How luxury brands can mitigate the impact of cyber risks

February 2023

Introduction

Cyber-attacks present an ongoing threat as malware becomes more sophisticated and easier to access. With remote working and increasingly complex supply chains, criminals are finding more routes to infect and disable IT systems.

Luxury brands can be seen as a prime target for cyber criminals because of the sensitivity of their customer and corporate data – and the risk to their reputation if such data were to be compromised.

In this webinar, we looked at the changing cyber risk landscape, how it is affecting the luxury brands sector and what brands can do to protect themselves.

Read on to find out more about:

- Why cyber-attacks are on the rise
- The specific threats facing luxury brands
- The impacts and costs of cyber-attacks
- How luxury brands can reduce their cyber risks
- Best practice in cyber security
- How cyber insurance works
- What luxury brands need to consider when buying cover

Speakers

Andrew Hill
Global Head of Cyber Coverage and Innovation
WTW

Olivia Lovitt
Transportation and Retailer Lead
WTW

How are luxury brands at risk from cyber threats?

Luxury brands invariably collect large amounts of personal data as part of providing a tailored experience for customers. In view of the industry sector, it can be expected that a significant quantity of this information belongs to high net worth individuals (HNWIs) who may be sensitive about who has access to their data. For this reason, such data holds a particular appeal for criminals.

Unsurprisingly, luxury brands are keen to avoid the reputational damage associated with a data breach. This makes the sector a particularly attractive target for ransomware attacks, because criminals believe brands are more likely to pay ransoms rather than risk damaging their existing and future customer relationships should the data be released into the public domain. The consequences of such attacks can be far-reaching.

Disruption to production and distribution

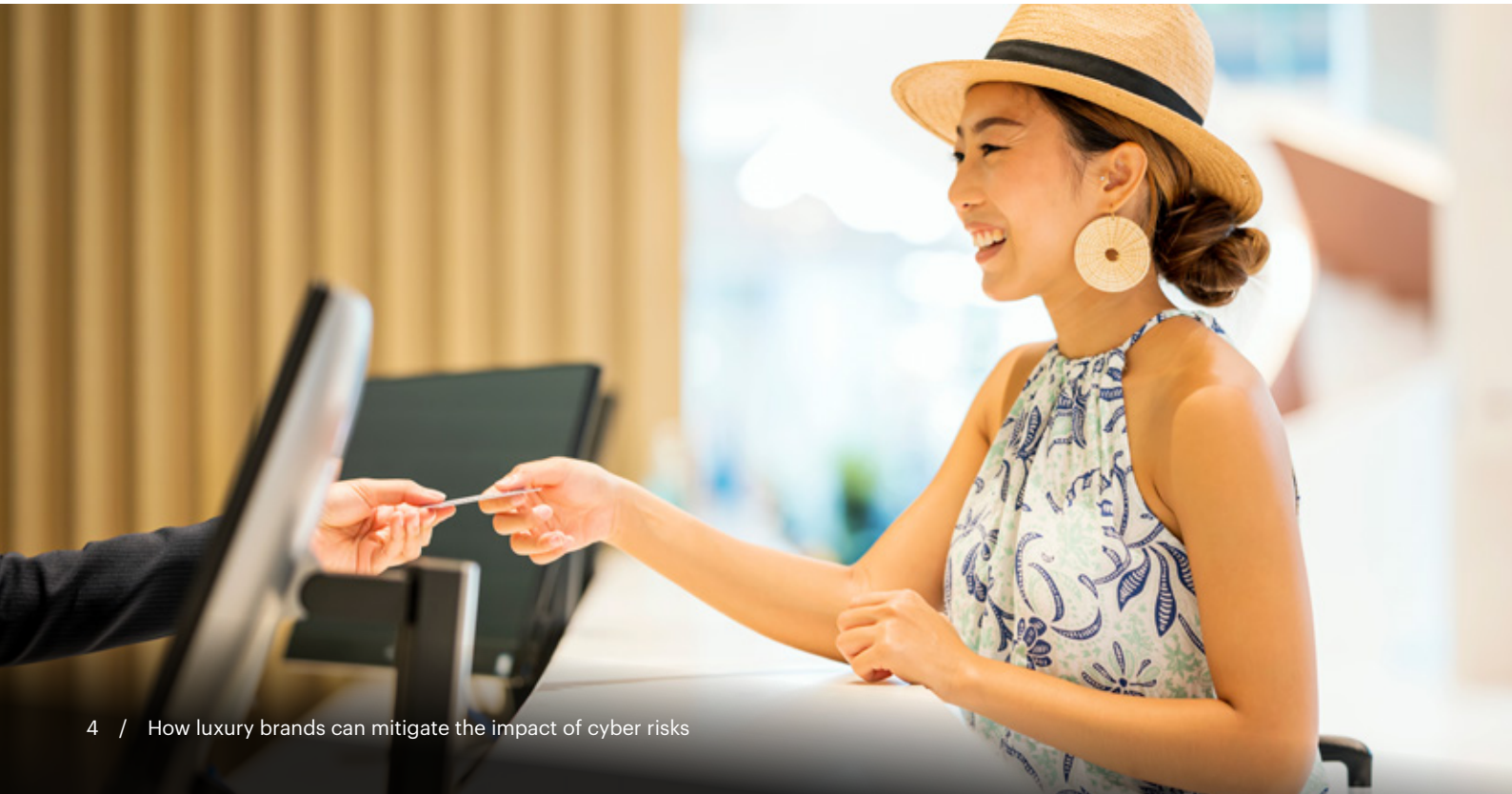
Many luxury brands are manufacturers and logistics operators as well as retailers, which presents its own challenges from a cyber threat perspective. Specifically, if a cyber-attack corrupts their information technology (IT) and/or operational technology (OT), this could lead to lost productivity at the factories, with knock-on disruption to logistics and failure to meet customer orders. These impacts could lead to significant business interruption costs.

