NAVEX™

Vendor Risk 2022: How to Boost Cyber Resilience in Your Supply Chain

- Peter Gregory, Senior Director, Cyber GRC, GCI

About the Presenter

Peter Gregory

Senior Director, Cyber GRC @ GCI Communications | pgregory@gci.com

Peter Gregory is the Senior Director, Cyber GRC at GCI. He is responsible for the oversight of cybersecurity policy, cyber risk management, compliance, privacy, third-party risk management, business continuity and disaster recovery, crisis management, and information governance. Peter holds a CISA, CISM, CRISC, CDPSE, CIPM, CISSP, DRCE, and CCSK. He is the author of over 40 books on security and privacy. Peter serves on advisory boards for cybersecurity continuing education at University of Washington and University of South Florida. He is a member of InfraGard, FBINCA Alumni Association, CyberEdBoard, Forbes Technology Council.

Disclaimer: The content and opinions herein do not necessarily represent the positions, strategies, or opinions of NAVEX, my current employer, or any previous employer.

Survey Question

Which of the following best reflects your current and near-term responsibilities to cybersecurity initiatives at your organization?

a) We are learning more about cybersecurity initiatives and I would like to speak to an expert for guidance

b) It is not my area of responsibility, but my organization is focused on this and we'd like to speak to an expert

c) It is not my area of responsibility, but I have been asked to contribute in efforts relating to cybersecurity initiatives

d) I am responsible for some/all cybersecurity initiatives and am interested in educating myself more

Agenda

- Introduction
- Ransomware Trends and Statistics
- Steps to Prevent Attacks
- Protecting Against Ransomware
- Supply Chain Attacks
- Third Party Risk Management
- Q&A

Ransomware

What is a Ransomware Attack?

- An attack on an organization's systems where the attacker encrypts business information, making it unavailable.
- Only the attacker has the decryption key, and demands a ransom in exchange for the decryption key.
- Victims are usually required to make the ransom payment using a cryptocurrency, which is difficult to trace to a real person.

Ransomware Attacks on the Rise

- Suspected ransomware payments nearly doubled in 2021
- Increased vulnerability due to remote and hybrid work
- BYOD and IoT expand the attack surface
- Greater sophistication with ransomware technology
- Attacks on third parties give access to other larger organization’s information

NAVEX™

More About Ransomware Attacks

- About half of organizations that pay the ransom are able to recover their data using the encryption key.
- More recent ransomware attacks also include a threat to publish business data, which may lead to reputational damage.
- Paying ransoms may be unlawful if the attacker is a terrorist organization or located in an embargo country.

NAVEX™

How Do Ransomware Attacks Occur?

- Phishing
  - malicious attachment
  - malicious website
- Watering Hole Attack
- Direct attack on a targeted system
- USB drop
- Supply chain

