CYBER

SAFEGUARDING YOUR BUSINESS AGAINST DIGITAL THREATS

Allianz

INTRODUCTION

Digitalisation is revolutionising the way businesses operate, bringing benefits such as cost savings, enhanced customer service and improved access to a global marketplace.

CONTENTS

But it also brings significant risk. With everything from customers' and employees' personal data to the business's intellectual property stored electronically, there's the potential for this data to be mislaid or targeted by cyber criminals. Similarly, with businesses reliant on the internet for many of their operations, anything that prevents access can be very damaging.

Understanding the risks and taking the necessary steps to minimise them is essential. The insurance industry has an important role to play here too, with brokers able to advise their clients on the evolving risks and how cover could help to limit the financial and operational impact caused by a cyber attack or data breach.

And, with the internet and connected technologies part of virtually every business, offering this support and expertise is rapidly becoming an essential element of risk management and insurance advice.

The average total cost of a data breach was $3.68m (£2.82m) in the UK in 2018.[1]

1 Ponemon Institute (2018). 2018 Cost of a Data Breach Study: Global Overview.

THE EMERGING NEED FOR CYBER INSURANCE

A cyber attack or data breach can be devastating for a business, with consequences ranging from lost sales and business interruption through to reputational damage and fines from the regulators.

Taking appropriate steps to ensure data is held securely can help to minimise risk but with the number of incidents increasing year on year, and new cyber threats emerging all the time, organisations need to be vigilant.

The size of the problem can be seen in figures from the Cyber Security Breaches Survey 2019[2] published by the Department for Digital, Culture, Media and Sport. In this, 32% of businesses reported that they had experienced a breach or attack in the last 12 months. And, with Ponemon Institute research[3] showing the average cost of a breach in the UK to be $3.68m (£2.82m), it's something no business can afford to ignore.

Also helping to sharpen business focus on cyber security is the introduction of the General Data Protection Regulation (GDPR). This came into effect in May 2018 and, as well as introducing new requirements around data protection and breach notification, it also increased the maximum fine that can be imposed by the Information Commissioner's Office (ICO). Now, rather than the £500,000 cap which was in place under the Data Protection Act 1998, a serious failing could lead to a fine of up to €20m or 4% of global turnover, if higher.

Cyber incidents are the joint most significant risk to global organisations, alongside business interruption.[4]

2 Vaidya, R. (2019). Cyber Security Breaches Survey 2019. Department for Digital, Culture, Media & Sport. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018
3 Ponemon Institute (2018). 2018 Cost of a Data Breach Study: Global Overview.
4 Allianz Risk Barometer 2019. https://www.agcs.allianz.com/news-and-insights/news/allianz-risk-barometer-2019.html

GLOBAL COST OF A DATA BREACH[5]

Average total cost of a data breach	$3.86 million
Average cost per lost or stolen record	$148
Likelihood of a material breach recurring over the following two years	27.9%
Average total one-year cost increase	6.4%

GDPR applies across the EU but businesses trading outside of this region will also need to consider data protection regulations in these other territories to ensure compliance. This can be complex. For instance, as data protection regulation in the U.S. is determined on both a national and a state level, a UK business with U.S. customers can find itself having to get to grips with up to 50 different sets of requirements if it suffers a data breach.

With both the risk and the consequences ramping up, cyber insurance has a growing part to play in protecting businesses. Policies can include cover for third-party losses resulting from a data breach as well as for first-party losses such as breach costs, damage to a computer system, business interruption and ransoms in the event of cyber extortion.

While it will look after some of the financial losses associated with a cyber attack, for many businesses, the most valuable part is the crisis management support that is available in the event of a loss. How a business manages a cyber attack or data breach can have a significant impact on the total cost as well as its reputation and survival. Being able to access support from specialists including forensic and IT experts, lawyers and PR professionals can help keep damage to a minimum.

For smaller businesses, which won't necessarily have the in-house resources necessary to respond to a cyber attack or data breach, this support can be particularly important.

The average global cost per lost or stolen record was $148 (£121) in the UK in 2018.[6]

5 Ponemon Institute (2018). 2018 Cost of a Data Breach Study: Global Overview.
6 ibid.

UNDER ATTACK: WHAT ARE THE POTENTIAL CONSEQUENCES OF A DATA BREACH?

Data breaches can take many forms. As well as malicious cyber attacks that may lead to data being stolen or services being disrupted, internal system issues and human error can also leave data exposed.

