Cybersecurity Insurance

LARRY JOSEFOWSKI

DIRECTOR, CITY OF DOVER

Why Insurance?

- Incidents involving data theft continue to proliferate
- Average Ransomware cost - $300K
- Reputation
- Data leakage
- Political fall out

Why Us?

- SLTTs are high value targets for attackers
  - Valuable/sensitive data
    - Property Tax information
    - SSNs
    - Credit Card/bank information
    - Tax/Voter records
  - Budget restraints
  - Costs of tools
  - IT Staffing/Experience/Training
  - Non-standard/ “Exceptions” to standards

What does insurance cover?

- Types of network security failures
  - Cyber Extortion
  - Malware infections
  - Fraudulent Email/compromise
  - Potential Data breaches
  - Liability
- Types of data Breaches of all sorts
  - Social Security numbers
  - Credit Cards
  - Health Records
  - Drivers license numbers

Value added services

- Lawyers
- Forensic Firms
- Ransomware interdiction/Negotiation
- Data Recovery
- Identity Theft Services
- Crisis Communication
- Training
- Metrics
- Table-Top Exercises

Why Not Insurance

- 60% did NOT pay Ransomware
- Cost: Ransomware is Expensive – coverage limits are increasing
- Increase in exclusions
- Unpredictable annual requirements
- Improved controls and safeguards can limit exposure (self-insurance)
- Insurance requirements are going to get you very secure.

Potential “up side” to Insurance issues

- Premiums starting to stabilize from sharp increases over past years
- Improved processes and controls
- Insurers better able to define risk
- Decreases in paid ransomware

Needed regardless of insurance

- Minimize risks throughout infrastructure
- Incident Response Plans
- Business Continuity
- Backups

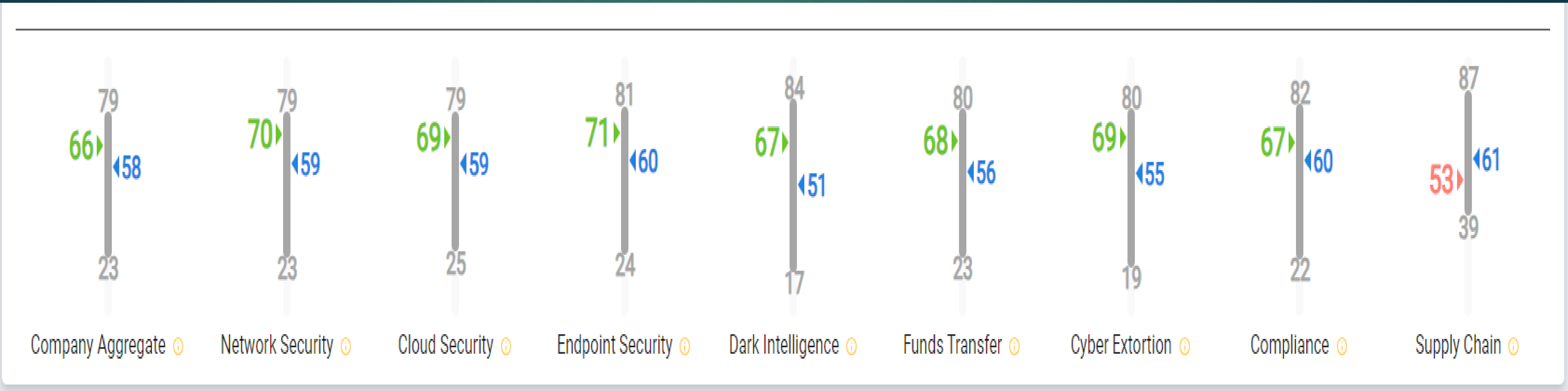
What to expect

- Increasing complexity and detail of questions
- Tough questions for line of businesses – not just IT
- Unexpected, last minute requirements

IT Security Controls

- Multifactor Authentication
- Admin/Privileged Access Management
- Endpoint Detection and Response
- Secure, encrypted, air-gapped backups
- Email/Web Filtering
- Patch and Vulnerability Management
- Incident Planning and Testing
- Cybersecurity training/Phishing testing
- Hardening Techniques
- Logging and monitoring (SEIM)
- End-of-Life plan
- Supply Chain Management

What do Insurers consider?



Ultimate questions to ask

- What is the financial stability of the entity?
- What is the cost of premium versus additional security measures?
- Are coverage exemptions becoming unreasonable?
- How good is your entities cyber security controls?
- How developed is your Incident Response Plan(s)

Questions?