ALSTON & BIRD

Cyber Threats and Cyber Crime: What Every In-house Counsel Needs to Know

September 1, 2021

ALSTON & BIRD

Welcome and Introductions

Kim Peretti

- Kim Peretti is co-leader of Alston & Bird's Privacy, Cyber & Data Strategy Team.
- 22 years as information security professional and lawyer
- Manages technical cyber investigations, assists in responding to data security-related regulator inquiries, and advises boards and senior executives in matters of cybersecurity and cyber risk.
- Former director of PwC's cyber forensic services group and a former senior litigator for the Department of Justice's Computer Crime and Intellectual Property Section.
- Certified Information Systems Security Professional (CISSP).

Session Objectives

1. Discuss the current state of ransomware attacks and Government's response including executive and legislative action.	2. Consider guidance from regulators on best practices for defending against a ransomware attack and discuss counsel's role.	3. Discuss the renewed focus on supply chain security and the Government's responses to recent attacks.

ALSTON & BIRD

Ransomware: an Overview and Recent Government Response

The Ransomware Threat Landscape

- Ransomware is a global problem.
- Ransomware attacks more than doubled from 2019 to 2020
- Attackers received an estimated $412 million in ransom payments last year.
- On average, it takes a company 287 days to recover from a ransomware attack, and *the average downtime whether or not you pay, is 19 days*.

What is a Ransomware Attack?

Usually, these are a targeted, human-operated attack rather than something purely automated.

The attacker establishes initial access usually through phishing, exploiting unsecure remote access protocols, or another known vulnerabilities.

Once they have a foothold, they usually engage in reconnaissance stealing credentials, escalating privileges, and moving laterally (i.e. moving to other systems) within the environment. Their goal is to identify critical systems, data stores, back-ups, and other assets.

Exfiltration and Encryption

Remember: Initial compromise can occur weeks or even months prior to ransomware deployment.

Double Extortion: Exfiltration and Encryption

The criminals first steal or exfiltrate your data.

Then they use a scripted deployment of ransomware to encrypt the systems.

This gives them multiple points of leverage to pressure for a ransom payment.

Pay us in order to decrypt your systems.

Pay us or we will publicly leak your data on the dark web or sell it to the highest bidder.

They may use custom malware that encrypts and spreads throughout the environment. They may also just use off the shelf tools like Bitlocker or the built-in encryption capabilities in Windows.

Paying the Ransom Is a Challenge

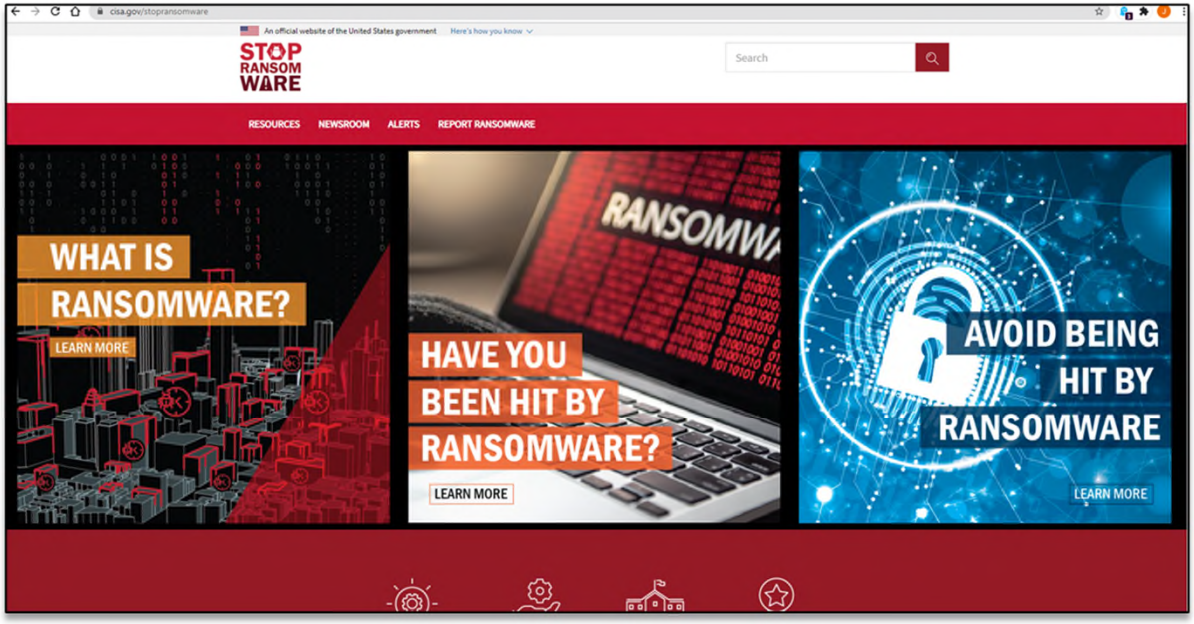
- The Washington Post reports that average payments are between $100k-200k. But larger incidents on high profile targets have garnered payments in the millions of dollars.
- Recent guidance from Office of Foreign Asset Controls (OFAC) and the United States Treasury Department reiterates that ransom payments arising from ransomware raise significant sanctions compliance issues.
- OFAC emphasizes the importance of working with law enforcement as a potential mitigating factor in the event that a ransom payment is later determined to raise specific sanctions-related concerns.

