

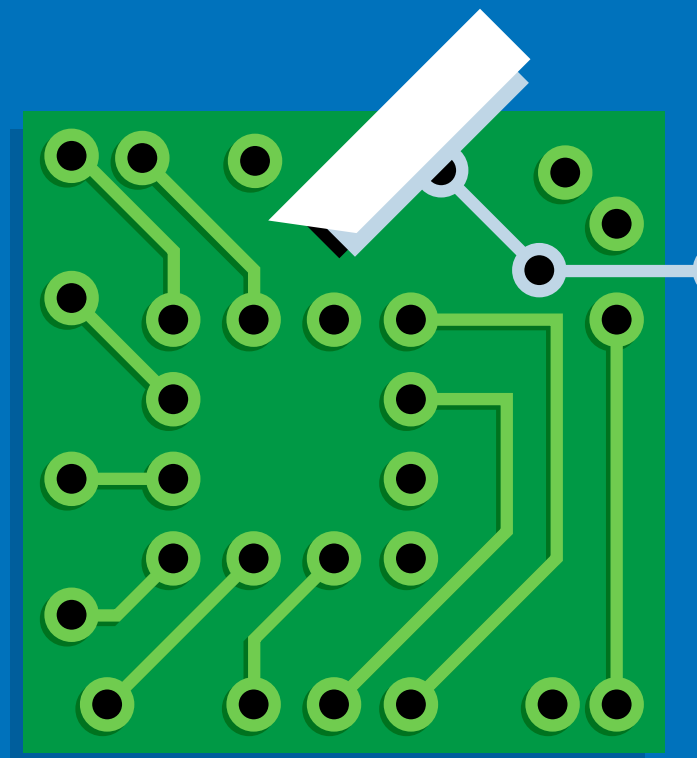


Closing the Gap

**Cyber Security and
the insurance sector**

July 2017

kpmg.co.uk/closingthegap



The changing threat

As much as new technology has provided a platform for business innovation and growth, it has also brought new risks. One of these, that is never far from the headlines, is cyber security. The attacks seem to keep on coming. The WannaCry ransomware attack in May 2017, for example, impacted more than 200,000 systems worldwide.¹ This was swiftly followed a month later by the Petya (and variants) ransomware attack that had its epicentre in Ukraine and caused widespread disruption.








This is an adaptation of 'Closing the Gap: Insuring your business against evolving cyber threats', a report produced in association with KPMG in the UK, international law firm DAC Beachcroft and Lloyd's of London. To read the full report, visit kpmg.co.uk/closingthegap.

Globally, cybercrime is now estimated to cost \$400bn a year, meaning cyber risks are among the top issues that businesses have to consider when it comes to their resilience and continuity planning.²








What makes cyber risks so challenging to deal with is the rapid pace of change in the digital space.

How are insurance companies faring in the cyber battle, and what should their priorities for action be?

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. |
|  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of people from a certain organisation or geography, and criminal infrastructure to leverage vulnerabilities in often out of date software.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, commodity ransomware, denial-of-service attacks, SQL injection |

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. |
|  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, business email compromise fraud / CEO fraud, targeted ransomware |

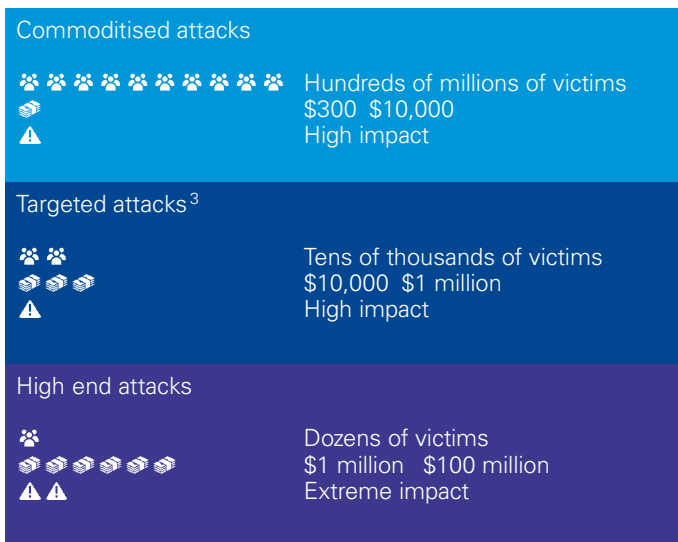
High end attacks

| |
|--|
|  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. |
|  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, disrupting critical infrastructure |

¹ <https://www.ft.com/content/82b01aca-38b7-11e7-821a-6027b8a20f23>

² Net Losses - Estimating the Global Impact of Cyber Crime, Center for Strategic and International Studies, June 2014

Organisations including insurance companies are not, by and large, dealing with scattergun attacks.



