CISO SINGAPORE 2022

Supply Chain – A New Attack Vector

Anthony Lim

Fellow, Cybersecurity & Governance

SUSS

22 Sep 2022

v.1.2

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES

CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

Corinium connected thinking

suss.edu.sg cscis.org

Supply Chain – A New Attack Vector

(Not-so)

PROLOG

- Supply chain networks are increasingly driven by technology and digital transformation.

- While it makes them faster and more efficient, it also gives rise to new cybersecurity concerns.

- A recent European Union Agency for Cybersecurity study finds attackers have shifted their attention to suppliers, related third parties and ecosystem organisations.

- The latter are usually smaller companies that don't always follow the cybersecurity and compliance requirements of the main organisation.

- Impacts of these attacks include service downtime; manufacturing disruption; supply and logistics challenges; monetary loss; and reputational damage.

- This session will look at mitigation and risk management steps organisations need to take to minimise or protect against supply chain cyberthreats.

Note –
This is a treatment of "old-school" supply chain & ecosystem cyber attack, not so much about the "Solarwinds" or Log4j software attack type, although we will talk abit about this.

PROLOG

Supply Chain Cyber Attacks –Considerations

("old school")

- **Association of supply chain attacks with OT (operational technology), CII (critical information infrastructure) and IOT (Internet of Things, including IIOT Industrial Internet of Things)**

- **fallouts of supply chain attacks include**
  - ✓ disruption to key public services
    - water & energy supply, telecoms, healthcare, essential services, defense, transport & logistics
  - ✓ loss, leakage or abuse of data
    - whether personal data, confidential corporate data or intellectual property

- **not just disruption to commercial, retail or industrial services**

- **smart nation program increasingly dependent on increasing number of ecosystem partners**

At least 5 other speakers at this event speak about or mention Supply Chain issues, which suggests the importance of this matter today.

*** Psychological warfare – disruption of morale – of staff, customers, citizenry.**

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

Singapore orders recall of two Haagen-Dazs ice cream products due to presence of pesticide

Yasmin Begum

8 July 2022 Friday

cna

Latest Report Uncovers Supply Chain Attacks by North Korean Hackers

October 27, 2021 Ravie Lakshmanan

Lazarus Group, the advanced persiste
has been observed waging two separ
into corporate networks and target a

Japanese beauty retailer Acro blames third-party hack for breach of 100k payment cards

Adam Bannister 04 March 2022 at 15:57 UTC
Updated: 04 March 2022 at 16:21 UTC

Japan | E-Commerce | Data Breach

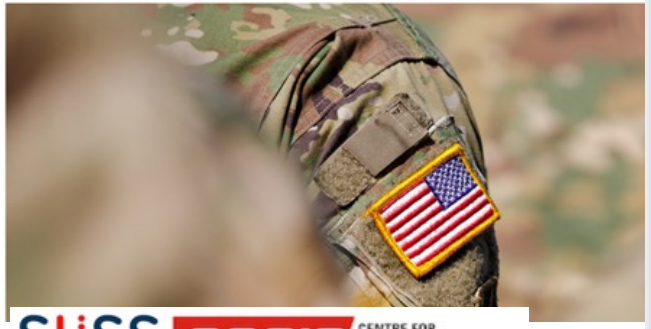
Company traces compromise to vulnerability in payment processor's systems

Russian nation-state hackers targeting US contractors for sensitive defense information, FBI warns

Jessica Haworth 17 February 2022 at 13:48 UTC

Hacking News | Government | Cyber Warfare

Cybersecurity and military secrets among documents accessed

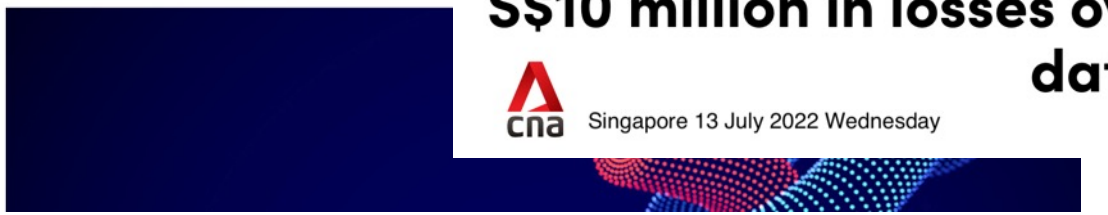


Critical Axeda vulnerabilities pose takeover risk to hundreds of IoT devices

Adam Bannister 09 March 2022 at 15:35 UTC
Updated: 10 March 2022 at 10:53 UTC

Vulnerabilities | Healthcare | IoT

Serious supply chain threat posed to downstr



Gaming firm Razer sues IT vendor for nearly S$10 million in losses over leak of customers' data

cna Singapore 13 July 2022 Wednesday

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES | CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

Supply Chain Ecosystem - Example

Not exhaustive

Marketing Agency

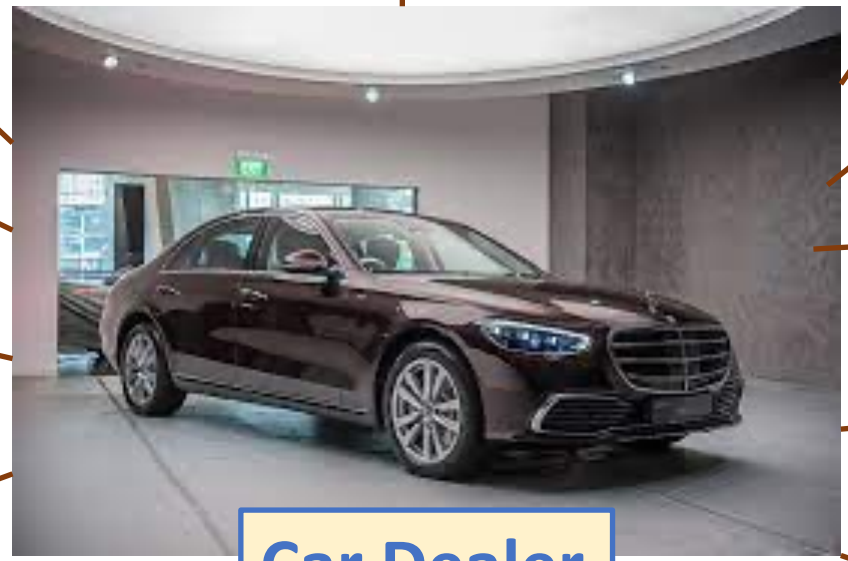
Spare Parts

Sub-contractor

Trade-in, used-car sales, scrap

Government (LTA)