The Government Has Responded By Providing New Resources and Education

After the Colonial Pipeline attack, the Department of Justice, the Department of Homeland Security, and other federal partners launched StopRansomware.gov.

This is a collaborative effort across the federal government and is the first joint website created to help private and public organizations mitigate their ransomware risk.

The site the first central hub consolidating ransomware resources from all federal government agencies. Its goal is to reduce the fragmentation of resources by integrating federal ransomware resources into a single platform that includes clear guidance on how to report attacks, and the latest ransomware-related alerts and threats from all participating agencies.



Congress and Others Pushing For Increased Reporting Requirements

On July 27, 2021, the United States Senate Committee on the Judiciary held a hearing titled America Under Cyber Siege: Preventing And Responding To Ransomware Attacks.

The Department of Justice, FBI, Cybersecurity and Infrastructure Security Agency, and the Secret Service all testified and recommended some level of increased reporting of ransomware incidents from the private sector to the government.

They also encouraged insurance providers to stop reimbursing for ransom payments.

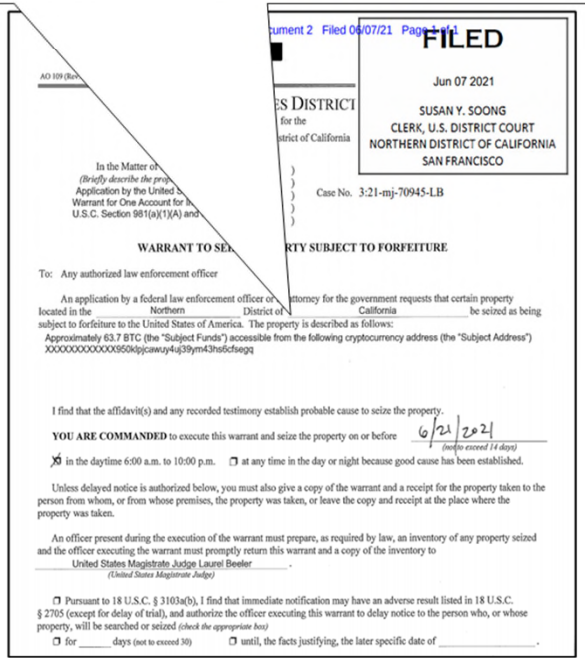
The Government is Following the Money

After Colonial Pipeline paid its ransom in May 2021, the Government investigated the cryptocurrency trail and ultimately seized 63.7 bitcoins (approx. value $2.3 million) tied to the threat actors.

In the Government's view, "following the money remains one of the most basic, yet powerful tools we have."

It still remains unclear *how* the FBI obtained the private key.

34. The private key for the Subject Address is in the possession of the FBI in the Northern District of California.



FILED
Jun 07 2021
SUSAN Y. SOONG
CLERK, U.S. DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO

Case No. 3:21-mj-70945-LB

WARRANT TO SEIZE PROPERTY SUBJECT TO FORFEITURE

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or attorney for the government requests that certain property located in the Northern District of California be seized as being subject to forfeiture to the United States of America. The property is described as follows:
Approximately 63.7 BTC (the "Subject Funds") accessible from the following cryptocurrency address (the "Subject Address")
XXXXXXXXXXXX950kdpjcawuy4uj39ym43hs6cfsegq

I find that the affidavit(s) and any recorded testimony establish probable cause to seize the property.

