# An Introduction to Cyber Insurance

DELIVERED BY DIANE JENKINS ACII, CHARTERED INSURANCE BROKER

JANUARY 2022

nick thomas + associates

The Insurance Institute of Preston and Blackpool
Chartered Insurance Institute

# Introduction/housekeeping

Welcome and thank you!

Webinar format – muted and video off. Interactive features – polls, Q&A

60 minutes including short period of Q&A

Diane Jenkins

- Background in Insurance Broking Sector – technical programme design, M&A due diligence, BI reviews
- Former chair and education secretary of London Business Interruption Association

Nick Thomas & Associates

- Up to the moment solutions addressing the challenges of the modern insurance professional
- Technical insurance, sales, business and soft skills, performance, resilience and wellbeing, leadership and management training
- Specialists in virtual and hybrid solutions for sales, client interaction, management, performance and wellbeing

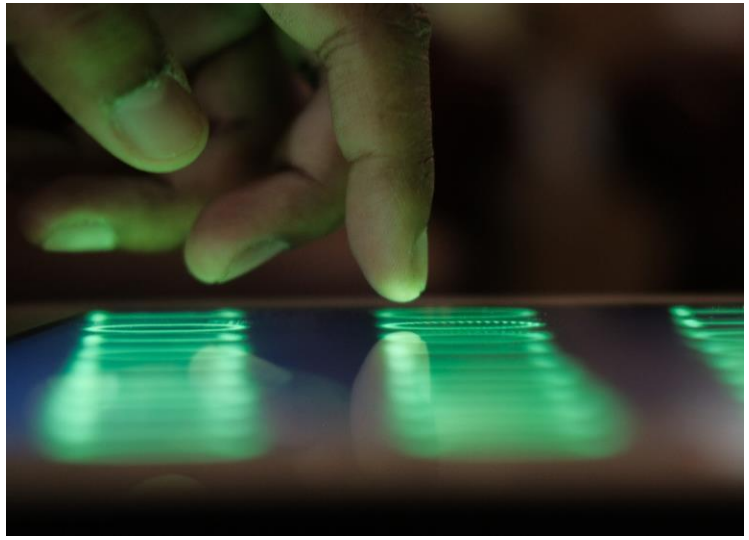
# Objectives

- Understand the cyber risks covered in an SME cyber policy.
- Be aware of key cyber insurance market developments and their practical implications for brokers and insurers.
- Be aware of cyber market innovations and their potential use for clients

# What are cyber risks?

IRM definition:

“any risk of financial loss, disruption or damage to the reputation of an organisation from some sort of failure of its information technology systems”



# Specialist cyber policies

Cyber cover

- Standalone policies
- Packages
- Cyber extensions in non-cyber policies
- Buy backs in explicit cyber exclusions

Lots of variations in wordings

No common terminology

Definitions are key

- e.g., does computer include industrial control systems

# Specialist cyber policies

Costs associated with data breaches

- Forensic investigation fees -what, where, how, when
- Customer/regulator notification
- Legal fees
- Call centres/credit monitoring services
- Fines for a breach of data protection legislation (where legal to insure)

# Data breach issues

Discovery trigger usual
- Is there a retroactive date?

Does policy cover potential as well as actual breach?

Does claimant have to use insurer's response service?

Is calling response service a claim notification?
- Check who pays if no cover in policy for incident
- Know if excess is applicable from minute one

# Specialist cyber policies

- Reputation and response costs
- Cyber terrorism
  - Not always included
- Cyber extortion
  - Ransom
  - Forensic costs
  - Professional fees for independent advisors

# Extortion issues

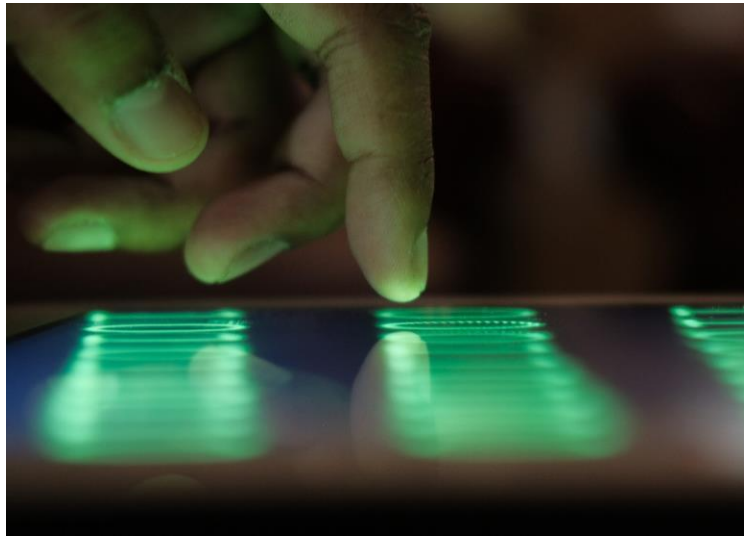
Does insurer hold bitcoin wallet?

