June 14, 2022

Cybersecurity & the Supply Chain: Top Tips to Mitigate Your IT Risk

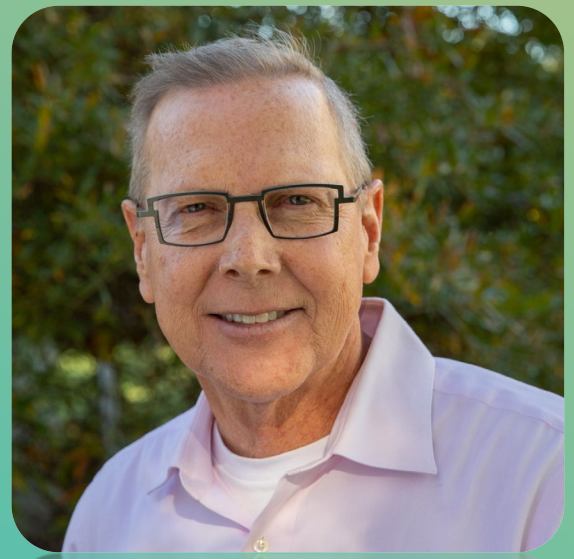
AHFA

Tom MacKenzie

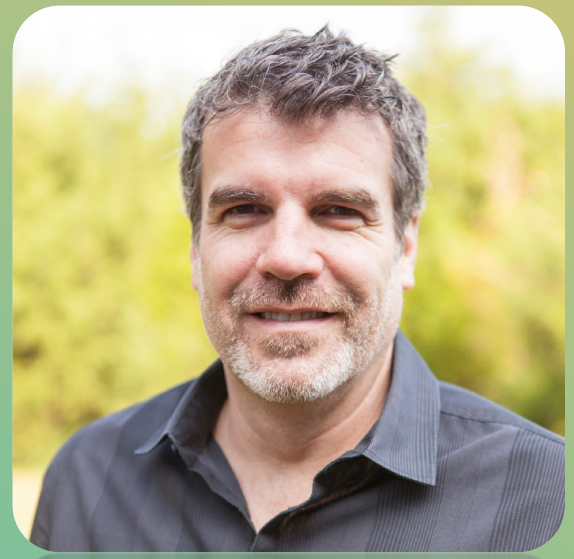
Greg Michalek

Steve Wujek

Panelists



Tom MacKenzie
Security Compliance and Privacy, Co-Lead
TCDI



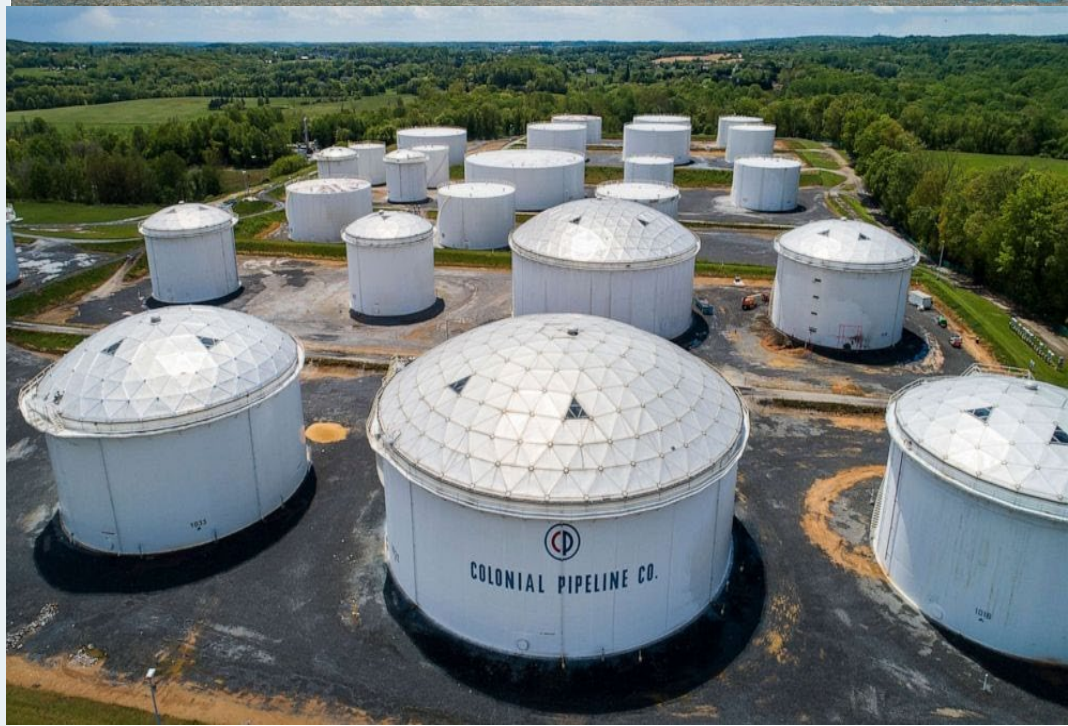
Steve Wujek
Senior Network & Cybersecurity Engineer
TCDI

Ransomware attack cost Expeditors $60m in remediation, lost business

192 Days on Average
for transportation companies to detect a data breach. It takes another 60 days to contain it.

186% Increase
in weekly ransomware attacks against the transportation industry.