Manufacturer



Car Dealer

Customer

3rd Party Accessories

Sub-dealer

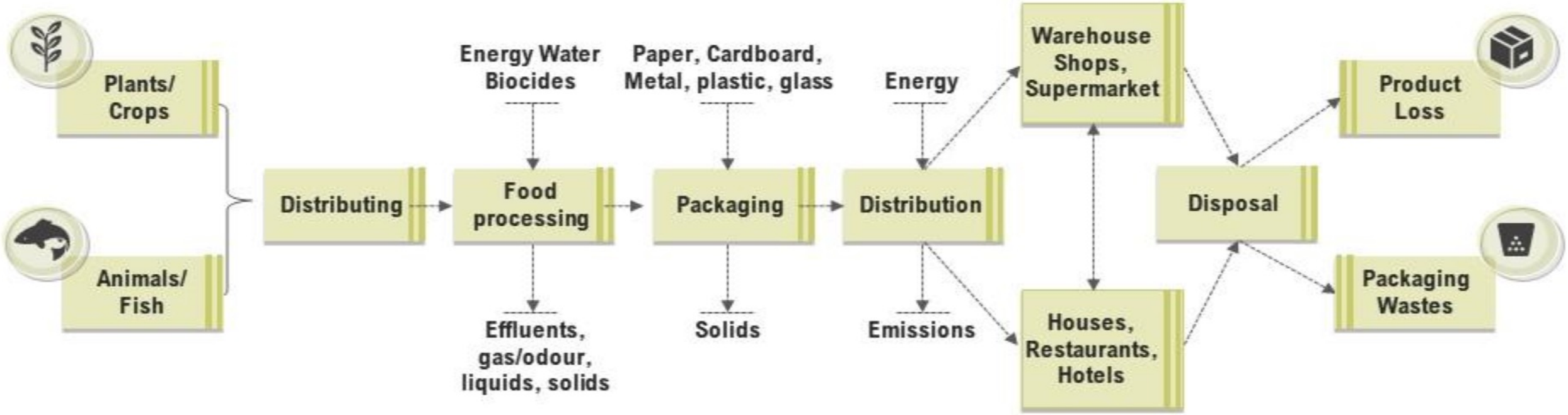
Insurance Co

Bank (Loans)

To the customer, the dealer is a one-stop shop – you pay, sign some Papers, drive home the car. Behind unseen is a whole plethora of Entities working in tandem to make all this happen and more.

Another Example

Food Industry Supply Chain Flow



It can get more complicated

Manufacturing Supply Chain Flow Chart

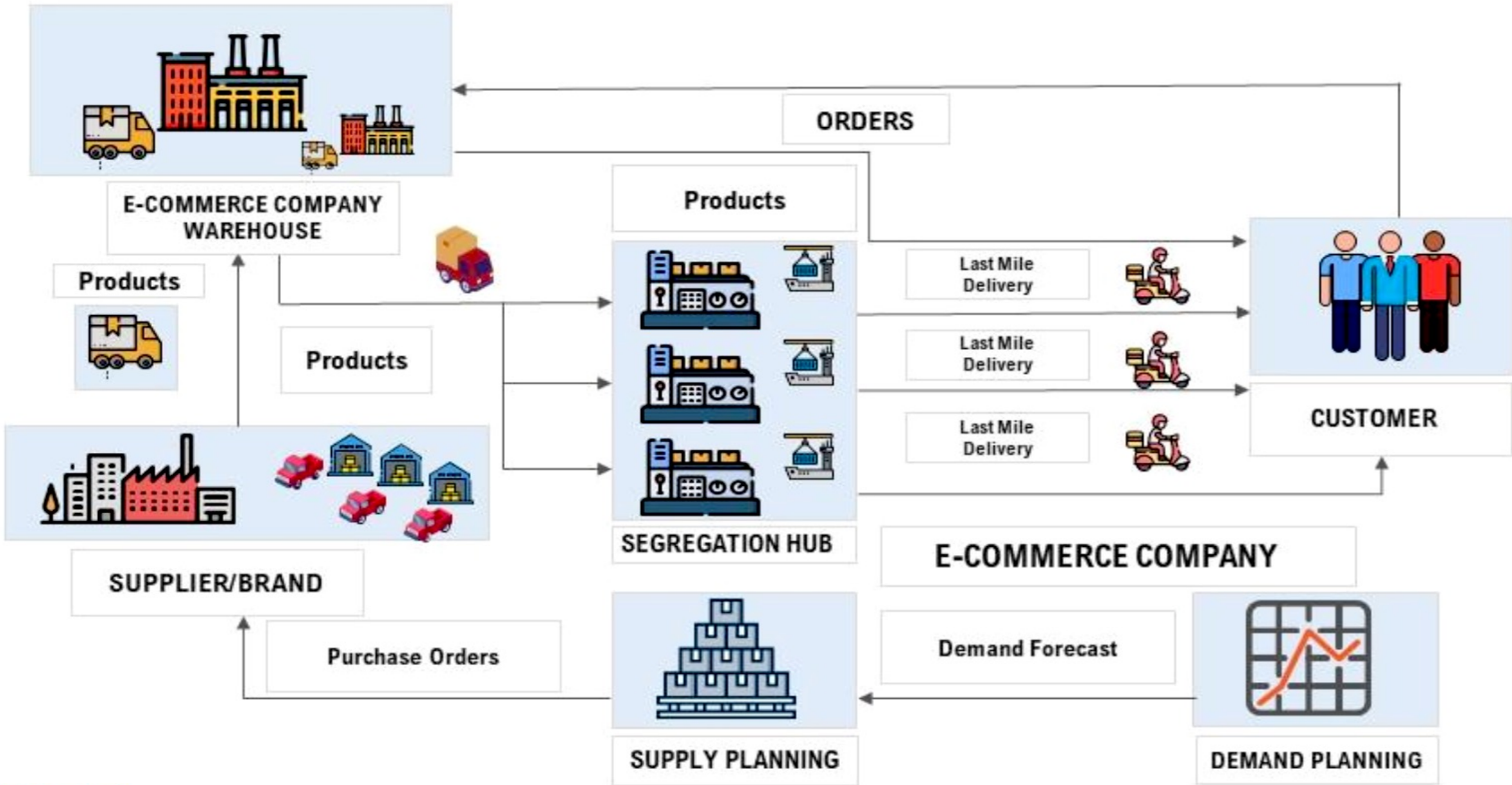
Communications service
Other costs
Refuse removal
Computer hardware software, and other equipment
Professional technical, and data services
Consumer demand
Design
Volume of production
Net inventories shipped
Depreciation
Net income
Shipments
Payroll, benefits and employment
Capital expenditures: building & other structures (new and used)
Capital expenditures: machinery and equipment
Materials, parts, containers, packaging, etc. used
Contract work and resales
Purchased fuels and electricity
Maintenance and repair
Intermediate goods
Recycling
Waste

Have we ever tried to map it all?

And keep
It updated?