Should ransoms be paid?

- OFAC issues
- Involvement of police/FBI
- Sanctions clauses
- Breach of confidentiality condition

Check trigger and who carries out extortion e.g., employees as well as third parties

Some policies link ransom payment to BI loss – proof?



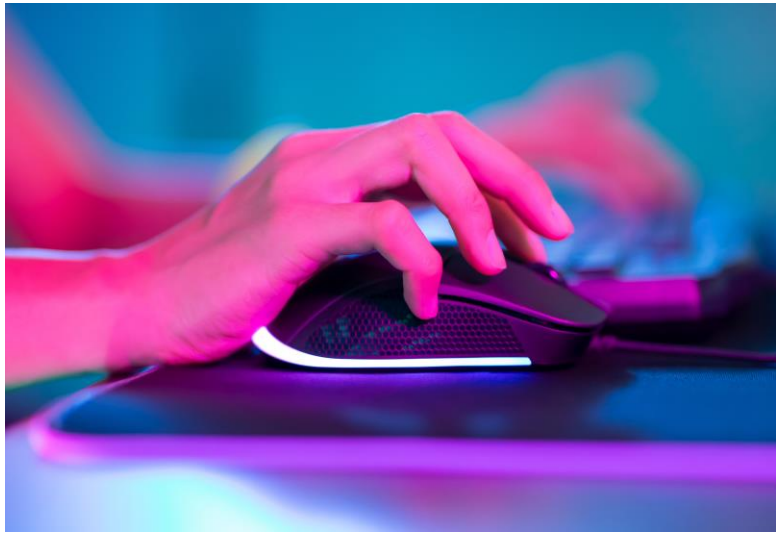
# Specialist cyber policies

Business interruption/extra expense

- Waiting periods or monetary excess
- Short indemnity periods

Basis of settlement – calculation of limit may be difficult

- Gross profit (definition may not be same as property BI)
- Net profit
- Revenue/income
- ICOW/AICOW



# BI issues

IP or period of restoration

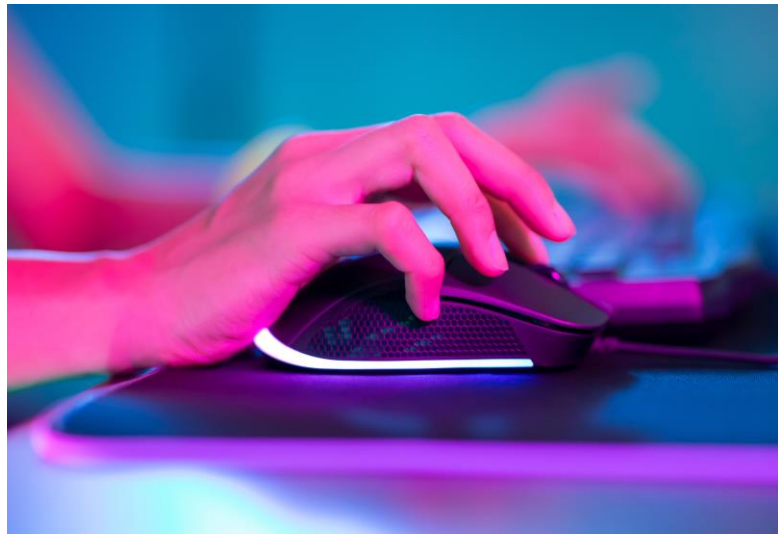
- Does cover include loss of reputation/loss of clients?
- When triggered/ended