Figures from the Ponemon Institute's research show that a higher percentage of data breaches in the UK are now due to malicious or criminal attack – 50% in 2017 compared with 37% in 2014.[7]

FINANCIAL

Financial losses can arise from the attack or breach itself but also from the remediation process and lost sales. There are likely to be costs incurred from the use of forensic or IT experts to investigate the breach and to repair the damage and restore data. Legal assistance will likely be required to advise the insured on their legal and regulatory duties, such as notifying third parties and/or the regulator. Further, there may be costs such as operating a temporary call centre to handle enquiries from affected customers and suppliers.

The Ponemon Institute reported that the average cost of a malicious or criminal data breach incident in the UK was $179 (£147) per record in the UK, compared to $147 (£121) and $127 (£104) for system glitches and human error respectively.

BUSINESS INTERRUPTION

Where an attack brings down a company's systems, there will also be business interruption costs to consider, especially if an attack leads to loss of service or requires system downtime to restore services or data. The quicker a breach can be identified and contained, the lesser the impact to operations. However, it seems it's taking longer for companies to manage such attacks; the mean time to identify (MTTI) increased from 190 days to 196 days between 2017 and 2018 and the mean time to contain (MTTC) increased from 66 days to 69 days on average.[8]

REPUTATIONAL DAMAGE

Reputational damage can also be an unfortunate by-product of a cyber attack, especially where the organisation doesn't respond promptly and effectively. This can have far-reaching effects, including a hit on profits, a fall in the share price and potential management resignations.

7 Ponemon Institute (2018). 2018 Cost of a Data Breach Study: Global Overview
8 ibid.

COMMON TYPES OF CYBER ATTACK

Industry experts project that global losses from business email compromise scams will exceed US$9bn in 2018.[9]

86% of companies surveyed worldwide reported at least one cyber incident in 2017.[11]

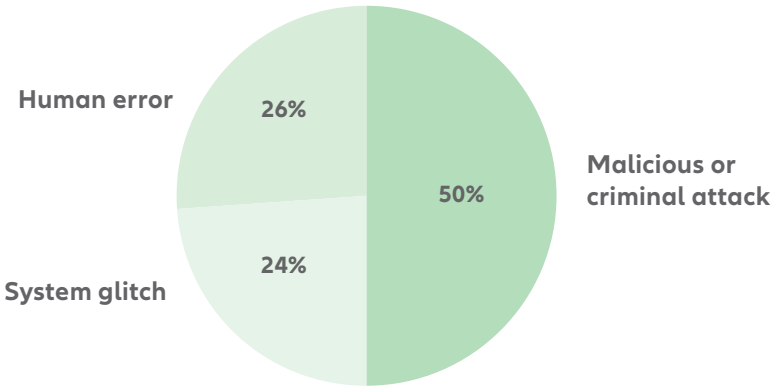
Hacking – cyber criminals can use several different methods to break into an organisation's IT systems and access sensitive data. These include taking advantage of a weakness in an organisation's cyber security or spear phishing, where the cyber criminal sends a targeted email seeking access to information. Organisations can also become victim to hacker theft, where a criminal makes unauthorised payments on the company's behalf.

Ransomware – this is a form of malware, often distributed through emails, which can take over a computer, locking it and, in some cases, encrypting the user's files. The cyber criminals then demand a ransom to restore the computer.

Businesses have experienced a 5% increase in criminals impersonating their organisation in emails or online.[10]

9 Vaidya, R. (2019). Cyber Security Breaches Survey 2019. Department for Digital, Culture, Media & Sport. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018
10 ibid.
11 Kroll (2019). Global Fraud and Risk Report: 10th Annual Edition - 2017/18. [online] Available at: https://www.kroll.com/en/insights/publications/global-fraud-and-risk-report-2018

DATA BREACH ROOT CAUSE IN 2017 IN THE UK[12]



The WannaCry ransomware attack in May 2017 infected 300,000 devices across 150 countries (NCSC).

Distributed Denial of Service –another variation on a ransom demand type attack is a distributed denial of service (DDoS) attack. With these, the organisation's systems or internet sites are bombarded with huge amounts of data in order to block their access, with the criminals often demanding a ransom to cease the attack. These are usually thought-out, planned and targeted attacks on businesses and use a vast amount of system resources, involving groups of hackers working together in order to bring about the attack.

