2023-11-08

Steps to Comply With The New SEC Public Company Cybersecurity Rules and What May Come Next

Rick Borden
Frankfurt Kurnit Klein + Selz

Doug Howard
Pondurance

Privacy+ Security Forum

PONDURANCE

Frankfurt Kurnit Klein + Selz PC

INTERACTIVE SESSION

SEC REGULATIONS AND UPDATES

SEC PUBLIC COMPANY RULE

CYBER INSURANCE TRENDS

RISK TO EXECUTIVES AND CISOs

REFERENCE ARTICLES

ITS STILL ABOUT THE BASICS

CLOSING

SEC –PUBLIC COMPANY RULE – REGULATION THROUGH DISCLOSURE

- Incident Response:
  - Form 8-K, Item 1.05 to require registrants to disclose information about a **material cybersecurity incident** within **four business days** after the registrant determines that it has experienced a material cybersecurity incident.
  - Must determine materiality without undue delay.
  - Describe the material aspects of the nature, scope, and timing of the incident, as well as the material impact or reasonably likely material impact of the incident on the registrant, including its financial condition and results of operations.
  - Requires enhanced Cybersecurity **Disclosure Controls**

SEC –PUBLIC COMPANY RULE – REGULATION THROUGH DISCLOSURE (CONTINUED)

- Risk Management and Governance – Annual Disclosure:
  - Add Item 106 to Regulation S-K and Item 16J of Form 20-F to require a registrant to:
    - Describe their processes, if any, for assessing, identifying, and managing material risks from cybersecurity threats, as well as whether any risks from cybersecurity threats, including as a result of any previous cybersecurity incidents, have materially affected or are reasonably likely to materially affect the registrant.
    - Describe the board of directors' oversight of risks from cybersecurity threats and management's role and expertise in assessing and managing material risks from cybersecurity threats.