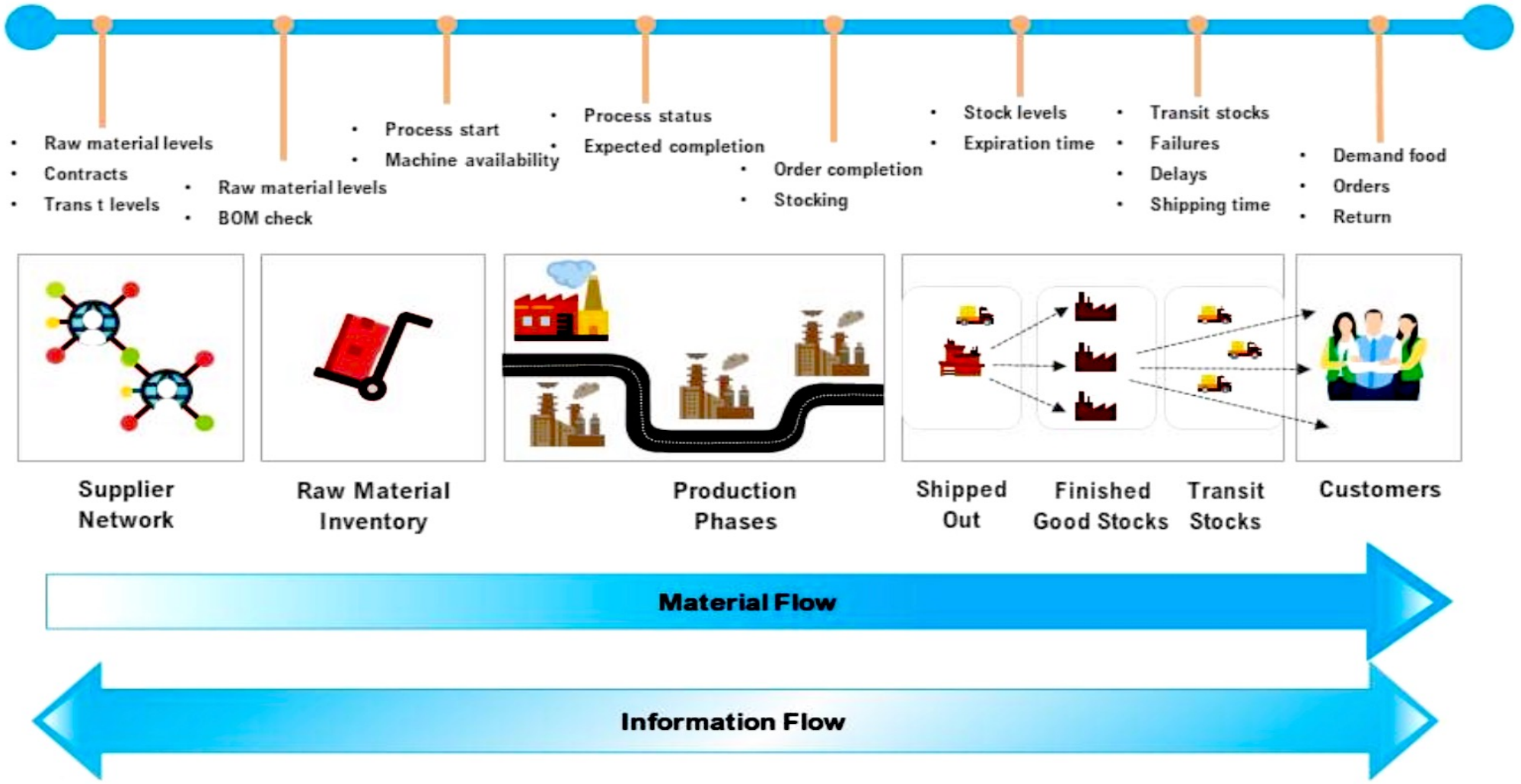
Do we know
Which staff
Owns which
Supplier partner
Relationship and
Who is contact
Person there?

E-Commerce Supply Chain Flow



Emerging Today

IOT Manufacturing Supply Chain Flow

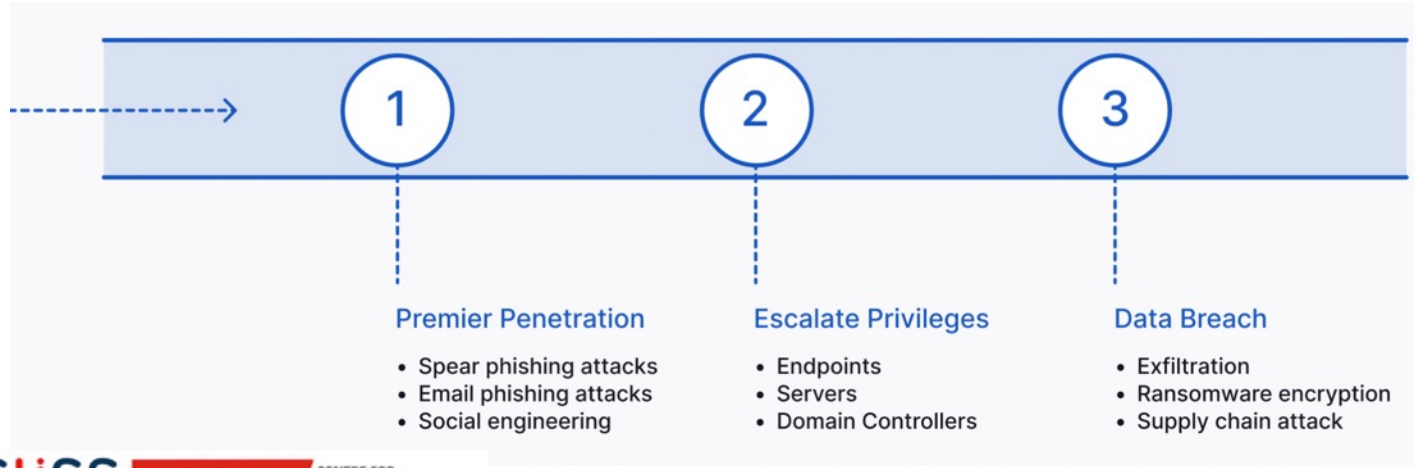


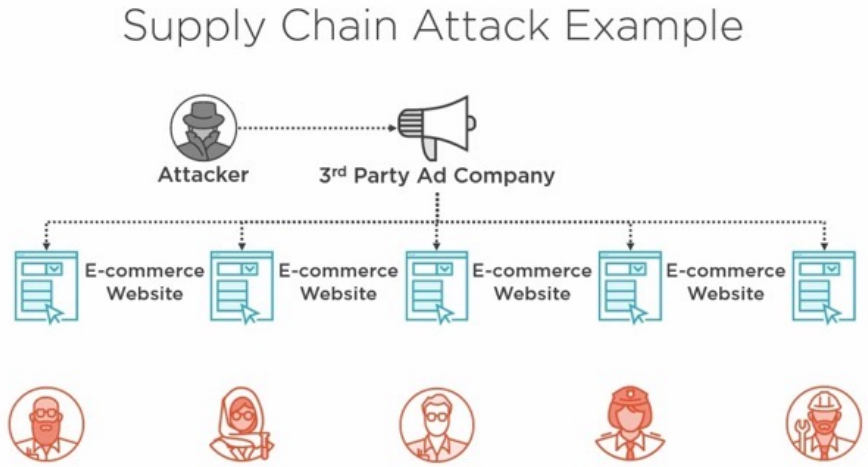
What is a Supply Chain Attack?

- A supply chain attack is a type of cyberattack where an **organization is breached though vulnerabilities in its supply chain**. These vulnerabilities are usually linked to vendors with poor security postures.

- Vendors require access to private data to integrate with their users, so if a vendor is breached, its users could also be compromised from this shared **network or data pool.**

- Because vendors have a vast user network, a single comprised vendor often results in multiple businesses suffering a data breach. This is what makes supply chain attacks so efficient - instead of laboriously breaching each target individually, **multiple targets can be comprised from just a single vendor.**





Some types of supply chain cyber attacks

- **Upstream server attacks**

most common; a malicious actor infects a system that is “upstream” of users, such as through a malicious update, which then infects all the users “downstream” who download it. (SolarWinds case).

- **Midstream attacks -** target intermediary elements such as software development tools.

- **Dependency confusion attacks**

exploit private internally created software dependencies by registering a dependency with the same name but with a higher version number on a public repository. The false dependency is then likely to be pulled into the software build instead of the correct dependency.