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.

But what of the insurance sector specifically? How are insurance companies faring in the cyber battle, and what should their priorities for action be?

Pressure rising on the insurance sector

Insurers confidently deal with massive risks every day. Indeed, insurers whole business is a form of risk management. But when it comes to cybersecurity, the sector has perhaps lagged behind other financial services sectors – notably banking – in cyber investment, focus and capabilities.

In part, this has been due to necessity: banks were getting pummelled by cyber-attacks and needed to move quickly to protect their reputations, customers and bottom lines. The cyber war has traditionally been much quieter on the insurance front.

But the signs are that this is changing. As other financial sectors become more secure, attackers are moving on to find weaker targets and this is bringing insurance companies into the firing line. The stakes are high, as insurers hold enormous amounts of data on individuals across all sorts of areas of their lives, such as health and

personal property to name but two. At the same time, regulators have started to ask insurance CEOs difficult questions about their cyber resilience position.

The urgency of the situation is illustrated by KPMG's recent Global CEO Outlook survey, in which less than half of the insurance CEOs surveyed (43%) said that their organisation is fully prepared for a cyber event.⁴ This was broadly in line with the cross-sector average, but nevertheless, in an industry dealing with financial transactions and personal data, it is a worryingly low percentage.

Cyber risk today

Analysis completed by KPMG in the UK shows that attackers tend to be clustered into three main groups, using either 'commoditised', 'targeted' or 'high-end' approaches to victim selection and exploitation.

Of these three, set out below, it is commoditised and targeted attacks that pose the greatest threat to the insurance sector.

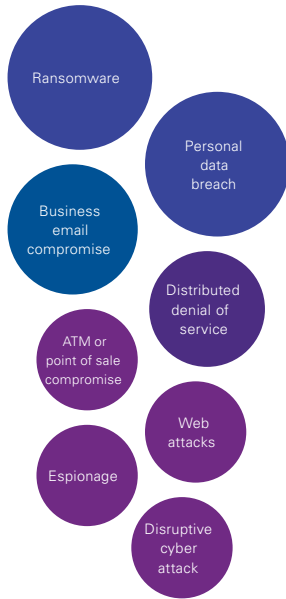
The KPMG Global CEO Outlook survey found that insurance CEOs feel least prepared to deal with ransomware and distributed denial-of-service attacks (only 32% and 37% respectively feel fully prepared).⁵ They feel most prepared to deal with business data theft attacks (55%).

³ <https://home.kpmg.com/uk/en/home/insights/2016/07/taking-the-offensive-working-together-to-disrupt-digital-crime.html>

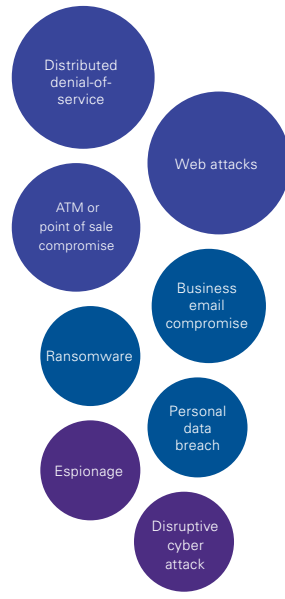
⁴ <https://home.kpmg.com/uk/en/home/insights/2017/06/2017-ceo-outlook.html>

