

DIFFERENTIATING CYBER RISKS: POST COVID-19

Insurance Institute of Leeds, Wednesday 21st April 2021

Cyber
Claire 

AGENDA

1. The Cyber Risk Landscape Post Covid-19
2. Cyber Insurance: How it responds
3. Cyber Insurance: Coverage Considerations



LEARNING OBJECTIVES

1. Provide participants with a more detailed understanding of cyber risk, how this triggers insurance coverage and interacts with other lines of insurance
2. Examine cyber risk in light of the COVID19 global pandemic
3. Support practitioners in having more advanced discussions with clients regarding cyber risk



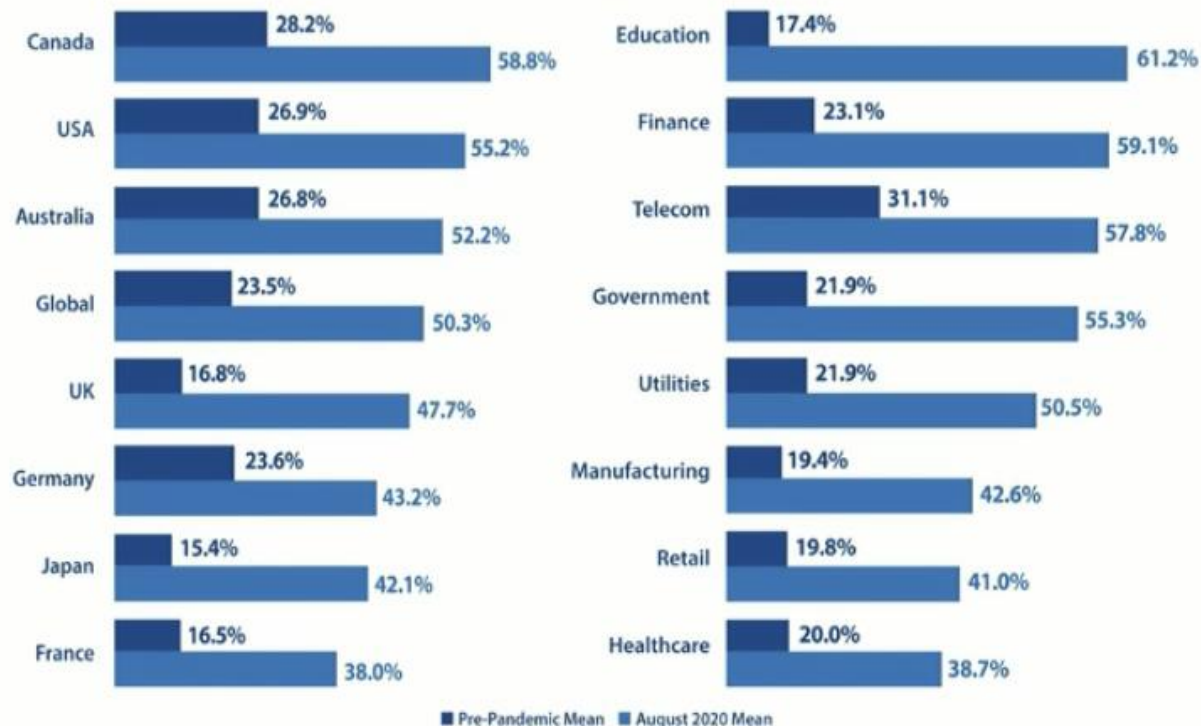
THE CYBER RISK LANDSCAPE POST COVID-19





Despite some workers returning to the office, as of August 2020, the average enterprise remote workforce is 114% larger than before the pandemic.

Percentage of global workforce working from home before and during the pandemic, by country and industry



Source: "The Impact of COVID-19 on Enterprise IT Security Teams," CyberEdge Group, October 2020

POST COVID TRENDS IN CYBER RISK

Increased investment on location-agnostic infrastructure.

Greater focus on endpoint management.

Convergence of security tools.

More consumer and financial data 'floating' online.

An increase in staff turnover

A stabilisation > reduction of cyber insurance purchases.





