C-SUITE
SERIES

CYBER

Prepare for the expected
Safeguarding value in the era of cyber risk

FT MARKETING SERVICES

AON
Empower Results®

Cyber risk takes centre stage

Introduction

The cyber threat is producing some alarming statistics. The cost of global cyber losses is predicted to reach $6 trillion annually by 2021.[1] Cyber security spending will exceed $1 trillion from 2017 to 2021.[2]

Barely a week passes without the fallout of a cyber-attack on a major corporation hitting the headlines. In July 2019, the data breach at Capital One exposed the records of almost 106 million people in the US and Canada.[3] In Europe, Norsk Hydro was forced to halt production following a cyber-attack in March 2019, which is expected to cost the firm up to $51 million.[4]

Organisations are starting to see the significant financial impact of non-compliance with data privacy and the General Data Protection Regulation (EU) 2016/679 ("GDPR"). The UK Information Commissioner's Office (ICO) issued a notification of intention to impose a £183 million fine on British Airways in July 2019.[5] In the same month, the US Federal Trade Commission (FTC) issued a $5 billion civil penalty against Facebook for violations of an earlier FTC order. The fine has been described as both "record-breaking and history-making".[6]

[1,2] Cybersecurity Facts, Figures, Predictions, And Statistics For 2019 To 2021, Sausalito, Calif, 2019

[3] Information on the Capital One Cyber Incident, 2019

[4] Operational and market update, first quarter 2019, 2019

[5] Intention to fine British Airways £183.39m under GDPR for data breach, 2019

[6] FTC's $5 billion Facebook settlement: Record-breaking and history-making, 2019

C-suite leaders are aware of these threats to their businesses, but are they fully prepared? Do they have the tools in place to deal with a cyber-attack as soon as it occurs? A cyber-incident, no matter what kind or if it makes headline news, holds the potential to have a catastrophic impact on an organisation's balance sheet.

The C-suite are being held accountable for their actions, and plausible deniability is no longer an excuse. Boards of directors and management need to include cyber perils and solutions in corporate governance discussions, as they seek to understand and manage the financial impact of high-profile cyber-incidents.

> Organisations that fail to prepare will be left in the dark on the day of a cyber-attack, facing escalating costs and irreparable reputational damage.

Our expert interview panel

Christophe Blassiau
Senior Vice President,
Digital Security & Global CISO
Schneider Electric, France

Paolo Borghesi
Group Chief Information Security
Officer, Nexi, Italy

Patrik Bless
CISO, Partners Group, Switzerland

Charlie Cannell
Digital Director,
Inflexion Private Equity, UK

Alessia Carnevale
Head of Risk Management,
Nexi, Italy

Andrew Darwin
Global Co-Chairman & Senior
Partner, DLA Piper, Global

Gorka Díaz de Orbe
CISO, Bankia, Spain

Rosa Kariger
CISO, Iberdrola, Spain

Alexander Mahnke
CEO of Insurance, Siemens
Financial Services, Germany

Dr Deborah Pretty
Founding Director,
Pentland Analytics, UK

Elizabeth Queen
Vice President of Risk Management,
Wolters Kluwer, Global

Andy Rhodes
General Manager, Global Head
of Commercial PCs, HP, US

Andy Simpson-Pirie
CTO, Lloyds Development Capital, UK

Mal Smyth
Global Head of Risk Governance,
Risk & Control, Vodafone, UK

Aon

Onno Janssen
CEO Risk Consulting
& Cyber Solutions EMEA, Aon

Vanessa Leemans
Chief Commercial Officer,
Cyber Solutions EMEA, Aon

Spencer Lynch
Managing Director Cyber Security,
Cyber Solutions EMEA, Aon

David Molony
Director Cyber Risk,
Cyber Solutions EMEA, Aon

Chapter 1

Cyber risk: Counting the cost

It can take months or even years to realise the full cost of a cyber-attack, and some firms may never recover.

When businesses are hit by a cyber attack, the financial losses can be crippling – from immediate crisis expenses and regulatory fines to longer-term, knock-on costs such as those related to reputational damage, a fall in share price or downgrading of their credit rating.

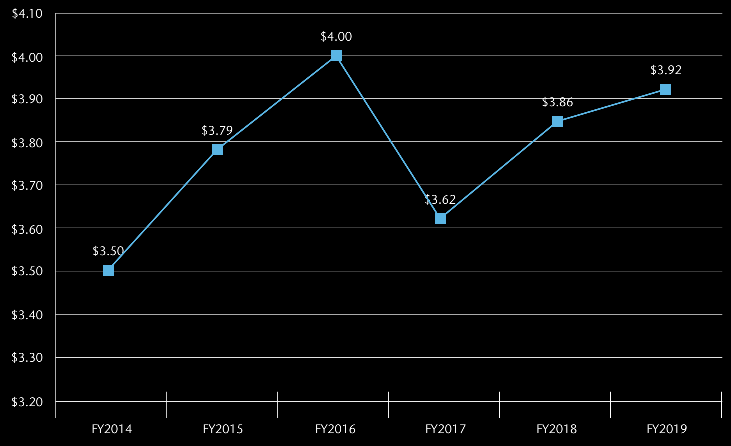
Not **if**, but **when**

The prospect of a cyber-security incident is not a matter of if, but of when. More than half of EU firms surveyed for a Kaspersky Lab report released in March 2019 had experienced a cyber-attack in the previous two years.[7]

"For us, cyber is not a theoretical risk," says Andrew Darwin, Global Co-Chairman & Senior Partner at DLA Piper. "It's probably the most real and vivid risk that we think about, knowing first-hand what the implications are when the risk becomes real."

