Cybersecurity Awareness: A 3-Step Approach to Preparedness and Operational Resiliency

PRESENTER THOMAS BYRD

Disclaimer

- Disclaimer: The opinions expressed in this presentation and on the following slides are solely those of the presenter and not necessarily those of my employer.

Introduction

- The challenges created by accelerating technological innovation have reached new levels of complexity and scale.
- Detection, mitigation, and management should be core components of your cybersecurity pedagogy.
- Governments, businesses, and academic organizations all face growing security threats against their infrastructure making it is imperative that organizations integrate best practices into business and management strategies.
- Following a multifaceted approach to detection, mitigation and management cybersecurity preparedness and operational resiliency can be achieved.

Introduction

- By following a multi-faceted approach to detection, mitigation and management, cybersecurity preparedness and operational resiliency can be achieved. Elements include:
  - Promote (Technology Lifecycle) Cyber Hygiene Initiatives
  - Promote Workforce Awareness of Known and Emerging Cyber Threats
  - Improve the ability to identify, acquire and manage vendors, risk, and performance

Definitions

- Cyber Hygiene: The Carnegie-Mellon University definition is a set of practices for managing the most common and pervasive cybersecurity risks.

- Cybersecurity Management: The practices for designing, implementing and maturing the cybersecurity program to protect critical business information, processes and IT assets across the enterprise.

Definitions

- Organizational Resilience: The development of IT operations to address the risk to business service delivery in meeting organizational objectives.

- Security Awareness: As defined in the NIST Special Publication 800-50, Awareness is not training. The purpose of awareness presentations is to focus attention on security. Awareness presentations are intended to motivate individuals to recognize IT security concerns and respond accordingly.

- Reducing Human Risk: Implement practices to contribute to an ongoing education process.

Use Case:
Detection, mitigation, and management should be core components of your cybersecurity pedagogy.

Resources:

- U.S. Select Senate Hearing on Intelligence, ***Open Hearing: Hearing on the Hack of U.S. Networks by a Foreign Adversary.*** Date: February 23, 2021- 2:30pm https://www.intelligence.senate.gov/hearings/open-hearing-hearing-hack-us-networks-foreign-adversary

- U.S. Government Accountability Office (GAO). ***GAO-21-119SP, High-Risk Series: Dedicated Leadership Needed to Address Limited Progress in Most High-Risk Areas. Published:*** March 02, 2021. https://files.gao.gov/reports/GAO-21-119SP/index.html

- U.S. Government Accountability Office (GAO). ***GAO-17-768, Defense Supply Chain: DOD Needs Complete Information on Single Sources of Supply to Proactively Manage the Risks.*** Published: Sep 28, 2017. https://www.gao.gov/assets/gao-17-768.pdf

