# Strengthening the Weakest Link: Cybersecurity in the Supply Chain

Network security is heavily reliant on a strong Cybersecurity Supply Chain Risk Management (SCRM) program

ICA Cybercon – May 2024

VantagePoint
EMPLOYEE OWNED

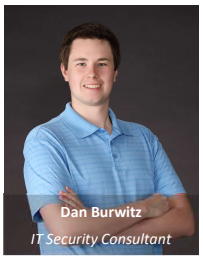
1

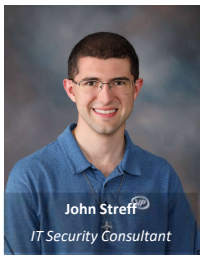
## About the Presenter

**James Taylor –**
**Sr. IT Security Consultant**

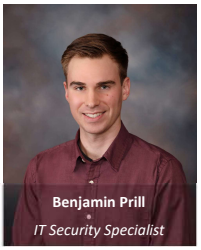
- Vantage Point Solutions, started 2016
- Background:
  - Dakota State University with B.S., Computer Science (Information Security)
  - Colorado University with A.S., Criminal Justice
- Father of 3 boys (23,22,19, my wife is a saint) and 2 dogs
- Hobbies, computer stuff, outdoor stuff, woodworking stuff
- James.Taylor@vantagepnt.com

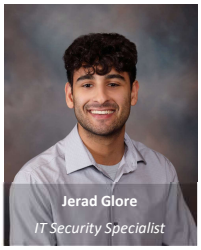
2







## Meet the Security Team

- James.Taylor@vantagepnt.com
- Dan.Burwitz@vantagepnt.com
- John.Streff@vantagepnt.com
- William.Gonzalez@vantagepnt.com
- Jerad.Glore@vantagepnt.com
- Benjamin.Prill@vantagepnt.com
- Justin.jaunay@vantagepnt.com