Loss of customer information – medical records, financial records or other highly confidential personal information – is one of the immediate costs of a cyber-attack. According to IBM's 2019 Cost of Data Breach Report, the average total cost of a data breach to an organisation is $3.92 million – up from $3.86 million the previous year – with the average cost per lost or stolen record standing at $150.[8]

Figure 1. The average total cost of a data breach ($ million)



Source: 'Cost of Data Breach Report', IBM Security & Ponemon Institute, 2019

[7] Kaspersky Lab Financial Cyberthreats Report, 2019

[8] 'Cost of Data Breach Report', IBM Security & Ponemon Institute, 2019

Regulation with teeth:
GDPR raises the stakes

The EU brought in its GDPR on 25 May 2018 in an effort to hold companies accountable for their data use and management. It has led to more stringent enforcement of data breach fines, which can now reach €20m or 4% of an organisation's annual global turnover, whichever is higher.[9]

Since the introduction of GDPR, organisations have received a series of heavyweight fines. In July, it was announced that British Airways is facing a £183 million fine from the ICO following a data breach it suffered in 2018.[10] In the same month, the UK's data security watchdog announced its intention to fine Marriott International £99.2 million following a data breach last year, which led to the exposure of approximately 339 million customers' personal details.[11]

> **"This is regulation with teeth. The size of the fines levied is a direct function of what companies did ahead of time to protect themselves, what steps they took afterwards, and how swiftly, to mitigate harm."**

Dr Deborah Pretty
Founding Director, Pentland Analytics

Figure 2. Notable GDPR enforcement actions (as of July 2019)

Austria
A betting shop (€4,800): extensive CCTV monitoring of public space

Belgium
City major (€2,000): misuse of personal data for election campaign

Bulgaria
Telecoms service provider (€27,100): subscribing customers to prepaid services without consent

Cyprus
No concrete information on individual cases

Czech Republic
No concrete information on individual cases

Denmark
A company (€200,000) misuse of personal data for election campaign

France
Search engine (€50 million): breach of transparency and information duties

Germany
Unknown (€80,000): unlawful disclosure of health data

Hungary
A company organising festivals (€94,000): untransparent collection of visitor ID cards

Italy
Political party (€50,000): breach of data security on party's online platform

Lithuania
Payment services company (€61,500): breach of information data minimisation and data security duties

Malta
A public authority (€5,000): lack of security measures on website

Netherlands
Tax Authority (prohibition of processing): no legal ground for processing

Norway
Municipality (€170,000): failure to protect employee and pupil records of a primary school

Poland
Data analytics (€220,000): breach of information obligation

Portugal
Centro Hospitalar Barreiro Montijo (€400,000): breach of patient data confidentiality

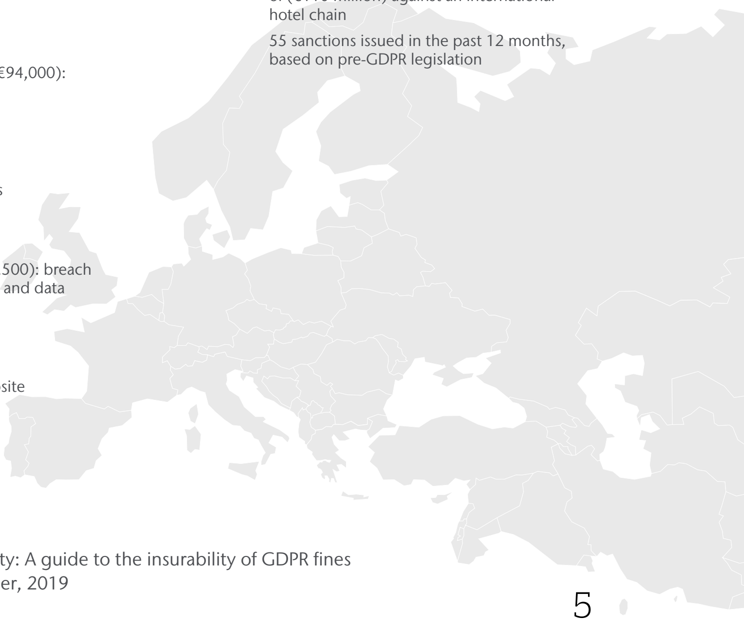
Romania
Financial services company (€130,000): failure to implement sufficient TOMs

Spain
An association (€250,000): unlawful processing of app users personal data

UK
Notice of intent to impose a fine of (€204 million) against an airline

Notice of intent to impose a fine of (€110 million) against an international hotel chain

55 sanctions issued in the past 12 months, based on pre-GDPR legislation



Source: 'The Price of Data Security: A guide to the insurability of GDPR fines across Europe', Aon and DLA Piper, 2019

[9] 'The Price of Data Security: A Guide to the Insurability of GDPR Fines Across Europe', Aon and DLA Piper, 2019
[10] Intention to Fine British Airways £183.39 million Under GDPR for Data Breach, 2019
[11] Intention to Fine Marriott International, Inc. More than £99 million Under GDPR for Data Breach, 2019

Insuring the fine: An ongoing debate

The magnitude of GDPR fines means that organisations are keen to know whether they can insure against them. As the insurability of GDPR fines is a dynamic and fluid matter, Aon and DLA Piper published a 2nd edition of their guide, *The Price of Data Security: A guide to the insurability of GDPR fines across Europe*, which sets out the latest findings with regard to the insurability of GDPR fines across Europe. The guide also looks at insurability of costs associated with GDPR non-compliance (e.g. litigation, investigation and compensation), as well as the insurability of non-GDPR regulatory fines.