- **Stolen SSL and code-signing certificate attacks**

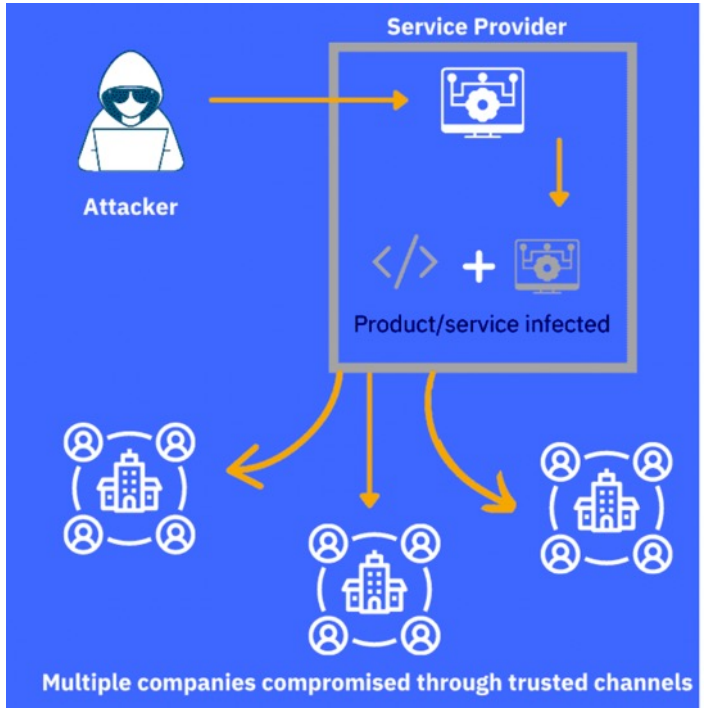
compromise the private keys used to authenticate users of secure websites and cloud services. (Stuxnet)

- **CI/CD infrastructure attacks**

introduce malware into the development automation infrastructure, such as by cloning legitimate GitHub repositories.

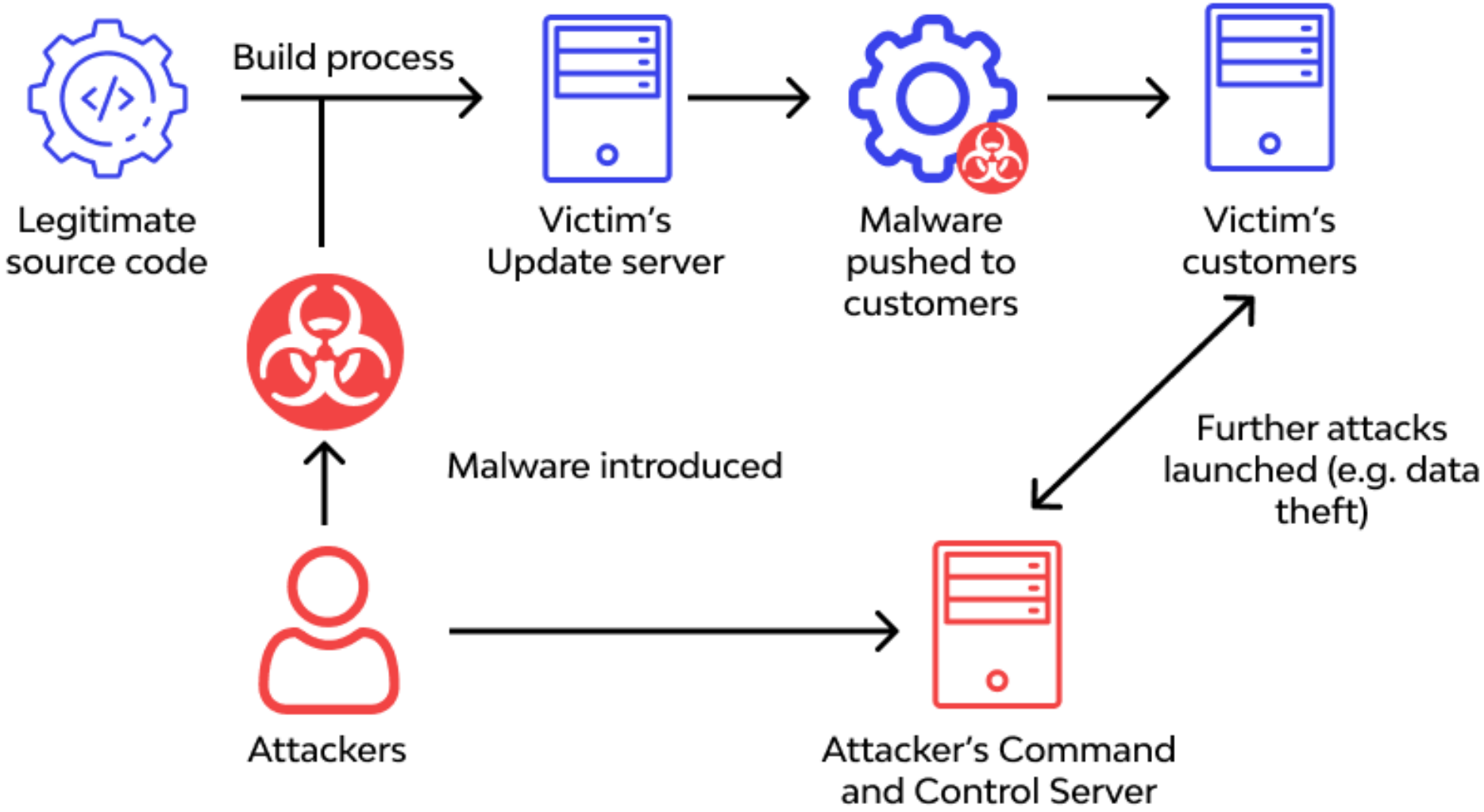
- **Open source software attacks**

introduce code into builds that propagate downstream to those who use the build.



Software Supply-Chain Cyber-Attack

wallarm

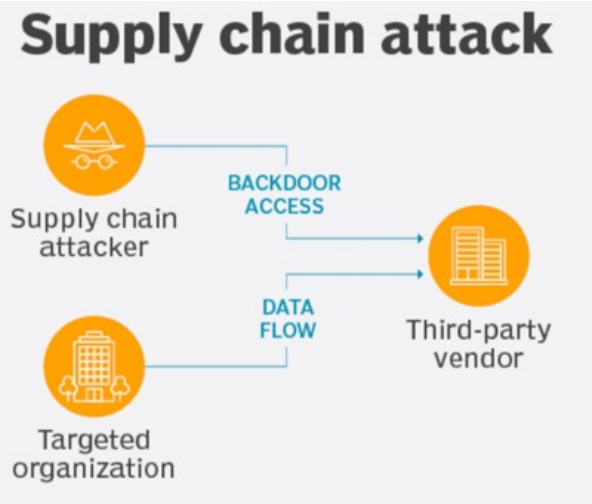


SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

Some Supply Chain Attack Statistics

Per CrowdStrike's 2021 Global Security Attitude Survey:

- 84% believe that **software supply chain attacks could become one of the biggest cyber threats** to organizations like theirs within the next three years
- Only 36% have **vetted all new and existing suppliers for security purposes** in the last 12 months
- 45% of respondents' organizations **experienced at least one software supply chain attack in the last 12 months**, compared to 32% in 2018
- 59% of organizations that suffered their first software supply chain attack did not have a response strategy



- **Attacks on the Rise**

Supply chain attacks are on the rise by **430%** because as enterprises have become better at hardening their environments, malicious attackers have turned to softer targets and have also found more creative ways to make their efforts difficult to detect and most likely to reach desirable targets.

Per a Recent European Union Report

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES
CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

Some Common Risks to Supply Chain Businesses

Security Boulevard

- **Data leaks**

- can happen through external and internal attackers. Employees, hackers, malicious competitors, and managers can all leak sensitive data and personal information outside the business, often inadvertently.

- **Security breaches**

- usually occur when a hacker or malicious user infiltrates an operating system or network without permission. The target is often to cause chaos within the system through data deletion, replication, and corruption.

- **Malware attacks**

- Viruses can infect the system, or trojans can gain access through a back door.
- Also ransomware attack (especially so for OT environments)

- **Phishing attacks**

- One single email phishing for information or that has a link that an employee clicks on can lead to data corruption and loss. If the phishing email is successful, the business could find a username and password used externally to gather information within the system. This could lead to unforeseen competition and serious leaks that can harm the entire corporation.

