Supply Chain Risk Management

Team 1

Purpose

Raise awareness about supply chain risk management and share steps that can be implemented in our own organization to reduce these risks

Table of **contents**

01

Introduction

02

Incidents

03

Challenges

04

Best Practices

01

Introduction

What is a Third-Party?

A relationship between parties that is not the primary relationship; however, that third-party relationship is relied on to fulfill the primary relationship.

Vendors

Suppliers

Service providers

Outsourcers

Resellers

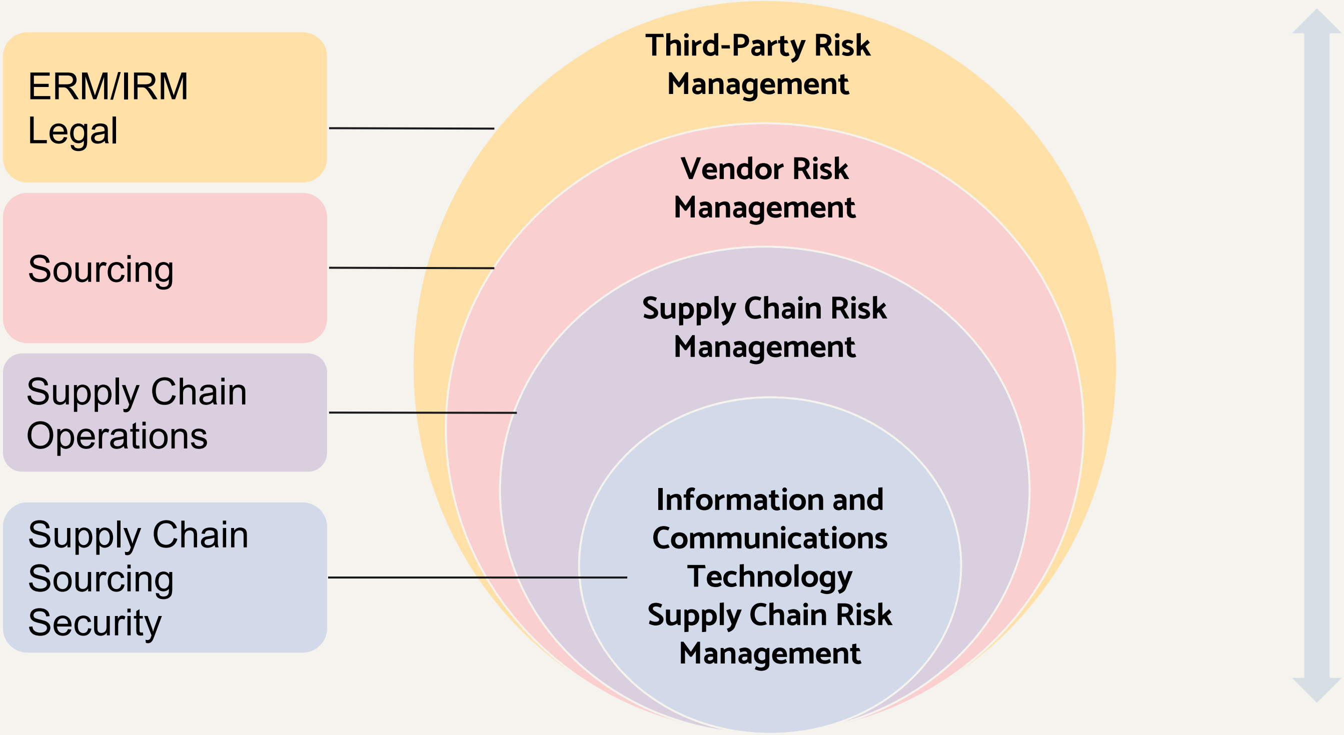
Agents

Channel, brand and joint venture partners

Market utilities

Intermediaries

Risk Management Layers



ERM/IRM
Legal

Sourcing

Supply Chain Operations

Supply Chain Sourcing Security

Third-Party Risk Management

Vendor Risk Management

Supply Chain Risk Management

Information and Communications Technology Supply Chain Risk Management

Source: Gartner 2021

02

Incidents

solarwinds

The Power to Manage IT

Third party attack
Patching gone wrong!!

Why SolarWinds?

