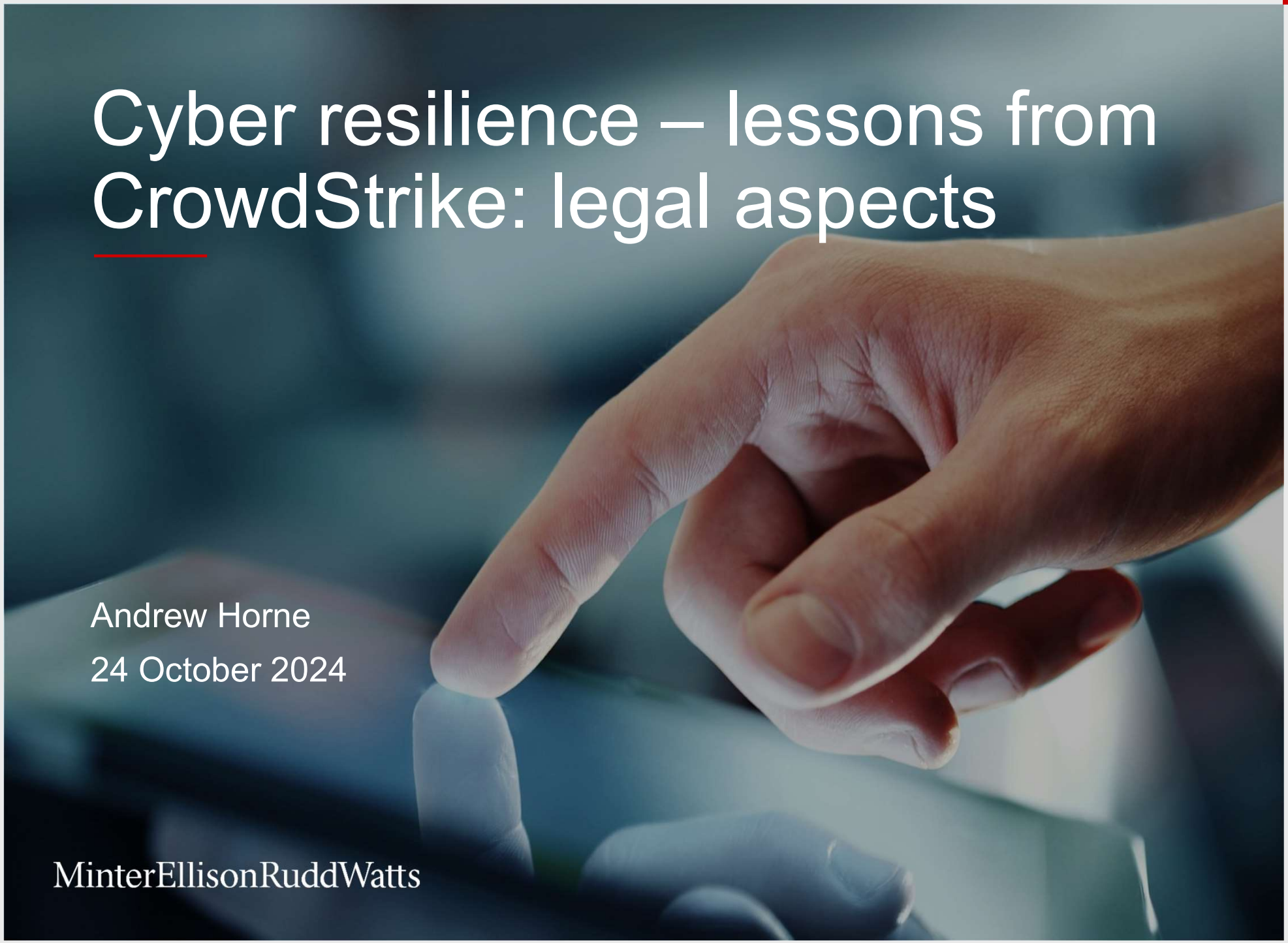
Cyber resilience – lessons from CrowdStrike: legal aspects