160+

More than 160 instances of high-risk and critical vulnerabilities shared with NHS Trusts



200+

More than 200 incidents the NCSC responded to this year related to the UK's coronavirus response



230

Victims supported by the NCSC who faced incidents that were related to coronavirus



235

Rolled out Active Cyber Defence (ACD) services, including Web Check, Mail Check and protective DNS, to 235 front-line health bodies across the UK, including NHS Trusts



1.4 million

Performed threat hunting on 1.4 million NHS endpoints to detect suspicious activity



260

Blocked 260 SMS Sender IDs which were likely to or have been used in malicious SMS campaigns with coronavirus as their theme, such as spoofing legitimate government or healthcare IDs



15,000

More than 15,000 coronavirus-related malicious campaigns taken down by the NCSC and its commercial partner, Netcraft

CYBER ATTACKS & CLAIMS IN THE MIDST OF COVID-19

Emergence of COVID-19 health-care and vaccine related attacks

Surge in Ransomware attacks

More tailored, sophisticated phishing emails

More social engineering and theft of funds

Potential privacy claims by employees

Source: The National Cyber Security Centre Annual Review 2020



CYBER INSURANCE: HOW IT RESPONDS



CYBER INSURANCE: AN OVERVIEW

**Regulatory Fines
& Penalties**

Incident Response Costs:

- Legal
- Forensics
- Crisis Management
- Credit Monitoring
- Notification
- PR

Data Restoration

**Business
Interruption**

**Security & Privacy
Liability**

Cyber Extortion



TRIGGERS FOR CYBER INSURANCE COVERAGE

Security Failure	EHR / NHS Digital, 2020 External/accidental	Fire Eye, 2020 External/malicious
System Failure	IBM Cloud, 2020 External/accidental?	AWS, 2020 Internal/accidental



CYBER INSURANCE: COVERAGE CONSIDERATIONS



CYBER COVERAGE CONSIDERATIONS IN THE PANDEMIC

The screenshot shows the FCA (Financial Conduct Authority) website. The header includes the FCA logo and a search bar. Below the header are navigation tabs for 'About us', 'Firms', 'Markets', and 'Consumers'. The main content area features a breadcrumb trail: 'Home / Firms / Insurance and coronavirus (Covid-19): our expectations of firms'. The article title is 'Insurance and coronavirus (Covid-19): our expectations of firms'. Below the title, it states 'First published: 19/03/2020 | Last updated: 12/01/2021 | [See all updates](#)'. The main text begins with 'Many consumers are currently in a vulnerable position because of the coronavirus (Covid-19) pandemic. We expect insurers, given the unprecedented impact of coronavirus, to be aware of the circumstances that customers find themselves in. This web page is aimed at helping firms understand the FCA's position. Read about our expectations of insurance firms.' Below this is a dark blue box with the text 'Sign up to receive FCA coronavirus updates' and a link to 'Subscribe to receive daily email round-ups of FCA coronavirus news and publications when we publish on our website'. The article continues with two paragraphs: 'We expect firms to consider very carefully the needs of their customers and show flexibility in their treatment of them. We are likely to see customers' behaviours change because of the pandemic. For example, this could mean that customers may need to work from home or commute by car. We would not expect to see their ability to claim impacted by circumstances over which they have little control.' and 'We expect firms to clearly communicate any policy exclusions that may impact the cover and use of individual policies. This applies both to new sales or changes to existing policies (either mid-term or at renewal) – they must clearly meet consumers' demands and needs.'