In extreme cases, these attacks can be focused on causing mass disruption, so rather than demanding a ransom from one business, their intention is to cause chaos. If hackers target large data centres that hundreds of businesses rely on for cloud computing resources and data storage, then businesses are blocked from accessing their data, using software, and ultimately operating as a business. Hackers could have numerous reasons for carrying out such attacks, from political motivations to disgruntled former employees.

In both ransomware and DDoS cases, ransoms are usually in a virtual currency such as Bitcoin, where its anonymity makes it impossible to trace. Cyber criminals often set ransoms relatively low, working on the principle that more people will pay. However payments from the victim are rarely advisable since they could lead to rising ransom demands and may not even guarantee recovery of the data.

Supply chain compromise – cyber criminals can also exploit the weakest link in a supply chain, targeting that organisation with security flaws or malware which can then be passed along the supply chain. As well as looking for suppliers with weak cyber security, managed service providers can also be targeted due to the potential for spreading the malware to a large number of customers.

12 Ponemon Institute (2018). 2018 Cost of a Data Breach Study: Global Overview

POTENTIAL NEW AND EMERGING THREATS

Cyber threats are constantly evolving, both in line with advances in technology but also as the criminals find new ways to make money. Understanding these changes, and ensuring that cyber security is up-to-date is essential. These are some of the emerging threats.

CYBER HURRICANE

This is the name given to an event where hackers disrupt a large number of organisations by targeting common internet infrastructure and/or service providers. As an example, a cyber attack on a major cloud computing company could affect all of its customers.

INTERNET OF THINGS

As more smart devices become connected in the Internet of Things, it will increase exposure to cyber risk, especially where connected devices might have lower levels of security. For instance, criminals may be able to gain access to an organisation's IT systems through employees' mobile devices or the company's connected kettle.

Computerised controls, including alarms, environmental controls and CCTV can provide a back door for cyber criminals because they often utilise cost effective but non-supported operating systems. Unsupported systems can be open to security threats and provide easy access to computer systems, bypassing firewalls and enabling hackers to gain access to business's private or confidential data.

CRYPTOJACKING

Cryptojacking, which is also known as cryptomining malware, is where a hacker hijacks a computer or mobile device and uses it to mine cryptocurrency on their behalf. As well as the security and ethical issues this raises, it can also push up operating costs and potentially slow down legitimate work.

HOW CYBER ATTACKS AFFECT DIFFERENT INDUSTRIES AND SECTORS

Businesses of all shapes, sizes and sectors can experience a cyber attack but with the criminals looking to make as much money as possible, those with the most to lose are often the most targeted.

This means that organisations that hold a large amount of personal data are often selected, with prime sectors including financial services, telecommunications and services.

This is changing though. More recent cyber attacks such as ransomware work on scale by attacking as many computers as possible. Then, by setting the ransom relatively low – for example Wannacry's ransom was $300 – it only requires a small percentage of those infected to pay, and the criminals have made a significant return.

Similarly, mandate and business compromise emails can affect businesses of any size or sector.

One such victim was Dublin Zoo, where cyber criminals stole nearly €500,000, and according to NCSC, the art industry has also suffered a string of attacks with art galleries and dealers among those targeted.

SECTORS EXPERIENCING THE MOST DATA BREACHES[13]

Financial services	77
Services	71
Industrial manufacturing	66
Technology	62
Retail	35

13 Ponemon Institute (2018). 2018 Cost of a Data Breach Study: Global Overview

Business email compromise scams are a serious threat to organisations of all sizes and across all sectors. It represents one of the fastest growing, lowest cost, highest return cyber crime operations.

HOW CYBER BREACHES HAVE AFFECTED COMPANIES

WANNACRY

WannaCry was a ransomware attack that affected more than 300,000 computers around the world in May 2017. A self-replicating worm, it exploited a vulnerability in the Windows operating system. Although Windows had released a patch, plenty of computers hadn't updated their systems.

Once infected, a computer would become encrypted, preventing it from being used. To unlock it, the user had to pay a ransom of US$300 in Bitcoin.

Organisations of all types and sizes were affected by the attack, including Spanish telecommunications company Telefonica, the Russian Ministry of Internal Affairs and, in the U.S., FedEx. In the UK, the NHS was a major casualty, with more than a third of England's NHS trusts affected.[14] As a result, more than 6,900 appointments were cancelled and some patients had to travel further for accident and emergency care.