- Secure software solutions for DevOps, SecOps and DBAs
- They have more than 300,000 customers
- **ORION**
  - IT performance measurement tool
  - Logs and system performance data
- Nobelium - nation-state hackers

Attack Life Cycle of Solarwinds

9/4/19	Threat Actor(TA) accessed solarwinds
9/12/19	TA injected trial code and started trial run
11/4/19	Test Code injection ended
6/4/20	TA removes the malware from build VM’s
12/12/20	Solarwinds notified about SUNBURST
12/14/20	Solarwinds notifies shareholders and customers
12/15/20	Solarwinds released a software fix

Impacts of Solarburst on Organizations

- Biggest cybercrime breaches of 21st century costing upto **$900 million**.
- Disrupted supply chain of 18,000 organizations.
  - US government (local, state, federal)
  - 40 companies were targeted by the actors
- Access to data and collection of sensitive information for extreme period of time
- Impact on annual revenue, **14% in USA, 8.6% in UK and 9.1% in Singapore**

Third Party Risks are a growing threat

Third party Risks

In 2022, Supply chain attacks were **40% higher** than malware attacks

633% increase

Known malicious software supply chain attacks grow from **12,000** in 2021 to **88,000** in 2022

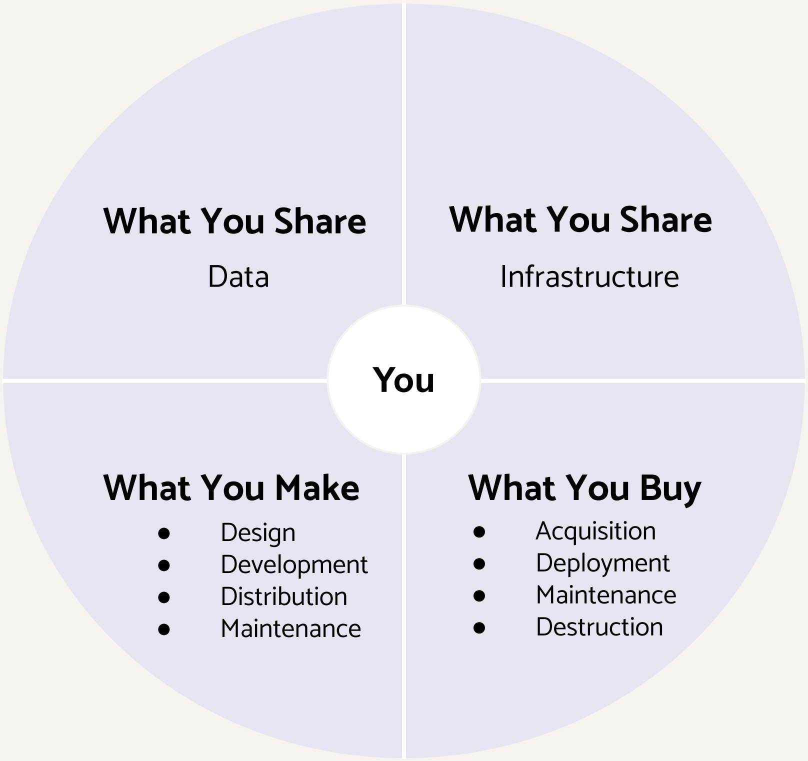
Cyber resilience

90% of Business and Cyber leaders are concerned with third party security frameworks to avoid **collateral damage**

03

Challenges

Main Categories of ICT Supply Chain Security Risks



What You Share

Data

What You Share

Infrastructure

You

What You Make

- Design
- Development
- Distribution
- Maintenance

What You Buy

- Acquisition
- Deployment
- Maintenance
- Destruction

Source: Gartner 2021

Current State

Management of these risks across four main categories is absent/fragmented. This leaves organisations exposed.

Supply chain regulations and frameworks are emerging globally. US efforts alone will have large impacts on organizations.

Given the complexity of supply chain ecosystems and the scale of data/assets to protect, **risk management efforts are largely in awareness phase and remain siloed.**

Early **best practices** are emerging.