General Premise

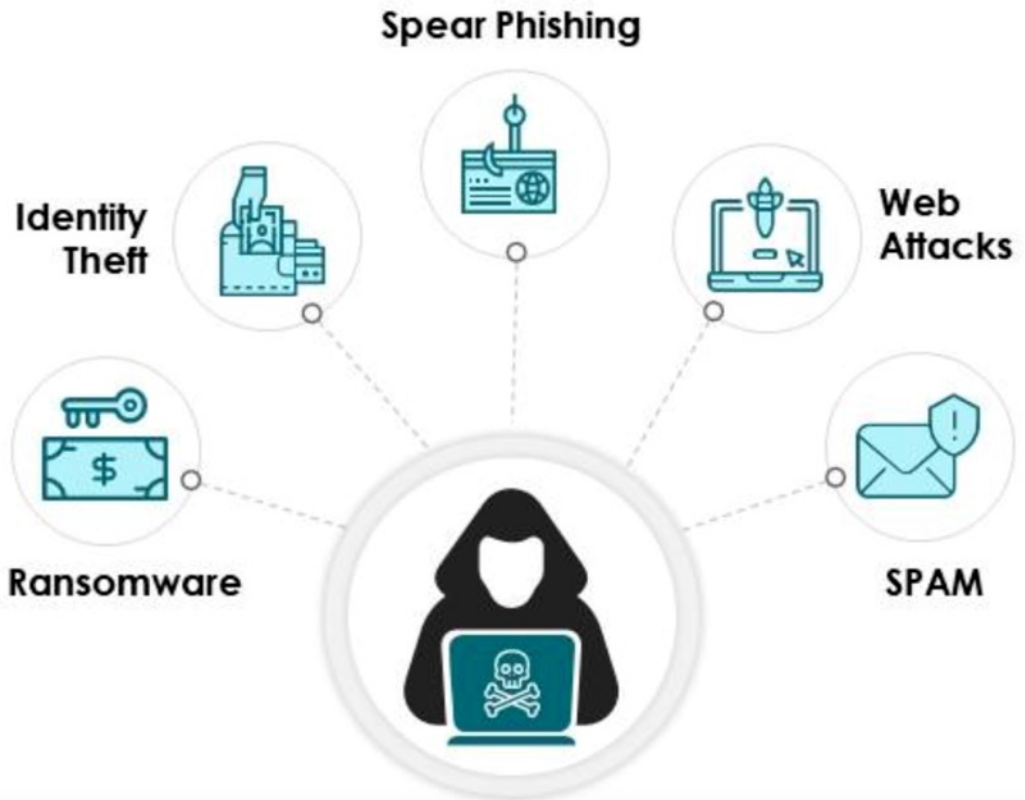
Hackers know the target, a big company, will usually have good cybersecurity so they attack through the supply-chain partners, which are seen as smaller companies with less cybersecurity.

Key Statistics of Cyber Security in Small Businesses

Cyber attack and breaches

- **60%** Cyber attack in small business
- **55%** of small businesses recognized as cyber attack victims
- **32%** Cyber attacks are on manufacturers
- **$59K** Is approximately the cost of data breach

Cyber attack and breach type



SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

Not all suppliers are small companies

In 2019 hackers attacked Rolls Royce to get into Airbus to steal intellectual property

TechXplore

Hackers target Airbus suppliers in quest for commercial secrets

26 September 2019, by Daphne Benoit, Fabien Zamora, Laurent Barthelemy and Mathieu Rabechault

This picture shows an Airbus A-320 of the Iberia airline during take-off on September 24, 2019 at the airport in Duesseldorf, western Germany.

European aerospace giant Airbus has been hit by a series of attacks by hackers targeting its year.

AFP's sources said the hackers targeted British engine-maker Rolls-Royce and the French technology consultancy and supplier Expleo, as well as two other French contractors working for Airbus that AFP was unable to identify.

Airbus did not immediately reply to a request for comment.

A spokesperson for Rolls-Royce declined to comment on the specifics of any attack but said: "We have experience of attempts to gain access to our network and we have a team of experts who work closely with the relevant authorities to ensure that we combat these attempts and minimise any potential impact."

Expleo said it would neither "confirm nor deny" that it had been targeted.

Some Supply Chain Cyber Attack Mitigations

1. Properly identify and inventory access points

An important starting point for securing systems and data is by identifying all points of access. To understand which of those represent the highest risk, you need to determine whether a breach of an access point would have expansive consequences, such as a threat to the health and safety of personnel or the public, inability of the business to fulfill its core mission or material loss of revenue.

2. Establish zero trust policies

When assigning access rights and privileges to users, embrace the principle of zero trust, which grants users access only to the information and applications required to do their job and nothing more. This applies to both internal and third-party users.

3. Restrict access through fine-grained controls

Controlling who can access your critical assets, data and systems is the best way to keep any access point safe. Whether it's through multi-factor authentication, time-based controls or other methods, restricting who can walk through that metaphorical door keeps the assets behind that door safe.

infosecurity GROUP MAGAZINE

- Privileged Access Management (PAM)
- Network Segmentation
- Zero Trust
- Identify potential insider threats
- Cyber threat awareness training
- Identify and protect vulnerable resources
- Minimize access to sensitive data
- Implement strict shadow IT rules
- Send regular third-party risk assessments
- Monitor vendor network for vulnerabilities
- Identify all vendor data leak
- Third-part external threat intelligence

Supply-chain Cybersecurity – more considerations

- **Limit the number of suppliers you use**

– It is a lot easier to manage a few outside parties instead of many.

- **Develop a minimum cyber standard for suppliers**

– Put the cyber standard you want your suppliers to adhere to in your contract. Use a recognized third-party standard so everyone is working to a standard set of rules.

- **Check your suppliers are following some standard**

– Regularly monitor your suppliers' adherence to an agreed standard.

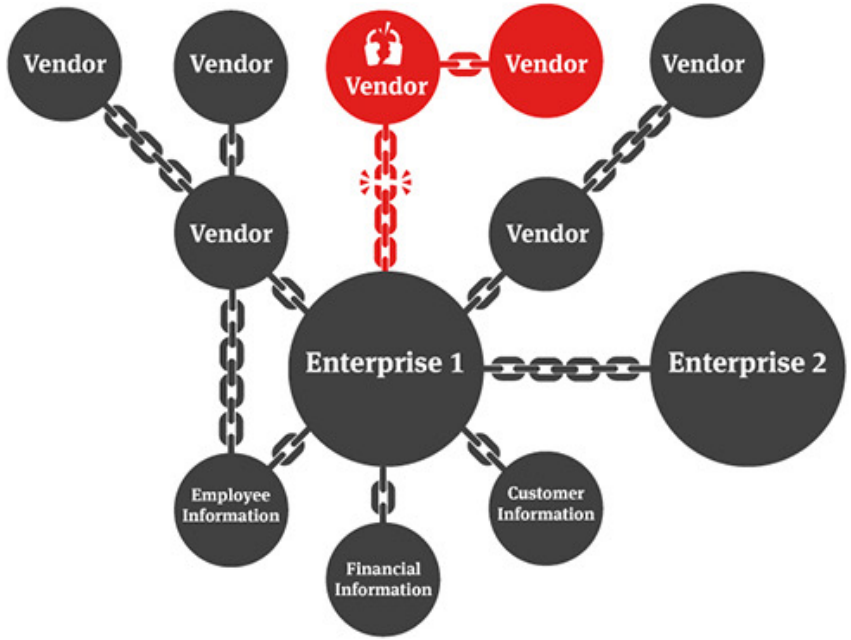
- **Share information on how to improve**

– Let your suppliers know what you and others in your industry are doing to improve your data security so that they can adopt similar measures.

