Aalto-yliopisto
Aalto-universitetet
Aalto University

Cybersecurity Management

Utilizing external service providers and expertise in security solution procurement

Lecture 2: Analyzing Cybersecurity Procurement for various Sectors

Euroopan unionin rahoittama – NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

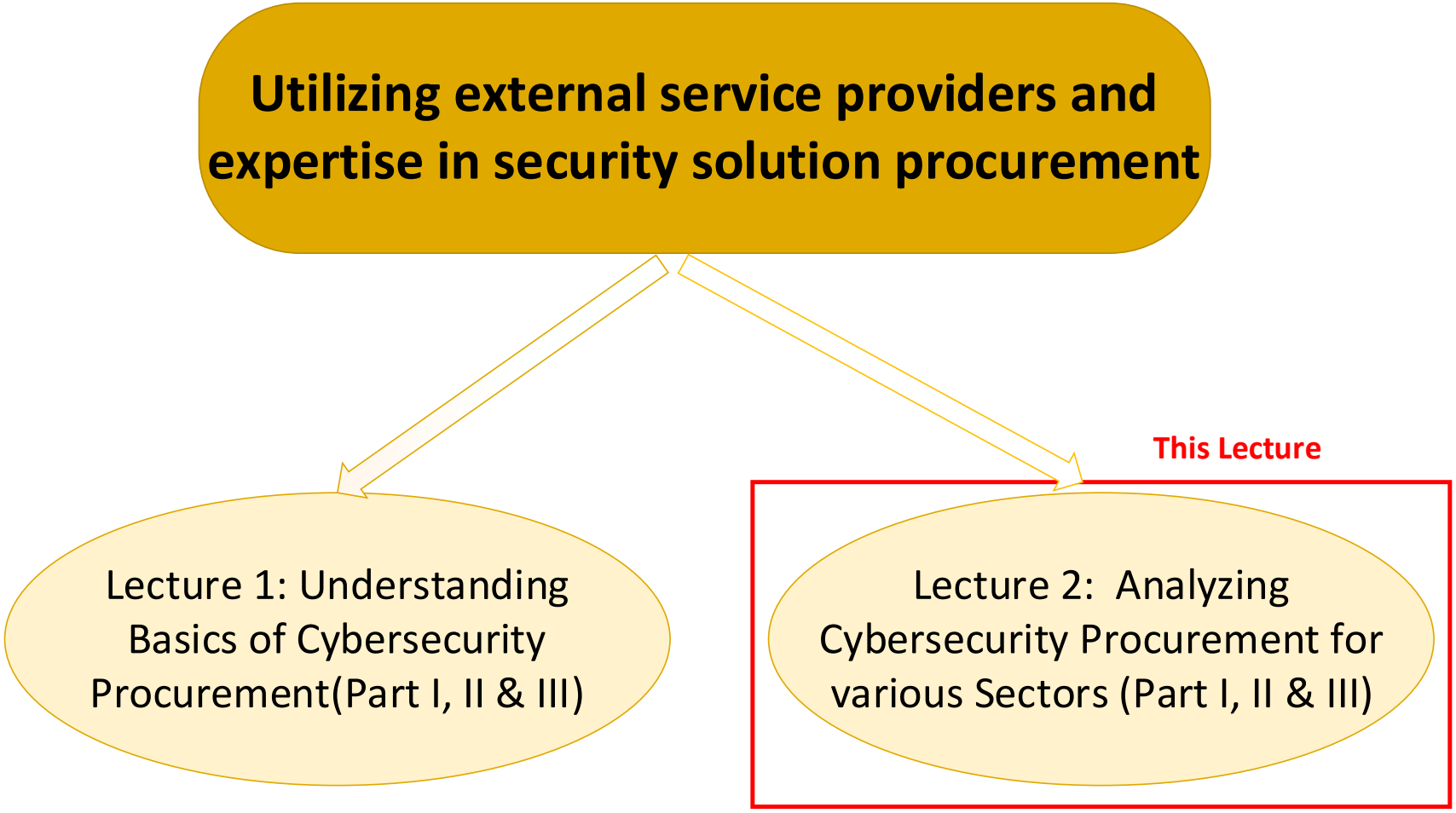
Cybersecurity Management

Dr. Tanesh Kumar

Staff Scientist,
Department of Information and
Communications Engineering, Aalto University