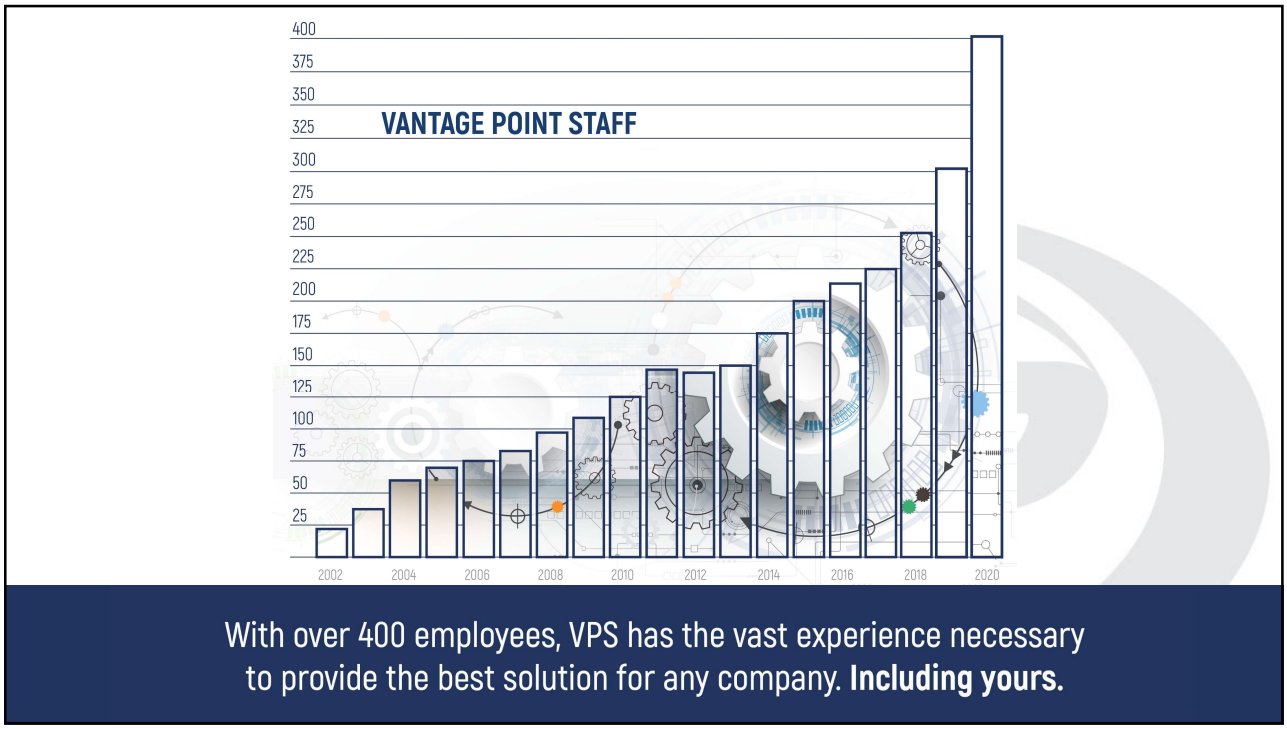
VantagePoint EMPLOYEE OWNED

3

## **Vantage Point Solutions**, Mitchell, SD.

www.vantagepnt.com

4


VANTAGE POINT STAFF
400
375
350
325
300
275
250
225
200
175
150
125
100
75
50
25
2002
2004
2006
2008
2010
2012
2014
2016
2018
2020
With over 400 employees, VPS has the vast experience necessary to provide the best solution for any company. **Including yours.**

5


VPS serves **hundreds of clients**, large and small, across the country and internationally.

6

## Here for all your questions

ENTERPRISE RISK MANAGEMENT

AUDIT

REGULATORY COMPLIANCE

INDEPENDENT CREDIT REVIEW

CYBERSECURITY

NETWORK MONITORING

SERVER VIRTUALIZATION

DATA NETWORKING

7

## Todays Objectives

- Exploring the critical role of Cybersecurity Supply Chain Risk Management (C-SCRM)
- Importance of C-CSRM in maintaining secure network infrastructure
- Strategies for identifying vulnerabilities within the supply chain
- Best practices for remediating supply chain vulnerabilities
- Enhancing overall security through supply chain risk management
- Ongoing cybersecurity requirements for E-ACAM funding

8


9

## Why should you utilize C-SCRM

- Increase security posture and mitigate risk
- Improved resilience of critical systems
- Regulatory Compliance
- Better insight and transparency into supply lines and suppliers

VantagePoint
EMPLOYEE OWNED

10

## Your network is only as strong as its weakest link.

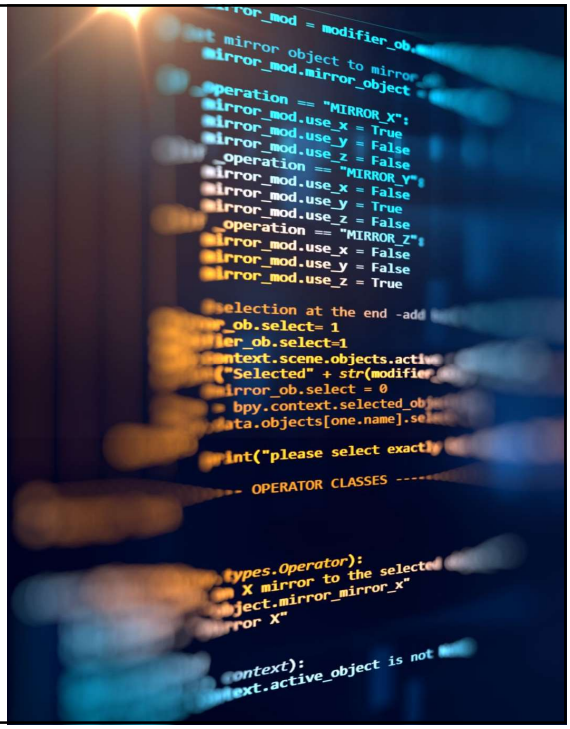
- Many different suppliers of good, services and products
- Vulnerabilities and Exploits and filter down the chain
- Importance of vigilance and continuous monitoring of the risk process

VantagePoint EMPLOYEE OWNED

11

## Malicious Actors Targeting the Supply Chain

- Increasing Attacks on Supply Chains
- Compromised Supplier Systems – looking at the “bigger” picture
- Introduction of malware, keyloggers and ransomware
- Making changes to software and code itself
- Creating backdoors or persistent access for a later date



12

## Unintentional Risks of Poor Supply Chain Management

- Poor Development Practices – "We have always done it that way"
- Inadequate Security Protocols
- Human Error
- Lack of knowledge of security practices or security staff