Wannacry's spread was stopped when a security researcher registered WannaCry's kill switch domain. This meant that when the ransomware contacted this domain, it effectively turned itself off.

TALKTALK

In October 2015, a cyber attack on telecommunications company TalkTalk enabled thieves to exploit vulnerabilities in its webpages to access customers' personal data including names, addresses, dates of birth and financial information. In total 156,959 customers' personal details were accessed, including the bank details for 15,656 customers. A problem was first identified when internal reports showed its network was operating more slowly than normal. Further investigation found there had been an attack and TalkTalk replaced its websites with a holding page, reported the data breach to the Information Commissioner's Office (ICO) and started telling its customers.

The ICO's investigation found that TalkTalk had failed to take appropriate measures to keep its customers' personal data secure and issued its largest ever fine at the time - £400,000.

EQUIFAX

A cyber attack in 2017 exposed the personal details of up to 146 million people. Although the majority of these individuals were in the U.S., it included up to 15 million people in the UK, of which almost 700,000 individuals had information such as names, dates of birth and telephone numbers exposed.

Although the compromised systems were in the U.S., the ICO launched an investigation into the steps Equifax had taken to protect the personal information of UK individuals. This found there were multiple failings at the credit reference agency, which led to personal information being retained for longer than necessary and vulnerable to unauthorised access. In total it contravened five out of eight data protection principles under the Data Protection Act 1998.

The ICO issued Equifax with a £500,000 fine for the breach – the maximum fine allowed at the time under the Data Protection Act 1998.

14 Hughes, O. (2018). Department of Health and Social Care puts cost of WannaCry to NHS at £92m. [online] Digital Health. Available at: https://www.digitalhealth.net/2018/10/dhsc-puts-cost-wannacry-nhs-92m/

RISK MANAGEMENT

Taking a robust approach to cyber security is a must. This needs to include policies and procedures to minimise risk and keep data and infrastructure secure but also training to ensure that everyone is aware of the potential threats. The following steps should form part of an effective cyber risk management strategy:

POLICIES AND PROCEDURES

Formalise a cyber security strategy by putting together policies and procedures. These should cover how to use the organisation's IT systems, including aspects such as passwords, home and mobile working and the use of removable media such as USB drives.

PROTECT IT SYSTEMS

Firewalls and always-on antivirus software are essential to prevent the bad guys getting into a company's network but, as the WannaCry attack demonstrated, it's also important to keep systems up-to-date. As new threats emerge, this will ensure that systems are as robust as possible. Monitoring systems and running regular vulnerability scans will also help to check that security is able to respond to the latest threats.

SAFEGUARD DATA

Encryption is important for any sensitive data but this can be further enhanced by implementing multi-factor authentication. This helps to ensure that data is only accessed by those authorised to do so. Where data is particularly sensitive, or valuable, it may also be prudent to restrict access to it. Password manager tools can also help to improve security. These force employees and other users to adopt strong passwords, and change them regularly.

AWARENESS CAMPAIGNS

Raising awareness of cyber security is essential, especially as it's often an innocent employee who inadvertently lets the criminals in. Where possible, employees should be formally trained to recognise cyber threats and have awareness of the steps they can take to protect the organisation's data. This will help to reduce the risk and encourage them to share any potential issues they see. It's sensible to extend this to any other users of the IT system, such as contractors and freelance staff.

MANAGE SUPPLY CHAIN RISK

Cyber criminals will attack the weakest link in a supply chain so it is important to ensure that contractors and third-party suppliers have adequate cyber security. To do this, it may be worth stipulating a minimum standard in contracts.

Likewise, restrict access to your networks where possible to reduce the risk of 'inviting' the criminals in.

BE PREPARED

Even with the most robust security in place, cyber attacks can happen. Having incident response, business continuity and IT recovery plans in place will make it easier to respond quickly and effectively if an attack or data breach does occur.

CONSIDER CYBER INSURANCE

In combination with risk management methods, cyber insurance can minimise the financial, operational and reputational impact in the event of an attack or breach, helping to get a business back up and running swiftly.

CONCLUSION

Cyber risk affects virtually every organisation regardless of size or sector.

Understanding the risks and taking appropriate steps to mitigate them will help these businesses beat the cyber criminals and continue to enjoy the benefits technology brings.

allianz.co.uk

Allianz Insurance plc.
Registered in England number 84638
Registered office: 57 Ladymead, Guildford,
Surrey, GU1 1DB, United Kingdom.

ACOM8458 09.19