Email: **tanesh.kumar@aalto.fi**

Lecture Distribution



Outline: Lecture 2

- Lecture 2 is divided in three parts:
  - **Part I: Analyzing Cybersecurity Procurement: Warehouse Logistics & Freight Forwarding**
    - **Introduction**
    - **Overview of Cybersecurity threats**
    - **Areas/operations to consider for cybersecurity procurement**
    - **Which cybersecurity services can be Outsourced**
    - **Selecting the vendor for cybersecurity procurement**
  - Part II: Analyzing Cybersecurity Procurement: Retail Companies
  - Part III: Analyzing Cybersecurity Procurement: Media Companies

Aalto-yliopisto
Aalto-universitetet
Aalto University

Cybersecurity Management

Utilizing external service providers and expertise in security solution procurement

Lecture 2: Analyzing Cybersecurity Procurement for various Sectors

Part-I

Analyzing Cybersecurity Procurement: Warehouse Logistics & Freight Forwarding

Euroopan unionin rahoittama – NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Introduction

Analyzing Cybersecurity Procurement: Warehouse Logistics & Freight Forwarding

Introduction

- Warehouse Logistics and Freight Forwarding are two highly important sub-sectors in the entire supply chain management/logistics.
- ***Warehouse logistics:*** sub-part of overall supply-chain management and involves physical flow of goods/data/information from receiving to shipping/distribution.
  - Good receiving, storage, inventory management, picking, packing, good distribution.
- ***Freight Forwarding:*** sub-part of overall logistics/supply chain provides strategic planning/coordination and international transportation of goods from origin to source.
  - customs clearance, coordinating international transport, pick-up & delivery services.
- Both of these have multiple overlapping cybersecurity requirements to ensure that various business operations are protected.
- The kind of attacks both the domain face are quite similar as well, however, the context and severity of the attacks may be different.
  - Frequent occurrence of data breaches, phishing, DDoS, malware/ransomware.

A!

Source: https://logisticsviewpoints.com/2024/03/14/cybersecurity-the-first-line-of-defense-for-your-warehouse/
Source: https://cybercompare.com/benefits-of-a-comprehensive-cybersecurity-procurement-process/
Source: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=934690

Overview of Cybersecurity Threats

Analyzing Cybersecurity Procurement: Warehouse Logistics & Freight Forwarding

Analyzing Cybersecurity Procurement: Threat Landscape

Cybersecurity Threats in Warehouse Logistics

Data Breaches	Since warehouses contain massive volume of sensitive data, hackers or cybercriminal can steal it
Ransomware Attacks	Type of malware injected to gain system/data access by attacker and corresponding ransom is asked
Phishing Threats	Attacker can get unauthorized access to warehouse systems through malicious links/email/messages
DDOS Attacks	Flooding of massive traffic to warehouse network that may cause service disruption
IoT/Automation Attacks	Adversaries target IoT devices, RFID, equipment, machinery and get unauthorized access to warehouse
Malware	Injection of malicious software in system/network of warehouse that cause disruption in operations
Third-Party Attacks	Attacker exploit cybersecurity shortcomings associated third-parties & compromise devices/data

Cybersecurity Threats in Freight Forwarding

Data Breaches	Hackers aim to target freight companies to access sensitive data, e.g., customer data, shipment details
Malware/ Ransomware Attacks	Attackers inject malware and encrypt data access by attacker and ransom is asked in return
Phishing Threats	Malicious links/email are sent to freight companies personal to get unauthorized access data
Third-Party Attacks	Attacker exploit cybersecurity shortcomings associated third-parties & compromise devices/data
DDOS Attacks	Massive amount of fake network traffic is generated to overload the network of freight companies
IoT/Automation Attacks	Adversaries target IoT devices, RFID, equipment, machinery and get unauthorized access to freight

A!

Source: https://www.lucasware.com/fortifying-warehouse-and-distribution-centers-against-cyberattacks/
Source: https://scnafrica.com/2023/09/06/cybersecurity-in-modern-warehouses-what-it-means-for-the-supply-chain
Source: https://softlinkglobal.com/cybersecurity-for-freight-forwarders-protecting-data-in-a-digital-world/

Areas/Operations to consider for Cybersecurity Procurement

Analyzing Cybersecurity Procurement: Warehouse Logistics & Freight Forwarding

Analyzing Cybersecurity Procurement: Where Needed

Protection of Sensitive Data

Customer information, shipment schedules, financial data, inventory details.