YOU ARE COMMANDED to execute this warrant and seize the property on or before 6/21/2021 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must also give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

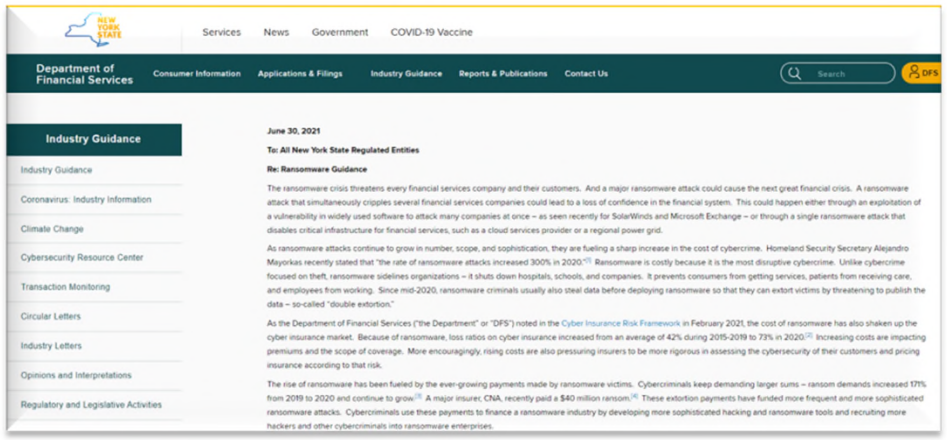
An officer present during the execution of the warrant must prepare, as required by law, an inventory of any property seized and the officer executing the warrant must promptly return this warrant and a copy of the inventory to United States Magistrate Judge Laurel Beeler (United States Magistrate Judge).

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)
☐ for _____ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of _____.

ALSTON & BIRD

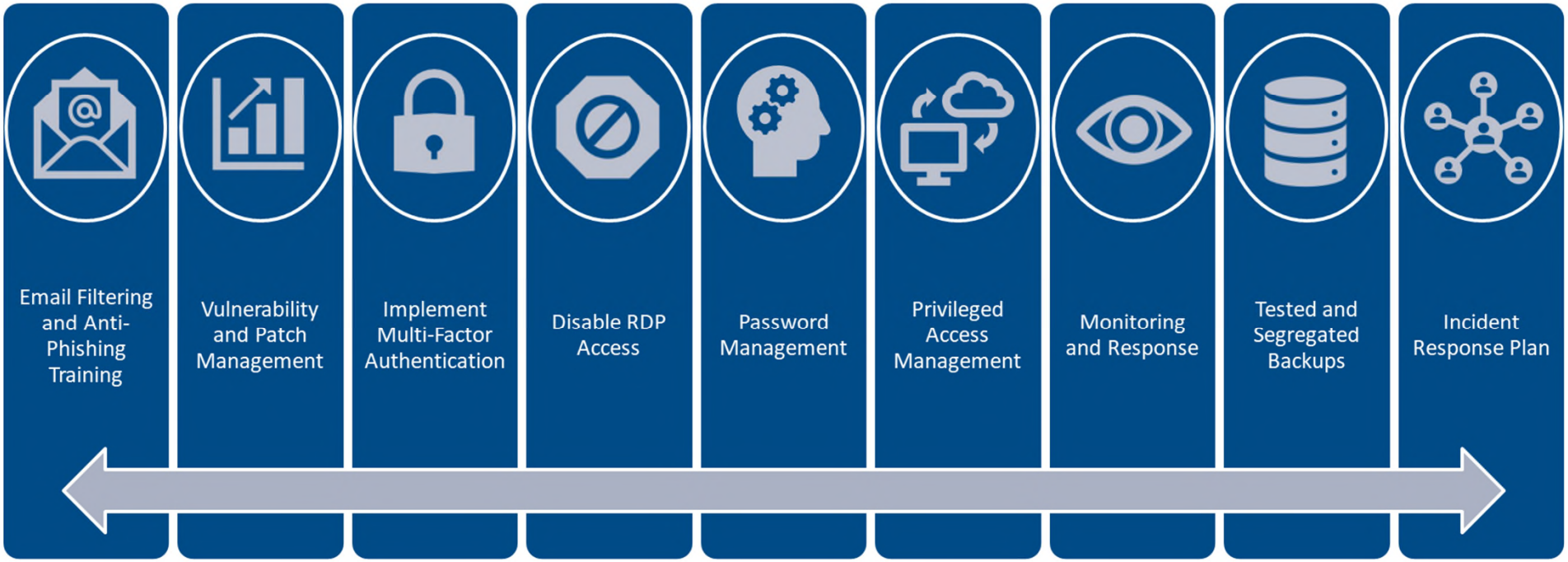
Ransomware: Regulators Identify Best Practices

