m in credits[25]. H2 revenues for TalkTalk grew by just 0.2% compared with the previous six-month growth of 4.75%, a potential $19m of lost revenue and circa $25m impact from the lower customer base with which TalkTalk entered Q4. Customer satisfaction declined from 69% in September 2015 to a low of 64% in January 2016. Since that time TalkTalk has rebuilt brand confidence, reaching customer satisfaction levels of 80%, and has reduced customer churn[26]. The parliamentary select committee for Culture, Media and Sport has now concluded its inquiry into TalkTalk, with its chair calling for the public disclosure of an independent report on the incident by PwC. In October 2016 the UK Information Commissioner levied its largest ever fine of $496,000 against TalkTalk for its security failings.

Where UK pounds are converted to US dollar fgures, the exchange rate used was 1:1.24
21 https://help2.talktalk.co.uk/oldoct22incident
22 http://www.independent.co.uk/news/uk/crime/talktalk-hack-second-teenage-boy-arrested-in-connection-with-attack-a6714591.html
23 http://www.bbc.co.uk/news/uk-37990246
24 TalkTalk Telecom Group Plc Q3 FY16 Trading Update – 2 February 2016
25 https://www.theguardian.com/business/2016/feb/02/talktalk-cyberattack-costs-customers-leave
26 Talk Talk, Annual General Meeting Year to March 2016, Presentation

3 The true cost of cyber crime

Data on cyber breaches remains relatively sparse, with many organisations reluctant to disclose such attacks. This means there is a lack of structured cost and impact data. There are benefits to the business community of improving the transparency of incident reporting, as it allows both companies and the insurance sector to make better decisions on cyber risk.

One lesson is clear though – by reacting swiftly to mitigate the impacts of a cyber breach once it has occurred, thereby minimising immediate costs, companies could reduce their exposure to subsequent slow-burn costs.

Expert opinion from the Lloyd's market

A breach handled badly can not only be an embarrassment to a business but can also cause real harm. Of the worst handled breaches out there, one incident involved a policyholder advising 10,000 consumer clients of a breach, in advance of conducting IT forensics, to subsequently discover the only information breached was that of a specific client subset, only totalling 200. Conversely, some public reports even cite a well handled breach as a PR success, and one which might drive even more business in that company's direction, so breach response efforts really should be of utmost importance to all companies.

Scott Bailey, Head of Emerging Risks - Professional and Financial Risks, Markel International

Section 4
The four drivers increasing cyber-risk complexity

4 The four drivers increasing cyber-risk complexity

Cyber threats have risen up the agenda for businesses in the past couple of years, propelled by some of the high-profile incidents referenced in earlier chapters. The average cost of a serious breach nearly tripled from 2014 to 2015[27] according to some estimates, and this number is likely to grow even further as the cyber risk landscape becomes ever more complicated.

These factors must be considered by all businesses and governments. They can be more easily mitigated than most costs associated with cyber incidents but, if managed badly, can have serious financial ramifications.

The following are the views of legal and insurance experts on the factors most likely to influence the complexity and cost of future breaches.

1. Changes to European regulations, by Hans Allnutt, Partner, DAC Beachcroft

Cyber risk is a significant societal threat recognised by governments around the world. The UK, for example, continues to rank cyber-attacks as a Tier 1 threat alongside terrorism, international military conflicts, major human health crises and major natural hazards[28].

Criminal laws and international treaties can only go so far in deterring and punishing those responsible for cyber-attacks and threats. Therefore, governments are updating and passing new laws to improve the security and resilience of electronic networks, systems and data. One key feature of these new laws is the potential for an increase in penalties and sanctions levied at businesses that fail to adhere to their requirements.

Just as any businesses that operate electronically or hold electronic data will be exposed to cyber risk, so they are likely to be subject to one or more of these new laws. In Europe, two pieces of forthcoming legislation will significantly increase the burden on such businesses: the European General Data Protection Regulation (GDPR), which seeks to protect citizens' privacy and data security; and the Network & Information Security (NIS) Directive, which aims to protect critical electronic networks (see below).

After a long legislative negotiation process, the text of the GDPR has been finalised and will apply across European member states on 25 May 2018[29]. It aims to bring European data protection laws up to date with the modern technological possibilities of the "Big Data" age, harmonise the varied data protection laws across Europe and bring companies situated outside the EU within the scope of European law in certain circumstances.

The GDPR is further reaching and more onerous than current law. Key aspects include:

- The extension of jurisdictional scope to include any business that offers goods and services to EU citizens, regardless of where it is located.
- A requirement for businesses to recognise customers' enhanced data rights, including the "right to be forgotten", the right to have their data transferred to other businesses and the right to object to profiling activities.