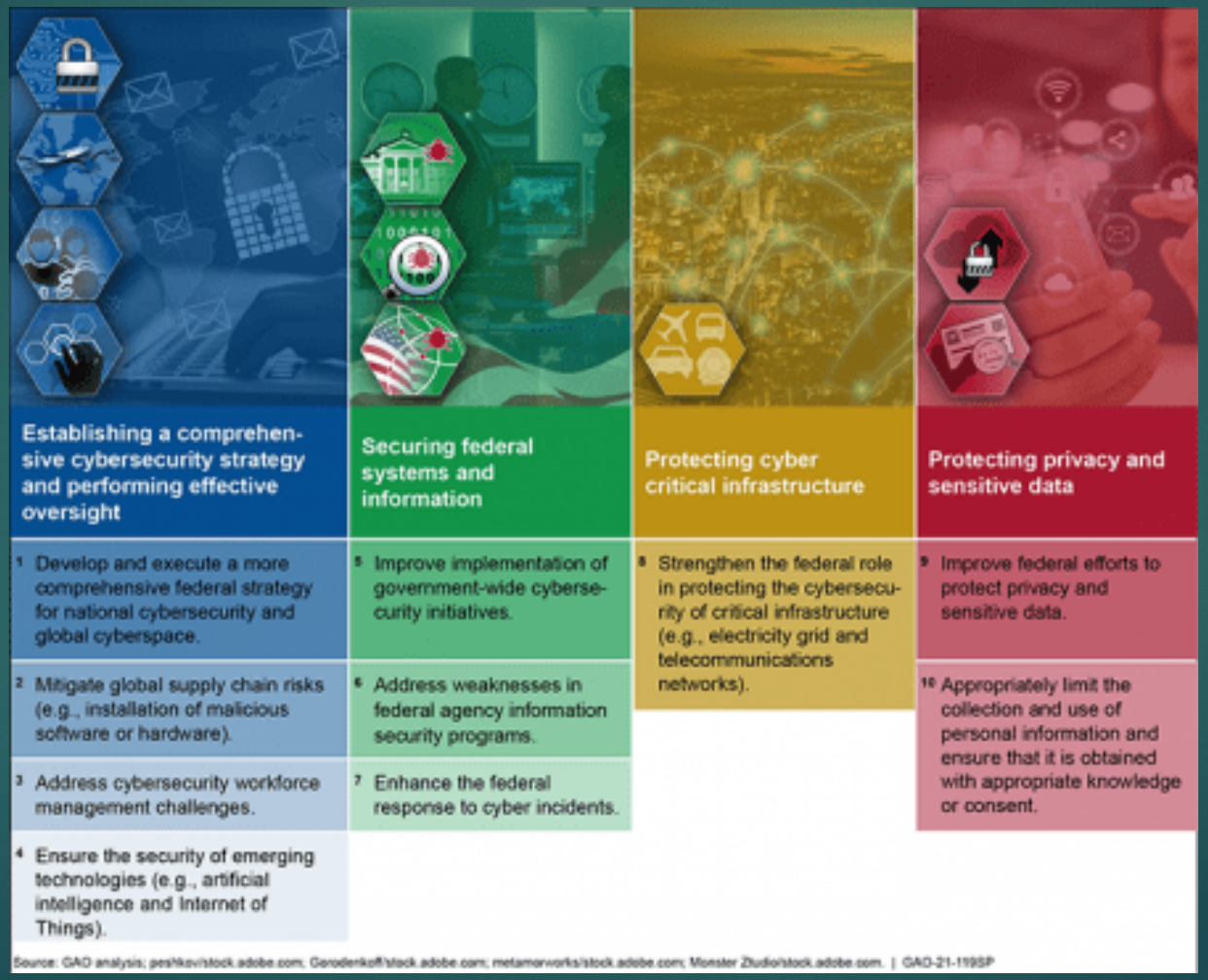
Scope of the Use Case Discussion

- Scope of todays analysis and discussion is limited to Cybersecurity Awareness and the associated impact of the SolarWinds implant that led to dozens of organizations being breached, and thousands more becoming vulnerable, and the fact that victim companies had no idea they had been compromised until they were notified by either law enforcement or business partners…

The Importance of what the GAO does

- The U.S. Government Accountability Office (GAO) prepares reports and testimonies on various topics. Requests for GAO reports must come from congressional committees, subcommittees, or members of Congress.
- Recipients include:
  - President/Vice President
  - Congressional Leadership
  - Heads of Major Departments and Agencies
  - General Public

The Importance of what the GAO does



The Importance and Impact of what the U.S. Senate Select Committee on Intelligence does.

- Mission: The Committee was created by the Senate in 1976 to "oversee and make continuing studies of the intelligence activities and programs of the United States Government."
- And to "provide vigilant legislative oversight over the intelligence activities of the United States to assure that such activities are in conformity with the Constitution and laws of the United States."