Third-Party Risks

Interconnected with multiple entities in entire supply chain/ logistics

Compliance and Regulations

Industry specific standards & regulations (transportation, customs, trade, data protection)

Securing IT systems & networks

Ensuring protection of overall IT infrastructure and communication network

Security of IoT Devices/OT Systems

Protection of various smart devices, mobile devices, and operational technologies

Staff Training and Awareness

Whether staff require training about some specific cybersecurity solutions

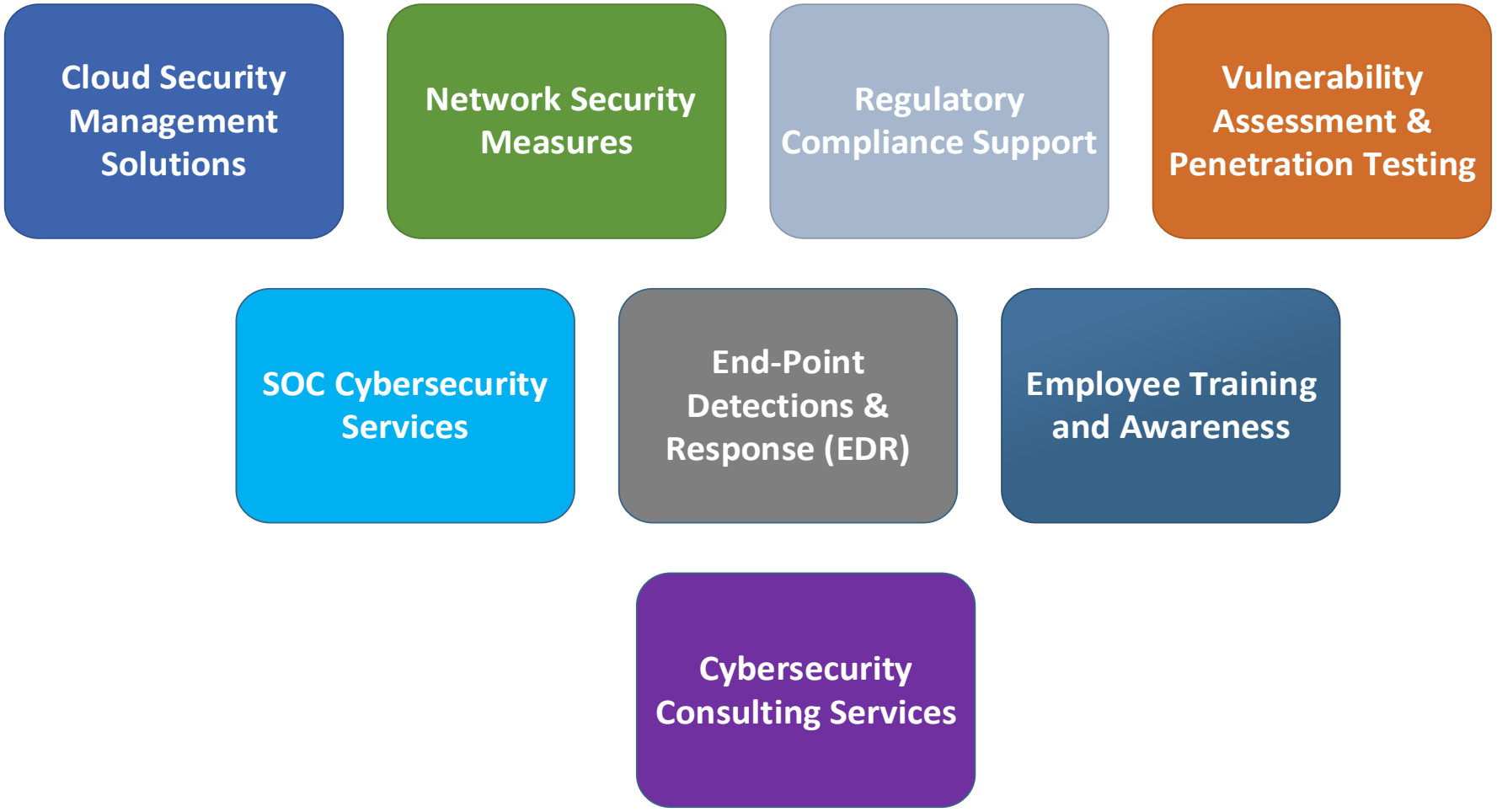
Source: https://www.goworkwize.com/blog/procurement-outsourcing-comprehensive-guide-for-it-teams
Source: https://windowsmanagementexperts.com/supply-chain-cybersecurity-solutions-for-logistics-and-distribution/
Source: https://intellisoft.io/security-logistics-the-guide-to-supply-chain-security-management/

Which Cybersecurity Services can be Outsourced?

Analyzing Cybersecurity Procurement: Warehouse Logistics & Freight Forwarding

A!

Analyzing Cybersecurity Procurement: What Services can be ?