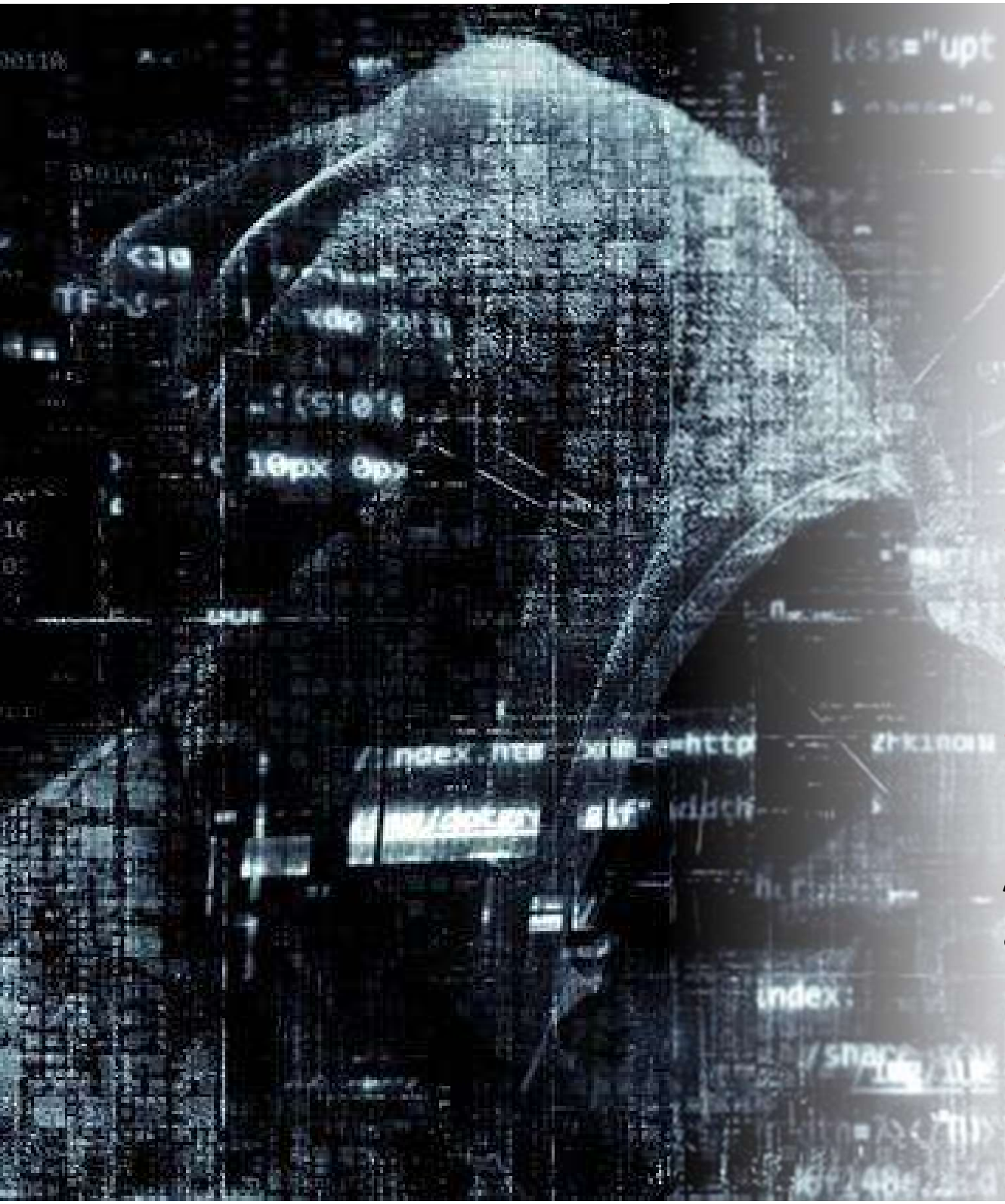
Andrew Horne

24 October 2024

MinterEllisonRuddWatts

Legal aspects

- Losses, liabilities
- Regulatory obligations
- Insurance



Losses from cyber events

- Business profits
- Loss of reputation
- Liability to customers
- Liability to investors
- Fines and penalties

A complex web of losses and claims

Regulator focus on cyber risk

Cyber risk is a key threat to the financial system

Increased expectations

New obligations for technology resilience

- FAPs
- Banks, deposit takers, insurers
- MIS, DIMS etc

What are the requirements?

Full FAPs – SC 5

Material incident reporting	Within 10 working days
Ensure operational resilience	Confidentiality, integrity, availability of systems
Business continuity plan	Not limited to technology, updated annually
Extent of BC plan	Reflects size, complexity, exposure

What are the requirements?