Business, interrupted

Beyond loss of customer information and fines by the regulators, there is another serious cost of a cyber-attack: business interruption. The chaos caused by an attack can stop the business from trading or disrupt core operations for a period, which affects sales and revenue. “There are a range of costs directly related to a cyber-incident: fines, legal, communication and litigation, to name a few. Yet the most expensive cost of a breach, in most cases, is not being able to do your business.” says Onno Janssen, CEO Risk Consulting & Cyber Solutions EMEA at Aon.

“If systems go offline and you lose your data, there is a massive downturn in productivity, as people are simply unable to work”, says Andy Rhodes, General Manager, Global Head of Commercial PCs at HP. “It’s a soft cost that people find difficult to quantify, and has a massive impact to their top and bottom line.” he adds.

The NotPetya ransomware attack of 2017 brought companies across the globe to a standstill, costing billions of dollars in lost revenue.

Global shipping firm A.P. Moller-Maersk was one of the many businesses affected. The company stated in its annual report that the effect on its profitability was $250-300 million.[12]

Norsk Hydro, meanwhile, was brought to its knees in March 2019 by a cyber-attack that paralysed its computer networks. The resulting production shutdown cost the aluminium and energy company an estimated $51 million in the first quarter of 2019 alone.[13]

These attacks have exposed serious vulnerabilities in companies’ operating systems, and many businesses are still not sufficiently prepared for ransomware attacks. The Ponemon Institute found that, while 66% of companies recognise that ransomware is a serious threat, fewer than 13% were prepared for a ransomware attack in 2017.[14]

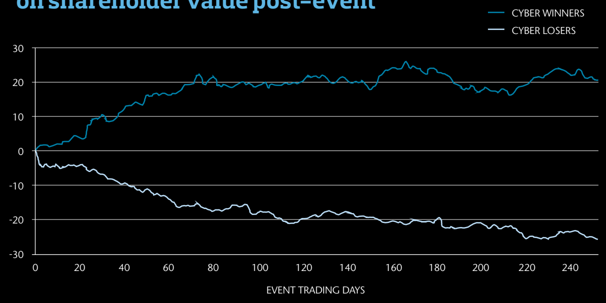
The snowball effect

Even if executives can get to grips with the upfront costs of a cyber-incident, the full cost will not be understood until much later. Post-attack, businesses may have to embark on a long and costly journey to understand the full scope of its financial impact, not to mention regain brand loyalty and repair reputational damage. “Reputation is an intangible asset that sits very firmly on many top companies’ balance sheets and, correspondingly, their incident response plans,” says Elizabeth Queen, Vice President of Risk Management at Wolters Kluwer. “Therefore, having a robust crisis communications plan is critical to the successful management of any such incident.”

“Financial losses can have a snowball effect, transforming into wider losses such as reputational risk and loss of shareholder value,” says Vanessa Leemans, Chief Commercial Officer, Cyber Solutions EMEA, at Aon. “These losses are often uninsurable, and much harder to recover from. It can take years, and some companies may never recover,” says Christophe Blassiau, Senior Vice President, Digital Security & Global CISO at Schneider Electric. “If we have a data breach, we may create a risk in terms of brand reputation. If we have repeated issues with customers, we may lose valued customers and create a customer loyalty problem.” he adds.

A reputation crisis can have a direct link to a loss of shareholder value. A 2018 study conducted by Pentland Analytics and Aon found that a company’s preparedness to mitigate reputational risk and its management’s behaviour in the immediate aftermath of a crisis can either add 20% or lose up to 30% of its share price value.[15] The below chart, taken from this report, highlights the impact of cyber-attacks on shareholder value.

Figure 3. The impact of cyber-attacks on shareholder value post-event



Source: ‘When Crisis and Technology Collide: Protecting reputation in the digital age’, Pentland Analytics & Aon, 2018

[12] Maersk Annual Report, 2017

[13] Operational and Market Update, First Quarter 2019, 2019

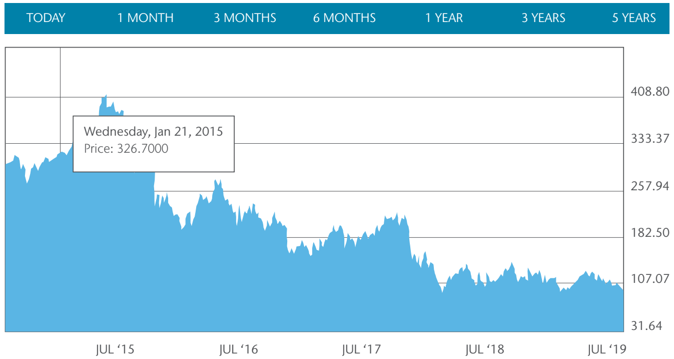
[14] ENISA Threat Landscape Report 2018, 2019

[15] ‘When Crisis and Technology Collide: Protecting reputation in the digital age’, Pentland Analytics & Aon, 2018

The high-profile TalkTalk data breach in 2015 caused huge reputational issues for the firm: not only had the personal details of 156,959 customers been compromised, but the attack also cut trading revenue by over $20 million and led to the loss of 101,000 customers.[16] By the end of the first year following the attack, one-third of the company's market value – about $1.4 billion – had been wiped out.[17] Four years later, the stock market valuation is still well below the level of the 2015 data breach.