Attacks

Software threat vectors:

- Hijacking updates
- App Store Attacks
- Open-Source Compromise
- Undermining Code Signing

solarwinds®

Hardware threat vectors:

- Code injection
- Tampering
- Counterfeits

SUPERMICRO®

Attacks

APACHE HTTP SERVER PROJECT

webmin

node JS

Kaseya

LEAGUE of LEGENDS

Java

Software threat vectors:

- Hijacking updates
- App Store Attacks
- Open-Source Compromise
- Undermining Code Signing

VESTA

me doc

МІЙ ЕЛЕКТРОННИЙ ДОКУМЕНТ

Hardware threat vectors:

- Code injection
- Tampering
- Counterfeits

android

Google Play

Windows Vista

Adobe

solarwinds

SUPERMICRO

git

ASUS

npm

mobileme

mimecast

04

Best Practices

Recommendations

Security and Risk Criticality

Prioritize efforts based on security and risk criticality filters

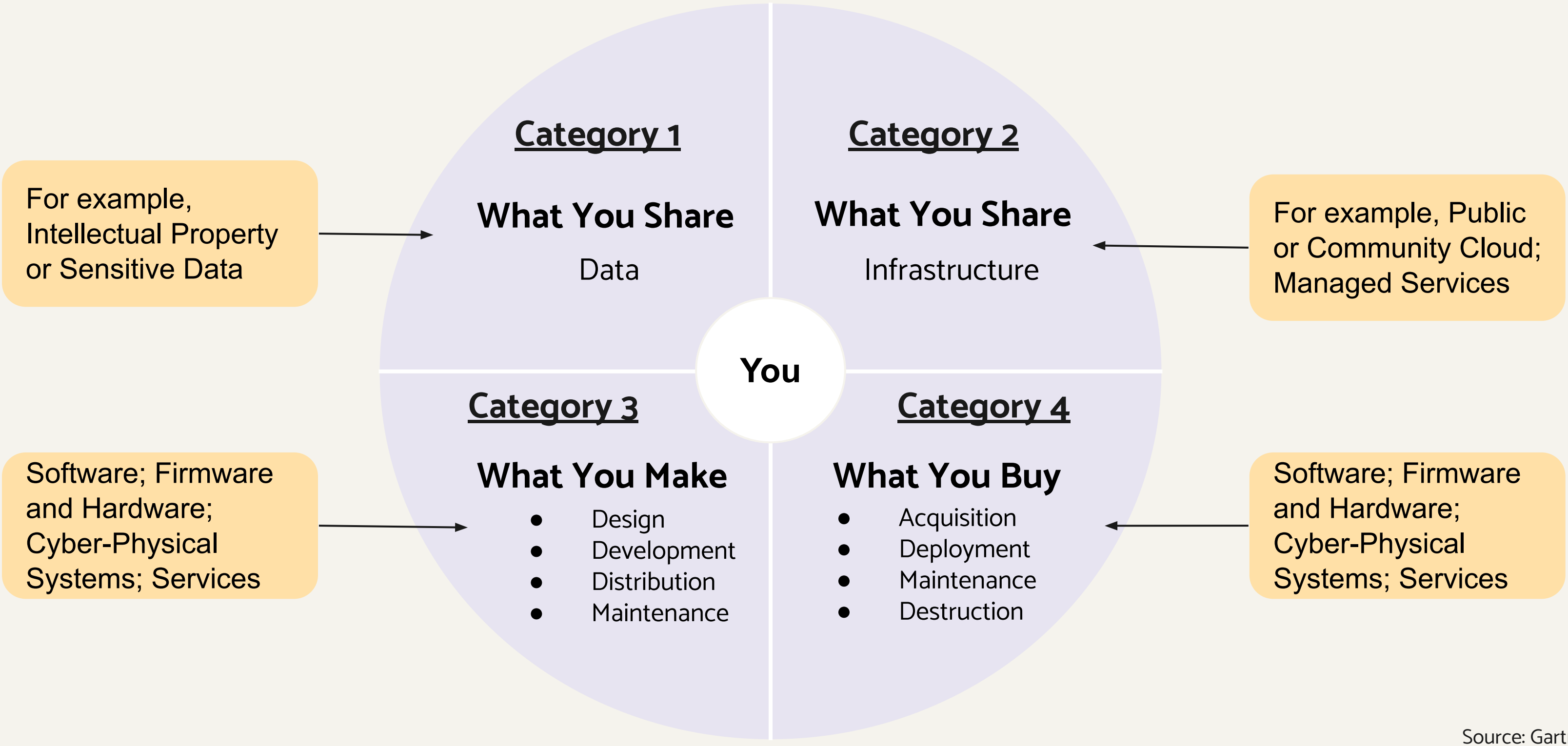
New Regulatory mandates

Prioritize efforts to meet new regulatory mandates if you are subject to them, or learn from them