- **Encourage open reporting**

– If a problem does arise, you want to know about it as quickly as possible.

Security Boulevard



SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

How can supply chain attacks be prevented

wallarm

1 Limit User ability to install software

Limiting your users ability to install software can greatly reduce the opportunity for attacks.

2 Review access to sensitive data

Regular reviews of your sensitive data and controlling who has access to it can ensure that software and users that do not have more access than they need.

3 Evaulate your supplier network

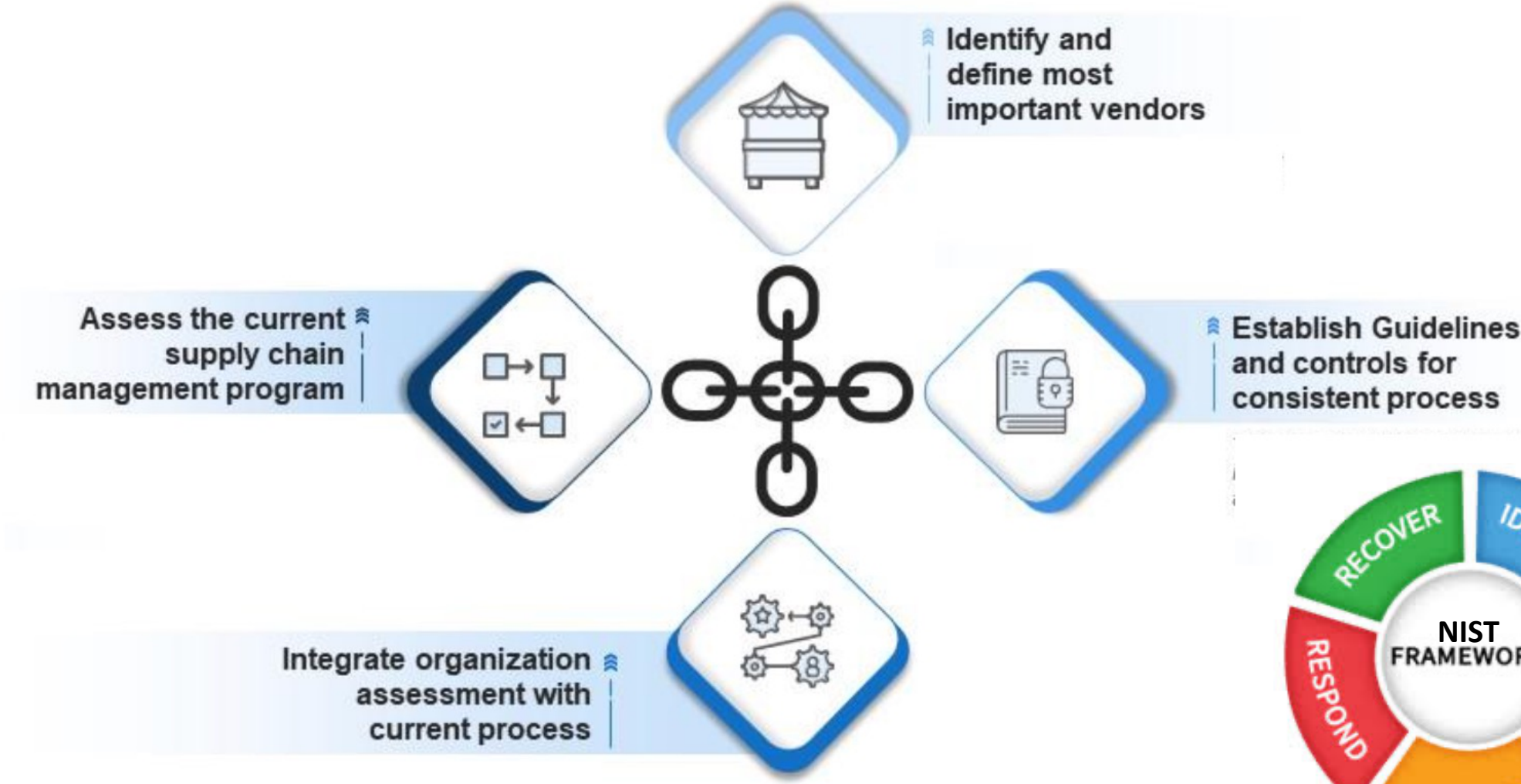
Third-party service providers and software vendors must maintain a certain level of trust and transparency. On average 470 third-parties have access to sensitive information and keeping it safe is imperative.

4 Continually monitor and review

The nature of cyber-attacks is continually evolving. New exploits and vulnerabilities are coming out all the time. The true way to combat these threats is to continually assess, design, execute and protect.

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

Key Approaches for assessing Supply Chain Risk Management



Key Steps for implementing Supply Chain Risk Management

(Not something new)

Identify

- Identify the key risks involved in supply chain

Quantify

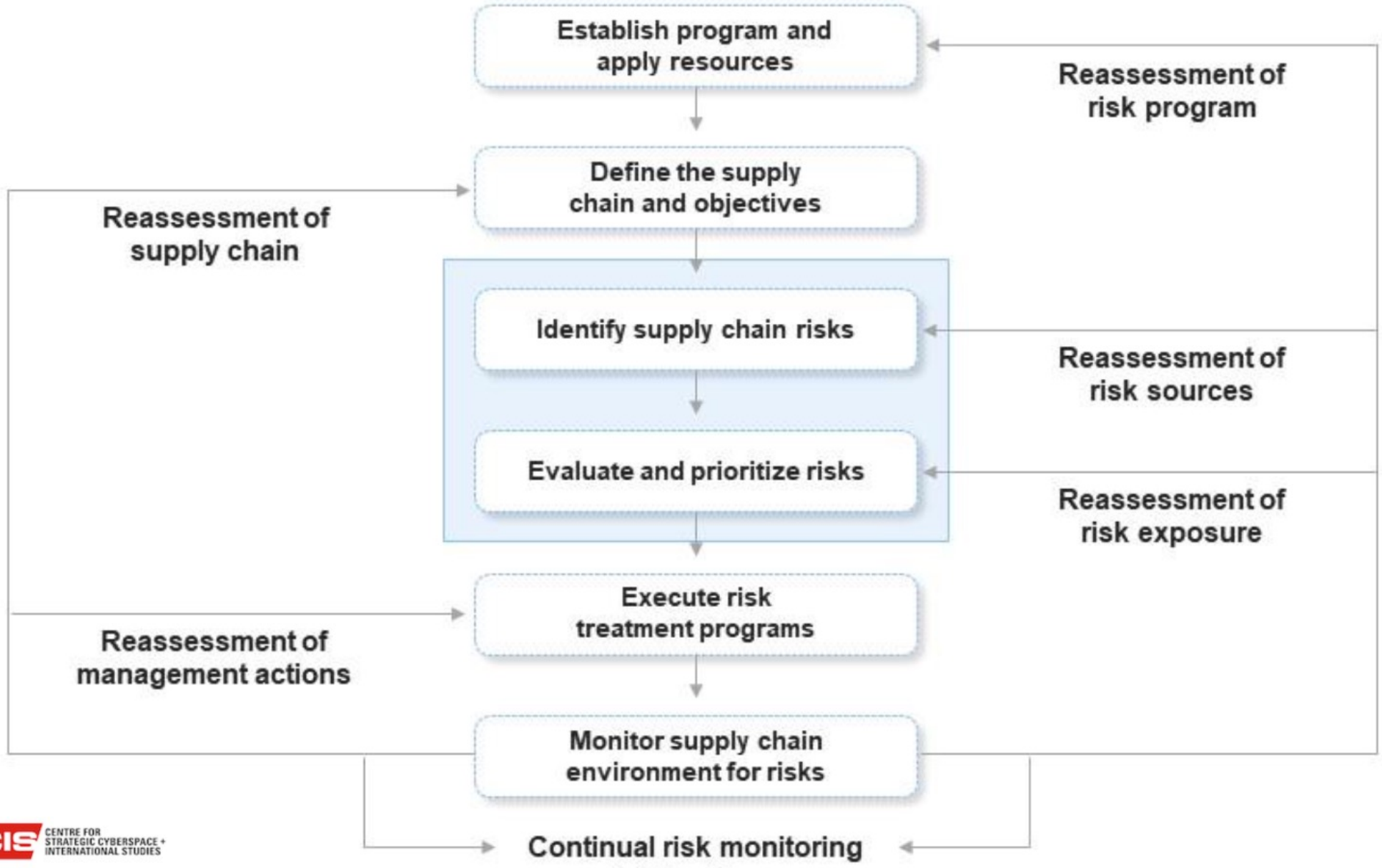
- Analyze the impact on sales and profitability