Reputational damage that affects customer trust can lead to other problems down the line – such as limiting companies' digital transformation efforts.

Figure 4. TalkTalk share price tumbles post-attack



Source: London Stock Exchange

> **"If we create a problem of trust in this digital space, it will hurt our potential markets. Further to that, customers will not embrace our digital transformation at large."**

Christophe Blassiau
Senior Vice President, Digital Security
& Global CISO Schneider Electric (France)

Credit risk: The unforeseen consequence

There is another significant financial penalty that companies might not see coming: a credit-rating downgrade.

The 2017 Equifax data breach caused significant financial losses for the company following the exposure of at least 147.9 million pieces of personal data. The firm stated in its Q1 2019 earnings release that, since the announcement of the cybersecurity incident in September 2017, they have incurred a total of $1.4 billion in costs related to the incident, incremental technology and data security costs, and an accrual for losses associated with legal proceedings and investigations.[18] Under a settlement filed in July, Equifax agreed to spend up to $425 million to help those affected by the breach.[19]

But the breach was also ground-breaking for another reason: it was the first time an organisation's credit-rating outlook was affected by a cyber-attack. In May 2019, Moody's revised its outlook for Equifax from 'stable' to 'negative'.

The downgrade holds long-term implications for Equifax: future loss of investment, loss of share price value and an increased cost of credit – all of which could add up to more than the cost of the breach itself. "Moody's decision definitely opened up a few eyes, both from a director and a C-suite perspective," says David Molony, Director of Cyber Risk, Cyber Solutions EMEA at Aon. "This was an unforeseen consequence of a major loss, and it really hit home."

Equifax's downgrade was the first, but it will not be the last. Moody's is in the process of integrating cyber risk assessment into its credit ratings process, so businesses will have to be ready for more and more scrutiny of their cyber assessment practices – and be ready for any breach to affect their credit rating.[20]

[16, 17] 'When Crisis and Technology Collide: Protecting reputation in the digital age', Pentland Analytics & Aon, 2018
[18] Equifax Releases First Quarter Results, Equifax Inc, 2019
[19] Equifax Data Breach Settlement: What You Should Know, Alvaro Puig, 2019
[20] Moody's Credit Ratings, Equifax Inc, 2019

Towards cyber resilience

Counting the cost of a cyber-attack is not straightforward. Firms have to understand not only the initial effects of an attack – lost data, crisis expenses and regulatory fines – but also the cost of business interruption and the knock-on consequences of reputational damage. An attack can have financial ramifications for years after the event, and some firms may never recover.

When responding to the threat, there is no one-size-fits-all approach or quick-fix solution. The C-suite must prepare in advance by building resilience from within. In Chapter 2, we explore the steps needed to build cyber resilience.

Chapter 2

Building cyber resilience in an interconnected world

Building resilience within an organisation is crucial to heading off the cyber threat – but it is a more complex task than ever.

The increasing use of smart devices, the Internet of Things (IoT) and Artificial Intelligence (AI) technology means that the 'attack surface' for cyber-criminals is constantly expanding.

> "Connectivity is like oxygen now. People can't live without it, so the cyber threat is growing."
>
> **Mal Smyth**
> Global Head of Risk Governance, Risk & Control
> Vodafone

The number of IoT devices installed worldwide is expected to exceed 75 billion by 2025.[21] The integration of this technology into existing legacy systems can expose vulnerabilities within an organisation's security framework. "All this new technology entering the ecosystem can pose risk," says Rosa Kariger, CISO at Iberdrola. "This risk holds the potential to affect the entire security ecosystem." she adds.

Against this intricate backdrop, organisations need to rethink what 'cyber resilience' means, and how they can give themselves the best chance of fending off an attack – or effectively dealing with the fallout if an attack succeeds.

[21] 'Internet of Thing (IoT) Connected Devices Installed from 2015 to 2025 (billions), Statista 2019

Four steps to cyber resilience

1. Take it from the top

Cyber risk management has to be an enterprise-wide effort, but clear accountability at the top of the organisation is also crucial. Boards need to understand the costs and consequences of a cyber-attack on their global organisation.

Yet, for many organisations, this knowledge is not easily attainable. **"It is still surprising that some companies don't fully understand the impact of various different cyber-attacks on their business,"** says Aon's Janssen. **"There needs to be a deeper understanding of what the worst-case scenarios could be in terms of the financial impact on the business. This insight is crucial in order to develop an effective cyber resilience strategy,"** he adds.

"Ultimate responsibility for all risk management efforts resides in the boardroom," says Pentland Analytics' Deborah Pretty. "That's where the buck stops."

"We work a lot with partners to support businesses reacting to an attack, whether it is the first hour, the first day or the first week," says Simpson-Pirie. "And to do that effectively, we need to prepare the board and the C-suite, in advance, to be able to react in the right way to protect their business."