Creating partnerships

Create partnerships with key IT, procurement, supply chain, operations, system owners and create joint governance model

Main Categories of ICT Supply Chain Security Risks



For example, Intellectual Property or Sensitive Data

Category 1

What You Share

Data

Category 2

What You Share

Infrastructure

For example, Public or Community Cloud; Managed Services

You

Software; Firmware and Hardware; Cyber-Physical Systems; Services

Category 3

What You Make

- Design
- Development
- Distribution
- Maintenance

Category 4

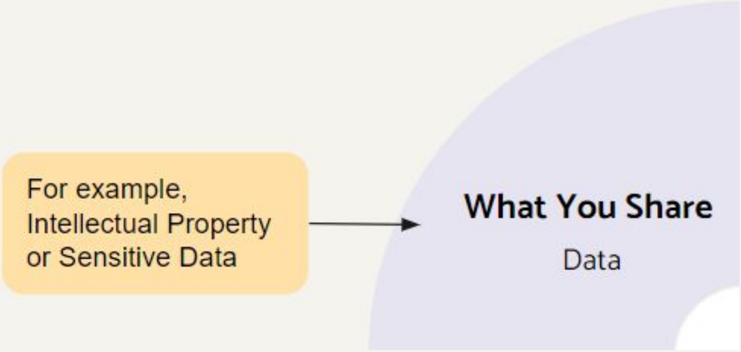
What You Buy

- Acquisition
- Deployment
- Maintenance
- Destruction

Software; Firmware and Hardware; Cyber-Physical Systems; Services

Source: Gartner 2021

Category 1



For example, Intellectual Property or Sensitive Data

What You Share

Data

Actions:

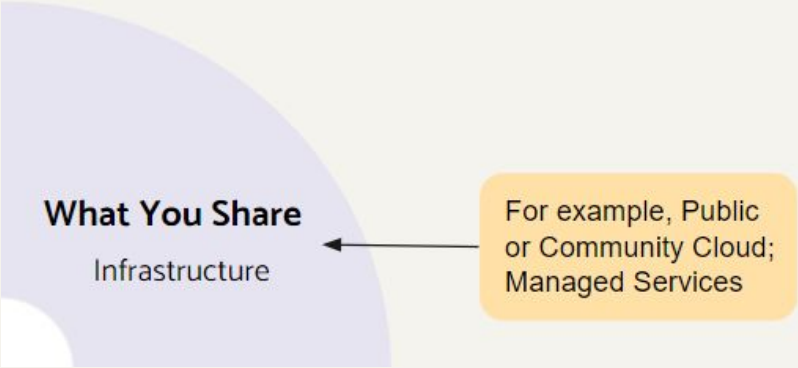
- Due Diligence efforts
  - Requests for information
  - Security certifications
  - Secure development practices
- Contractual requirements
- Service-level agreements (SLAs)

Source: Gartner 2021

Category 2

Actions:

- Same as Category 1 with additional contractual requirements to receive independent security assessments



Source: Gartner 2021

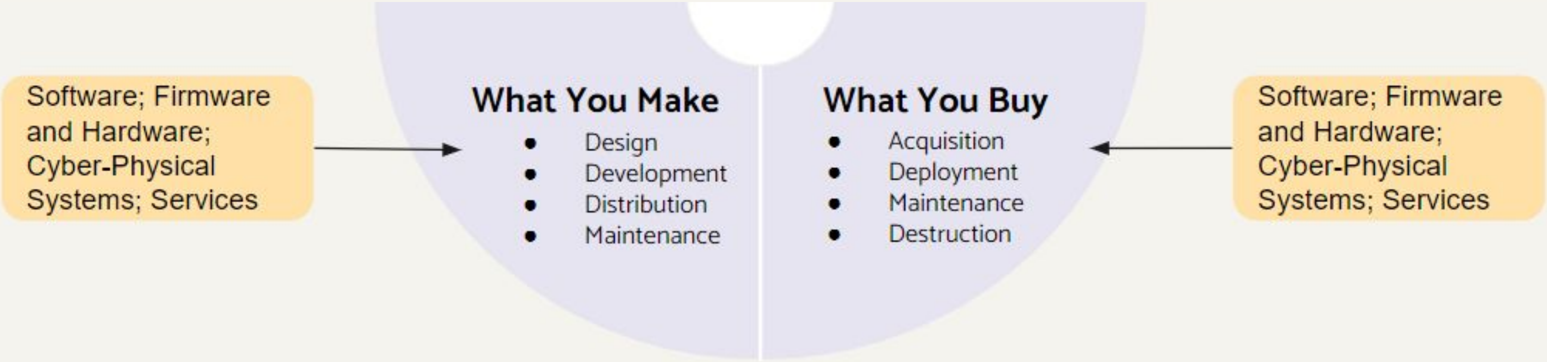
Category 3 & 4

Software-related - led by security team:

- Software encryption
- Using software bills of material (SBOMs)
- Adopting DevSecOps approaches to continually test software quality
- Follow NIST and CISA guidelines

Firmware/Hardware - led by development teams:

- Creating guidelines for purchasing directly from qualified OEMs
- Use hardware bills of materials
- Use content disarm and reconstruction techniques to prevent malicious code injection



Software; Firmware and Hardware; Cyber-Physical Systems; Services

What You Make

- Design
- Development
- Distribution
- Maintenance

What You Buy

- Acquisition
- Deployment
- Maintenance
- Destruction

Software; Firmware and Hardware; Cyber-Physical Systems; Services

Source: Gartner 2021

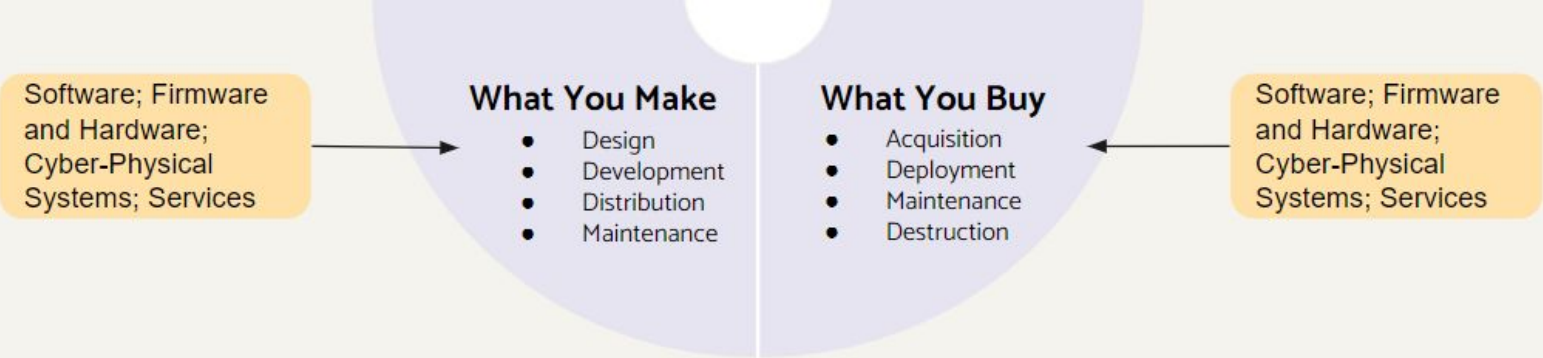
Category 3 & 4 (cont.)

Cyber-physical systems related:

- Contractual requirements to show adoption of vertical- industry specific frameworks
  - NERC-CIP or NIST CSF
- Asking for certifications from labs that test for alert/logging, cryptography, authentication, etc.

Services-related:

- Due diligence efforts, including requests for information on various topics such as location of operations
- Open source information checks on credit worthiness, and whether there have been any history of lawsuits pertaining to IP theft



Software; Firmware and Hardware; Cyber-Physical Systems; Services

What You Make

- Design
- Development
- Distribution
- Maintenance

What You Buy

- Acquisition
- Deployment
- Maintenance
- Destruction

Software; Firmware and Hardware; Cyber-Physical Systems; Services

Source: Gartner 2021

Governance Best Practices

Usually led by enterprise risk management teams or chief security officers. Efforts include:

- Setting up supply chain risk management councils.
- Prioritizing high-value assets (such as critical systems across the enterprise, including cyber-physical systems as well as information).
- Deploying organization wide asset discovery and management solutions.
- Embracing NIST CSF 1.1.
- Including key suppliers in resilience and improvement activities.