27 http://www.pwc.co.uk/services/audit-assurance/insights/2015-information-security-breaches-survey.html
28 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf
29 http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

4 The four drivers increasing cyber-risk complexity

– A stipulation that, in certain circumstances, security breaches must be reported to a relevant regulator within 72 hours and to affected citizens without "undue delay".

– The ability to impose fines of up to 4% of annual worldwide turnover or €20m (whichever is higher). Individuals may also claim compensation from organisations for not only financial loss but also any non-material damage (e.g. distress) that is suffered.

The second piece of new EU legislation, the Network and Information Security Directive, will focus on the security of essential digital infrastructure and services which underpin economic and societal activities. The NIS Directive sets a deadline of 9 May 2018 for EU member states to incorporate its provisions into national law (as a regulation, the GDPR has direct effect on all member states, whereas a directive does not).

As part of the incorporation of the directive into national law, each member state will identify "operators of essential services" within the jurisdiction. These are services that are critical for society and the economy, and which would suffer significant disruption from a cyber incident. Such providers encompass energy, transport, telecommunications, health, banking and drinking water supply sectors. Once identified, businesses that operate these services will be required to take appropriate and proportional security measures and to notify serious incidents to the nominated authority.

Because member states are currently in the process of incorporating the directive into national law, the exact requirements, authorities and sanctions have yet to be determined (some observers have commented that sanctions will be similar to those of the GDPR). The important aspect of the directive is that businesses may be subject to the new law irrespective of the data they hold: it is a law that is focused on protecting essential or digital services that are exposed to cyber risk.

2: Trends in litigation by Hans Allnutt, Partner, DAC Beachcroft

Businesses that suffer security breaches of any type of information are increasingly likely to receive legal action from individuals and organisations to which the information belongs or relates to. In particular, there is a global trend for individuals to bring compensation claims where the information is their personal data or where it affects their privacy. This so-called "compensation culture" has been spurred on by changes to privacy and data protection laws, and is expected to grow further as the GDPR comes into force in 2018.

Recent legal precedent in the UK[30] has recognised that data security and privacy breaches can have detrimental effects on individuals, causing both financial loss and emotional distress. Failures to ensure the security of medical information, private communications and confidential information are all recent examples where judges have awarded compensation for the emotional distress caused to individuals.

The GDPR will formalise the rights of individuals to bring such claims against businesses that fall within its scope. Furthermore, the GDPR provides a mechanism for member states to establish not-for-profit organisations to pursue compensation claims on individuals' behalf - potentially ushering in an era of consumer-group litigation across Europe.

These developments have increased, and will continue to increase, the costs of defending and compensating data breaches.

30 Various cases, in particular Vidal-Hall v Google, Inc. [2015] EWCA Civ 311

4 The four drivers increasing cyber-risk complexity

3: Supply chain security

Large businesses and governments are increasingly seeking to impose cyber-security obligations on their major suppliers, as well as seeking assurances that third-party liability insurance cover is in place to allow such suppliers to meet their contractual obligations and indemnify the client against potential damage. Mature vendor management protocols and processes are critical to ensuring a well-secured network ecosystem.

For example, the UK Government now requires suppliers to be certified to a baseline cyber security standard – known as Cyber Essentials – if they process personal or government information. Cyber Essentials outlines a series of requirements that businesses must adhere to, ranging from basic technical protection and the creation of user access controls, to the implementation of malware defences and correct management of software patches. Similar obligations are being imposed by major financial organisations, reflecting both their own risk management protocols and cyber-security requirements imposed by regulators.

It is likely that supply-chain security obligations will grow as other firms (including critical national infrastructure (CNI) operators and firms involved in the handling of sensitive personal data, such as pharmaceuticals) pay greater attention to third-party assurance.

Expert opinion from the Lloyd's market

Global technology-dependent supply chains are a way of life for modern business but bring with them significant challenges and risks. Integrating supply chains by connecting different systems creates opportunities for cyber criminals to infiltrate the chain by penetrating the weakest link.

Cyber risk is not just an IT risk: it is now recognised as an enterprise risk management challenge with the potential for significant effects on a business. Organisations must understand this, as well as the extent of their operational interconnections - both internally and with respect to supply chains.

Key personnel within the organisation should be tasked with identifying how much and what kind of data is held, and where it sits. This classification process is the first step to understanding potential data risks. The supply chain should be audited, in as far as it is feasible, and protections put in place through contracts with suppliers and vendors, including regular audit capabilities. An insurance professional can then advise on risk mitigation, and the right insurance cover needed to help protect against cyber threats and other supply chain risks. The goal is to recognise the threats, limit exposure and ensure supply-chain risk is reduced.

