THE EVOLUTION OF THE SUPPLY CHAIN AND CYBERSECURITY:

WHAT THE NEXT GENERATION OF PRACTITIONERS NEEDS TO KNOW

OCTOBER 6

CELERIUM®

PRESENTED BY

CELERIUM®

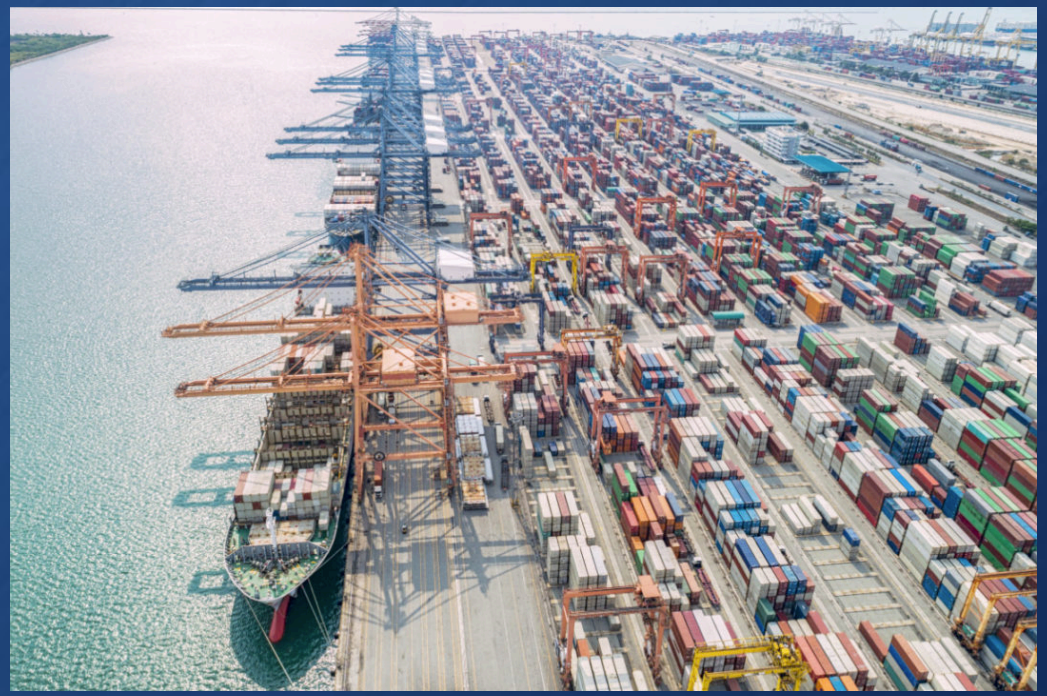
CYBER DEFENSE NETWORK

Agenda

1. Supply Chain Crisis
2. Escalating Ransomware Threat
3. Strategic Resilience and Three Key Dimensions for Business Executives
4. Summary and Observations for Education, Training, and Research