Data privacy breaches, fines and prosecutions

The collection and/or processing of personal data potentially exposes organizations to a raft of regulatory regimes, such as GDPR in Europe. Such legislation can place more obligations on businesses to protect the personal data of customers and employees. Breaching those obligations may result in fines as well as legal costs and potentially further reputational damage.

Supply chain cyber risks

Luxury brands are also exposed to cyber risks through their supply chain in two distinct ways. First, a partner who is relied upon for the production or distribution of goods will have their own cyber risk to contend with. Any interruption to their IT/OT could have adverse consequences for the brand. Second, is the risk associated with connectivity of networks. For example, even if the brand's internal IT controls are robust, malware can migrate through systems that are linked or shared with a supplier if the supplier's controls are exploited.



Some of the cases involving luxury brands that have made headlines recently:

Parent Company of Fast-fashion Brand Shein to Pay New York State USD1.9 million for Data Breach.

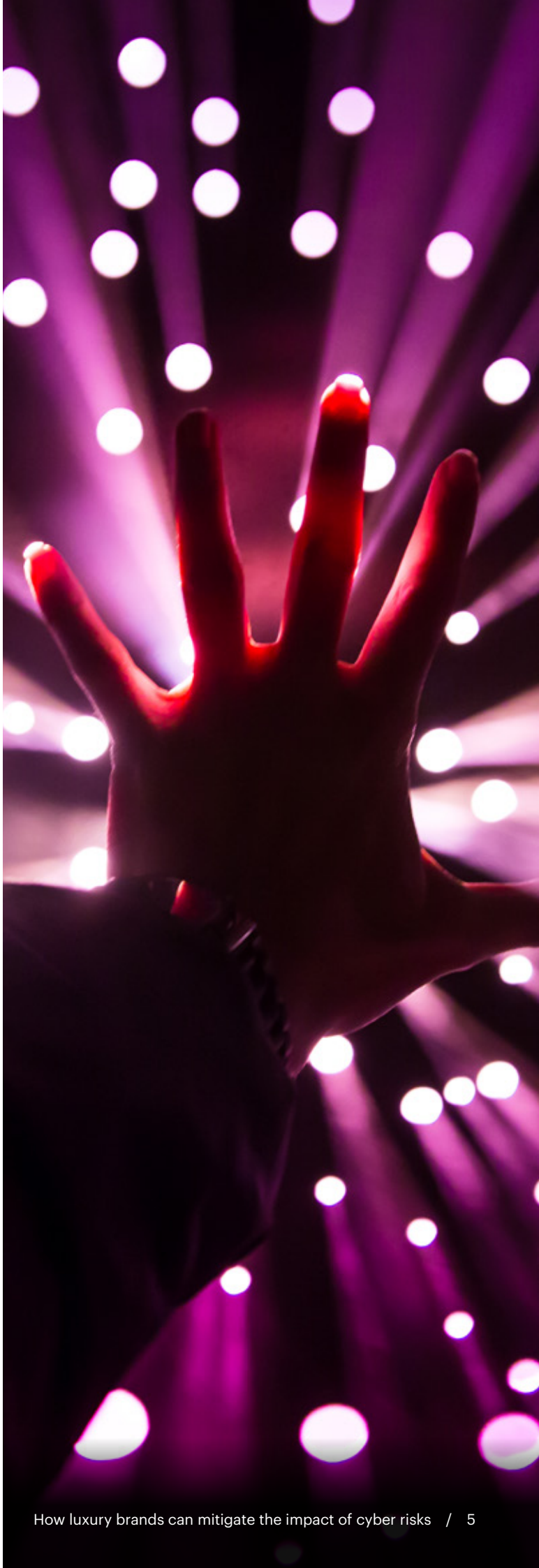
Personal information of millions of Shein customers was stolen in 2018 data breach.