Oliver Brew, Global Head of Cyber Risk, Aspen Insurance

4 The four drivers increasing cyber-risk complexity

4: The internet of things and integrated systems

From the relatively basic incidents of the 1980s to the global cyber warfare and organised crime of today, as technology has advanced so too has cyber risk. What is clear is that this evolution isn't stopping – no sooner do organisations learn how to deal with one threat than a whole new generation of threats emerges.

Top among the threats with the potential to dominate in the near future are those linked to the internet of things. As more devices and processes become connected to the network – as many as 50 billion by 2020, according to some estimates[31] – so more ways into it are created, increasing exponentially the potential for hacking, ransomware and denial-of-service attacks.

Not only will this create a new, consumer-focused market for cyber risk as individuals look to cover themselves against cyber-attacks, but it will also generate a host of new liability concerns for organisations ranging from technology companies to retailers. From smart lighting to building monitoring systems, a huge range of devices will become connected to the internet, meaning companies will require sophisticated insurance solutions to minimise their risk exposure.

Summary

The combined impact of these four trends set out above is a clear warning for organisations to heed. As the risk of cyber-attack increases, so do the legal and cost ramifications of dealing with them. Regulatory sanctions and compensation, combined with increasing complexity, represent a significant financial risk to businesses that fail to adequately secure their electronic networks, assets and data, and fail to hold and use data in accordance with privacy laws.

31 https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf

Section 5
Closing the cyber-insurance gap

5 Closing the cyber-insurance gap

Although Europe's economy is a similar size to that of the US, the level of cyber insurance purchased by EU businesses is far lower: one estimate suggests that American companies spend around $2.5bn on cyber insurance per annum, compared to just circa $150m by those in Europe[32]. Many businesses operating in the EU have not yet taken the necessary steps to protect their business against cyber-attacks.

In the US, demand for cyber risk coverage was created, and continues to be driven, by privacy breach laws that place onerous requirements on businesses that suffer a data loss and can vary from state to state.

The absence of similarly stringent measures in the EU to date may contribute to the relative lack of awareness around cyber insurance on the continent: a recent Lloyd's survey of more than 350 senior decision-makers across European business revealed that almost three quarters had a limited knowledge of cyber insurance, with around 50% unaware that they could seek insurance cover for data breaches.

This is worrying, particularly considering the rapid advances in technology that are changing the nature of cyber risk for many organisations and given the potential impacts set out in this report. The prospect of a fine and the costs of lost data are no longer the only considerations in the event of a breach. Retailers that lose payment card information may incur financial penalties from card issuers, and lawyers whose systems are hacked for details of an upcoming M&A deal may find themselves in breach of their client retainer. Even a music-streaming provider may have to compensate its customers under its own terms and conditions if its services were taken offline by malicious activity.

Plus, with cyber-risk liability being increasingly driven down the supply chain and written into contracts drawn up between trading partners, it's no longer just "clicks and mortar" companies with strong commercial online presence that are being targeted.

The Lloyd's market pioneered cyber insurance and has a comprehensive understanding of cyber risk and cyber risk mitigation. As part of this report, we carried out in-depth interviews with expert cyber underwriters in the Lloyd's market to find out what companies can do to mitigate the risks of cyber-crime and protect themselves should a cyber-attack take place.

This research led to the following four conclusions:

1. Understand your unique risk profile – and share it

For underwriters, insuring cyber risk involves compiling in-depth information on their customers to determine their exposure to cyber-attacks. This information includes the size and type of business, as well as more complex detail, including the volume of sensitive data held and the value of that data; the different security protocols the company observes (e.g. adherence to ISO quality standards around security); the potential motivations for attack; the geographies the company operates in, the vulnerability of the supply chain; and the profiles of the executive team.

Lloyd's underwriters can combine this information with the cyber-risk trends they are seeing to come up with a bespoke, accurately priced cyber policy that covers companies' specific insurance needs.

The more information businesses have, and the more they share with their insurer, the more effectively insureres are going to be able to price and mitigate cyber risk.

32 https://www.ft.com/content/69db580c-4d37-11e4-8f75-00144feab7de?mhq5j=e1

5 Closing the cyber-insurance gap

2. Prepare for today's risks – and tomorrow's

One of the most challenging aspects of mitigating cyber risk is keeping up with the pace it changes. The rapid advancement of digital technology is providing criminal hackers with fertile ground on which to trial and deploy new tactics, either by adapting existing techniques or exploiting entirely new weaknesses. New technology around the internet of things – such as smart lighting and building monitoring systems – will have an impact on business risk exposure.

Keeping up to date with these threats is a tough operational challenge but one that businesses must try to stay on top of.

The onus is on insurers to do the same, so as well as helping their customers identify current and future challenges, they also put in place a number of measures to ensure cyber risk insurance is flexible and comprehensive enough to take these rapid developments into account.