1 Month of Disruption
can be expected every 3.7 years for logistics firms.



But I Have Cyber Insurance…

Sneak Peak Into the Future of Cyber Insurance

Capacity Decreasing

Capacity for cyber insurance is decreasing while demand is increasing, resulting in skyrocketing premiums

Premiums Increasing

27.5% increase in cyber premium price in the first quarter of 2022 – expectations are that premiums will double in the near future

Requirements Increasing

Carriers are requiring more from companies in order to be approved for cyber insurance

Lloyd's of London

Discouraging syndicates from providing cyber insurance

Published contractual language excluding coverage for cyber war and operation activities

But I Have Cyber Insurance…

Why are Cyber Insurance Premiums Skyrocketing?

Cyber-Attacks are Happening More Frequently

Ransomware Demands are Increasing

Inability to Manage Supply Chain Partner Risk

Lack of Cyber Hygiene / Basics

Complexities Associated with the Work From Home Movement

Cyber Insurance Trends

Implement Multifactor Authentication (MFA)

- Most insurance companies will deny claims if MFA is not enabled
- Easy to implement and difficult to bypass
- Should be implemented on backups, remote access, VPN logins, email accounts, and privileged / IT accounts on network domains

End-of-Life Software

- Operating systems or software that are no longer supported and will not receive security updates or patches for new vulnerabilities
- Must have a phase in and phase out plan before transitioning hardware or software

Zero-Trust (Not Just a Buzzword)

- Only allow permissions to systems and data necessary for to perform the duties for that role

Intrusion Detection System (IPS)

- Create a baseline to better detect anomalies
- Have a process in place to escalate events to incidents and incidents to breaches

Real-World Cyber Threats

Some Things Never Change…

Malware (Ransomware)

- Deny access to critical components of a network
- Goal is to steal information and render systems inoperable

Phishing / Social Engineering

- Most common method to distribute malware
- 2.9% of employees still click on phishing emails – unchanged since 2008
  - 50 Employees = 1.5 clicks
  - 100 Employees = 2.9 clicks
  - 250 Employees = 7.25 clicks
  - 500 Employees = 14.5 clicks
  - 1,000 Employees = 29 clicks

Real-World Cyber Threats

Most Common Threats Resulting in a Malicious Data Breaches

Phishing, Business Email Compromise (BEC), and Compromised Credentials

Cloud and Network Misconfiguration

Third-Party Software Vulnerability

Ransomware

Malicious Insiders

Supply Chain Attacks

Vectors:

- Software
- Hardware
- Remote Access

- Supply-chain attacks target distributors within the supply chain
- If successful, the hacker can infiltrate hundreds or thousands of client networks (e.g., SolarWinds)

Cyber Warfare Continues to Evolve

- Other nation states continue to peek around the corner – always looking for an advantage

- Malicious traffic originating from Russia increased by 3,000% since the beginning of the Russian – Ukrainian war

Top Cybersecurity Tips

Top Cybersecurity Tips

Independent Cybersecurity Assessment

tcdi

Top Cybersecurity Tips

Security Program with Strong Policies and Processes

tcdi

Top Cybersecurity Tips

Access Controls and Reviews

tcdi

Top Cybersecurity Tips

Incident Response Preparation

tcdi

Top Cybersecurity Tips

Employee Security Awareness Training

Top Cybersecurity Tips

Well Configured Firewall

tcdi

Top Cybersecurity Tips

Vulnerability and Penetration Testing

tcdi

Top Cybersecurity Tips

Antivirus and Malware Protection

tcdi

Top Cybersecurity Tips

Regular Backups

Backups

Move Offline and Test Regularly

Questions?

Tom MacKenzie
Security Compliance and Privacy, Co-Lead, TCDI
t_mackenzie@tcdi.com

Greg Michalek
Senior Director, Business Development, TCDI
g_michalek@tcdi.com

Steve Wujek
Senior Network & Cybersecurity Engineer, TCDI
s_wujek@tcdi.com