VantagePoint EMPLOYEE OWNED

13

## Parts of a C-SCRM

- Scope and Purpose
- Roles and Responsibilities
- Vendor Selection and Onboarding
- Risk Assessments
- Contractual Security Clauses
- Monitoring and Continuous Improvement
- Incident Response
- Reference to relevant standards and frameworks

14

## Scope and Purpose

- Clear definition of the scope outline supply chain coverage
- Emphasize the importance of managing cybersecurity risks within the supply chain
- Allows for focused efforts
- Give clear goals and prioritization
- Communication and Collaboration

VantagePoint
EMPLOYEE OWNED

15

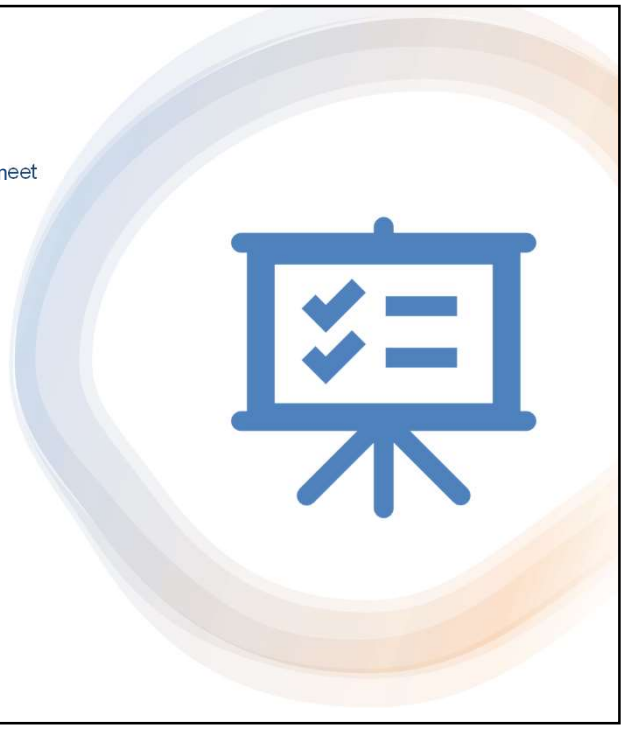
## Roles and Responsibilities

- Assign detailed and clear roles and responsibilities for:
  - Vendor selection and onboarding
  - Risk assessments of vendors
  - Contractual security clauses
  - Monitoring vendor security posture
  - Incident response procedures
- Accountability and ownership
- Reduce confusion, overlap and improve efficiency
- Faster incident response

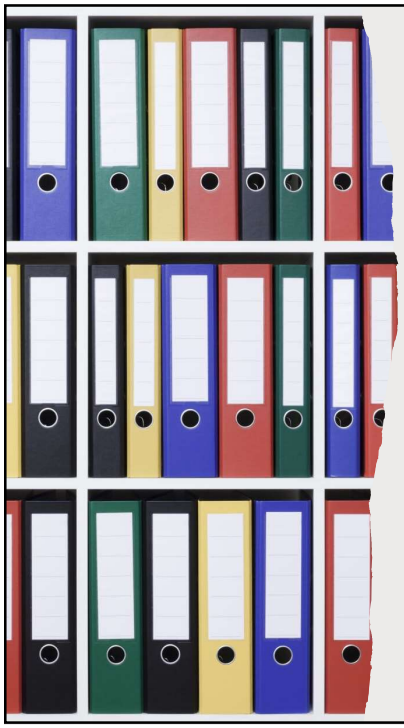
16

# Vendor Selection and Onboarding

- Establish a process for vendor selection and ensure they meet your cybersecurity requirements
- This process should involve:
  - Security Questionnaires
  - Background and credit checks
  - Security audits and attestation review
- How to determine criticality
  - Impact on Business Disruption
  - Data Volume and Type
  - Regulatory Requirements
  - Vendor Type
  - Specific Services Provided