Wolters Kluwer's Elizabeth Queen agrees that educating the C-suite is vital: "The board needs accessible cyber expertise to help them set the tone at the top and make informed decisions," she says. "Moreover, involving them in Incident Management training empowers them to prepare for events and to trust their teams to well manage them."

2. Unite your business

A cyber-attack has implications for the whole business, so it can no longer be viewed as just an IT issue. It calls for a multi-discipline, multi-level response that involves every relevant stakeholder within the business. "We really need to undo the misconception that cyber is just an IT risk", says Kariger. "It's a business risk. And businesses need to understand that they own and are accountable for this risk."

"Some organisations are still stuck believing that, if the IT security team does its job properly, they won't be the victim of an attack," says Spencer Lynch, Managing Director Cyber Security, Cyber Solutions EMEA, at Aon. "That's ultimately a very foolish approach."

Instead, they need to shift their mindset from viewing cyber-incidents as an IT risk to seeing them as a business risk, where the business defines the risk appetite. If the worst does happen, getting the right people – Risk, IT, board members, Legal, Compliance and HR – around the table for strategic risk discussions will ensure a robust and integrated response.

"A cyber-resilient organisation has adopted not just the technical skills, but also organisational cohesion in order to prevent and manage a cyber-attack," says Paolo Borghesi, Group Chief Information Security Officer at Nexi. "It is important that people at all levels, from the board down, are aware of the impact their behaviour can have from a cyber security perspective." he adds.

One key feature of a cyber-resilient organisation is clear dialogue between the Risk and Security functions. "These two functions should be indelibly linked." says Aon's David Molony.

As the two functions do not work with one another on a day-to-day basis, they will need to work on building a natural dialogue. This is crucial if they are to have any hope of putting together a risk transfer initiative or an insurance policy, for example, that is both appropriate and proportionate.

3. Get ahead of the game

"You don't want to put a team together on the day of the match," says Janssen. "Preparing for an incident is an extremely important part, and it should be a multi-discipline and multi-level focus to make enterprises ready for handling cyber-incidents." he adds.

Incident-response training is critical in preparing organisations for a cyber-attack. Scenario-planning helps them to understand their operational vulnerabilities and the threats they are exposed to.

Once it has made an honest assessment, an enterprise can make contingency plans. And once the cyber response plan is in place, it has to be tested. Having executive teams and boards practise simulations of potential cyber-attacks equips them to respond quickly when the real thing happens. The goal of the simulation is to test for flaws in the response plan and improve response capabilities. When leaders fully understand the risks, they can contemplate them on an enterprise basis, including how insurance plays a part.

"If you want to have a sustainable, long-term insurance programme to address cyber risks across the organisation, you have to make sure that you have your enterprise-wide cyber resilience in check."

Onno Janssen
Chief Executive Officer of Risk Consulting & Cyber Solutions, Aon

Leveling the playing field: Lessons from the US

US organisations have traditionally been more advanced than their European counterparts when it comes to their cyber security strategies.[22] This is especially true of cyber insurance, which has long been more of a purchaser's environment in the US. The cyber insurance market emerged in the US in the late 1990s. In Europe, however, the cyber insurance market is still in its infancy.

Yet, following large business interruption losses resulting from the high-profile ransomware attacks that took place in 2017, along with the introduction of GDPR regulation in 2018, European firms are increasingly turning to cyber insurance solutions. Yet cyber insurance market penetration levels are still relatively low: only 30% of EMEA companies surveyed in the 2019 Aon Ponemon Global Cyber Risk Transfer Comparison Report purchase cyber insurance.[23]

Change on the horizon

Yet this looks set to change in the near future: insurance and reinsurance marketplace Lloyd's of London is set to mandate that all policies clearly state whether they will provide affirmative coverage for cyber risks. From 1 January 2020, Lloyd's underwriters will be required to clarify whether first-party property damage policies affirm or exclude cyber cover.[24]

"In Europe, financial institutions were quick to buy cyber insurance in the lead up to the GDPR regulation coming into effect," says Vanessa Leemans. "Now, we are beginning to see buyers from other industries, such as manufacturing, critical infrastructure, pharmaceutical and life sciences." she adds.

Alexander Mahnke, CEO of Insurance at Siemens Financial Services, explains why it is important for insurers to learn by looking beyond borders: "Whenever you go into a new area of insurance, the first thing you have to understand is there will probably not be a very long loss history that you can actuarially understand and underwrite. If you can and are willing to look into losses and loss history in other markets, such as the US, then you're well advised to do so."

[22] Cybersecurity Policy Making at a Turning Point, 2019
[23] Aon Ponemon Global Cyber Risk Transfer Comparison Report: EMEA, 2019
[24] Lloyd's Market Bulletin Ref. Y5258, Providing clarity for Lloyd's customers on coverage for cyber exposures, 4 July 2019

4. Protect your balance sheet

A cyber-incident, regardless of its form or whether it makes headline news, holds the potential to seriously dent an organisation's balance sheet. The recent introduction of GDPR fines for non-compliance – which carry a maximum penalty of €20 million or 4% of an organisation's annual global turnover, whichever is higher – has created a sense of urgency among European firms to put appropriate cyber controls in place.[25]

While cyber insurance may protect an organisation's balance sheet, by providing a financial pay-out after things have gone wrong, it may also offer expert consultancy to improve security and on-the-ground incident response support during the period of crisis.