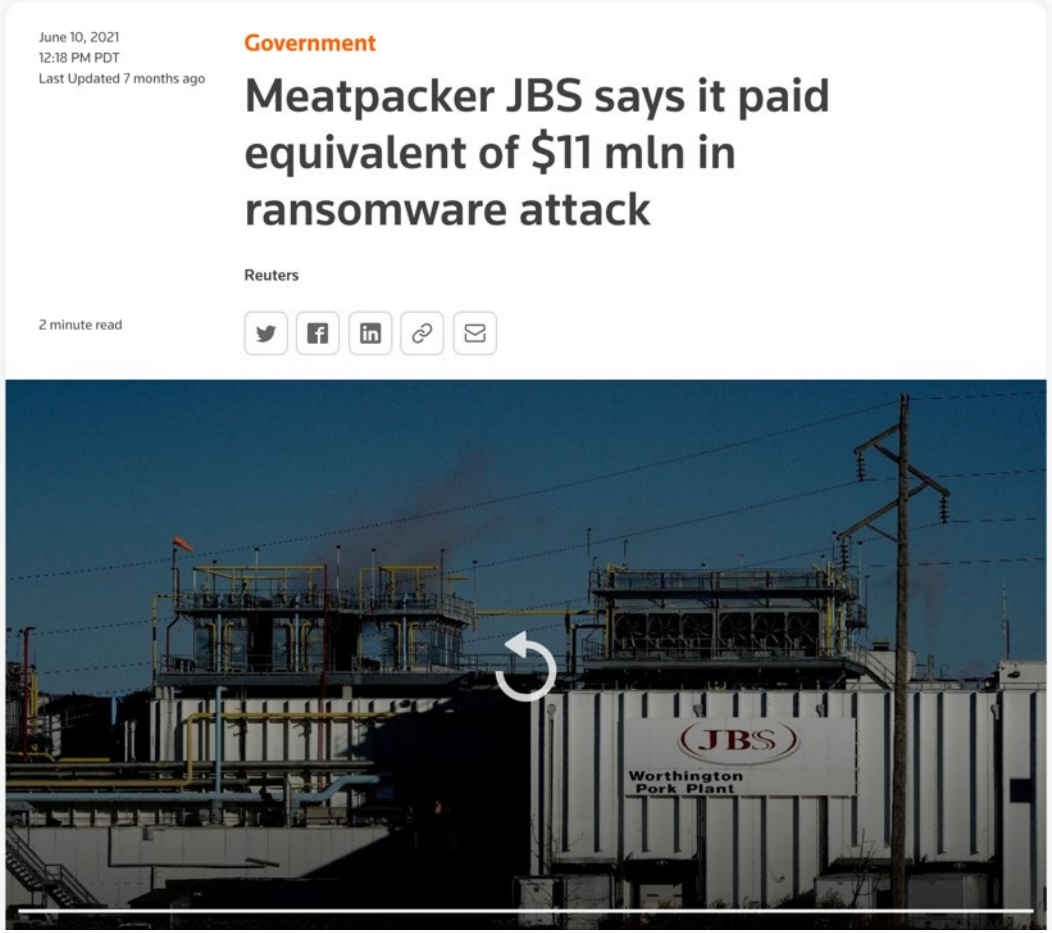
Ransomware Attack Statistics

37% of global organizations were victims in the last year

82% of companies give highly privileged roles and access to vendors

70% of companies anticipate being remote or hybrid moving forward, increasing devices with access and complexity of securely managing them

Ransomware Attacks in the News



June 10, 2021
12:18 PM PDT
Last Updated 7 months ago

Government

Meatpacker JBS says it paid equivalent of $11 mln in ransomware attack

Reuters

2 minute read

image from Reuters

- Kasaya – an IT infrastructure management service provider. 1,000+ businesses affected. $70M ransom demanded.
- Quanta – a major supplier to Apple, Inc. Product blueprints held for ransom, demanding $50M.
- JBS – a major meat processing company. All U.S. and Australia operations halted. $11M ransom demanded and paid.
- …there are thousands more like this.

Protecting Against Ransomware

- Hardware / software inventory
- Patching and secure configuration
- Security awareness training
- Spam filtering
- Web content protection
- Intrusion prevention systems
- Security incident response planning
- Backups of critical data
- Test and practice!

Addressing a Ransomware Attack

- Ransom payment
- Disclosure to law enforcement, business partners, customers, regulators
- Attorney-client privilege
- Breach investigation service
- Cyber incident insurance

Supply Chain Attacks

What is a Supply Chain Attack?

- An attack on an organization’s key supplier of products or services.
- Attacker disrupts or alters supplier operations or steals supplier data (which may be your organization’s data).
- An attack can disrupt your own organization's operations, or compromise the confidentiality, integrity, or availability of critical or sensitive data.
- Despite that the attack was out of your control, you still bear responsibility: you selected the supplier and should have performed due diligence.

NAVEX™

Supply Chain Attacks in the News

- Solar Winds – intruders planted malware the software distribution system, thereby infecting thousands of customer organizations.
- Log4j – intruders discovered a critical vulnerability in this software that is used in thousands of software products.
- RSA – intruders stole multi-function authentication secrets and used them to attempt to break into DoD organizations.
- …there are more like this.

Supply chain compromise exploits the trust between the supplier and its customer.

Supply Chain / Third-Party Risk Management

- Third-party risk is YOUR risk
- Perform due diligence when entering into business with a supplier
- Evaluate third-party risk levels and audit regularly
- Follow up on audit findings and respond promptly

NAVEX™

Where to Begin With Third-Party Risk Management

- Centralize your Third Parties
- Manage Entire Vendor Lifecycle and Measure Performance
- Conduct Due Diligence by Collaborating with Internal Stakeholders
- Automated Scoring of Risk Assessments from Third Parties
- Track Findings and Corrective Action Plans
- Leverage Reports & Dashboards to Drive Decisions
- Identify and Respond to Risks
- Integrate your Data to Gain a 360 Degree View of Risk

Supply Chain Risk Management vs Third Party Risk Management

- For our discussion, consider these as synonymous.
- The differences are subtle, but the concepts are the same: identify and manage risks associated with suppliers, vendors, and other external organizations that are a part of your organization's business.