Respond

Mitigate

- Develop mitigate strategies and tactics to minimize the risks

Supply Chain Risk Management Model with key Areas



Supply Chain Cybersecurity – there's hope yet

Cybersecurity Supply Chain Risk Management C-SCRM

Publications

The following NIST-authored publications are directly related to this project.

Series & Number	Title	Status	Released
SP 800-161 Rev. 1	Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations	Final	05/05/2022
NISTIR 8276	Key Practices in Cyber Supply Chain Risk Management: Observations from Industry	Final	02/11/2021
NISTIR 8272	Impact Analysis Tool for Interdependent Cyber Supply Chain Risks	Withdrawn	08/25/2020
NISTIR 8179	Criticality Analysis Process Model: Prioritizing Systems and Components	Final	04/09/2018
ITL Bulletin	Increasing Visibility and Control of Your ICT Supply Chains	Final	06/15/2015
White Paper	Final Report: Leveraging the Cyber Risk Portal as A Teaching & Education Tool	Final	06/10/2015
NISTIR 8041	Proceedings of the Cybersecurity for Direct Digital Manufacturing (DDM) Symposium	Final	04/10/2015
SP 800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations	Withdrawn	04/08/2015
White Paper	Summary of the Workshop on Information and Communication Technologies Supply Chain Risk Management, National Institute of Standards and Technology, October 15-16, 2012	Final	07/10/2013
White Paper	Proof of Concept for an ICT SCRM Enterprise Assessment Package	Final	12/01/2012
ITL Bulletin	Practices for Managing Supply Chain Risks to Protect Federal Information Systems	Final	11/27/2012
NISTIR 7622	Notional Supply Chain Risk Management Practices for Federal Information Systems	Final	10/16/2012
White Paper	The ICT SCRM Community Framework Development Project: Final Report	Final	12/01/2011
White Paper	Assessing SCRM Capabilities and Perspectives of the IT Vendor Community: Toward a Cyber-Supply Chain Code of Practice	Final	04/01/2011

NIST Special Publication
NIST SP 800-161r1

Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations

Jon Boyens
Angela Smith
Computer Security Division
Information Technology Laboratory

Nadya Bartol
Kris Winkler
Alex Holbrook
Matthew Fallon
Boston Consulting Group

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-161r1

May 2022

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

There's hope yet …
ISO-27036 : Cybersecurity — Supplier relationships

- Create an information security policy for supplier relationships that outlines policies and procedures and mandates controls for managing risk.
- Establish contractual supplier agreements for any third party that may access, process, store, communicate, or provide IT infrastructure to an organization's data.
- Include contractual requirements to address risks associated with information technology services and product supply chains.
- Monitor, review and audit supplier service delivery.
- Manage changes to supplier services and re-assess risks when necessary.

There's hope yet (cont'd) – ISO-27036 : Some more examples of attributes

The standards covers risks such as:

- Acquirer's reliance on providers, complicating the acquirer's business continuity arrangements (both resilience and recovery);
- Physical and logical access to and protection of second and third party information assets;
- Creating an 'extended trust' environment with shared responsibilities for information security;
- Creating a shared responsibility for conformity with information security policies, standards, laws, regulations, contracts and other commitments /obligations;
- Coordination between supplier and acquirer to adapt or respond to new/ changed information security requirements;

... and more.

- Preliminary analysis, preparation of a sound business case, Invitation To Tender etc., taking into account the risks, controls, costs and benefits associated with maintaining adequate information security;
- Creation of explicit shared strategic goals to align acquirer and provider on information security and other aspects (e.g. a jointly-owned 'relationship strategy');
- Security management procedures, including those that may be jointly developed and operated such as risk analysis, security design, identity and access management, incident management and business continuity;

Some Additional Solution Approaches to Supply Chain Cyber Attacks

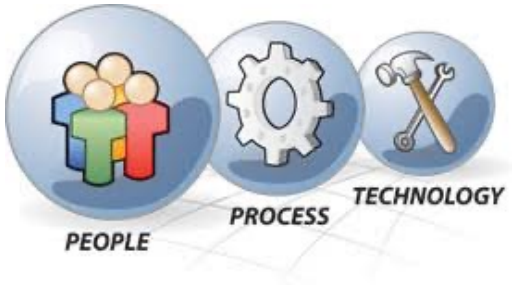
- Firmware security assessment
- Third-party external threat intelligence service
- Requiring suppliers to have application security testing
- Implement Zero Trust across supply chain eco-system.

- (supplier also means eco-system partner, sub-contractor, consultant, intern, temp staff etc.)
- Don't forget your cloud service providers (if any)

But before you go worry about the supplier …

- **Fully understand the threat to the supply chain business.**
- **Assess your own cybersecurity measures.**
- **Improve your current measures.**
- **Treat cybersecurity as an ongoing process.**

(Matt 7:3-5)



Third-party External Threat Intelligence

- **Identify Active Threats Impacting Your Third Parties**

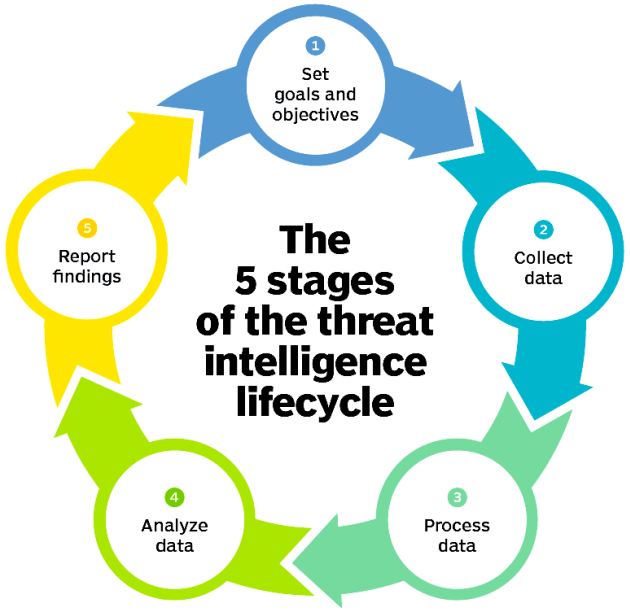
- clear, deep and dark web.