Regulators Are Identifying Best Defensive Practices

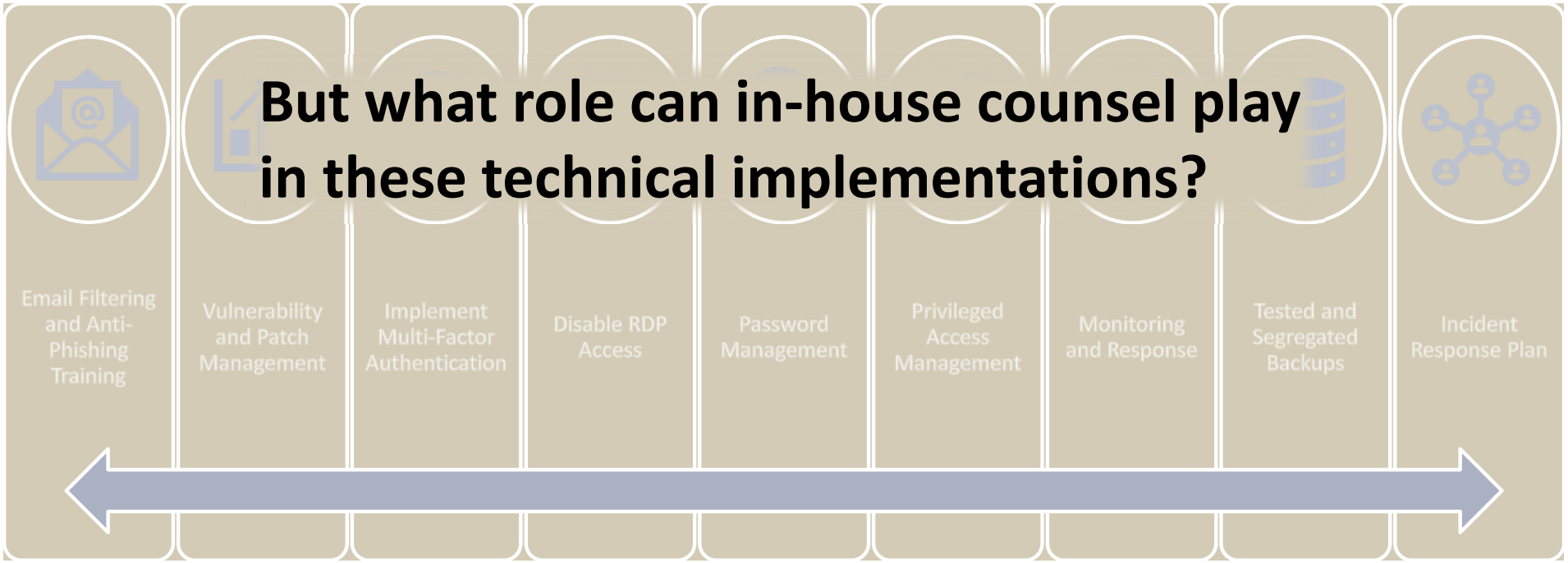


- In June 2021, the New York Department of Financial Services (NYDFS) published nine security controls that "when implemented together, significant reduce the risk of successful ransomware attack."