Standalone cyber insurance typically provides coverage for legal costs and damages from claims alleging a privacy breach or network security failure, but also for the potentially costly business interruption losses and increased working costs following a cyber-incident. A key benefit of cyber insurance is pre-loss prevention and post-loss services, which help organisations to recover more quickly post-attack.

> **"We bought cyber insurance coverage to protect against a worst-case scenario. For us, the major benefit of insurance coverage is immediate, in the form of notification and forensic costs. Yet we also have coverage for business interruption, in the case of lost profits post-attack."**

Alessia Carnevale
Head of Risk Management, Nexi

> **"Cyber insurance is not only about risk transfer."**

Alexander Mahnke
CEO of Insurance, Siemens Financial Services

"It's also about risk management, and I think this is important to understand: No matter if you want to take out insurance or not, you will need to look into this area as part of your overall business risk." he adds.

The standalone cyber insurance market is evolving in terms of both its capacity to underwrite cyber risk and the scope of its coverage.

> **"With around $1 billion in capacity available in the standalone cyber insurance marketplace, the purchase of buying cyber programmes for large corporates is more relevant now than ever before. Whist the available limits still lag behind those in other markets, like property, risk managers are now far more able to see the value of cyber insurance for balance sheet protection."**

Vanessa Leemans
Chief Commercial Officer of Cyber Solutions EMEA, Aon

[25] Is Cyber Risk A D&O Risk? 2019

New thinking

The C-suite should not be tempted to think it has produced a cyber-resilient organisation simply by investing in expensive security software. True resilience goes far beyond cyber defence.

It should be driven by a clear chain of command, originating at board level, and involving extensive preparation – including incident response training – by the entire organisation.

Building resilience in the M&A process: The importance of due diligence

The M&A process can expose cracks in an organisation's resilience, so sophisticated cyber due diligence during the M&A process is essential. Instances where companies have acquired a target firm, unaware that it had previously suffered a cyber-attack, demonstrate the dangers.

In the case of Marriott's acquisition of Starwood Hotels, unauthorised access to Starwood's room-reservation network started in 2014 – a year before Marriott announced the acquisition. Marriot incurred $28 million of expenses in the fourth quarter of 2018 and recognised $25 million of insurance proceeds; $44 million of expenses in the first quarter of 2019 and recognised $46 million of insurance recoveries; and $22 million of expenses in the second quarter of 2019 and recognised $22 million of insurance recoveries related to the data security incident it disclosed on 30 November 2018.[26]

In 2017, Verizon's acquisition of Yahoo! was affected by a data breach in which 1 billion user accounts were exposed. Fortunately for Verizon, the breach was revealed prior to the acquisition, which allowed it to reflect potential breach liabilities in the purchase price – a downwards revision of $350m, or 7% of the acquisition price.[27]

> **"Cyber due diligence helps you understand exactly what your tech footprint is, and what exactly your digital surface area is to external audiences. It helps to see if someone left the equivalent of a digital back door open."**
>
> **Charlie Cannell**
> Digital Director, Inflexion

For more insight into assessing cyber-risk in pre-transaction due diligence, see Aon's C-suite series M&A report, *Leaving Nothing On The Table: Unlocking Off-Radar Transaction Value.*

[26] InfoSec 2018. TalkTalk hack – lessons learned - the board perspective
[27] Marriott International Reports Fourth Quarter 2018 Results, 2019

Chapter 3

Picking up the pieces: When a cyber-attack hits

No organisation can ever be truly ready for a cyber-attack, but preparation for the immediate aftermath can make a big difference to the long-term outcome.

In the event of a cyber-attack, a coherent response strategy can mean the difference between an organisation holding its nerve or going into complete meltdown.

“Unprepared organisations usually don’t even know how to communicate that an attack has occurred, and do not respond effectively on the day they learn of an attack,” says Aon’s Spencer Lynch.

> **“They are completely in the dark, with no supplies. Prepared organisations, on the other hand, can immediately kick-start an effective response plan; they’ve packed their emergency kits, and they know how to use them.”**
>
> **Spencer Lynch**
> Managing Director of Cyber Solutions, Aon

Figure 5. Winners and losers: How to deal with a cyber-attack

	THE WINNERS	THE LOSERS
1. PREPAREDNESS	Deep commitment to loss prevention and mitigation	Failure to prioritise risk preparedness
2. LEADERSHIP	Strong, visible leadership from CEO	Weak or delegated leadership, failure to take responsibility
3. COMMUNICATION	Accurate and well-coordinated communication	Opaque, partial or inconsistent communication
4. ACTION	Instant, global response and action	Delayed, absent or limited action
5. CHANGE	True remorse: commitment to meaningful change	Minimal, inauthentic, reluctant contrition (if at all)

Source: ‘When Crisis and Technology Collide: Protecting Reputation in the Digital Age’
Pentland Analytics & Aon, 2018

A view from the inside

In 2017, DLA Piper was one of the many businesses that fell victim to the NotPetya ransomware attack. Andrew Darwin, the firm's global co-chairman and senior partner, describes his experience leading the organisation through the crisis response.

"When a cyber-attack hits, you're potentially faced with an existential crisis that you've never faced before. You cannot underestimate the human response to such an incident, a situation that changes constantly requires a great degree of flexibility in your crisis-response plans. The board and executive committee are on such high alert, that it's difficult to stay within a rigid structure."