Waiting period

- Does this apply to ICOW

Calculation of loss

- Most policies missing usually BI formula



# Specialist cyber policies

Third party costs - legal liability

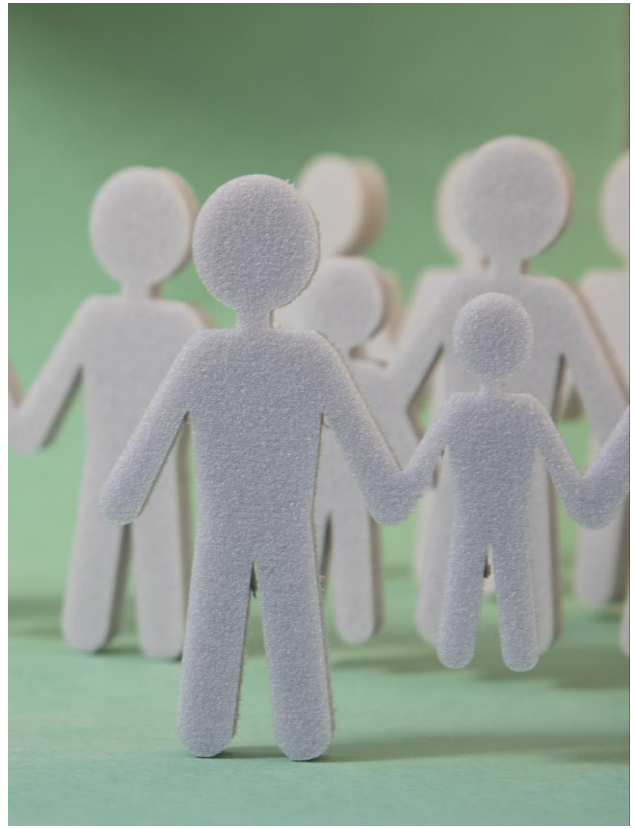
- Transmission of a virus
- Use of computer network for DoSA
- Data breaches
- Media content
- PCI

# Third party claim issues

Aggregation
- Limits
- Excess or deductible

Claims made
- Retroactive date – what does it apply to (cause?)
- Notification issues –circumstances (all layers)
- Excludes prior/pending
- Extended reporting/run off issues

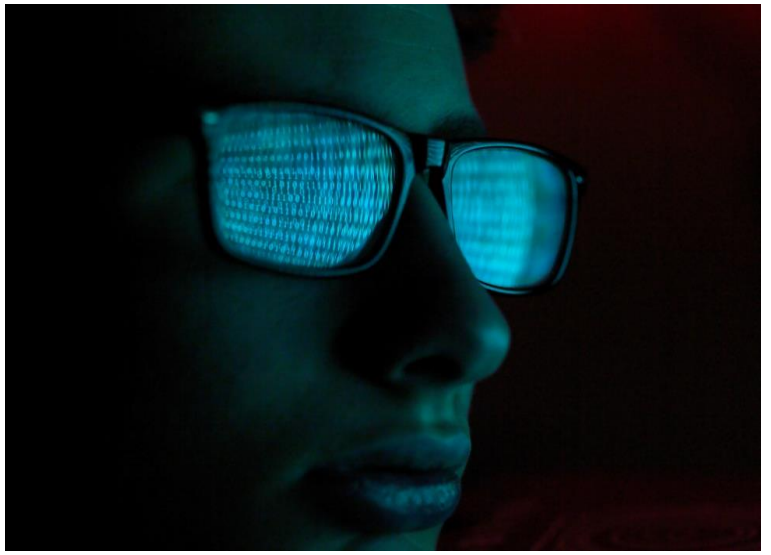
Excludes damage to third party property



# Cyber crime

Theft of money/property not data

- Funds transfer fraud
- Computer fraud
- Telephone phreaking
- Social engineering fraud
- Cryptojacking
- Spoof websites



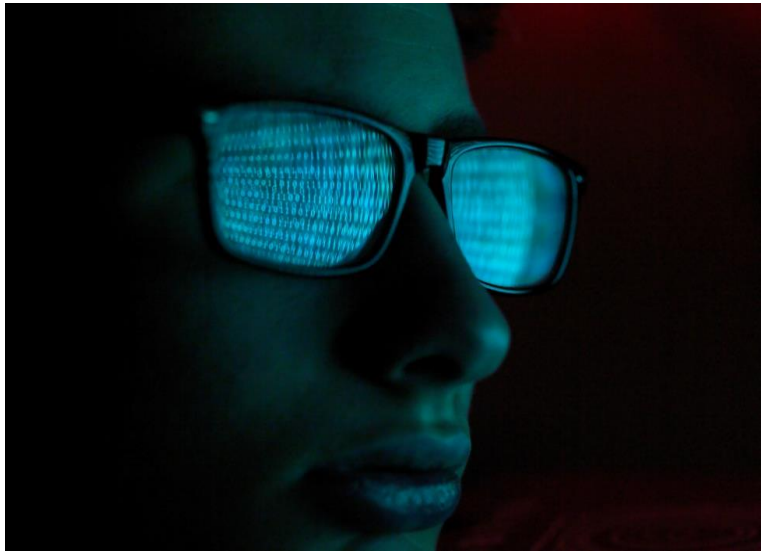
# Cyber crime issues

Social engineering fraud not always covered

- May be low sub-limit
- Often verification conditions apply – need to check compliance (may be condition precedent)
- Definitions of social engineering vary