Regulators Are Identifying Best Defensive Practices



Regulators Are Identifying Best Defensive Practices

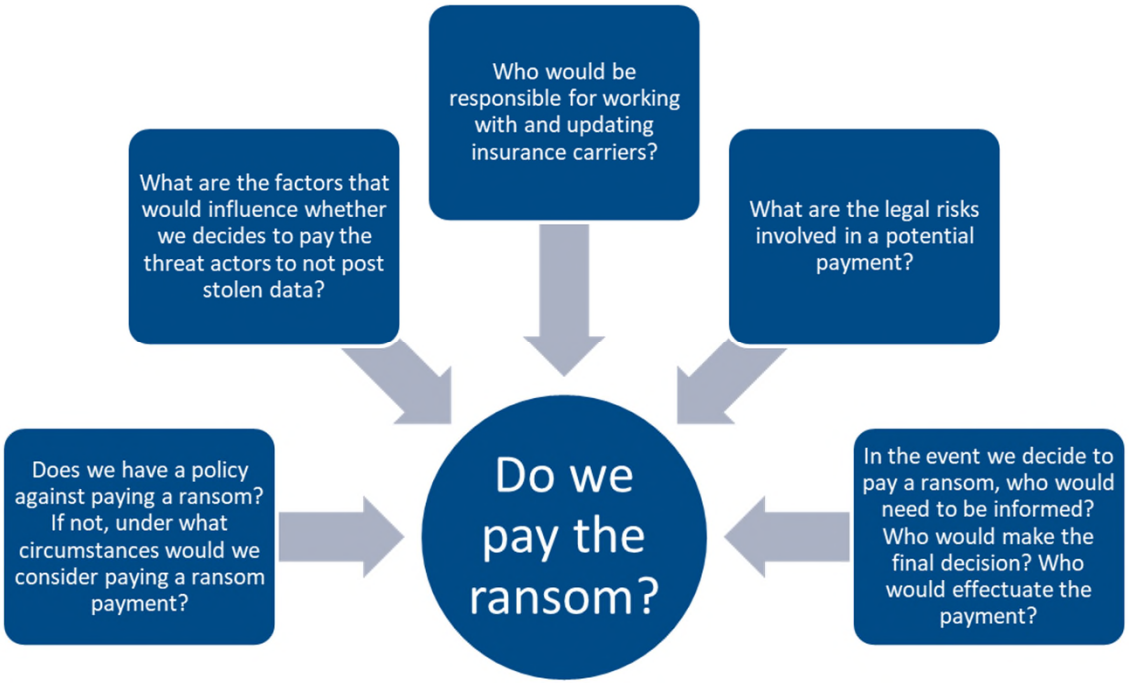


But what role can in-house counsel play in these technical implementations?

Ransomware Defense: Counsel's Role

- Initiate conversations with your technical teams; confirm these best practices are on their radar; and follow up at the audit/risk management level to confirm that the controls are implemented in a timely fashion.
- Take an active role in the training and engage any outside vendors under privilege.
- Build ransomware response into your incident response plan accounting for the special legal considerations in ransomware response.
- Test your plans at the operational and executive levels.

Paying a Ransom - Considerations



ALSTON & BIRD

Ransomware Response Best Practices

Four Parallel Workflows For Response Best Practices

Restoration

Inves

l

Communications

Restoration

Containment

Assess Systems, Data and Operational Impact

Develop a Restoration Plan

Restoration

Inves

l

Communications

Investigation

Engage a Forensic Vendor

Deploy Endpoint Protection and/or Forensic Data Collection Tools

Intelligence and Information Gathering

Review for Data Exfiltration

Restoration

Inves

Legal

Third-Party Intermediary

Law Enforcement/Insurance Notifications

Decide Whether to Pay the Ransom

Potentially Pay the Ransom

Determine Whether Other Notices Are Required

l

Communications

Restoration

Inves

l

Communications

Communications

Do You Need A Crisis Communications Firm?