Financial institutions - banks, non-bank deposit takers, insurers - SC5

Material incident reporting	As soon as practicable and within 72 hours
Periodic reporting	Large entities – 6 monthly Other entities - annually
Self-assessment	Large entities – annually Other entities – 2-yearly
Business continuity plan	Not limited to technology, updated annually
Ensure operational resilience	Confidentiality, integrity, availability of systems

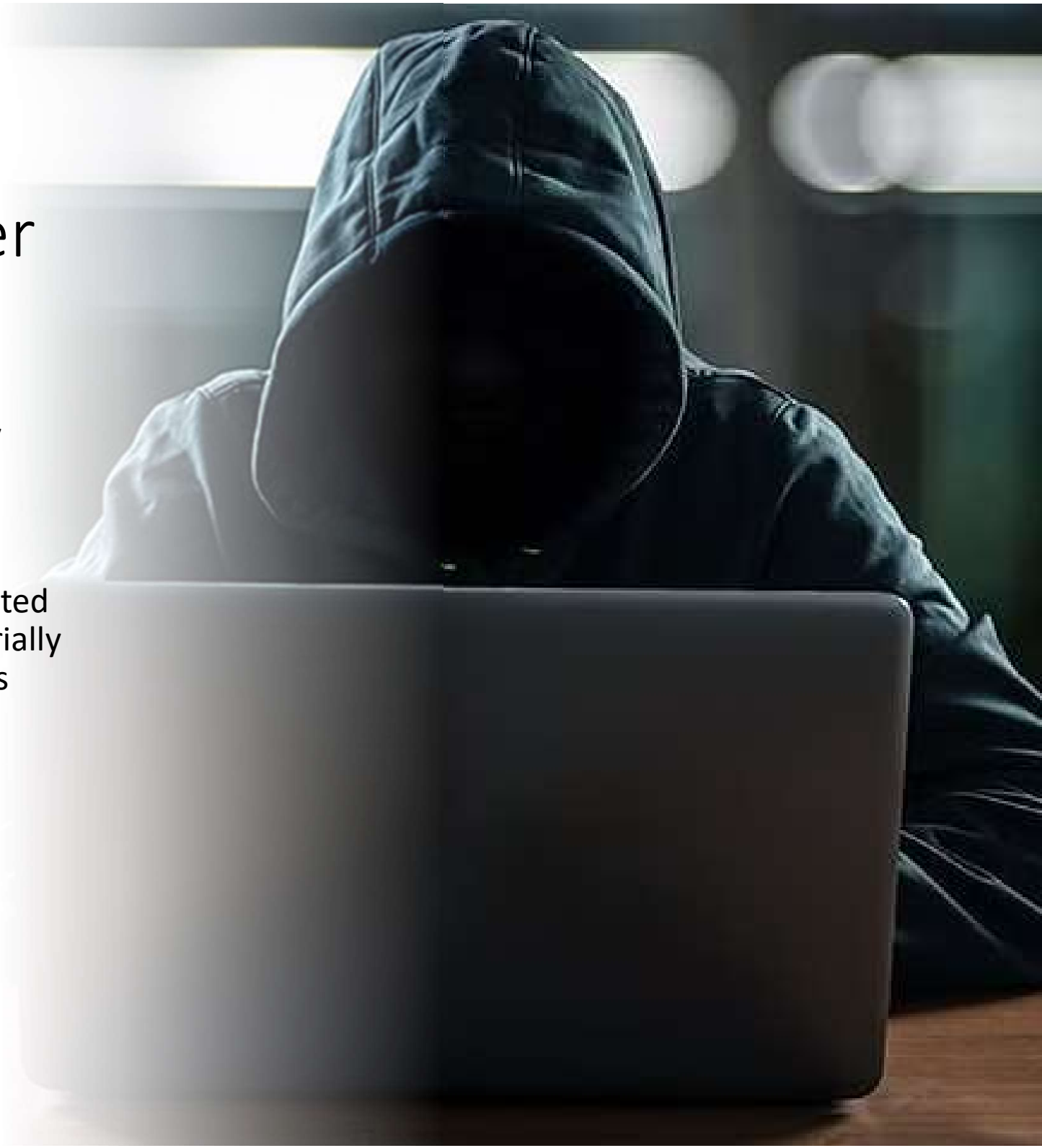
What are the requirements?

MIS managers (non-restricted, managed), DIMS providers, derivatives issuers, prescribed intermediaries – SC 9

Material incident reporting	As soon as possible and within 72 hours
Ensure operational resilience	Confidentiality, integrity, availability of systems
Business continuity plan	Not limited to technology, updated annually
Extent of BC plan	Reflects size, complexity, exposure

What is a material cyber incident?