Top French Luxury Brands Face Targeted Cyber Threats, Counterfeits.[1]

Italian Fashion Giant Moncler Confirms Data Breach After Ransomware Attack.

Zenga Luxury Fashion House Confirms Ransomware Attack.

[1]https://wwd.com/business-news/business-features/french-luxury-brands-targeted-cyber-threats-counterfeits-1235385037/



Why are ransomware attacks on the rise?

There are several possible factors behind the increase in ransomware attacks around the world:

- **Changes in working habits:** with more people working remotely and using personal devices for work, criminals may see an opportunity to exploit human vulnerabilities and weak links in systems.
- **Low risk of prosecution:** cyber criminals may feel they can get away with it. They often operate from jurisdictions where, even if identified, they cannot be prosecuted by law enforcement agencies from the targeted countries.
- **Easy to launch:** malware is becoming easier to develop and more accessible. Criminals can find ready-made malware on the dark web.

How are the authorities responding?

Governments are paying more attention to cyber security as it becomes a greater threat to critical infrastructure and how economies do business. While the governments in countries most exposed to cyber-attacks are encouraging businesses to take the appropriate steps to protect themselves (given the importance of critical infrastructure to the functioning of a state), legislation is being introduced (e.g. Network and Information Systems Directive in the EU) which sets standards for cyber security.

USD265 billion

Global ransomware damage costs predicted by 2031[2]

Counting the cost of a ransomware attack

Short-term costs

Getting back up and running as quickly as possible after a ransomware attack is generally the priority, However, in addition to any ransom payment that may be made to achieve that goal, other costs can quickly accrue, such as:

- Business interruption costs if the attack affects the company's ability to generate revenue.
- IT forensic specialists to investigate the attack, the type of malware used, which files and systems have been affected, and to repair any damage.
- Crisis consultancy on how to manage the situation and guidance on ransom payment strategy.
- Legal advice on the data protection obligations and potential liabilities if sensitive personal data or confidential corporate information has been compromised.