⁵ <https://home.kpmg.com/uk/en/home/insights/2017/06/2017-ceo-outlook.html>

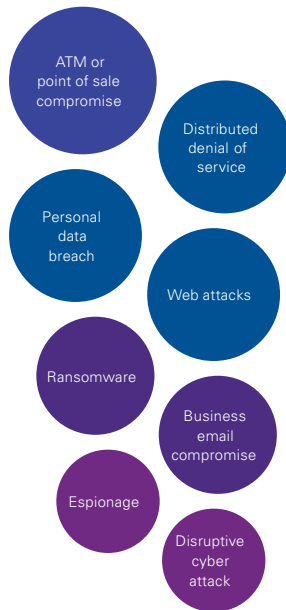
Healthcare



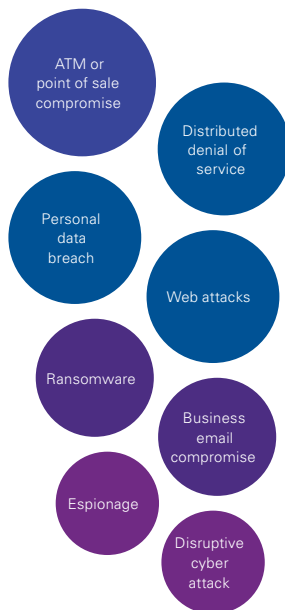
Financial services



Retail



Telecommunications



The changing threat

The threat landscape continues to evolve. Criminals are looking to repurpose attacks used against banks to target new institutions such as insurers, e-retailers and the healthcare sector. Industrialisation of cybercrime 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 shows the different types of attacks that insurers and companies in related sectors are subject to. The 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 including insurance companies 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.

Insurance

The increasing focus on moving customer interactions to digital channels means that strong cyber security discipline is more important than ever, as it provides a target for cyber criminals to attack. Insurers have a wealth of data points on individuals – across their health details, property, cars and other vehicles, and even their pets. If banks hold the money, insurers hold the data. Identity fraud is therefore a significant risk. Cyber attackers will move to the point of least resistance – as banks strengthen their defences, they may move their focus to the insurance sector amongst others.

Insurers have a wealth of data points on individuals

Banking

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 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.

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.

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.

Telecommunications

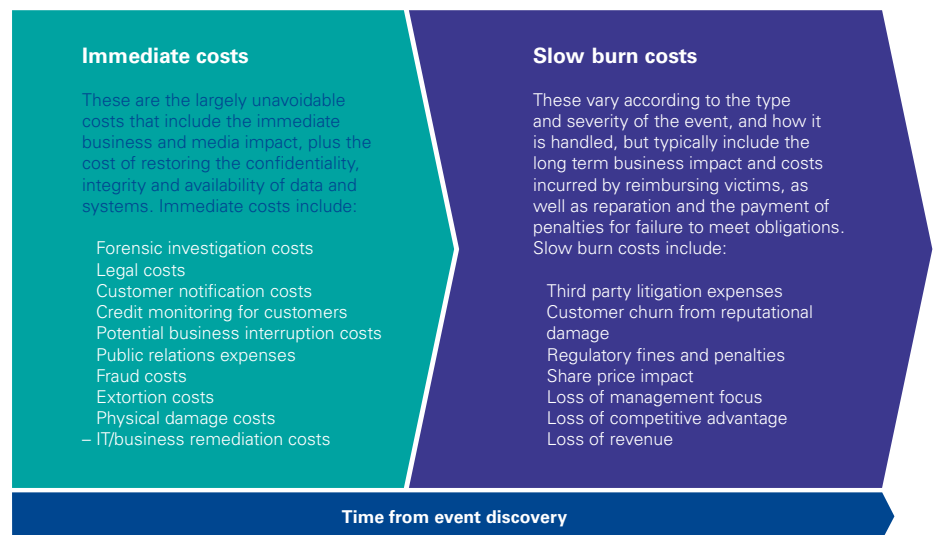
As the heart of our networked world, telecom firms attract criminal attention as a route to compromise mobile devices. They also find themselves a target for state espionage and, occasionally, infrastructure attacks.

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 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 the insurance/financial services sectors.⁶

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



Banks are locked in a battle with cyber criminals to secure digital banking channels and counter fraud.

⁶ <https://home.kpmg.com/uk/en/home/insights/2016/07/taking-the-offensive-working-together-to-disrupt-digital-crime.html>

Case study

Anthem Insurance Companies, Inc.

At a glance – A data security breach of Anthem’s systems in late January 2015 potentially exposed the personal records of around 78.8 million customers.⁷

Anthem paid out \$260m⁸ for security improvements and remediation, and a further \$115m⁹ in June 2017 to settle lawsuits from customers potentially affected.



Type of attack: Data breach



Total immediate cost: \$260m¹⁰



Total slow-burn cost: \$115m¹¹



Total gross cost: more than \$375m

What happened?

On 27 January 2015, Anthem Insurance Companies, Inc discovered a major data security breach. Anthem is the largest health benefits company by membership in the United States, with member insurers licensed to conduct business in all 50 states and the District of Columbia. The breach was eventually thought to have potentially exposed the records of around 78.8 million customers. Data affected reportedly included names, birthdays, social security numbers, addresses and email addresses, as well as employee information, but not credit card or medical data. Anthem immediately alerted its principal regulator as well as the FBI, and called in a firm of consultants to help it assess remediation steps required.