May be voluntary parting exclusion

Make sure you understand what cover client needs – crime policy with cyber extension might be better

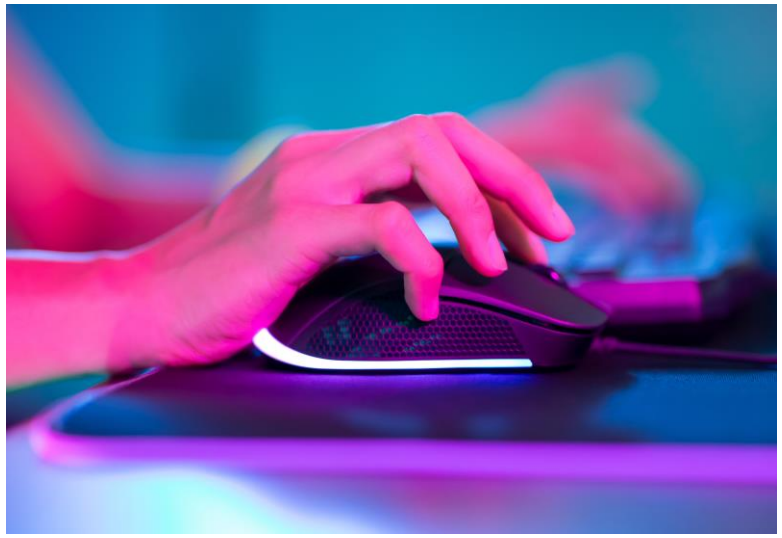


# Specialist cyber policies

Conditions precedent language

- Claims conditions/requirements
- Reasonable precaution or security conditions
- Confidentiality conditions

Change of control clause



# Cyber market developments

Rate increases/capacity reduced

Increased underwriting

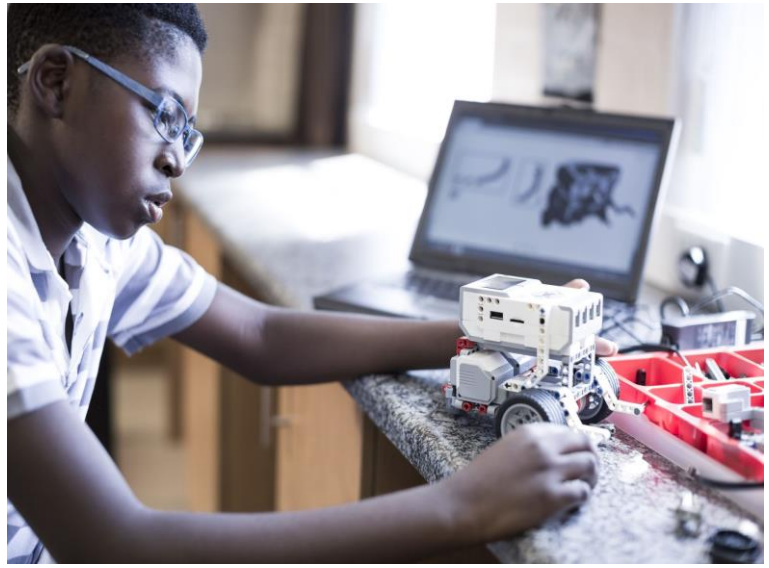
- More queries on security/staff training
- MFA required

Lloyd v Google – Nov 2021 Supreme Court decision

- Must be ‘damage’ for claim for data breach to succeed

Rolfe v Veale Wasbrough Vizards 2021

- Must be de minimis level of distress – not all data breach claims meet this level



# Cyber market innovation

Parametric

Standalone breach support

Cyber wrap – dealing with silent cyber and terrorism gaps

Industry specific policies – aviation, marine, manufacturing, retail

Packages: cyber plus - management liability, crime, financial lines (may be easier to place with other lines)

,

# Revisit Objectives

- Understand the cyber risks covered in an SME cyber policy.
- Be aware of key cyber insurance market developments and their practical implications for brokers and insurers.
- Be aware of cyber market innovations and their potential use for clients

# Thank you! Questions?

**Contact:**

Email: nick@nickthomasassociates.co.uk

Telephone: 07767 647812

LinkedIn: https://www.linkedin.com/in/nick-thomas-64046113/

LinkedIn Company: https://www.linkedin.com/company/nick-thomas-associates/

*'Up to the minute training solutions addressing the challenges of the modern insurance professional'*