#RSAC

RSAConference2022

San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **LAW-M01**

Victims & Vectors: Mitigating Legal Risks of Supply Chain Attacks

MODERATOR: **Susan Booth Cassidy**
Partner,
Covington & Burling LLP

PANELISTS:

Chris Hale
Executive Director and
Associate General Counsel,
Raytheon Technologies

Matti Neustadt
Director, Evangelist, Privacy
and Cybersecurity,
NetApp

Jim Sfekas
Assistant General Counsel,
Microsoft

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

RSAConference2022

MODERATOR:

Susan Booth Cassidy

Partner – Covington & Burling LLP

PANELISTS:

Chris Hale

Executive Director and Associate General Counsel,
Raytheon Technologies

Matti Neustadt

Director, Evangelist, Privacy and Cybersecurity,
NetApp

Jim Sfekas

Assistant General Counsel, M365 Security, Compliance and
Management, Microsoft

Threat Landscape - Vectors of Attack

- Supply chain attacks are becoming more common and are showing up in new and unexpected ways
  - Compromising legitimate software through automatic updates: NotPetya, SolarWinds
  - Compromising cloud infrastructure providers: Okta compromise by Lapsus$
  - Compromising managed service providers: Kaseya compromised by REvil
  - Vulnerabilities in software components: log4j, Spring framework
  - Business email compromise of vendors
- Digital transformation is expanding the size and scope of the supply chain, increasing the threat surface
- Ransomware continues to evolve and is increasingly seen in human-operated attacks focused on enterprise networks, with the addition of data theft to the classic encryption scenario
- Nation state tensions increase risks of cyber intrusions
- Increased connectivity expands the attack surface available to bad actors

Threat Landscape - Government Response

Increased Emphasis Among Governments On Identifying And Protecting Critical Infrastructure

- Cyber Incident Reporting for Critical Infrastructure Act of 2022
- Proposed SEC cybersecurity disclosure rules
- EU Directive on Security of Network and Information Systems (NIS Directive)
- China’s Cybersecurity Law and Data Security Law

Increased Legislation, Regulation, And Executive Orders From The US Government Tightening Oversight On Supply Chains

- May 2021 Cybersecurity Executive Order
- DoD’s pending Cybersecurity Maturity Model Certification regime
- NIST guidance on software labeling and SCRM practices
- DoJ Cyber Fraud Initiative

Threat Landscape - Commercial Market Response

Increased Reliance On Service Providers To Stay Ahead Of The Threats (Especially For Smaller Businesses)

Higher Expectations On Shorter Time Frames For Reporting

Evolution In Tools (AI And Machine Learning)

Increased Scrutiny Of Suppliers

Enhanced Training Of Employees

Legal Implications – Basic Concepts

Standard of Care

- Definitions and standards vary across jurisdictions, with some areas wholly undefined

Reputational harm

Impact on business opportunities

Contract breaches

Regulatory obligation

- Patchwork of evolving safeguarding and disclosur requirements

Mitigation

- Organizing cross functional groups to analyze and address supply chain cybersecurity risk
- Addressing supply chain incidents in your cyber incident response plan; running realistic table top exercises to test internal decision-making
- Clearly designating who is in charge of cybersecurity versus information technology

- Knowing who your vendors/suppliers are—particularly those with connectivity into your systems
- Conducting risk-informed data identification and analysis of data flows to vendors; clarifying who holds this responsibility when working with service providers; understand where crown jewels are stored and processed

Mitigation

- Ensuring IT and InfoSec professionals understand the sensitivity of data in the systems they are managing
- Conducting cybersecurity assessments on key suppliers
- Evaluating sufficiency of contractual requirements on suppliers
- Assessing adequacy of insurance coverage commensurate with the risks to the company
- Develop early warning programs for supplier breaches, such as internet or dark web monitoring for your data being spilled by others

Questions?