In the dark

"Despite having reasonably well-developed incident response and crisis management plans, the threat we faced was at times overwhelming. For a short period, we had no email, no telephony, no finance systems, no HR systems. We were literally relying on mobile phones, but with no mobile email."

"We did of course run many simulations before the incident and I would recommend that every organisation does so. But it's important to understand that human reaction will inevitably be very different in those circumstances, and an organisation needs to allow for that the best they can."

"One thing we learned is that you need cyber response advisors who actually live with you on an ongoing basis – not just on the day of the crisis and, even better, who get to know your business and leadership prior to an incident. These advisors can give your response a rhythm and a structure, which is very hard to do when you are in a crisis situation. They also provide independence, which is important for your stakeholders and a source of 'verification' for the people helping manage the response."

It will happen to you

"Our business now is much more resilient and stronger as a result of the cyber-attack, but we learned some huge lessons in a very painful way. My advice to firms looking to improve their cyber risk management strategies would be: don't underestimate the impact on your business. It will happen to everyone to a degree, so don't disregard this as something that happens to other people."

"Every board, every business has to proceed on the basis of, 'It will happen to us.'"

Andrew Darwin
General Counsel for Europe, AEW

When a cyber-attack hits, you're potentially faced with an existential crisis.

A tale of **two cyber-incident responses**

To the right are two examples of responses to a cyber-incident. The responses of the organisations were starkly different because of their different levels of preparedness.

Each incident caused the organisation huge financial losses, but Norsk Hydro's response enabled it to limit the financial damage.

The stark contrast between these two companies' experiences highlight the importance of having a robust response plan in place before a cyber-attack hits. Preparation is everything, and businesses cannot afford to be left in the dark.

TalkTalk's Director of Corporate Affairs and Regulation, Jessica Lennard, outlined the lessons the organisation had learned shortly after the attack: "One of the key learnings for us has been that cyber security is really a business issue, not a technology issue. As a complex, technical area, it's more likely to be dealt with in a silo by tech or IT departments, than properly understood and mitigated across the whole company. We've made a comprehensive effort since last year to truly embed security in everything we do."[30]

TalkTalk

A fractured and incoherent response following the cyber-attack in October 2015

- Closed down its website and froze social-media activity.
- Displayed a lack of knowledge of the scale of the attack (it was later found to be smaller than TalkTalk had anticipated).
- Attitudes towards how to respond differed across the organisation.
- The board did not have an adequate understanding of the technology.[28]

Norsk Hydro

Clear and open communication as part of an effective response plan following the cyber-attack in March 2019

- Used daily webcasts and social media posts to keep business partners and the media informed.
- Made it clear that it would not pay the ransomware attackers that had attacked its systems.
- Called in the police to investigate.
- Brought in experts to help.[29]

[28] InfoSec 2018. TalkTalk hack – Lessons Learned - The Board Perspective, Tony Morbin, 2019

[29] Experts Praise Norsk Hydro Cyberattack Response, Michael Heller, 2019

[30] Fraud and Risk Focus Blog, Jessica Lennard, 2016

Chapter 4

Cyber security: An ongoing journey

The C-suite must embark on a journey of constant improvement in order to stay one step ahead of the evolving cyber threat.

The cyber threat is amorphous, and the technology it exploits is advancing at a dizzying pace, so the risk landscape is never going to stand still. Leaders might think they have grasped the threats to their firms, only to feel that certainty slip away as the next attack reveals new vulnerabilities.

Organisations cannot afford to be caught out, and the C-suite will have to aim to constantly improve its cyber risk-management strategies to keep up. “A cyber-resilient organisation is one that is trained in the same way that people go to the gym every day,” says Gorka de Orbe, CISO at Bankia. “The organisation needs to train every day to achieve this goal.”

Emerging technologies create new entry points for cyber-attackers, but they can also offer a lifeline. In looking to find ways to improve visibility of new threats within their organisations, the C-suite will have to harness sophisticated new tools and the expert talent that can exploit them.

The data revolution

The C-suite is well aware of the cyber threat, but many leaders are not able to quantify its potential impact on their businesses. Data can help here: leaders can use historical data to predict imminent attacks.

Using big data analytics, businesses can develop baselines that show up the differences between normal and suspicious activity. “We have to start looking to outpace the attacker.” says Vodafone’s Mal Smyth.

> **“Cyber attackers are using data analytics as well, and vulnerabilities are becoming weaponised.”**

In this pressurised environment, drawing meaningful insights from data becomes even more important: “It’s all about making sure that data is recognised and understood within your own context and making sure that it is used in the correct manner,” says Aon’s David Molony. “That’s where we’ll start to see the real revolution.”

Smart risk management

Some organisations have gone one step further, working with data analytics tools and technologies that use machine learning and AI-type algorithms to assess the baseline of activity in their networks and systems. This opens up a new realm of possibilities for cyber risk management.

Automated solutions such as Edgescan both identify and risk-rank known and unknown vulnerabilities in real time. By using machine-learning techniques instead of traditional approaches, it can analyse and classify hundreds of thousands of characteristics per file to identify suspicious activity.[31]

> **“Through applying AI technology to detect suspicious behaviours, for both cyber and fraud-related threats, we have decreased at least 90% of the false positives that we had in the past.”**

Gorka Diaz de Orbe
CISO, Bankia

In 2018, 93% of malware observed by security firm Webroot was polymorphic – it could constantly change its code to evade detection.[32] “Machine learning helps us understand the constantly shifting nature of the cyber threat,” explains Lloyds Development Capital’s Andy Simpson-Pirie. “You don’t necessarily have to follow prescribed signatures or processes. An attack could just behave in a certain way. And those ways can change, as humans do. Machine learning capability supports the business taking that evolution into account.”

