Association of Corporate Counsel
HOUSTON

International Cyber Gangs:

What to Expect When Your Company Gets Attacked

Speakers

- Tyler Bridegan, Partner, Womble Bond Dickinson (US) LLP
- Vy Nguyen, Counsel, Jacobs Engineering Group

Goal

- Provide attendees with an overview of cybersecurity trends, as well as a practical view of a cyber incident and steps they can take to avoid impacts to their business

Agenda

- The Cybersecurity Landscape
  - Threat Actor Updates
    - Spotlight on Iran
  - The Regulatory Landscape
    - White House Cybersecurity Plan
- Responding to a Cyber Attack
  - On the ground picture
  - Negotiating ransom
  - Working with law enforcement
- Best Practices

The Cybersecurity Landscape:

- On the front end, threat actors are getting more sophisticated
- On the back end, regulators are getting more sophisticated and expecting more

Threat Actors

- Cyber breaches are at an all time
- Tend to target companies with “sensitive” data:
  - Healthcare systems and vendors
  - Defense contractors
  - State and local governments
    - E.g., City of Dallas
  - Critical infrastructure
    - E.g., SolarWinds

Threat Actors

- Spotlight on Iran:
  - Handala
    - Engage in wiper attacks
    - Not seeking ransom
  - Successfully targeted Stryker ($22 billion health tech company)
    - Obtained admin credentials to cloud management platform
    - Claims to have exfiltrated 50 terabytes of data before wipe
    - Simultaneously wiped data from 200,000 systems (servers, mobile devices, and corporate endpoints) across 79 countries

Regulatory Landscape

- White House released AI plan
- Federal agencies either increasing enforcement or conducting rulemakings:
  - Department of Justice Civil-Cyber Fraud Initiative
  - Department of Defendant DFARS and CMMC rules
  - Food and Drug Administration
  - Securities and Exchange Commission

Responding to a Cyber Attack

- Describe cyber attack scenario
  - Employees start noticing system is moving slow
  - IT notices documents with large attachments trying to be emailed externally
  - IT finds that whole systems have been zipped
  - IT finds a “ransom” note with a contact email

Responding to a Cyber Attack

- Immediate Steps
  - Consult incident response plan (assuming company has one)
  - Determine attack vector
    - Remediate immediately
    - Targeted or broad remediation
  - Determine affected systems
    - Operational disruptions or strictly encrypted data?
  - Loop in legal counsel, forensics firm, crypto broker, etc.

Responding to a Cyber Attack

- Key Decisions
  - Internal and external messaging
    - Employees?
    - Customers?
  - Law enforcement involvement
  - Ransom payment

Best Practices

1. Assess Current Security Posture & Vulnerabilities
    - Data Mapping: What do you have and where is it?
    - Security Measures: What do you have and what do you need?
2. Define Cybersecurity Goals & Objectives
    - Written polices and procedures; Set measurable targets
3. Create a Risk Management Plan & Develop Mitigation Strategies
    - Identify Information Assets: data, financial records, software
    - Assess Risks: internal, external, vendor, software (contracts, insurance)
4. Implement Strong Access Controls
    - Data minimization
    - Use, modification and access controls
5. Regularly Update Software and Systems (& upgrade legacy systems)
    - Patch management
    - Monitor vendor security updates

Best Practices

6. Conduct Cybersecurity Training
    - Training and reinforcement to create ***"culture of privacy"***: C-Suite/Manager, Employees
7. Monitor Network Traffic for Anomalies
    - Purchase the tools, establish the baseline, and perform regular log analyses
    - Don't Ignore the Ghost in the Machine
8. Have an Incident Response Plan in Place
    - Establish an Incident Response Team
    - Have a Playbook and Practice!
9. Perform Regular Security Audits
    - Internal and External auditors
    - Implement Continuous Monitoring
10. Stay Informed
    - Cybersecurity champion & open communication to management
    - Latest threats and trends