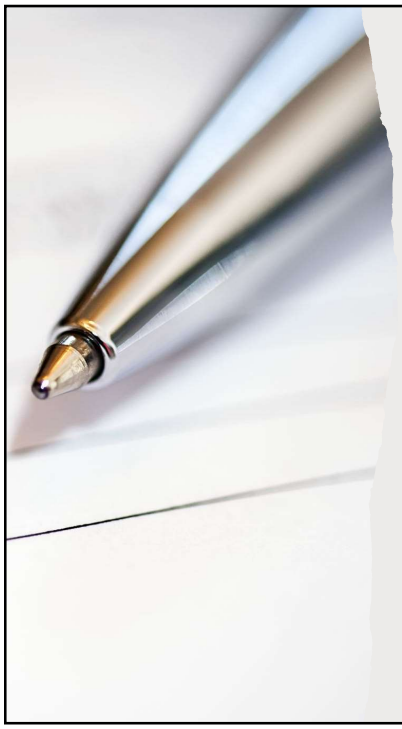
17



# Risk Assessment

- Defining vendor criticality – assign a metric or number
- Outline the service/product or devices provided
- What access does that vendor access to systems and data
- Review the security practices of the vendors

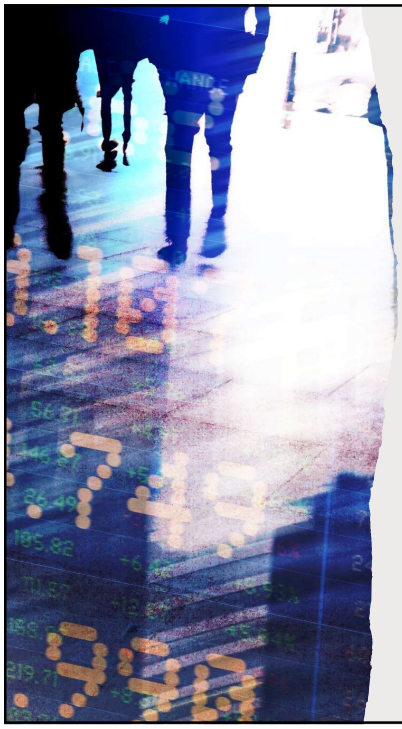
18



# Contractual Security Clauses in C-SCRM

- Mandatory Security Requirements
- Regular Security Audits
- Adherence to Security Standards
- Prompt Incident Reporting
- Continuous Improvement
- Termination Rights

19



# Monitoring and Continuous Improvement in C-SCRM

- Ongoing C-SCRM Process
- Regular Monitoring
- Adaptive Updates
- This is process is ongoing to address:
  - Cybersecurity as an evolving landscape
  - Vendors security postures changes over time
  - Limited visibility and mitigation processes
  - Improve decision making capabilities
  - Maintain compliance

20

# Incident Response (IR)

- Good IR planning is critical as it allows
  - Faster recovery from disruption
  - Reduce escalation with prompt efforts
  - Improve communication and collaboration
  - Preserving evidence
  - Lesson learning process
- This is achieved through
  - Proactive preparation
  - Vendor communication
  - Contractual obligations

21

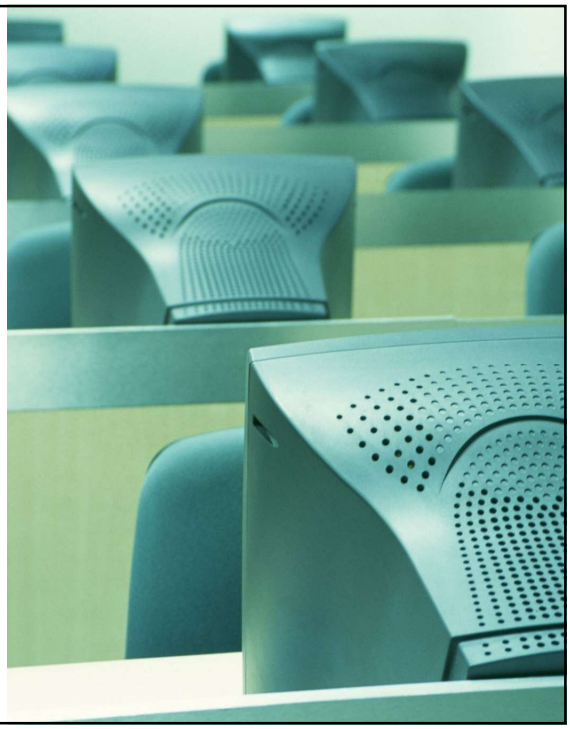
# Referencing relevant standards

- Why use a framework
  - Promote best practices
  - Raise awareness
  - Enforcement and accountability
  - Improved sharing opportunities