Medium to long-term costs

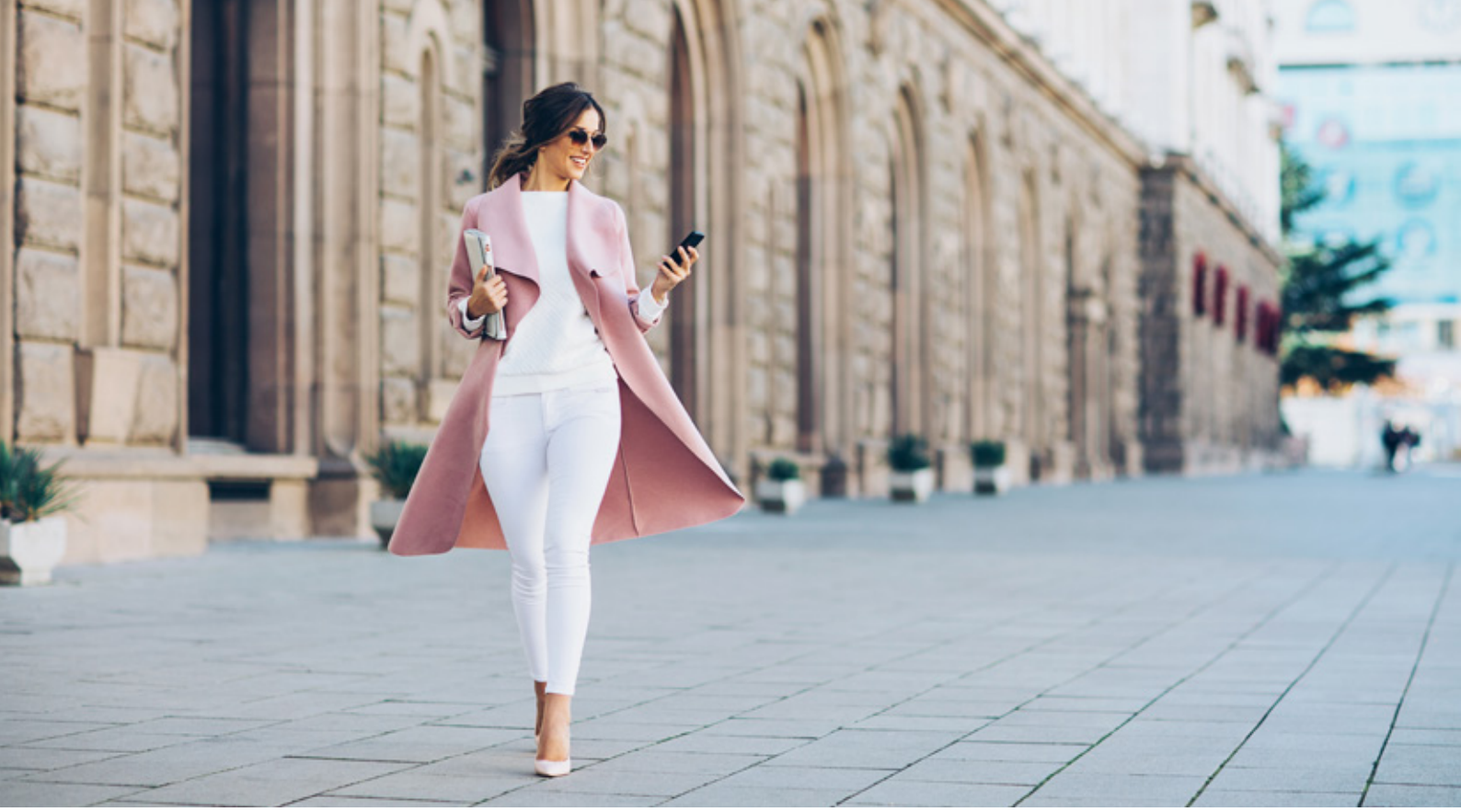
- Legal defence costs and potential fines if there is a regulatory investigation. In many cases, the process of investigation and prosecution may go on for years, taking up business time and incurring significant legal costs even before a fine is issued.
- The costs of any third party liability claims and associated legal defence costs.

What should firms consider before paying a ransom?

Any brand considering paying a ransom may want to consider taking appropriate legal advice before doing so. Examples of issues that will need to be considered include:

- Has an adequate level of due diligence been undertaken in terms of understanding where the ransom money is going?
- Have all applicable laws and sanctions been reviewed?
- It is illegal in many countries to finance terrorism. Check for applicable legislations and make sure the person or group you are paying are not classed as terrorists.

[2]Cyber Crime Magazine https://cybersecurityventures.com/global-ransomware-damage-costs-predicted-to-reach-250-billion-usd-by-2031



How to reduce your cyber risks

Your organization may wish to consider the following four-phase strategy to mitigate cyber risks and minimize the impact of an attack:

1. Identify critical assets

Categorize and document the most important assets in your organization that could be affected by a cyber-attack. This might include:

- Data assets, such as sensitive personal data, confidential business information, customer data records and contracts.
- Software assets, such as manufacturing or warehouse management systems.
- Services, such as internet service providers (ISPs) and utility providers.

2. Assess your controls

Ask what cyber security controls you have in place and whether they are robust enough? Approaches you can consider include:

- A gap analysis of your security controls linked to the cyber risks you face as a business.
- Penetration (PEN) testing, vulnerability scanning or an audit of your controls by an external provider.
- A strategy workshop or cyber risk review involving senior leaders and stakeholders.