X COVID exclusions

✓ Portable technology

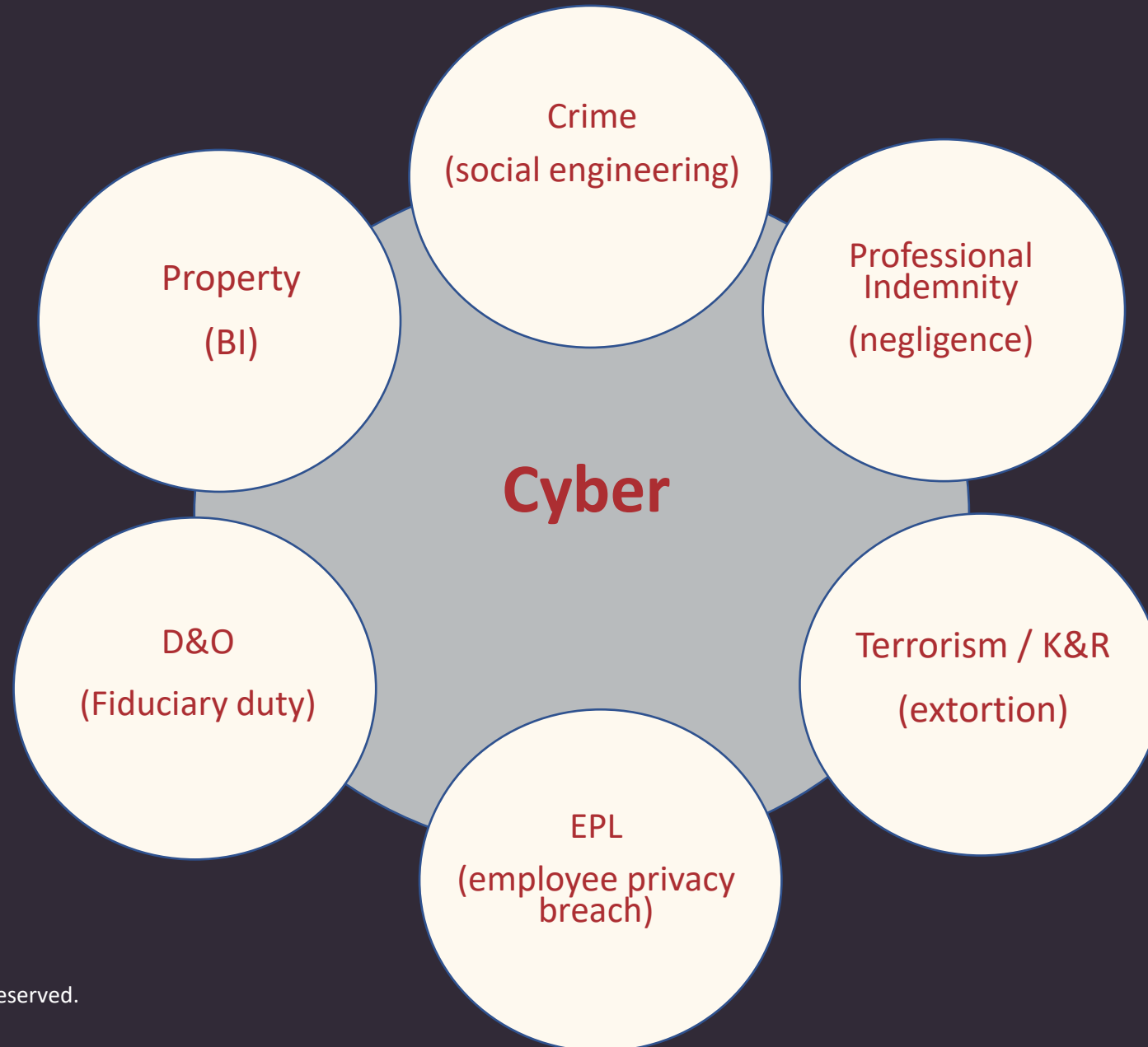
✓ BYOD

✓ Cloud infrastructure

? Furloughed staff?



COVERAGE OVERLAPS



LEARNING SUMMARY

1. Aware of how cyber risk has changed in light of COVID-19
2. Cognisant of the main triggers for cyber insurance coverage, and be equipped with claims examples that can be drawn upon in future discussions.
3. Able to articulate how cyber risk corresponds/overlaps with other lines of coverage



Cyber Claire

RISK MANAGEMENT
& CYBER SECURITY

www.cyberclaire.com | info@cyberclaire.com

+44 (0)208 191 0650 | +44 (0) 795 231 0026

www.linkedin.com/in/Claire-g-davey

Twitter: @CyberClaire_