- **Triage Your Third Party Risk**

- alongside other risk assessment solutions, identify third parties that have a high external threat profile

- **Compare Risks Based on Industry Benchmarks**

Rapid7 Intsights



Assessing Third-Party External Digital Risk -

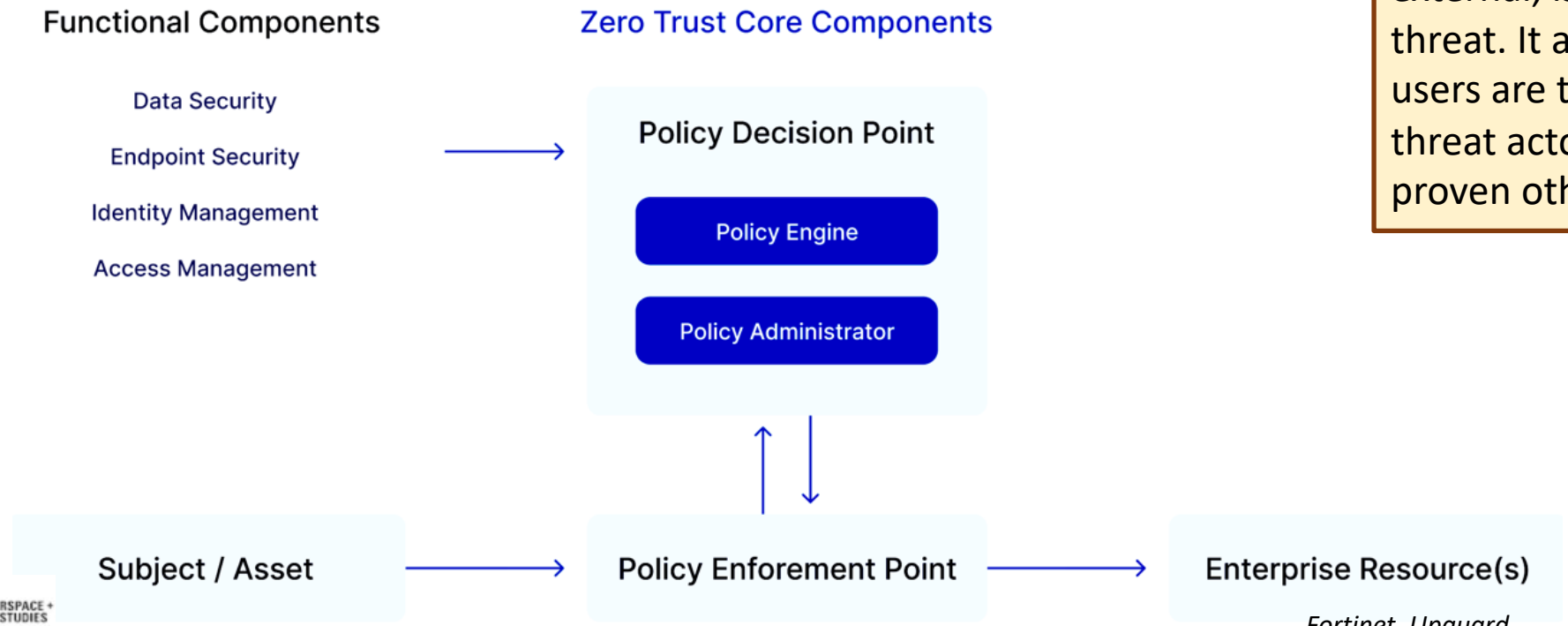
1. Leverage Your Digital Footprint for Context and Relevancy
2. Focus on Action, Not Searching
3. Leverage Automation & Integrations
4. Expanding Protection to Your Customers and Brand
5. Take Down Fraud Campaigns & Cyber Scams

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

Zero-Trust for Supply IT Chain Network Security

1. **Knowledge and Awareness**
   - Who is on the network
   - What is on the network
   - What happens to managed devices when leaving the network.
   - Intelligence and monitoring (when / what you can)

2. **Least Privilege Principle ("need to know" access)**



Zero Trust, a Cybersecurity architecture developed by US NIST, assumes all network activity, whether internal or external, is a security threat. It assumes all users are threats or threat actors until proven otherwise.

Fortinet, Upguard

Operational Technology (OT) Cybersecurity

The 10 Operational Technology Security Controls

Require of at least some of these practices of your Key eco-system partner

Also consider **IEC-62443** Framework for Securing industrial Automation and Control systems (IACS). Helps provide an effective solution for industrial supply chains.

Source: Gartner
743174_C

Supply Chain Cyber attack and security -

Don't Forget About Business Continuity ☺

Remember classic issue in cyber-security : Single Point Of Failure

(would Haagen Dazs have a second concurrent vanilla bean supplier to cut over to in the situation?)

A SCM BCP considers the following, for a start –

- What are the possible threats?
- What is the impact of each threat?
- Is it possible to mitigate a disruption?
- How will full operations be restored?

- **Which suppliers have a network access with your organization – VPN, intranet, extranet, cloud services**
- **Which suppliers relationships involve software application, software development or firmware?**

Inventory Status List of Supply Chain

- Have an updated, current list of all your suppliers, sub-contractors and ecosystem partners.
- Attempt to map out which ones in turn have sub-contractor suppliers that affect or roll up to you.
  - Ask them in turn how they ensure if any issue is mitigated so as to not or minimize disruption
- Decide which supply chain needs a 2nd-line or back-up or concurrent 2nd supplier, ready to activate.
- Decide which supply chain has too many suppliers of the same items and if 'right-sizing' is to be done.
- Ensure a clear and open incident response process between you and each supplier.

Proposed Framework : BCM for Supply Chain Resilience

Business Continuity Management

1. Examine Organizational Context of Supply Chain

- Creation of a supply chain map and formulating joint strategies for the supplychain.

2. Executive Leadership Commitment

- assigned executive owner

3. Prevention (Mitigation Tactics)

- Examination of supply chain map for vulnerable elements and sources of risk in all stages of the chain: procurement, internal operations, and distribution-side risks.

4. Recovery (Response Tactics)

- Planning for disruptions: Development of contingency plans (alternate suppliers, re-routing capabilities, including alternative communications lines, etc.) to address disruptions in supply, internal operations and distribution

5. Assessment of Plans

- Testing the procedures developed, with vendors, customers and key service providers through simulated disruptions

6. Continuous Improvement

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES

IEEE ENGINEERING MANAGEMENT REVIEW,VOL.48,NO.3, NIST, ISO-27036

Supply Chain Cybersecurity – A Closing Thought

- "Supply chain cyber-attacks will continue to proliferate in the digital space, and in time to come, companies could be required to demonstrate their cybersecurity posture when they conduct business as a way of providing greater assurance to their customers." – David Koh, Chief Executive, CSA

We need to push for international policy and behavior standards in cyberspace, with clear consequences around critical infrastructure attacks and commercial IP theft. This will help establish clear policy on malicious cyber activity, prevent cyber adversaries from using international borders to escape prosecution, and will spell out repercussions for attacks on critical assets.

FORTINET

… input mandatory expectations into contracts regarding security levels and assurance checks. Australia's mandatory breach reporting legislation is on the cusp of assent and affected business will need to comply. Where does the responsibility lie – with the business or the supplier?

KPMG

Thank you!

Supply Chain – A New Attack Vector
Anthony Lim
22 Sep 2022

SUSS SINGAPORE UNIVERSITY OF SOCIAL SCIENCES
suss.edu.sg

CSCIS CENTRE FOR STRATEGIC CYBERSPACE + INTERNATIONAL STUDIES
cscis.org

v.1.2

Corinium connected thinking