3. Develop a cyber-risk management strategy

Once you know your critical assets and the current state of your controls, ask these questions to help make decisions on how to manage risks:

- Can you tolerate the risk? If so, remember that risk does change over time, so monitor it regularly to make sure the level of risk is still acceptable.
- Can you reduce the risk by implementing better procedures or controls?
- Can you remove some risk by outsourcing an activity to an external provider? Remember, you will retain overall responsibility for what they do, so you may still be exposed.
- Can you transfer the risk through cyber insurance?

4. Review, test and manage

Put current controls and procedures to the test and review them to keep pace with latest threats:

- Nominate owners responsible for managing cyber risks.
- Run desktop exercises with key stakeholders, making sure to stress-test incident response and business continuity plans.
- Test the effectiveness of your cyber defences and action any findings.
- Hold regular planned reviews of cyber risks and threats.

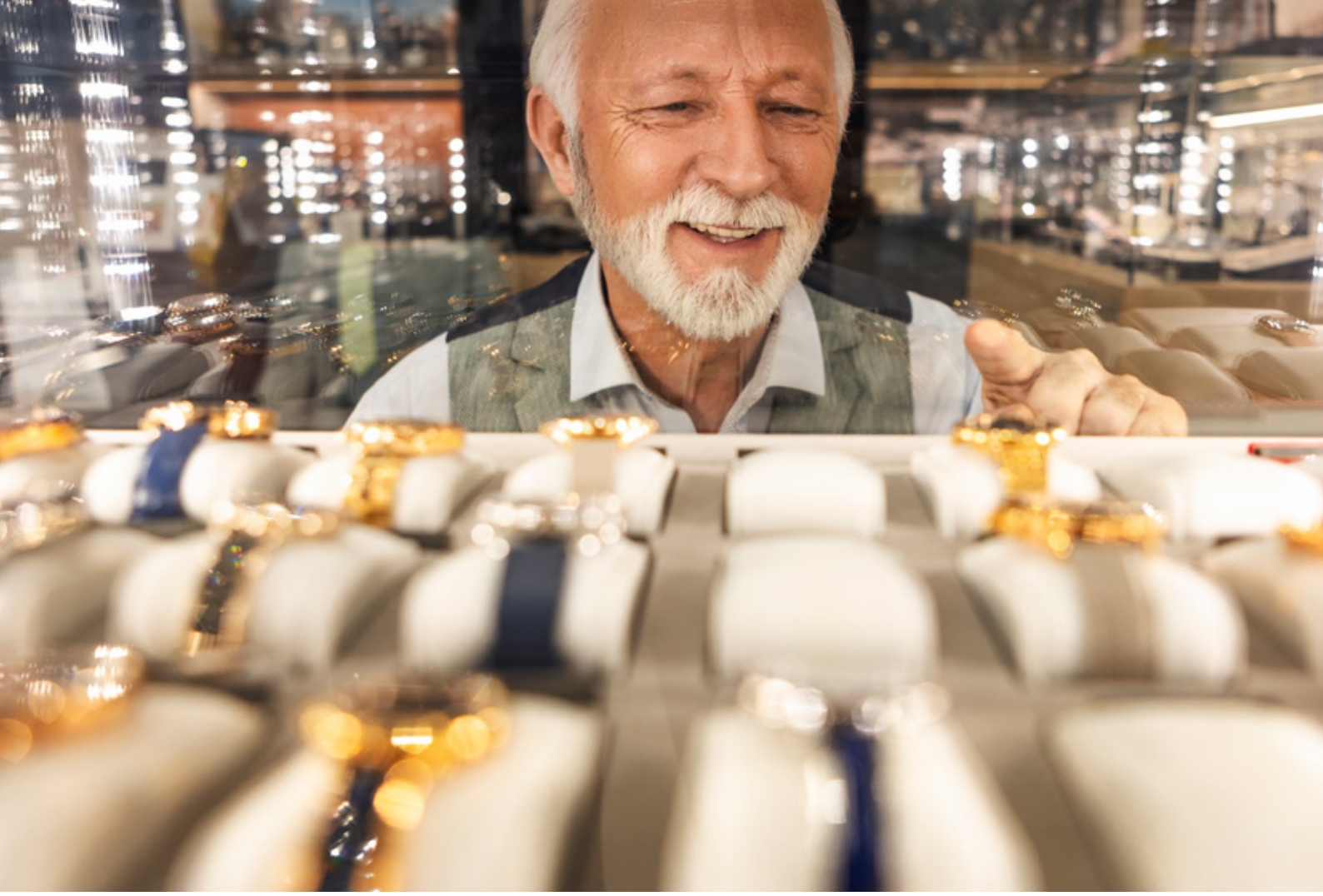
Cyber security controls best practice

Cyber security controls are the first line of defence against cyber threats. At WTW, we are seeing insurers decline cyber insurance business if a company's controls are not deemed sufficiently robust. The list below includes five of the IT controls typically required by insurers before they will issue a policy. This list is not exhaustive and if you would like more information please contact your cyber broker.

1. Do you have multi-factor authentication (MFA) in place across 100% of your network for all remote access and privileged admin access?
2. Do you have a privileged account management (PAM) tool in place to protect all high value accounts?
3. Are you deploying endpoint detection and response solutions fully across all endpoint?
4. Is your storage of back-ups separate from your primary network, for example, within a cloud service or data centre?
5. Do you regularly test the restoration and recovery of key server configurations and data from back-ups?

What if we don't have all of the required controls?

WTW can work with you to assess your existing controls and evaluate whether they meet insurer requirements. Where there are gaps, we can help you understand what steps you need to take to reach insurability. We can also provide context to insurers around your IT activities and progress, helping to reduce the barriers to cover.



How cyber insurance can help

Even with the most robust IT/OT controls, cyber incidents can still happen. Cyber insurance is designed to protect your balance sheets from a number of the most financially damaging impacts following a cyber event.