⁷ <https://www.commerce.alaska.gov/web/Portals/11/Pub/Companies/Exams/MCE16-09.pdf?ver=2016-12-12-083253-927>

⁸ <http://www.insurance.ca.gov/0400-news/0100-press-releases/2016/upload/Fully-Executed-RSA-2.PDF>

⁹ <https://anthemdatabreachlitigation.girardgibbs.com/wp-content/uploads/2017/06/2017-0623-Dkt-869-8-Settlement-Agreement.pdf>

¹⁰ <http://www.insurance.ca.gov/0400-news/0100-press-releases/2016/upload/Fully-Executed-RSA-2.PDF>

¹¹ <https://anthemdatabreachlitigation.girardgibbs.com/wp-content/uploads/2017/06/2017-0623-Dkt-869-8-Settlement-Agreement.pdf>

¹² <http://www.insurance.ca.gov/0400-news/0100-press-releases/2016/upload/Fully-Executed-RSA-2.PDF>

¹³ <https://www.infosecurity-magazine.com/news/anthem-to-fork-out-115m-in-breach/>

¹⁴ <https://anthemdatabreachlitigation.girardgibbs.com/wp-content/uploads/2017/06/2017-0623-Dkt-869-8-Settlement-Agreement.pdf>

¹⁵ <http://www.reuters.com/article/us-anthem-cyber-settlement-idUSKBN19E2ML>

Immediate costs: Very high

The costs of the incident have been truly considerable for Anthem. The initial cost of security improvements, remediation and clean up after the breach have been estimated at \$260m.¹² This is despite the fact that there is reportedly no evidence to date that any customer data has been bought or sold on the dark-net by cyber criminals. Indeed, this has led some observers to speculate that the attack could have been initiated by a nation state rather than a cybercrime gang. The California Department of Insurance said it had a “medium degree of confidence” that the attacker was affiliated with a foreign nation state.¹³

Slow-burn costs: High

In addition to these immediate costs, Anthem also faced a very stiff bill for the slow-burn effects. In late June 2017, it was announced that the insurer would be paying \$115m to settle litigation stemming from the attack. This settlement, at the time of writing, is still subject to the approval of the presiding US district judge.¹⁴ The money will be used to pay for two years of credit monitoring for those potentially affected by the attack.¹⁵ That is in addition to an initial two years of credit monitoring already offered by Anthem.

Web attacks are the biggest risk for retailers, as they target firms that offer rich digital services to clients.

Where from here?

KPMG suggests that insurers should focus on five key areas to address cyber risks.

Ownership: Cyber security is a business issue, not an IT issue. Some of the more successful insurers have elevated their Chief Security Officer to report directly to the COO, creating clear line of sight between the business and the risk.

Capabilities: New and improved cyber security capabilities are likely to be required. But insurers will also want to assess their current ‘pockets’ of cyber security excellence and ensure those best practices are shared across the enterprise. Leading insurers are starting by ensuring that their existing capabilities are being properly utilised.

Awareness: Improved awareness from the C-level down is key. In particular, insurers need to focus on improving their understanding of their ecosystem of third party participants – non-affiliated agents, outsourced service providers and other non-employees with access to data – to manage their risk in a consistent manner.

Organisation: CEOs will need to work with their business leaders to understand the right balance of centralised and decentralised services to most appropriately meet the cyber risks in each market. Creating the right structure for robust and consistent cyber security is key to fielding a responsible (and defensible) response.

Preparedness: Successfully activating a response and recovery programme takes practice, commitment and clear lines of responsibility. From ‘red teaming’ exercises that simulate the way attackers behave through to improved employee training and more frequent drills, insurance leaders need to carefully consider how to ensure their organisation remains prepared.

Contact us



Matthew Martindale
Cyber Lead – Insurance

KPMG in the UK

T: +44 79 1755 2588

E: matthew.martindale@kpmg.co.uk



David Ferbrache
Technical Director

KPMG in the UK

T: +44 7780 225463

E: david.ferbrache@kpmg.co.uk

kpmg.com/uk/insurance



The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2017 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name and logo are registered trademarks or trademarks of KPMG International.

CREATE | CRT084012 | July 2017