Source: https://intellisoft.io/security-logistics-the-guide-to-supply-chain-security-management/
Source: https://windowsmanagementexperts.com/supply-chain-cybersecurity-solutions-for-logistics-and-distribution/
Source: https://www.bluevoyant.com/knowledge-center/supply-chain-security-why-its-important-7-best-practices

Selecting the Vendor for Cybersecurity Procurement

Analyzing Cybersecurity Procurement: Warehouse Logistics & Freight Forwarding

Selecting the Vendor for Cybersecurity Procurement

Source: https://www.n-ix.com/outsourcing-cybersecurity-services/
Source: https://www.goworkwize.com/blog/procurement-outsourcing-comprehensive-guide-for-it-teams
Source: https://fastercapital.com/topics/vendor-selection-criteria.html
Source: https://www.techmagic.co/blog/cybersecurity-outsourcing/

Selecting the Vendor for Cybersecurity Procurement

1. Need Assessment

- Analyze current cybersecurity posture of company
- Overall risk assessment of various operations
- Identify critical data/information, e.g., customer, inventory details, shipment details
- Identify/assess various threats, e.g., IoT threats, automation vulunerabilites
- Assess third-party/supply chain vulnerabilities
- Define specific regulatory compliance requirements
- Budget estimation

Source: https://www.goworkwize.com/blog/procurement-outsourcing-comprehensive-guide-for-it-teams
Source: https://www.techmagic.co/blog/cybersecurity-outsourcing/

Selecting the Vendor for Cybersecurity Procurement

2. Setting the Selection Criteria

- **Industry Expertise:** Experience in providing cybersecurity solutions to warehouse logistics/freight forwarding sector.
- Range of **offered cybersecurity services** related to warehouse logistics/freight forwarding operations.
- **Security practices** during any cyber incident during warehouse logistics/freight forwarding operations.
- **Regulatory Compliance/Certification** related to freight warehouse logistics/freight forwarding sector.
- Where **v**endor understands value of cybersecurity of whole **supply chain risks**
- Analyze **price structure** and check value for cost
- Check suitable **communication/reporting** mechanism place
- Ensure s**calability and flexibility** to adopt with variable needs of warehouse logistics/freight forwarding
- What kind of different **staff training and awareness** programs it can offer

Source: https://www.goworkwize.com/blog/procurement-outsourcing-comprehensive-guide-for-it-teams
Source: https://www.techmagic.co/blog/cybersecurity-outsourcing/

Selecting the Vendor for Cybersecurity Procurement

3. Research Potential Vendors

- **Identify potential vendors** providing cybersecurity services for warehouse logistics/freight forwarding
- Consider **recommendation/referral** from peers/ professionals
- Review recent **industry reports, forum, articles** about potential vendors in supply chain/logistics**.**
- **Analysis/Assess vendors** based on, e.g., reputation/ expertise, service offering among other factors
- Create **Request for Proposal (RFP)** (vendor details, qualifications, services, technical details pricing)
- **Shortlist potential vendor candidates** based on RFP responses.

Source: https://www.goworkwize.com/blog/procurement-outsourcing-comprehensive-guide-for-it-teams
Source: https://www.techmagic.co/blog/cybersecurity-outsourcing/

Selecting the Vendor for Cybersecurity Procurement

4. Assess/ Evaluate Vendors

- **Meeting/Interviewing** Shortlisted vendors
- Ask for possible **presentation/demonstration/ site visits** to acquire more understanding
- Review **sample/previous reports** of selected vendors
- **Review security solutions/Incident response plan in context of warehouse operations/**
- **Alignment with regulatory compliance** (e.g., transportation, trade, customs, data protection)
- **Risk Assessment and Management**
- Assess **ease of integration**, i.e., compatibility/ flexibility with existing systems/solutions

Source: https://www.goworkwize.com/blog/procurement-outsourcing-comprehensive-guide-for-it-teams
Source: https://www.techmagic.co/blog/cybersecurity-outsourcing/

Selecting the Vendor for Cybersecurity Procurement

5. Negotiate Terms and Finalize Contract / Service Level Agreements (SLAs)

- Clearly **define scope** of required cybersecurity services, role, responsibilities, & expectations
- Agreement about **performance metrics**, e.g., incident response time/handling protocols
- Negotiate **Pricing and payment terms**
- Terms negotiation about **data protection and confidentiality**
- Discuss about **reporting/communication mechanism & support**
- Finalize **termination and exit Rules**
- Agreements on **security awareness & training**
- Terms about maintaining **partnership/future collaborations**

Source: https://www.goworkwize.com/blog/procurement-outsourcing-comprehensive-guide-for-it-teams
Source: https://www.techmagic.co/blog/cybersecurity-outsourcing/

Kiitos
aalto.fi