22

# Referencing relevant standards

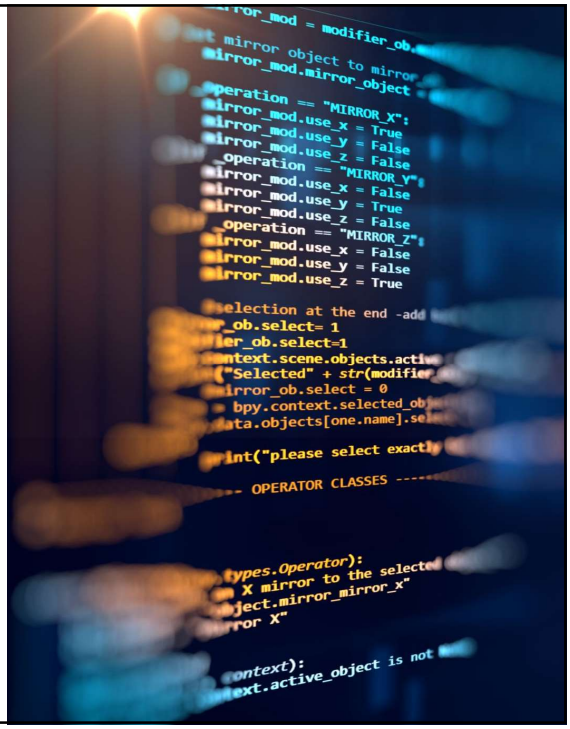
- Governing bodies that dictate policy:
  - National Institute of Standards and Technology (NIST)
  - Cybersecurity and Infrastructure Security Agency (CISA)
  - Federal Communications Commission (FCC)
  - Some local Public Utilities Commission (PUC) – Depending on state.



23

# NIST

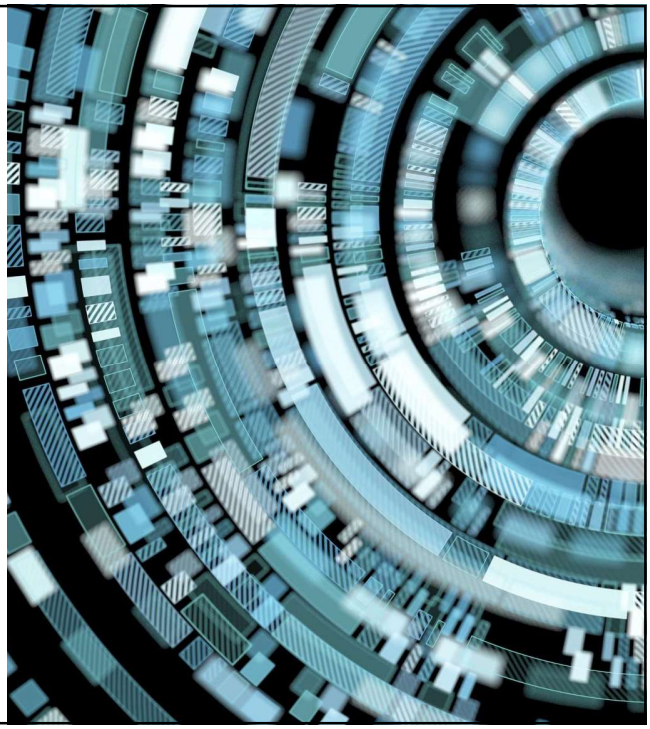
- Created special publication 800-161 – Defines supply chain risk management
- NIST Cybersecurity Framework (CSF) - Guidelines for managing cybersecurity risks. Contain sections consisting of; Identify, Protect, Detect, Respond, and Recover.
- NIST 2.0 - Standards and guidelines (newish)




24

## CISA

- Part of the Department of Homeland Security (DHS)
- Analyzes and communicates cybersecurity risks
- Collaborates between private and public sectors
- Critical and essential infrastructure security