- **Cyber incident** – adversely affects cyber security of an information system, whether malicious or not
- **Material** – materially affected or had the potential to materially affect the entity or customers



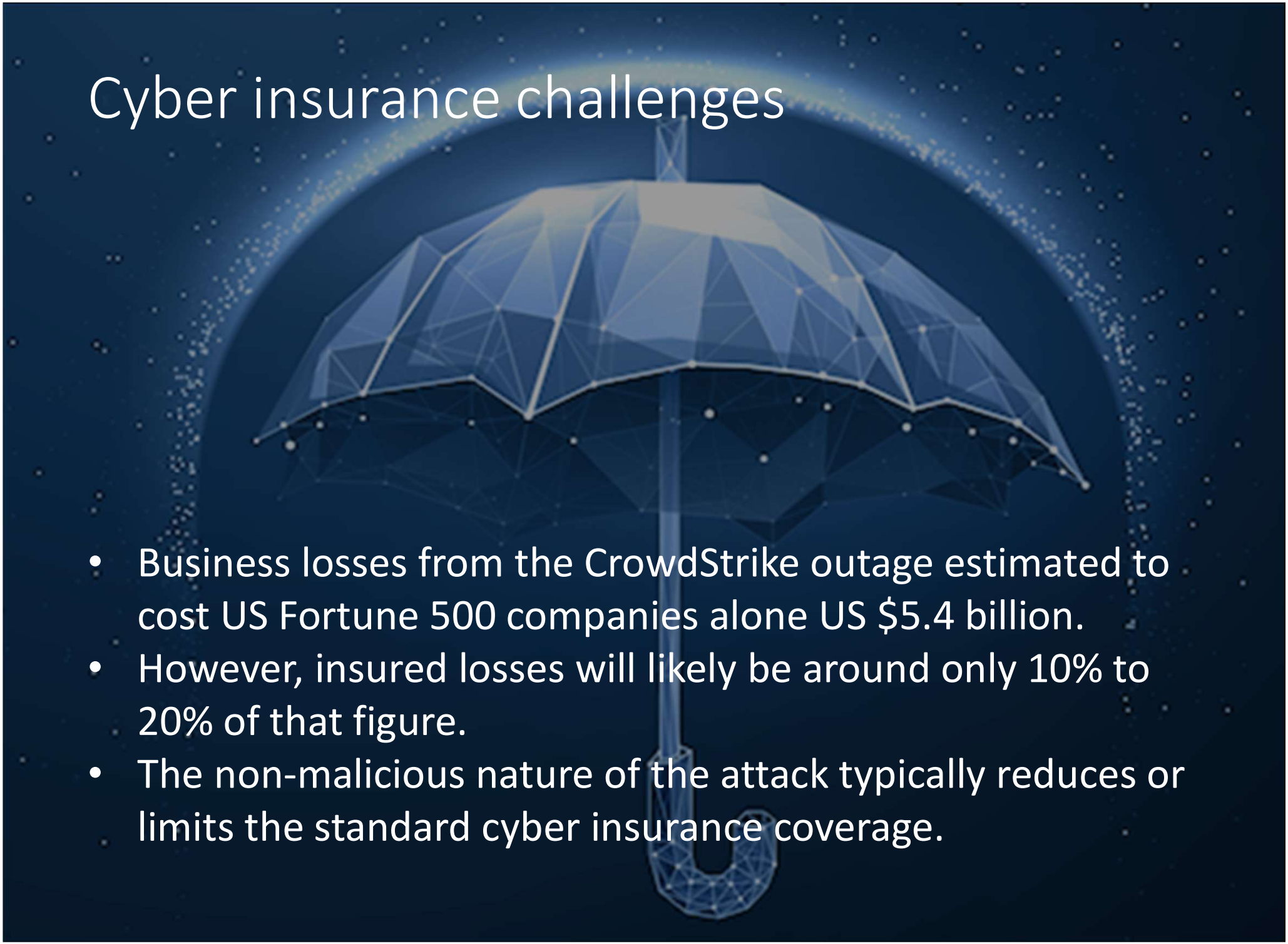
What needs to be reported?