Monitoring Third-Parties After Onboarding

- Relationship management versus risk monitoring
- Developing KRIs and risk thresholds
- Risk monitoring tools
- Escalation and exceptions
- Aggregated risk reporting
- Concentration risk

image from christiaanbrinkhoff.com

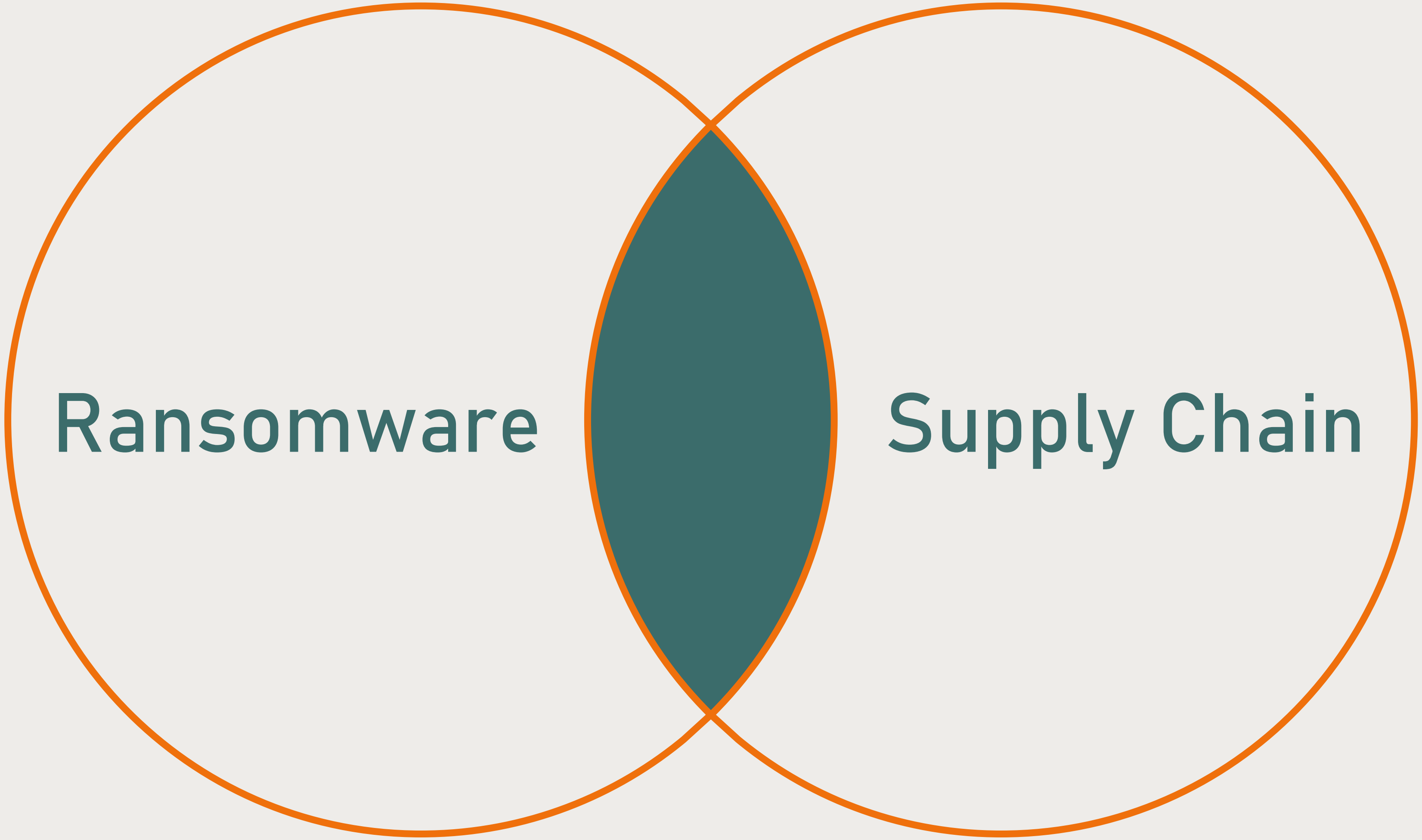
Challenges to Effective Third-Party Risk Management

- Increasingly sophisticated and numerous attacks
- Maintaining compliance with an increasing number of regulations and avoiding fines
- Accounting for all third parties and ensuring they don’t expose you to data breach or supply chain risk
- Meeting your customers’ contractual requirements
- Scrutiny from the board and executives
- Gaining organizational buy-in
- Constrained resources and headcount

Ransomware Attack at a Third Party

Risks:

- Disruption to your operations
- Data loss
- Data exposure
- Financial duress
- Reputation damage



The NAVEX IRM Advantage

Gartner named NAVEX a leader in the latest IT Risk Magic Quadrant report.

If you're interested in a deeper assessment of how NAVEX IRM can help your organization mitigate risks like ransomware, please check the box in the closing survey and we'll be in touch.

Thank you.

NAVEX™