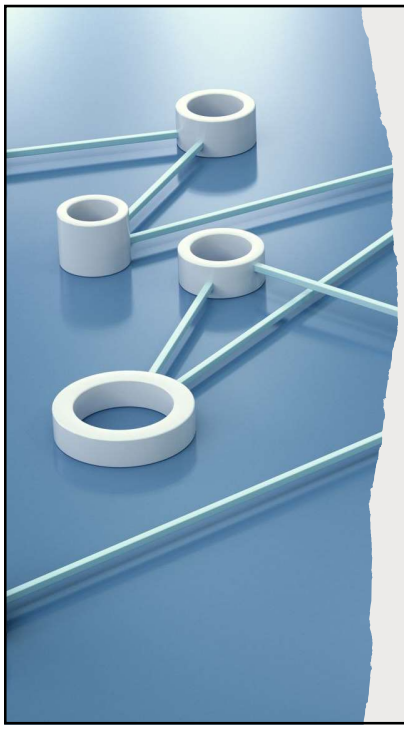
25

## FCC

- Cybersecurity labeling for IoT devices – can earn label "U.S. Cyber Trust Mark"
- Cybersecurity and Communications Reliability Division (CCR) works to ensure the reliability and security of communication networks
- The FCC collaborates with other government agencies like CISA to address cybersecurity issues

VantagePoint EMPLOYEE OWNED

26



## Center for Internet Security (CIS)

- Non-profit organization established 2000
- Develop best practices, controls and benchmarks for a wide range of industries, devices and software
- Global collaboration among IT professionals

27

## Real world supply chain incidents

- **Slack -** In December 2022, a malicious actor stole Slack employees' tokens and used them to gain unauthorized access to the company's resources. The data breach was a result of third-party vendor compromise.

- **Dollar Tree -** In November of 2023, Dollar Tree disclosed a data breach affecting nearly 2 million individuals, including employees' personal information, after a attack targeting service provider Zeroed-In Technologies in August 2023, with potential impacts on other Zeroed-In customers remaining unconfirmed

28

## Real world supply chain incidents cont'd

**Okta -** In October 2023, Okta's third-party, Rightway Healthcare, informed them that an unauthorized actor gained access to an eligibility census file maintained by Rightway in its provision of services to Okta. The security incident exposed personal and healthcare data of nearly 5,000 Okta employees and their dependents.

**AT&T –** In March 2023, AT&T announced that approximately 9 million wireless accounts had their customer proprietary network information accessed when an unauthorized person breached a third-party vendor's system. The vendor, who wasn't named, provides marketing services. While information, such as names, email addresses, phone numbers, the number of lines on an account and wireless rate plans were accessed, no Social Security Numbers, account passwords, financial information, or other sensitive personal information was stolen.

VantagePoint EMPLOYEE OWNED

29

# Cybersecurity Requirements for Enhanced-Alternative Connect American (E-ACAM) funding

30

# Ongoing cybersecurity requirements

**E-ACAM funded carriers must:**

Submit cybersecurity and C-SCRM plans to USAC within 30 days of making substantive modifications

**Which includes:**

A Cybersecurity plan within the NIST framework

A C-SCRM plan within the NIST framework

31

# Why should you utilize E-ACAM

- Faster Broadband for Underserved Areas
- Impact on communities – bridge the rural/urban divide
- Long term economic growth
- Advancements in education, telehealth, social wellness

32

# Adapting to future cybersecurity needs

- Proactive approach
- Embracing new technologies
- Holistic, layered security integration through all business processes
- Collaboration – you are not alone!

33

# Resources

- NIST SP (Special Publication)
  - 1800-34 – How to validate computing devices and their legitimacy
  - 800-161 – Identifying, chain
- CISA – Supply chain assessing, and mitigating cybersecurity risks throughout the supply in resource library - https://www.cisa.gov/ict-supply-chain-resource-library
- Cyber Supply Chain Risk Management for the Public - https://www.cisa.gov/resources-tools/resources/cyber-supply-chain-risk-management-public
- Cybershare - The Small Broadband Provider ISAC - https://www.cyber-share.org/

34

# Summary

- Exploring the critical role of Cybersecurity Supply Chain Risk Management (C-SCRM)
- Importance of C-CSRM in maintaining secure network infrastructure
- Strategies for identifying vulnerabilities within the supply chain
- Best practices for remediating supply chain vulnerabilities
- Enhancing overall security through supply chain risk management
- Ongoing cybersecurity requirements for E-ACAM funding

35

•Q&A

VantagePoint
EMPLOYEE OWNED

36


37