Action Plan **Avanade**

Improving governance and supply chain risk management efforts

Action 1: Upgrading Risk Assessment Framework

To accommodate continuous supply chain risk monitoring and regularly updating to incorporate emerging threats and changes

Our Proposal:

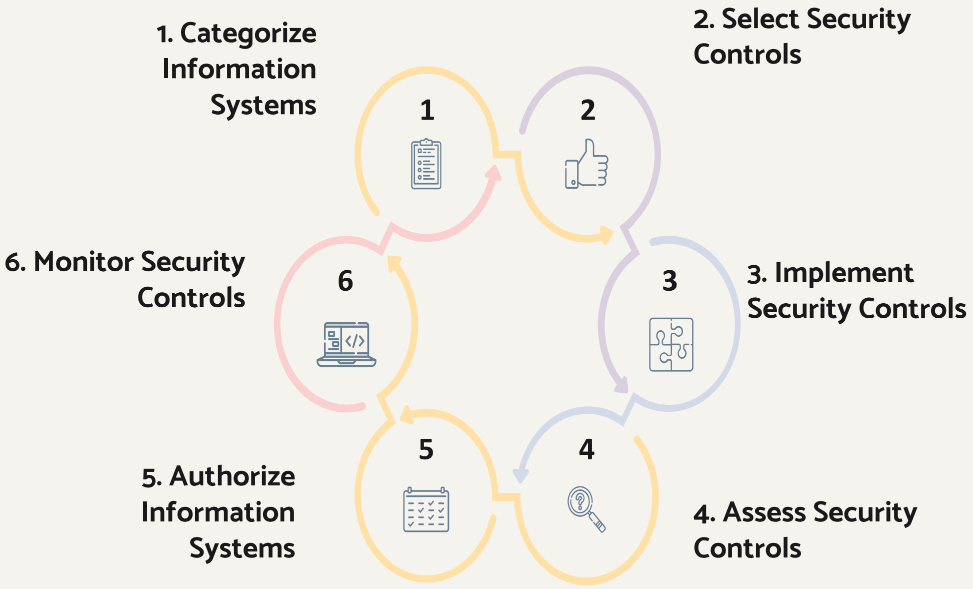
- Conduct Audit and reassessment of risk ratings
- Planned and detailed risk assessment plan

High

Priority Level

1 Month

Projected Timeline



1. Categorize Information Systems
2. Select Security Controls
3. Implement Security Controls
4. Assess Security Controls
5. Authorize Information Systems
6. Monitor Security Controls
1
2
3
4
5
6

Action 2: Supplier Risk Management Program

Will ensure that potential suppliers and vendors are vetted on their security practices

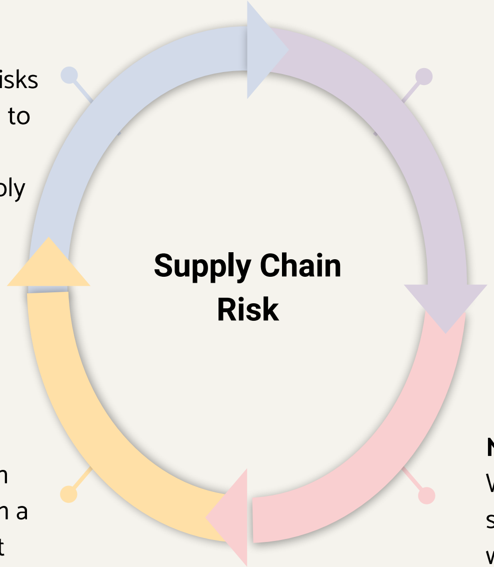
- Suppliers are fulfilling our organizations and regional government minimum security requirements
- Regular streamlined assessment of our partners
- Structured support for partners
- Our operations and procurement teams will be trained under this program

High

Priority Level

6-9 Months

Projected Timeline



Supply Chain Risk

Identify
What types of risks are we exposed to and where are they in our supply chain?

Quantify
What financial impact could these risks have on our sales and profitability?

Mitigate
What strategies/tactics do we have in place to minimise the disruption to our business?

Respond
How quickly can we recover from a disruptive event and return to normal operations?