Internal Communications

External Communications

Conduct Post-Incident Analysis

ROOT CAUSE ANALYSIS

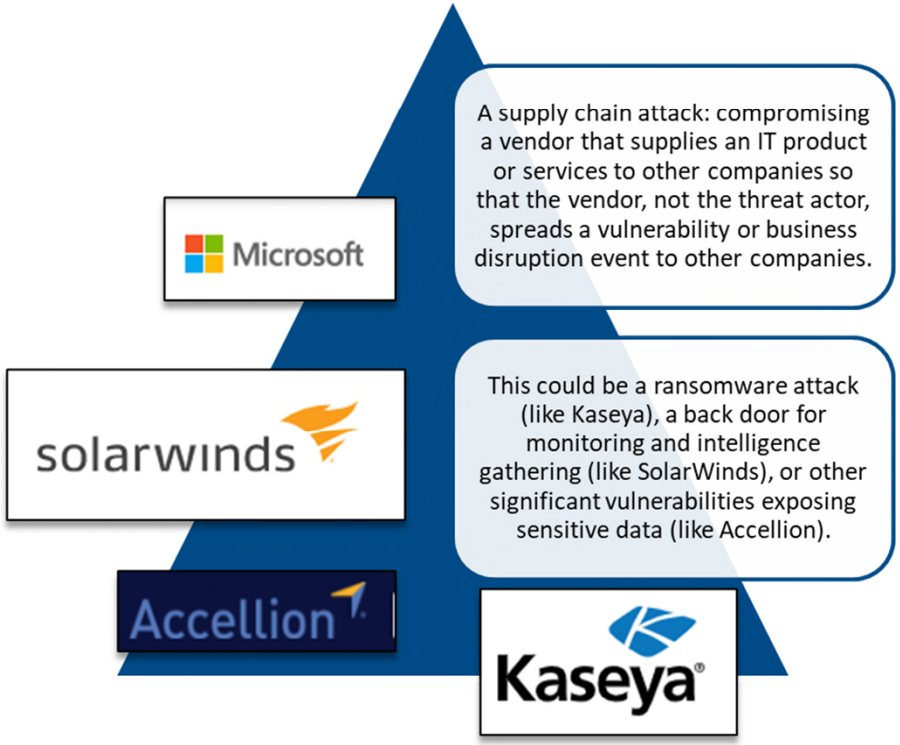
PROCESS IMPROVEMENTS

LESSONS LEARNED MEETING

ALSTON & BIRD

Supply Chain Security

Supply Chain Security is Under Attack



The Administration is Taking Action

December 14, 2020 – SolarWinds Attack Discovered

- Russian intelligence compromised the SolarWinds environment, then modified the build process and injected malicious code into SolarWinds' Orion software platform.
- Then, over 16,000 organizations downloaded the malicious update, leading to the known compromise of at least 9 federal agencies, Russian access to emails for multiple U.S. Attorney Offices, and the compromise of over 100 private sector companies.

Feb. 24, 2021 – Executive Order on America's Supply Chain

- Includes a 100-day review of the supply chains for certain vital products and a long-term review of supply chains in six different sectors of the U.S. economy, including the information and communications technology (ICT) industrial base.

April 15, 2021 – Sanctions announced against the Russian Government and private Russian entities for the SolarWinds attack.

- The Administration expressly links this activity to Russian intelligence actors.
- These sanctions are for cyber espionage activity – a new sanctions trigger in the cyber arena.

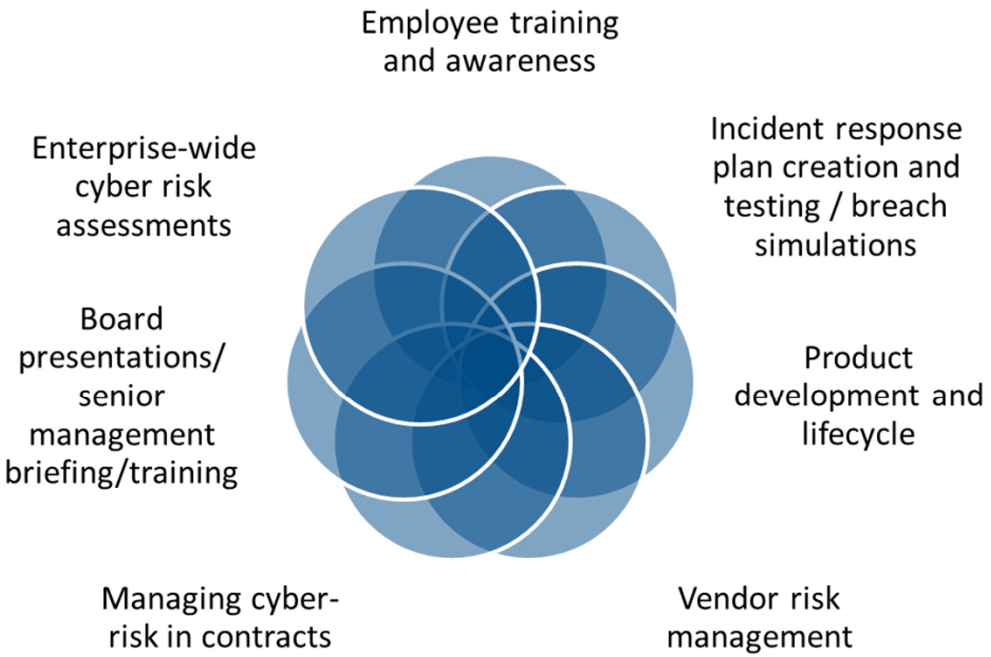
May 12, 2021 – Executive Order on Improving the Nation's Cybersecurity