What does it cover?

Risks and perils

Cyber insurance cover varies from one policy to another. However, in general, cover is provided for the following named perils:

- **Cyber-attacks:** e.g. ransomware, distributed denial of service attacks and other malicious activity targeted against the brand by criminals, rogue states or other bad actors.
- **Human error:** e.g. negligent acts while operating computer systems – for example, an employee clicking on a link in a phishing email or an engineer making a mistake during an IT upgrade.
- **Technical failure:** e.g. technology malfunctions without any malicious activity or obvious error – for example, during an IT migration where a new system has worked well in testing but fails when it goes live owing to unforeseen technical reasons.

Costs and losses

- **Business interruption:** lost profit as a result of a cyber incident, as well as the costs involved in getting the business back up and running.
- **Cyber extortion:** ransom payments and advisor costs.
- **Crisis management:** can include crisis consultancy, legal, forensic and public relations costs.
- **Data restoration:** the cost of restoring data to its pre-incident condition – even if a ransom is paid and files are unlocked, they may be damaged or corrupted.
- **Third party liability:** cover for damages and defence costs if a claim for breach of data privacy or corporate confidentiality is brought against the company.
- **Regulatory actions:** cover for fines (where they are insurable) and defence costs attributable to a regulatory action following a cyber incident e.g. a data breach.

What's happening in the cyber insurance market?

Claims are increasing

WTW has seen a significant increase in the number of cyber insurance claims in the last couple of years, including a rise in claims related to data theft.

Ransom demands are going up

USD10 million is not uncommon as a ransom demand. Criminals see it as quick and easy money.

Premiums have been rising

As the number, scale and cost of cyber-attacks has risen, so has the cost of claims, which has a knock-on impact on prices. Although cyber insurance premiums have risen to keep pace with these changes, there are signs that rates are stabilizing.

Market capacity is increasing

There is evidence that we are emerging from the challenging market place of recent years with insurers of traditional lines expanding into cyber insurance and introducing new capacity. An estimated USD20-35 million of new capacity has entered the market this year. Insurers' line sizes have increased by 25-50% towards a common maximum of USD10 million.

Policy coverage has expanded

Many policies now offer broad cover for a range of first party and third party costs.