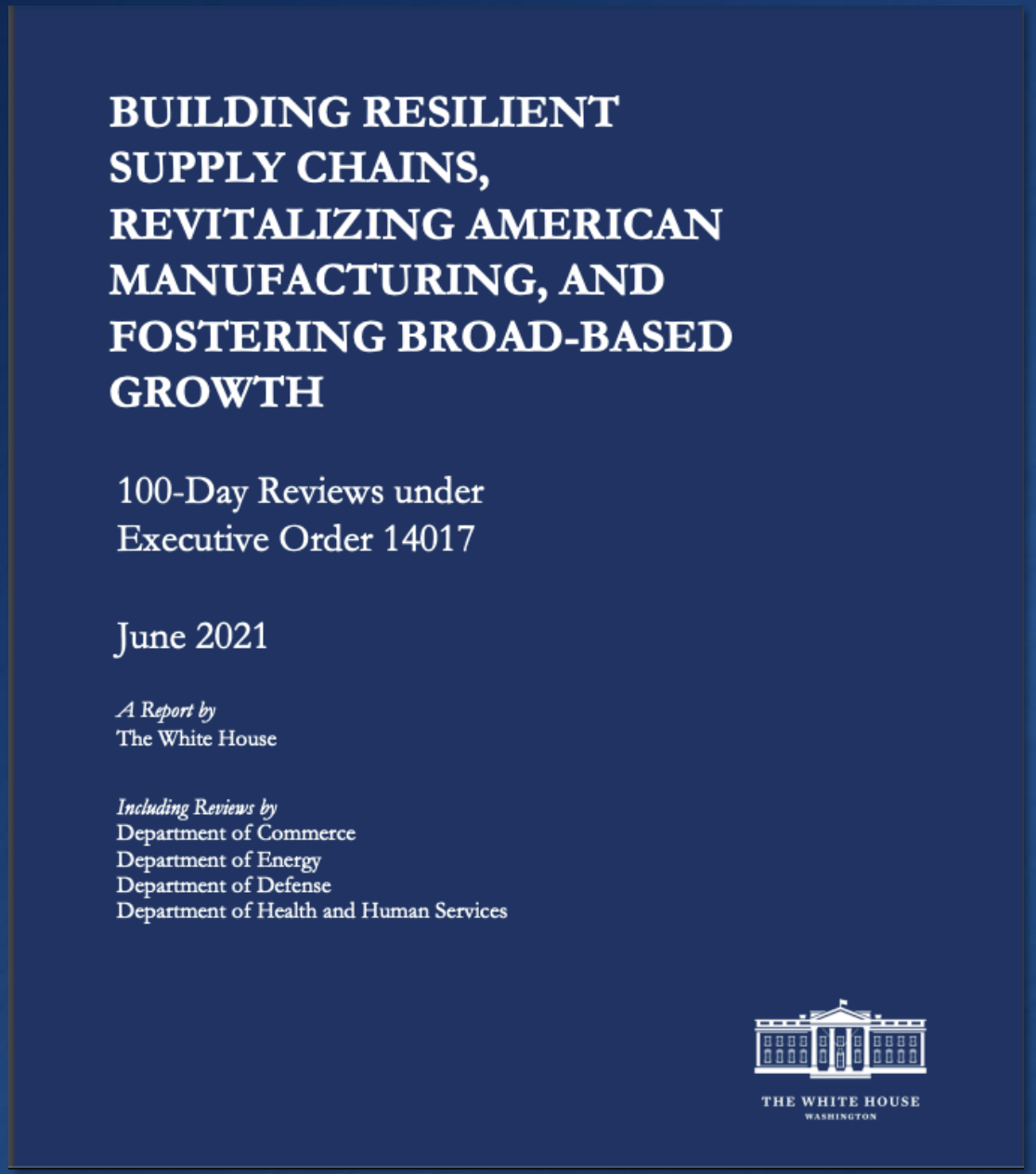
1. Supply Chain Crisis

- The COVID-19 pandemic has posed significant challenges for supply chains globally.



- Global shipping: Warehouse congestion developed at international ports that then spread to railroads and inland rail terminals, exasperating the trucking and chassis shortage that was already in place.

- Almost every industry affected from chemicals, retail, automotive, raw materials, electronics and all major economies (US, China, Germany, Russia, UK, and Australia)



Immediate Sector Focus

- Semiconductors
- Large Capability Batteries
- Critical Minerals & Materials
- Pharmaceuticals and APIs

Various Education and Training Recommendations Identified.

- Strengthen domestic production requirements in federal grants for science and climate R&D.
- Investment in diverse pipeline of engineers and computer scientists
- References made to America's Strategy for STEM Education

ONLY references to SCRM and Cybersecurity

House Armed Service Committee Defense Critical Supply Task Force July 22, 2021

“Throughout the pandemic, U.S. adversaries like China weaponized supply chain vulnerabilities in a way that threatened Americans’ health and security. Our Defense Critical Supply Chain faces similar weaknesses that, if exploited, would impair our ability to compete with our adversaries and respond to crises,” said Representative Mike Gallagher (R-Wis.).

