Institute
of Directors
Ireland

Cyber Security Risk: What a Director Should Know

with Paul Gillen, Chief Security Officer and Country Manager, Barclays Bank Ireland

13th November 2024

Sponsored by accenture

Agenda

- Intro
- Top Cyber Threats
  - Ransomware, IABs, AI Threats and Insider Risk (Accidental/Reckless/Malicious)
- Cyber Regulations NIS2, what a Director should know.
- What should we as Directors ask in the Boardroom now?
- Some practical tips for use after we leave today.
- **Caveats**: These are my opinions, this is not a lecture, it’s sharing, and I have nothing to sell you! ☺
- **Need to talk to me after? I am at: paul.gillen@barclays.com**

Cyber Threat Landscape

Executive Summary – Top Cyber Threats

- The deployment of **ransomware by organised cybercriminal groups** continues to represent a significant threat to organisations across all sectors and geographies
- Despite several successful law enforcement operations around the world, **ransomware operators continue to target organisations** in critical industries
- Campaigns distributing **malware which allows threat actors to gain a foothold on victim networks (IAB's)** continue at pace, and their symbiotic relationship with ransomware operators is almost certain to continue underpinning the cybercriminal ecosystem
- Failure of organisations to properly address **security vulnerabilities** can allow threat actors to access critical systems remotely, and lead to installation of malicious code, tools or software
- **Nation-state threat actors** continue targeting of organisations across multiple industries, with particular focus on technology companies which exist in supply chains across every sector
- The **increasing sophistication of AI** is likely to empower threat actors with greater automation, scale and complexity in their attacks
- Interdependence and third- and fourth-party concentration has the potential to create significant sector-wide and cross-sector disruption resulting from a single attack, incident or outage

Emerging Threat: Impact of Artificial Intelligence on the Insider Threat Landscape

The rapid development of artificial intelligence (AI) is transforming the threat landscape and has the potential to increase the likelihood and impact of insider threats. **As the development of artificial intelligence (AI) accelerates, and the tools become more sophisticated and accessible it is likely to drive an increase in insider risk.** This could result in significant impacts to the organisation, including the leakage of confidential information, cyber-attacks, financial losses and regulatory, reputational and legal impacts.

Examples of insider threats that are most likely to be impacted by the rise in AI are:

- **Data leakage** - significant developments in generative-AI tools had to led to an increase in employee populations using them to improve their work efficiency, however, **if employee used this technology for unauthorised business use it could result in data leakage, and subsequent regulatory, and legal impacts.**
- **Social engineering of colleagues** – threat actors are leveraging the rise of AI and machine learning to launch sophisticated **social engineering attacks which are likely to become more difficult for employees to detect and could be more likely to expose an accidental or negligent insider.**
- **Executive Impersonation –** As deepfake and voice cloning technology, and large language models become more advanced it is **likely to drive an increase in the threat of executive impersonation**, either by persuading colleagues to pay fake invoices, transfer funds, plant malware, leak important data which could affect share price, **this could result in significant business impacts including reputational damage.**
- **Employment application fraud** - Generative-AI is being widely used to help job seekers with writing CVs and application forms. **This could expose recruitment processes to fraud and result and could increase both accidental and negligent insider threats**, the impact of which could result in significant harm to the organisation, especially if threat actors were able to infiltrate the organisation within highly-skilled roles or high-risk user groups. **(this is real)**

Focus on compliance with laws & regulations

Use-case

NIS2 Directive – Aim to enhance the security and resilience of network and information systems in the EU

The NIS2 Directive sets out specific penalties for non-compliance:

- Non-monetary remedies
- Administrative fines
- Criminal sanctions

NIS2 gives national supervisory authorities the authority to enforce **non-monetary remedies**, including:

- compliance orders
- binding instructions
- security audit implementation orders
- threat notification orders to entities’ customers.

For essential entities, it requires Member States to provide a maximum fine level of at least **€10,000,000 or 2% of the global annual revenue**, whichever is higher.
For important entities, NIS2 requires Member States to fine for a maximum of at least **€7,000,000 or 1.4% of the global annual revenue**, whichever is higher.

NIS2 includes new measures to hold top management **personally liable and responsible for gross negligence in the event of a security incident**.

- Ordering that organisations make **compliance violations public**.
- Making public statements **identifying the natural and legal person(s) responsible** for the violation and its nature.
- And if the organisation is an essential entity, **temporarily ban an individual from holding management positions** in case of repeated violations.

Cyber Security Risk | What a Director Should Ask

Ensuring Directors have the right insights & skills to supervise and challenge their organisations

Results of Institute of Directors Ireland’s recent Cyber Security and AI survey:

- 68% of directors have no board-approved AI policy to guide staff
- Nearly 84% of Irish senior leaders do not fully understand new EU NIS2 cyber rules to be implemented imminently in Ireland *
- 41% not aware of our own personal liability under new NIS2 regulations
- Yet.... it seems Directors rate cyber security as a top risk to organisation in the next 12 months
- 87% concerned about impact of a third-party supplier on organisation’s cyber security resilience – note this if you are a supplier to an essential/important org under NIS 2.
- **Findings were discussed at IoD ‘Leading in Governance’ conference which took place 24th October in Dublin, you can follow up if you missed this.**

Questions you can ask to challenge your clarify your thinking with your security / technology teams:

- Are we an essential or important sector org? Are we a critical supplier to an essential or important sector Org?
- What is our cyber security and op Resilience posture and has it been independently tested? How was this scored? By TLPT or Questionnaire?
- If we assume we may fall foul of a cyber-attack how do we ensure Op Resilience while we are under attack?
- Do we have funded compliance programs in place tracked at board level which would mitigate sanctions if we fall foul in an attack?
- **To the tech/cyber team/cyber security provider:**
  - Are we intelligence driven in our approach?
  - What is the threat landscape for our/my industry sector?
  - What standards do we align to (NIST etc), why did we pick that one?
  - Are our KPI/KCIs/metrics relating to cyber fit for purpose to provide board assurance
  - Testing ‘whole company’ crisis/resilience response – what would board do if business operations were fully interrupted by ransomware

Further considerations

- Greater oversight of security issues, incidents and near misses at executive level
- Create or mature your Crisis Management and Incident Response capabilities- is it inevitable we will call get caught...?
- Create an environment where it is safe for colleagues to speak up about control gaps or other improvement opportunities
- Empower subject matter experts to engage problems on a proactive basis

Some Practical Tips

- Invest in sector relevant **threat landscape reports and intelligence feeds** (operational and executive) – ***He who defends everything, defend nothing Frederick the Great***)
- Invest in an end-to-end Cyber assessment **with 'hands on' testing** (Why?)
- **Use a Cyber Standard** (UED, NIST, ISO) - scoring is easy to understand and ensures the broadest outcome.
- Consider that the **Board pay for the assessments** and not the SME's (Why?)
- After the test, **begin a multi-year remediation program** tracked at board level
- **Repeat sector threat led tests at regular intervals,** homing in on variations in scores and metrics
- Remember if you are subject to increased regulatory scrutiny, and you are compromised anyway... **the above strategy is a mitigant to fines.**

Institute
of Directors
Ireland

Directors: Hack Cybercrime

IoD online short programme

8th April - 3rd June 2025

Book your place

Institute
of Directors
Ireland

Cyber Security Risk: What a Director Should Know

with Paul Gillen, Chief Security Officer and Country Manager, Barclays Bank Ireland

13th November 2024

Sponsored by accenture