CYBER INSURANCE

DRIVEN BY REGULATORY RISK AND BREACH TRENDS

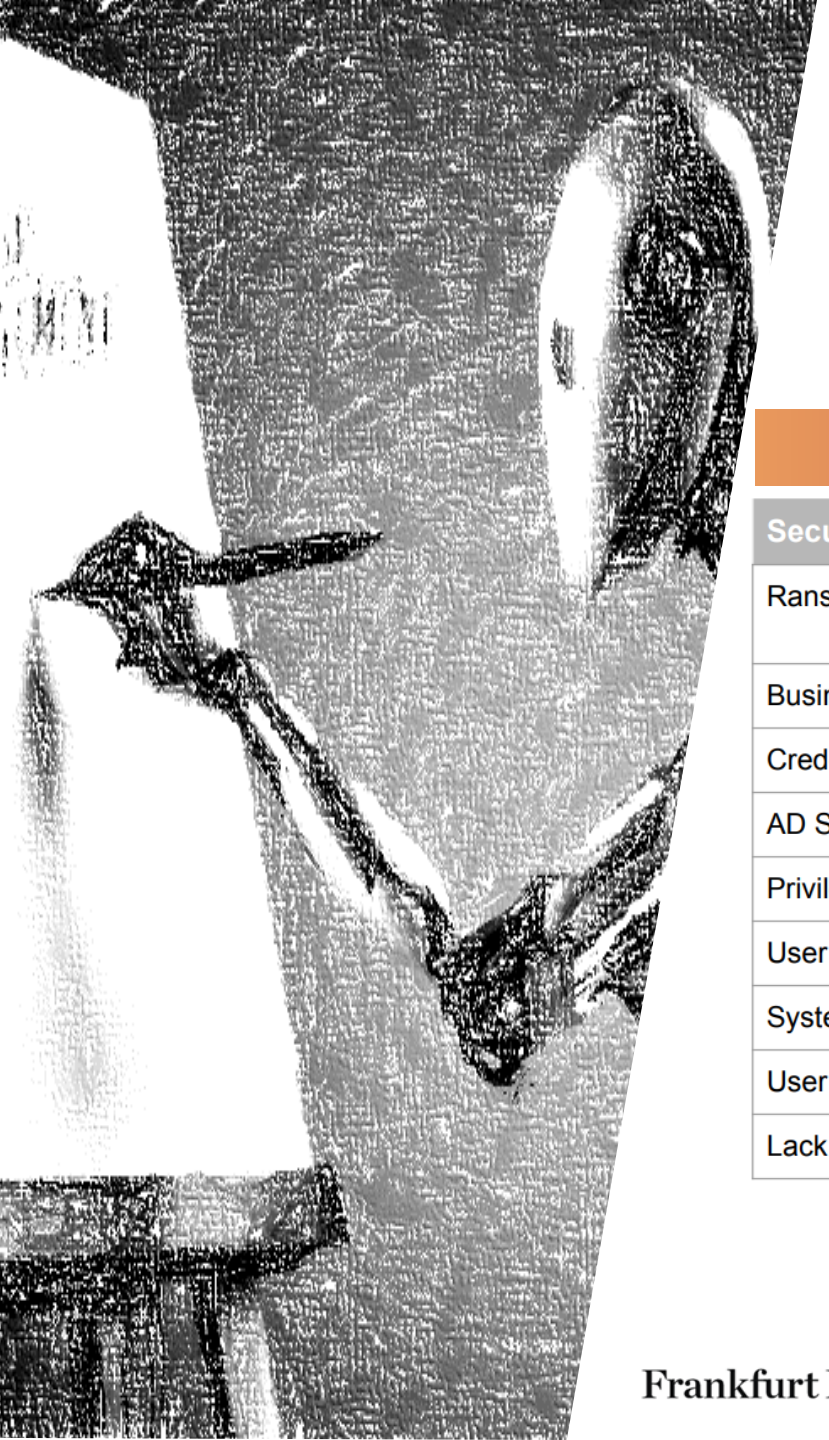
Cyber Insurance Trends and Predictions

Threat Landscape

- Hygiene and lack of monitoring
- GeoPolitical/Nation State sophisticated Attacks (APT)
- Unauthorized Access (Insider/External User, Network, System)
- Vulnerabilities
- Lack of data mapping and location awareness
- Poor User guardrails and trainings

Cyber Insurance Market Influences

- General policy that include Cyber Insurance and Cyber Insurance Claim Rates
- Causes for Cyber Insurance Claims (drives minimum requirements [currently Ransomware Supplement] and more and more Business Email Compromises)
- Future threat impact

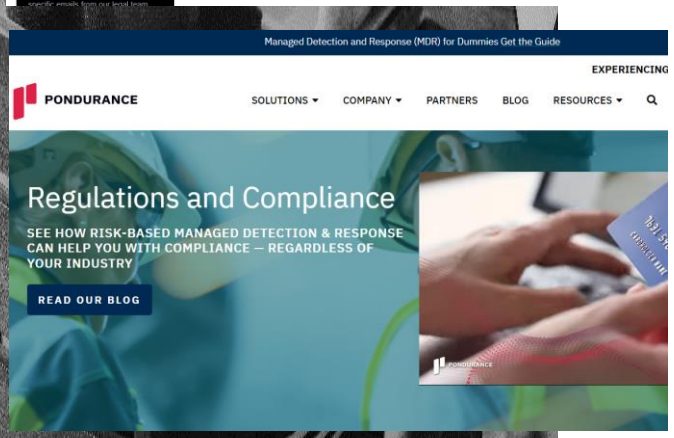


WHERE DOES REGULATORY RISK FIT IN THE SCHEME OF DRIVING POLICY ISSURANCE RATES AND CLAIMS?

HISTORIC INFLUENCE ON CYBER INSURANCE

Security Threat	Resulting Cyber Insurance Requirement
Ransomware	Backups, Endpoint Detection and Response (EDR) /Managed Endpoint Detection and Response (MDR)
Business Email Compromise	MFA, 24X7 Monitoring
Credential Compromise	Multi-Factor Authentication
AD Service Account Compromise	Reduction in service accounts/high degree of security of systems and access/MFA
Privileged Account Compromise	24x7 logging and monitoring of Privileged Account Escalations
User Awareness Training	User Training, Testing and Phishing Testing
System and Software Vulnerabilities	Vulnerability Scanning and Patch Management
User Errors	Awareness Training
Lack of System Inventory	Basic system inventory and active awareness/MAC Management

WHERE DOES AI FIT IN THE SCHEME OF DRIVING POLICY ISSURANCE RATES AND CLAIMS?



REFERENCE ARTICLES

FAST MOVING CHANGES

https://www.sec.gov/news/press-release/2023-227

https://fkks.com/news/six-steps-to-help-your-team-comply-with-the-new-sec-public-company-cybersecurity-rules

https://www.pondurance.com/cybersecurity-compliance/

Simplified Recommendation

Single-factor authentication is compromised more often than any one vector. Implement stronger authentication solutions and don't make exceptions. Build monitoring at a user level.

Know what assets you have and keep them patched. #2 most compromised vector. 1) few companies have an accurate inventory of assets, 2) they almost never keep them properly patched consistently across the enterprise, and 3) often, non-production, critical systems aren't properly prioritized

Communications and User Awareness Training and continuous role playing is critical. You can reduce risk for the average user. 1) train and test, 2) leverage email gateways, 3) Weed out the dummies and address, 4) Phish and Phish

Modernize your 24x7 detection capabilities with MDR/MxDR. Threats are 24x7, so must be your detection and response capabilities.

Malware is not going anywhere. We assume you have client-based anti-virus running, which is a start. **Enrich AV** with **network malware detection, sandboxing technologies** and **application whitelisting.**

Containerize and Encrypt all mobile devices! 1) Be careful to understand what MDMs do and don't do, 2) understand BYOD tradeoffs, 3) forecast – a reckoning is coming within mobile 3) containerize confidential data

Threat Intelligence if operationalized is powerful. 1) If it's in the news, it's probably too late, 2) customer specific intel and monitoring is critical, 3) A key is knowing what the next looming threat might look like and how to plan, recognize, respond and mitigate it as necessary.

… and disclosing the cyber risk you have

Frankfurt Kurnit Klein+Selz PC

PONDURANCE

FOCUS ON THE BASICS

Questions & Contacts

Frankfurt Kurnit Klein + Selz PC

Rick Borden

Partner
Frankfurt Kurnit Klein + Selz
rborden@fkks.com

PONDURANCE

Doug Howard

CEO
Pondurance
doug.howard@pondurance.com
+1.703.863.8568

WWW.PONDURANCE.COM

WWW.FKKS.COM