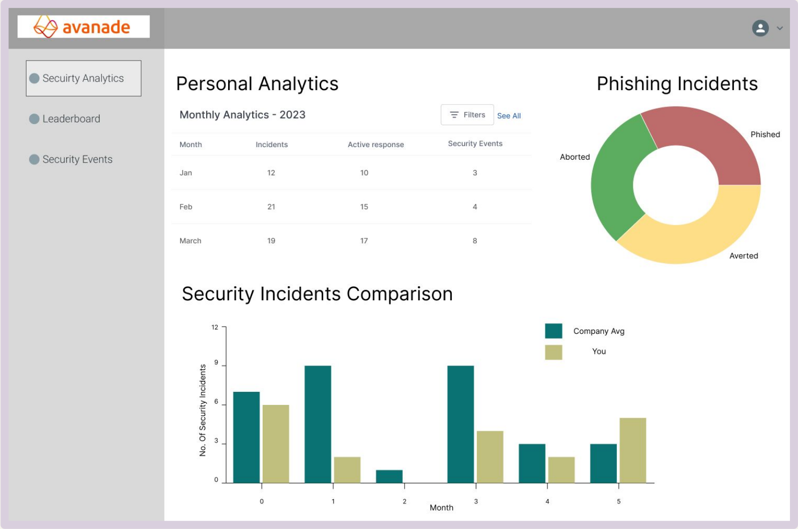
Action 3: Eliminating “Human Factor”

Improving human awareness of potential supply chain risks:

- Security Education, Training, and Awareness (SETA) programs
- For both in-house employees and critical partner employees

Our Proposal:

Development of **Security training platform**



Personal Analytics

Monthly Analytics - 2023

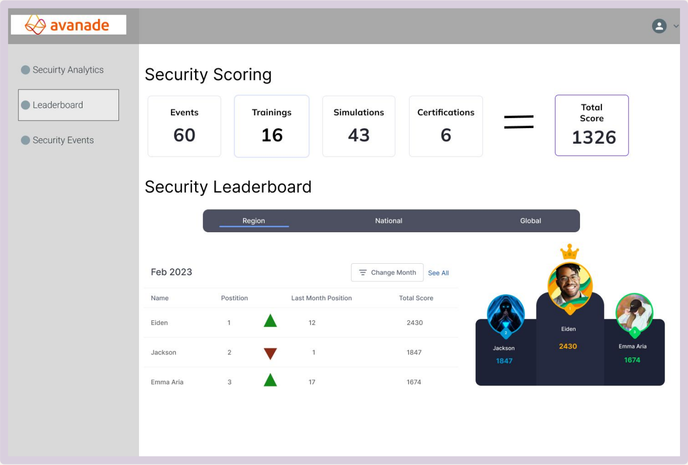
Month	Incidents	Active response	Security Events
Jan	12	10	3
Feb	21	15	4
March	19	17	8

Phishing Incidents

Security Incidents Comparison

Platform **Plan**

- Gamify training programs
- Provide incentives for users to complete structured programs



Security Scoring

Events	Trainings	Simulations	Certifications	=	Total Score
60	16	43	6		1326

Security Leaderboard

Feb 2023

Name	Postition		Last Month Position	Total Score
Eiden	1	▲	12	2430
Jackson	2	▼	1	1847
Emma Aria	3	▲	17	1674

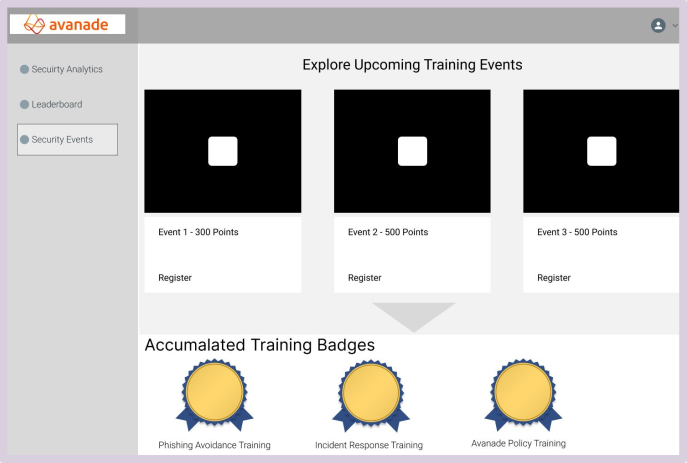
High

Priority Level

6 Months

Projected Timeline

- Product development: **4 months**
- Training program development and adoption: **2 months**



Explore Upcoming Training Events

Event 1 - 300 Points

Event 2 - 500 Points

Event 3 - 500 Points

Accumalated Training Badges

Phishing Avoidance Training

Incident Response Training

Avanade Policy Training

Action 4: Incident Response Plan

Activities:

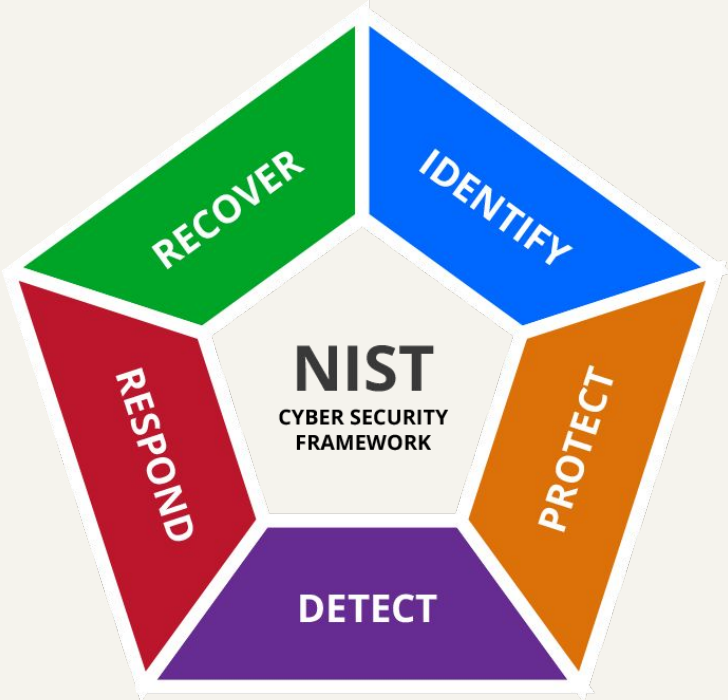
- Audit and updation of current Incident response plans, as per action 1
- Development of supply chain specific IRP, utilizing NIST framework
- Inclusion of critical vendors, stakeholders in supply chain specific IRPs

Medium

Priority Level

3 Months

Projected Timeline



Conclusion

Increasing globalization of services have lead to an increase in supply chain risks and incidents over the past few years. Hence, it becomes paramount for organizations to adopt best practices to shield ourselves from these attack areas.

Optimizing Security and Risk Criticality

- Streamlined auditing and updating security practices
- Prompt implementation of regulatory norms
- Action plan 1 and 2

Eliminating Human Factor

- Training workforce and Zero trust implementation
- Action plan 3

Creating critical partnerships and IRP

- Joint governance and implementation with critical vendors
- Action plan 2 and 4

Thanks!

Do you have any questions?

I DON'T CARE WHO YOU ARE, OR HOW BAD OUR VENDOR RISK ASSESSMENT IS
I WILL FIND YOU, AND I WILL AUDIT YOU.
imgflip.com

References

https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know
https://orangematter.solarwinds.com/2021/01/11/new-findings-from-our-investigation-of-sunburst/
https://www.fortinet.com/resources/cyberglossary/supply-chain-attacks
https://www.helpnetsecurity.com/2023/01/26/data-compromises-2022/#:~:text=However%2C%20in%202022%2C%20supply%20chain,cyberattacks%20affected%204.3%20million%20people.
https://heimdalsecurity.com/blog/solarwinds-attack-cost-impacted-companies-an-average-of-12-million/
ICT Supply Chain Risk Management Is Mission-Critical, but Best Practices Are Just Emerging: https://www.gartner.com/document/code/750091?ref=authbody&refval=4011688
Market Guide for Third-Party Risk Management Solutions: https://www.gartner.com/document/4022390?ref=solrAll&refval=358272806
3 Fundamental Steps to Effective IT Vendor Performance Management: https://www.gartner.com/document/code/765713?ref=authbody&refval=4023185
IT Vendor Ecosystem Management Primer for 2023: https://www.gartner.com/document/4023185
Market Guide for IT Vendor Risk Management Solutions:https://www.gartner.com/document/4019316?ref=solrAll&refval=358605681
Market Guide for Supplier Risk Management Solutions: https://www.gartner.com/document/4014686?ref=solrAll&refval=358605681
Global Cybersecurity Outlook 2023 (pg. 18): https://www3.weforum.org/docs/WEF_Global_Security_Outlook_Report_2023.pdf
5 Best Practices to Enhance Third-party Due Diligence – Insights (metricstream.com)
Third-Party Risk Management and Mitigation | Gartner