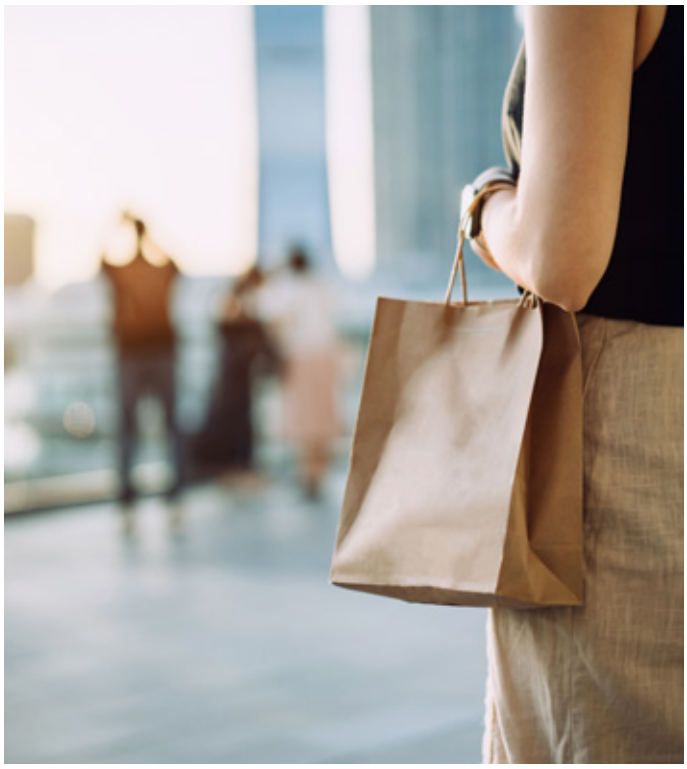
13%

Increase in the average cost of a data breach between 2020 and 2022.[3]

How to get the right cover for your needs

Look for bespoke cover: we advise not to buy off-the-shelf policies, but to explore bespoke cover with insurers. You are likely to have different exposures depending on your industry sector where your risk profile may differ considerably.

Quantify your risks: use analytics to model your risks and probable losses before you enter the market. It will help to inform the coverage and limits you need to buy.



[3]IBM Cost of a data breach report 2022 https://www.ibm.com/uk-en/security/data-breach

How WTW can help

We work with clients to help them understand what their potential losses could look like, what scenarios they should be concerned about, and advise on placement strategy.

Our analytics team offers powerful modeling tools and systems to help businesses assess risks and quantify probable losses.

We run workshops to help clients identify their cyber-risk exposures and bespoke insurance coverage to ensure it is fit for purpose and appropriate for their business.

Contact

For further information please contact:

Asia

Graham M. Edwards
Head of Sales & Client Management, Asia
+65 6958 2925
graham.edwards@wtwco.com

Australia and New Zealand

Anthony Kumar
Lead Associate
+61 478 307 113
anthony.kumar@wtwco.com

France

Frédéric Lucas
Industry Leader
+33 1 41 43 61 07
frederic.lucas@grassavoye.com

Italy

Alessandra Capua
Fine Arts Jewellery & Specie European Leader
+39 06 5409 5262
alessandra.capua@wtwco.com

North America

Jason Krauss
FINEX NA Cyber Thought & Product Coverage Leader
212-915-8374
jason.krauss@wtwco.com

Matthew Danielak
Senior Vice President, FINEX Cyber/E&O, North America
(312) 288-7835
matthew.danielak@wtwco.com

Spain

Juan Carlos Tárraga
Head of Travel & Tourism – WTW España
+34 971 71 83 57
juancarlos.tarraga@wtwco.com

UAE

Debbie Hewitt
Head of General Lines
+ 971 (0)50 513 0590
debbie.hewitt@grassavoye.ae

UK

Andrew Hill
Executive Director, Global Head of Cyber Coverage & Innovation, Cyber & TMT
+44 20 3124 8278
hillanx@wtwco.com

Olivia Lovitt
Transportation and Retailer Lead, Cyber & TMT
+ 44 (0) 207558 9320
olivia.lovitt@wtwco.com

About WTW
At WTW (NASDAQ: WTW), we provide data-driven, insight-led solutions in the areas of people, risk and capital. Leveraging the global view and local expertise of our colleagues serving 140 countries and markets, we help you sharpen your strategy, enhance organizational resilience, motivate your workforce and maximize performance. Working shoulder to shoulder with you, we uncover opportunities for sustainable success — and provide perspective that moves you. Learn more at wtwco.com.

wtwco.com/social-media

WTW-HP-2023-0678

wtwco.com