DATA BREACH RISK WEBINAR

Bennett Jones

OVERVIEW

- Landscape of evolving cybersecurity threats
- Critical strategies for ensuring your organization in cyber prepared
- Critical issues to address in the face of an attack
- Q&A

KEY STATISTICS – 2021 – Ponemon Study
- measured in US Dollars

- $5.4M - Average cost of data breach in Canada
  - Costs included: detection; notification; breach response; lost business cost
  - Average cost increased from $4.5M in 2020

- Several factors impacted range of costs

- **Security AI/Automation:**
  - $6.71M – no security AI or automation
  - $2.9M – fully deployed security AI and automation
  - Security AI/automation – associated with faster time to identify and contain breach
    - 184 days to identify & 63 days to contain – fully deployed
    - 239 days to identify and 85 days to contain – not deployed

KEY STATISTICS – 2021 – Ponemon Study - cont’d

- **Incident Response capabilities**
  - $3.25M - IR capabilities
  - $5.71M - No IR capabilities
- **Regulatory Compliance**
  - *Out of selection of 25 cost factors that either amplify or mitigate data breach costs, compliance failures was the top cost amplifying factor*
  - $5.65M – High level of compliance failures
  - $3.35 – Low level of compliance failures
- **Zero Trust**
  - *Zero trust – operates on assumption that user identities or network may already be compromised; relies on AI and analytics to continuously validate connections between users, data and resources*
  - $5.04M – without zero trust deployed
  - $3.28M – with zero trust deployed at mature stage

KEY STATISTICS – 2021 – Ponemon Study - cont'd

- **Encryption**
  - $4.87M – low standard of encryption/no encryption
  - $3.62 – high standard of encryption
- **Remote work**
  - $4.96M – remote work was factor
  - $3.89M – remote work not a factor
- **Digital transformation due to Covid-19**
  - $5.01M – no transformation
  - $4.26M – very significant transformation
  - 316 days to identify and contain breach – remote work greater than 50%
  - 258 days to identify and contain breach – remote work greater than 50%

LANDSCAPE OF EVOLVING THREATS

- Trends
- Some key questions to ask your team:
  - *Who is responsible for monitoring software vulnerabilities?*
  - *What resources do we rely on for intelligence about attack risks and who in organization is responsible for continuously and assessing these risks?*
  - *How many attempted attacks on our organization and how quickly are we detecting them?*
  - *What trends are we seeing in the type of attacks on us or within the relevant industry?*
  - *What do we know about risks to our suppliers?*

CRITICAL STRATEGIES - PREPAREDNESS

- Top vulnerabilities being exploited

- Some key questions to ask your team:
  - *Have we mapped out our worst case scenarios and properly tested our ability to respond?*
  - *Have we assigned a dollar value to these scenarios?*
  - *What have we done to resist threat of credential compromise?*
  - *What do we know about our employee ability to resist phishing attack?*
  - *Have we assessed shift in risk based on remote/hybrid structure?*
  - *Do we have experts on speed dial?*

CRITICAL ISSUES - RESPONSE

- Common errors in response

- Key issue in response:
  - *Privilege*
    - *Evolving area of the law regarding data breach reports*
    - *Factors considered by US courts in ordering production of forensic report (regardless of fact that they were retained by legal counsel):*
      - *Forensic firm working under statement of work that pre-dated breach*
      - *Organization reassured customers that it had retained "world leading cybersecurity firm"*
      - *Designation of retainer as business expense (as opposed to legal expense)*
      - *Circulation of report beyond those who need to be privy to legal advice*
      - *Remediation/containment recommendations in report*