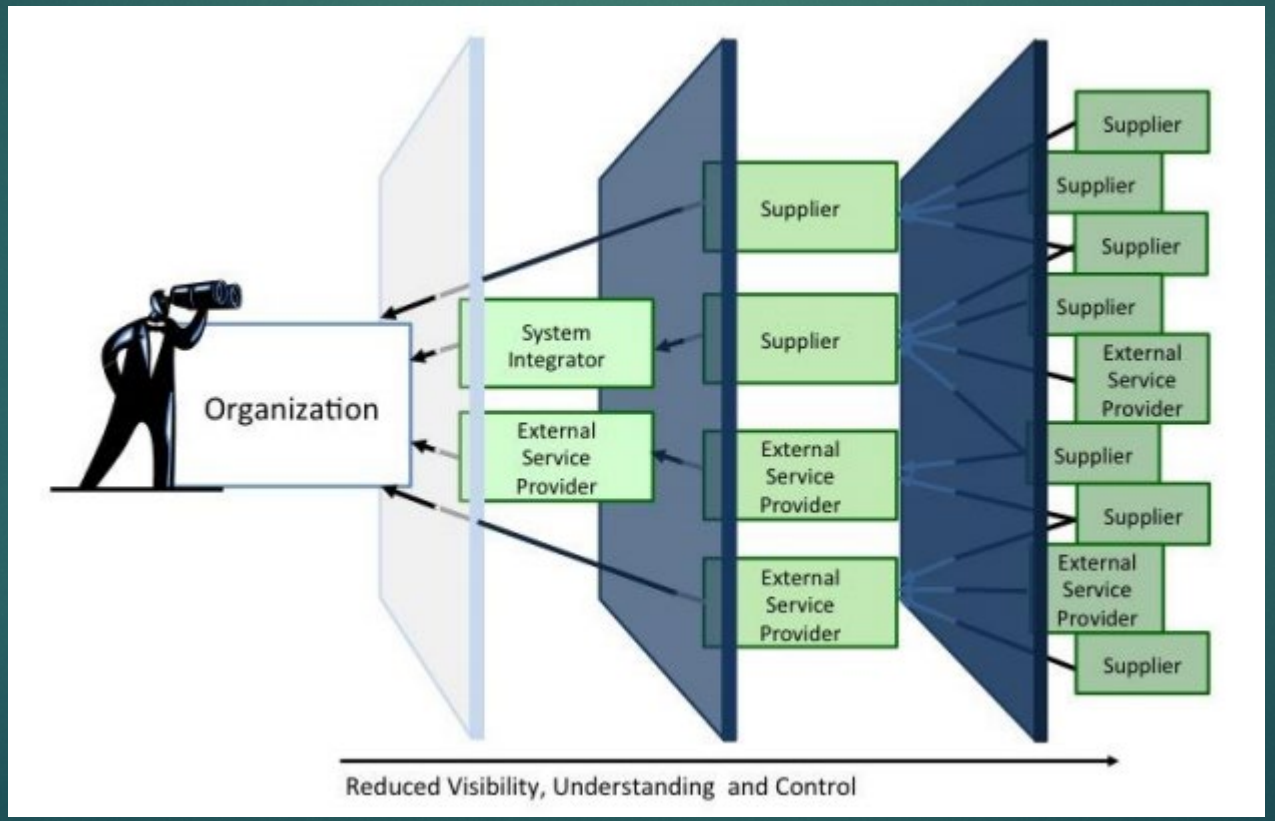
Senate Select Committee on Intelligence: Open Hearing on SolarWinds February 23, 2021

- Written Testimony of Sudhakar Ramakrishna
- Chief Executive Office, SolarWinds Inc.
- "We appreciate the opportunity to share our findings, lessons learned and our recommendations to promote the public-private information sharing, collaboration and support that we believe are necessary to protect us all against these types of operations in the future. "

Senate Select Committee on Intelligence: Open Hearing on the SolarWinds February 23, 2021

- Build on recommendations from the Cyberspace Solarium Commission and the Fiscal Year 2021 National Defense Authorization Act (NDAA):
  - Improving Industry Government Supply Chain Security Collaboration
  - Improving Federal Government Cybersecurity Standards
  - Improving Incident Notification to the Government

Senate Select Committee on Intelligence: Open Hearing on the SolarWinds February 23, 2021



Senate Select Committee on Intelligence: Open Hearing on the SolarWinds February 23, 2021

Figure 1-1: Four Pillars of ICT SCRM

Senate Select Committee on Intelligence: Open Hearing on the SolarWinds February 23, 2021

- Strengthening the Nation's Cybersecurity: Lessons and Steps Forward Following the Attack on SolarWinds.
- Written Testimony of Brad Smith President, Microsoft Corporation
- Senate Select Committee on Intelligence Open Hearing on the SolarWinds Hack February 23, 2021
- "No one should believe that this attack has yet been fully understood or is yet fully contained."

Senate Select Committee on Intelligence: Open Hearing on the SolarWinds February 23, 2021

- After reviewing what we have learned, I will address several specific concrete areas where action is essential:
  - First, strengthen supply chain security
  - Second, broaden use of cybersecurity best practices
  - Third, develop national strategy to strengthen how we share threat intelligence
  - Fourth, impose a clear, consistent disclosure obligation
  - Finally, strengthen the rules of the road for nation-state conduct in cyberspace.

Questions