Initial report

Incident update

Post-incident conclusions

Cyber insurance challenges

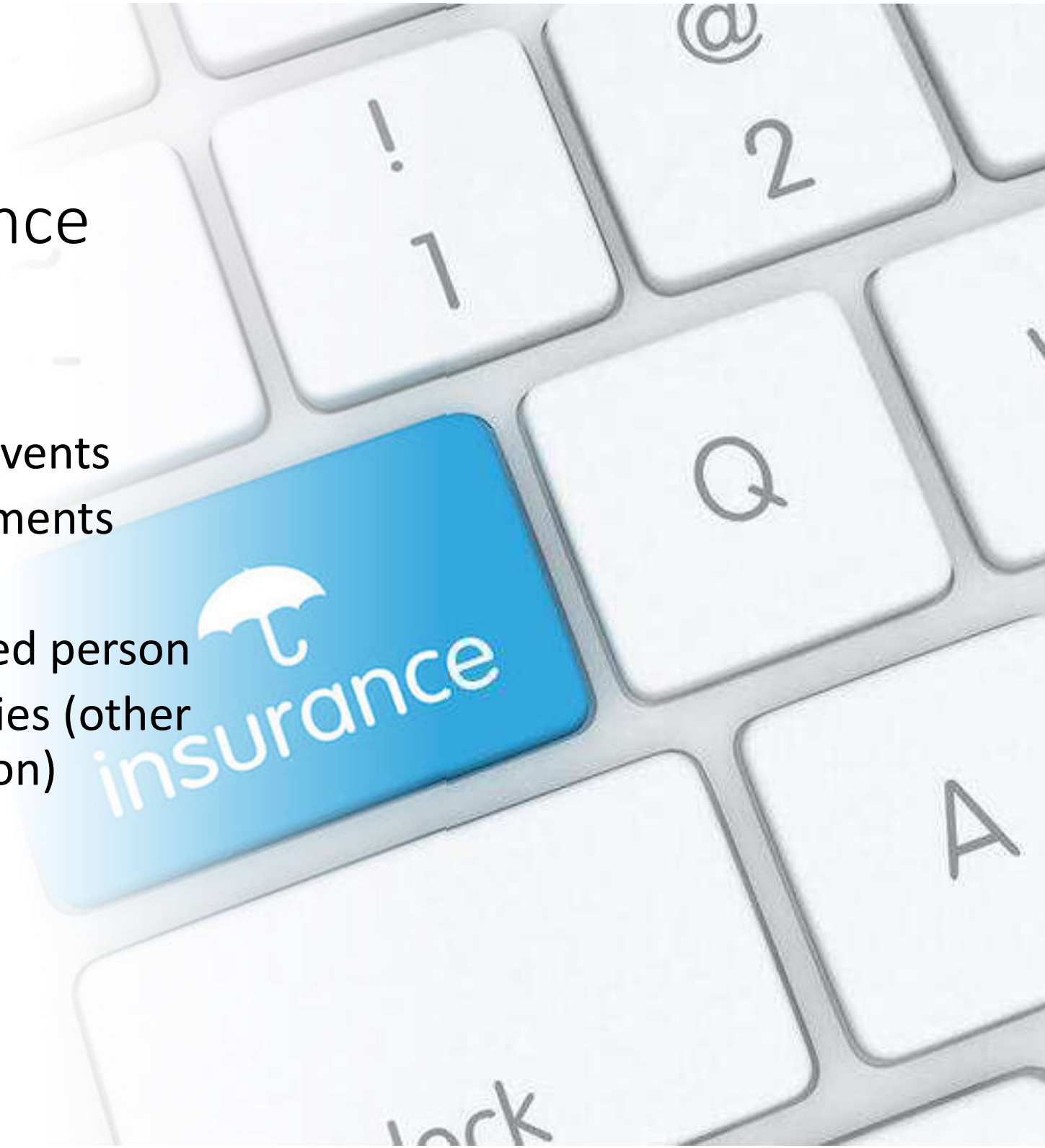


- Business losses from the CrowdStrike outage estimated to cost US Fortune 500 companies alone US $5.4 billion.
- However, insured losses will likely be around only 10% to 20% of that figure.
- The non-malicious nature of the attack typically reduces or limits the standard cyber insurance coverage.

Cyber insurance

- Hacking / malicious damage / virus
- Breach of statutory duty (eg privacy)
- Data restoration costs
- Ransom costs
- Fines, penalties and defence costs
- Hardware and software repair costs
- Business interruption costs – lost profit
- Liabilities to third parties and contract penalties
- Digital media claims – e.g. defamation

Cyber insurance



May not cover:

- Innocent cyber events
- Misdirected payments
- Usual perils
- Loss by authorised person
- Fines and penalties (other than data protection)

Other insurance

- Professional Indemnity
- Crime
- Statutory Liability
- Technology

Recommendations

Regulated firms should:

01

Prepare for regular reporting of non-material cyber events

02

Prepare an action plan for identifying and reporting material cyber events – use template

03

Prepare for self-assessment – read the templates, find the information and make improvements

04

Understand and implement appropriate cyber protections and incident response plans and be prepared to explain them

MinterEllisonRuddWatts

minterellison.co.nz