- DOD must treat supply chain security as a defense strategic priority
- DOD must have visibility on the defense supply chain to understand its vulnerabilities and develop risk mitigation strategies

Terminology Problem: “Supply Chain” threats

I) Physical Components

- Electronic components – chips, circuit board
- Machine equipment or parts

II) Industry – Aviation, Maritime, Chemical

- DoD CMMC

III) Prime Contractor and Suppliers

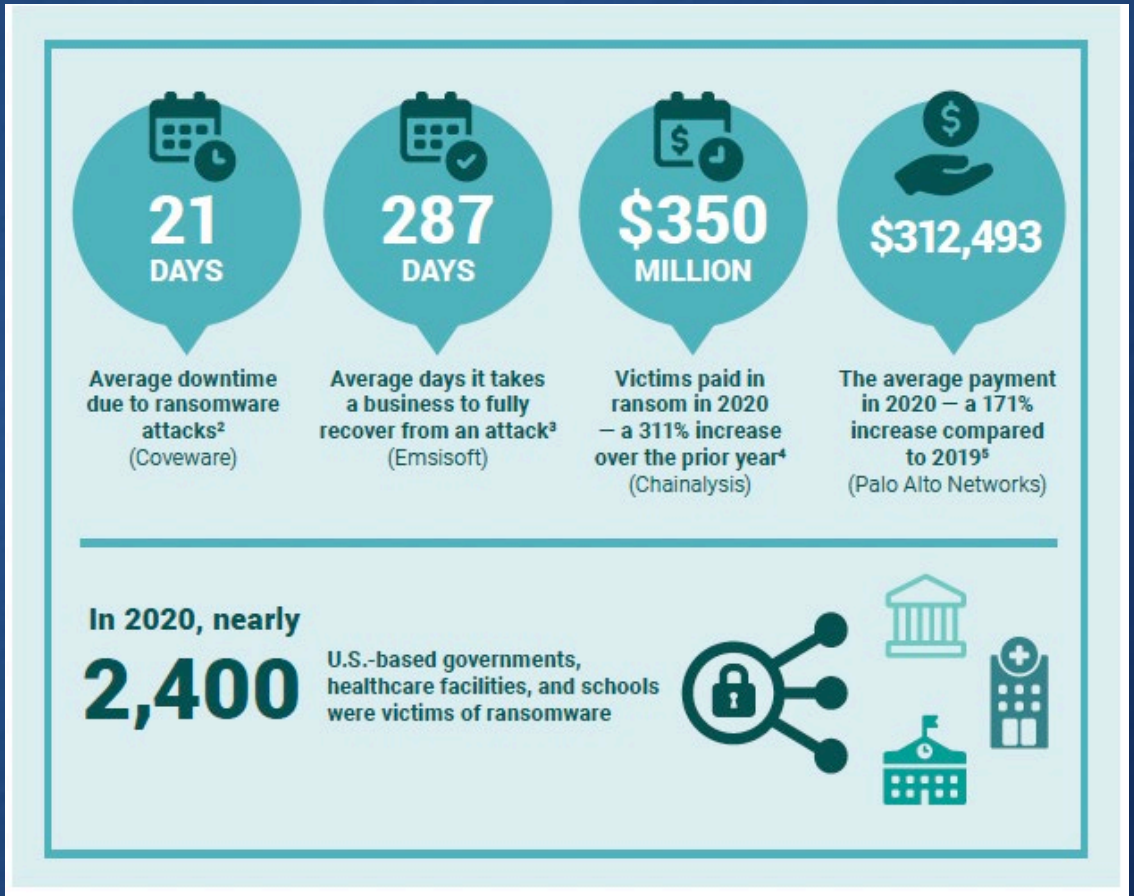
IV) Commercial off the Shelf (COTS)

- Application software – Maersk Shipping
- Update service – SolarWinds

solarwinds

2. Escalating Ransomware Threats

- Acknowledged as a National Security Threat by DHS in April 2021
- Institute for Security + Technology
- Largest paid ransom in 2019: $4.5 million
- Largest paid ransom in 2020: $40 Million
- *TTPs growing in complexity equal to APT*
- *MULTIFACETED EXTORTION*