- Signals increased reporting obligations for government contractors.
- Expands role for CISA In collecting and managing incident reporting information.
- Standardizing common cybersecurity contractual requirements across agencies.
- Includes new private sector recommendations for supply chain security.

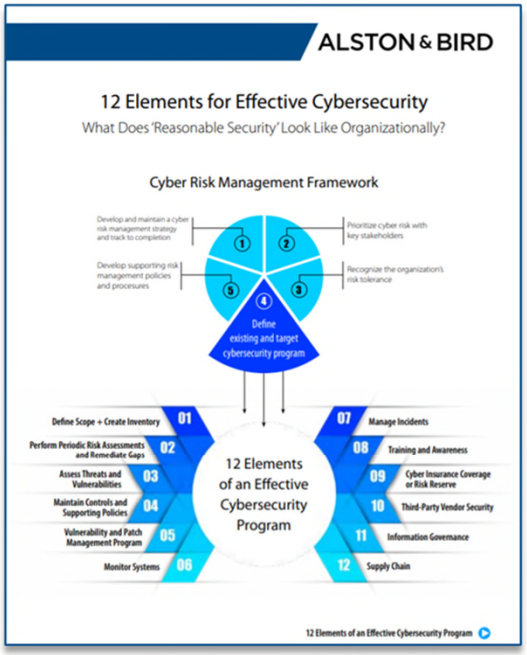
July 28, 2021 – National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems

- Directed to both public and private entities and envisions "collaboration."
- Hints at increased private sector reporting requirements.
- Identifies a need for baseline cybersecurity goals.
- NIST will play a role in crafting these baseline goals for critical infrastructure systems but it remains to be seen if these goals will become a standard for other industries as well.

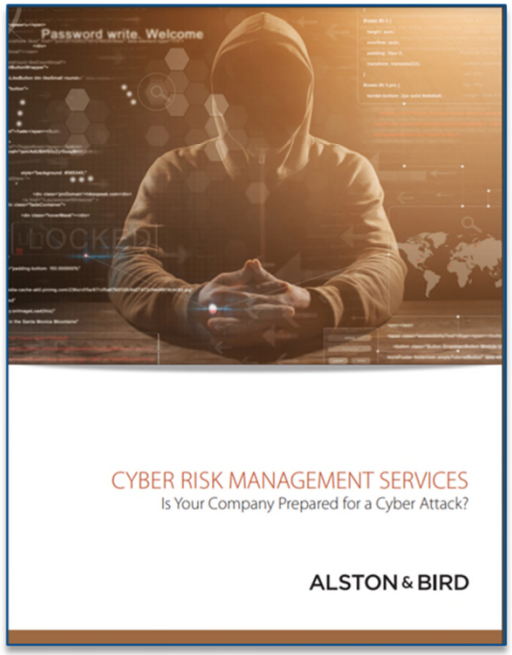
Cybersecurity Defense: Counsel's Role



Resources



https://www.alston.com/en/-/media/files/services/privacy/alstonbirdcoreareasforeffectivecybersecurity.pdf



https://www.alston.com/en/-/media/files/services/privacy/alstonbirdcyberriskmanagementservicesbrochure.pdf

ALSTON & BIRD

Questions and Closing