The more insight companies can give their insurer on the risks they might face in the future, the better insurers can protect businesses from the fast-evolving cyber threat.

Expert opinion from the Lloyd's market

Insurers are used to helping clients protect themselves against risks that stay relatively constant, year on year. Cyber risk isn't like that: it morphs and evolves at a rapid pace. To take just one example, we saw ransomware attacks against our clients more than quadruple last year and we expect them to double again in 2017. That said, cyber is not a typical "emerging risk" that cannot yet be quantified. Lloyd's underwriters, including Beazley, have been writing cyber risks for more than a decade and have handled thousands of data breaches successfully on behalf of clients – we know how to price the risk.

A major driver of exposures in all the territories where we do business is the regulatory regime. Cyber insurance developed earlier in the US than elsewhere because the US had a patchwork of data breach regulations (now extending to 47 states), plus an overlay of federal regulation in certain industries, such as healthcare. We see demand for cover growing rapidly in Europe prior to the coming into force of the EU's General Data Protection Regulation (GDPR) next May.

Paul Bantick, Senior Cyber Underwriter, Beazley

5 Closing the cyber-insurance gap

3. Company culture counts

A new dimension, now increasingly taken into consideration by underwriters, is the company culture towards cyber risk, and how it permeates across the organisation.

Employees are frequently exploited as the weakest link when a company is attacked. Social engineering vulnerabilities are an important consideration for any underwriter offering cyber risk insurance, as are the network access rights provided to tech and admin personnel, and the level of staff training on these issues. Underwriters may also explore how high profile cyber-security awareness is among board members, as it can provide a useful reflection of the organisation's overall attitude towards cyber risk. Specifically, insurers want to see evidence that cyber-risk awareness exists throughout an organisation.

Companies that demonstrate a culture of cyber security awareness and have in place the right cyber security technologies could benefit from lower insurance premiums.

Expert opinion from the Lloyd's market

Company culture counts – in fact it forms a critical part of underwriting the risk. All businesses should treat cyber as an organisational risk, not just an IT or technological one. It is just as much about staff awareness and training, and good processes too.

At a board level, someone in the C-suite must be able to raise their hand and say: 'I'm responsible for cyber risk.' And increasingly we are seeing CEOs do this.

Matthew Webb, Group Head of Cyber, Hiscox

5 Closing the cyber-insurance gap

4. Call in the experts

There is a huge amount of confusion around cyber insurance, which stems from the fact certain aspects of cyber threat may be covered by an organisation's current insurance policies. For example, existing property or business interruption insurance schemes may include some provision for cyber risk, but the specific circumstances will vary by insurer, policy and the nature of the policyholder's business.

Or while a business-interruption insurance policy might cover the insured for lost revenue in the event of denial-of-service attack that takes the company's website offline, the cover might not extend to the cost of customer compensation in the event of data loss or service unavailability. And when it comes to cyber, the impacts can be costly and long-lived.

Evaluating risk only in terms of the immediate loss or period of business disruption is no longer adequate, so underwriters always try to ensure that businesses are sufficiently shielded from the ongoing impacts of a breach such as customer churn, share-price impact and the loss of competitive edge. Reputational harm as an intangible form of loss is certainly on the rise.

If companies are not sure on what is and isn't covered – or need advice on any other aspect of cyber risk mitigation or insurance – they should contact their broker or insurer. Insurers have a range of experts they call on to offer businesses the best advice – and therefore give them the best protection.

Expert opinion from the Lloyd's market

A lot of companies think they're covered under their property or general liability policy. Some are, but the cover tends to be very restricted with significant sub-limits and narrow coverage, which would be window dressing in the case of a major breach.

One of the significant problems is that many companies don't know how much cyber coverage they need to buy. Some aspects of the coverage such as business interruption are quite easy for a company to work out, but when it comes to liability, class actions, bank assessments and fraud, it's very hard for a company to assess their requirements without the help of an insurer.

Laila Khudairi, Head of Enterprise Risk at Tokio Marine Kiln

Section 6
Conclusion

6 Conclusion

The cyber threat is evolving on a daily basis so companies must be better prepared for the consequences of a cyber breach. Not only are the costs – both immediate and slow-burn – likely to increase with the introduction of new European legislation but the number of ways companies can be targeted is increasing.

While it is not possible to be 100% secure from a cyber-attack, there are a number of measures companies can take to reduce the risk of it happening – and to help ensure they minimise the consequences and recover more quickly should a breach occur.

Insurance is part of this solution. Every day, Lloyd's specialist cyber underwriters work with thousands of companies, from multinationals to SMEs, across the world to understand their risks better and to provide them with the expert advice and insurance cover they need.

To find out how Lloyd's insurers can help you, visit **lloyds.com/cybercoverage**

Sector Attack Chart: Source Data