IST (2021). Combating Ransomware: A Comprehensive Framework for Action

Multifaceted Extortion

1. Multifaceted extortion is the number one cybersecurity threat to organizations world-wide

2. The impact may be significant, as it combines business disruption, data theft, public shaming and other harmful extortion techniques

3. Implementing resilient system backups addresses part of the problem, but more needs to be done to mitigate the risk and impact of mutlifaceted extortion attacks

4. Mutlifaceted extortion typically requires the victim to disclose the breach. Victims often lose control of this because threat actors may disclose the incident according to their own schedule

5. Multifaceted extortion payment demands usually fall within the 6, 7 and 8-figure ranges

Mandiant (2021)

Recent Media Updates

- **Sept 21: US Treasury Department advisory on ransomware**

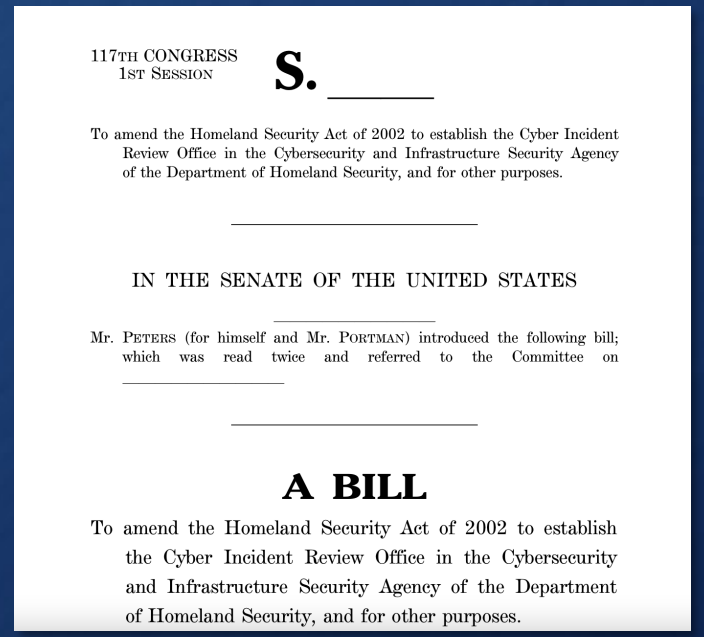
DEPARTMENT OF THE TREASURY
WASHINGTON, D.C.

Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments[1]

Date: September 21, 2021

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) is issuing this updated advisory to highlight the sanctions risks associated with ransomware payments in connection with malicious cyber-enabled activities and the proactive steps companies can take to mitigate such risks, including actions that OFAC would consider to be "mitigating factors" in any related enforcement action.[2]

- **Sept 22: Artic Wolf Ransomware Survey Research of 1400 Sr. IT decision makers:**
  - 78% of C-suite members would be willing to pay a ransom.
  - 56% are willing to pay over $100k in order to resume business operations.
  - 15% have confidence in the government's ability to be successful



117TH CONGRESS
1ST SESSION

S. _____

To amend the Homeland Security Act of 2002 to establish the Cyber Incident Review Office in the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. PETERS (for himself and Mr. PORTMAN) introduced the following bill; which was read twice and referred to the Committee on

A BILL

To amend the Homeland Security Act of 2002 to establish the Cyber Incident Review Office in the Cybersecurity and Infrastructure Security Agency of the Department of Homeland Security, and for other purposes.

- **October 1: Cyber Incident Reporting Act (pending)**

3. Supply Chain Strategic Resilience

1) From General Cybersecurity to Specific Ransomware Focus

2) From Internal Ransomware Defense to External Supply Chain Ransomware Defense

3) From Supply Chain Risk Assessment to IMPROVING Supplier Ransomware Readiness

4. Summary and Observations for Education, Training, and Research

- Ransomware Readiness
- Supply chain crisis and the ransomware threat support the need for sector-driven reporting and analysis
- Cyber threat sharing research
- Acknowledgement of educational progress in the past 25 years

Q&A

WEBSITE:
CELERIUM.COM

CONTACT US:
INFO@CELERIUM.COM