“There are approximately 365,000 pieces of new malware emerging every day, and there is no way to keep up in the long run. The only step companies can take to combat this is to use AI to understand what exactly a virus looks like”, says HP’s Rhodes. “Cyber-attackers are increasingly using AI technology as a tool, so you have to fight fire with fire” he adds.

Getting the right expertise on board

Technology underpins all aspects of business, so organisations are prioritising technological expertise in their hiring processes. The appointments of a Chief Technology Officer, Chief Information Security Officer or Chief Information Officer are attracting growing interest from business stakeholders and the media, and their presence on executive boards is becoming more commonplace.

> **“The CISO role is becoming much more of an enabler for the business in general.”**

Patrik Bless
CISO, Partners Group

“The focus is shifting from a purely compliance-driven approach, which is obviously still a necessity, to a strategic and risk-focused role. It’s important for the CISO to be involved in business decisions early on and to be involved in strategic initiatives. Becoming involved at a later stage can be very detrimental in terms of risk exposure, timeline, and also cost.”

Beyond the hiring and elevation of cyber security expertise, it is crucial to educate ‘non-technical’ leaders within the business. In this way, cyber security can be embedded in the fabric of the organisation – and plausible deniability is no longer an excuse. In order to achieve cyber resilience, different functions across the business must unite. “The risk function needs to be a strong communicator. It is important to build an open culture of information sharing,” says Bless. “It’s very important that executives feel empowered to speak up and ask questions.” he adds.

The introduction of GDPR regulation has had an important effect on improving C-suite awareness on cyber issues, says Inflexion’s Charlie Cannell. “GDPR has made a lot of companies really understand their systems, their processes, their storage and improve their internal understanding of the impact of the cyber threat,” he says. “I think that, as a particular process, has really allowed the acceleration of knowledge at the C-suite level in the past three years.”

[31] ‘Edgescan FullStack Vulnerability Management’, 2019
[32] ‘2019 Webroot Threat Report’, Webroot, 2019

A journey of constant improvement

In order to achieve cyber resilience, the C-suite must constantly look to improve its cyber risk-management strategy and processes.

Beyond developing an understanding of the cyber risks, businesses must now go further – by drawing actionable insights from data. Getting the right technological skills on the board is central to gaining a greater understanding of the threat. Educating non-technical leaders in cyber issues will ensure accountability across the organisation.

Prepare for the expected: Steps to cyber resilience

1. Take it from the top

The C-suite must understand and take accountability for what is happening within its business. Plausible deniability is no longer an excuse – directors can be sued if they fail to take effective preventative measures.

2. Unite your business

Cyber risk is not just an IT security issue, it is a threat to the whole enterprise. It calls for a multi-discipline, multi-level response that involves every relevant stakeholder within the business. The C-suite has a responsibility to unite its business against the cyber risk.

3. Get ahead of the game

The C-suite should work on prevention rather than cure – it can no longer rely on bringing in its response team after an attack. Incident-response training is critical in preparing organisations for a cyber-attack. Scenario-planning helps them to understand their operational vulnerabilities and the threats they are exposed to.

4. Protect your balance sheet

A cyber-incident holds the potential to seriously damage an organisation’s balance sheet. Cyber insurance can protect an organisation’s balance sheet by providing a financial pay-out after things have gone wrong. A key benefit of cyber insurance is pre-loss prevention and post-loss services, which help organisations to recover more quickly post-attack.

Contacts

Onno Janssen
Chief Executive Officer
Risk Consulting and
Cyber Solutions EMEA
Aon
+49 (0)40 3605 3608
onno.janssen@aon.com

Vanessa Leemans
Chief Commercial Officer
Cyber Solutions EMEA
Aon
+44 (0)20 7086 4465
vanessa.leemans@aon.co.uk

Spencer Lynch
Managing Director, Cyber Security
Cyber Solutions EMEA
Aon
+44 (0)20 7061 2304
spencer.lynch@aon.co.uk

David Molony
Director, Cyber Risk
Cyber Solutions EMEA
Aon
+44 (0)7775 227 008
david.molony@aon.co.uk

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

For further information on our capabilities and to learn how we empower results for clients, please visit: aon.mediaroon.com

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information and use sources we consider reliable, 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.

The information contained in this document should not be considered or construed as legal or tax advice and is for general guidance only. Accordingly, the information contained herein is provided with the understanding that Aon, its employees and related entities are not engaged in rendering legal or tax advice. As such, this should not be used as a substitute for consultation with legal and tax counsel.

All descriptions, summaries or highlights of coverage are for general informational purposes only and do not amend, alter or modify the actual terms or conditions of any insurance policy. Coverage is governed only by the terms and conditions of the relevant policy.

This research was conducted by Longitude a Financial Times group company and part of FT Marketing Services, the FT's commercial thought leadership offering.

Aon UK Limited is authorised and regulated by the Financial Conduct Authority.

aon.mediaroom.com

Aon
Empower Results®