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-II

Analyzing Cybersecurity Procurement: Retail Companies

Euroopan unionin rahoittama – NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Outline: Lecture 2

- Lecture 2 is divided in three parts:
  - Part I: Analyzing Cybersecurity Procurement: Warehouse Logistics & Freight Forwarding
  - **Part II: Analyzing Cybersecurity Procurement: Retail Companies**
    - **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 III: Analyzing Cybersecurity Procurement: Media Companies

Introduction

Analyzing Cybersecurity Procurement: Retail Companies

Introduction

- Retail sector are companies that sell products and provide services to consumers.
- Different nature of good/products in retail companies include:
  - groceries, electronics, household goods, clothing/fashion, and health/beauty.
- Types of retail sector:
  - Convenience Store, Supermarket, Department Stores, Discount Store, Chain Stores, Specialty store, Online Store.
- Demand of constantly online shopping/e-commerce are constantly growing: a huge boom is seen in e-commerce business specially since COVID-19 pandemic.
- Complex IT/OT setting of retail companies:
  - E-commerce platform, mobile apps, cloud services, online marketplaces, web shops,
  - digital payments, IoT devices, sorting machines/self check outs, warehouse.
  - Overall threat landscape of retail business is significantly wider, and thus cybersecurity procurements can be considered as one of key option.

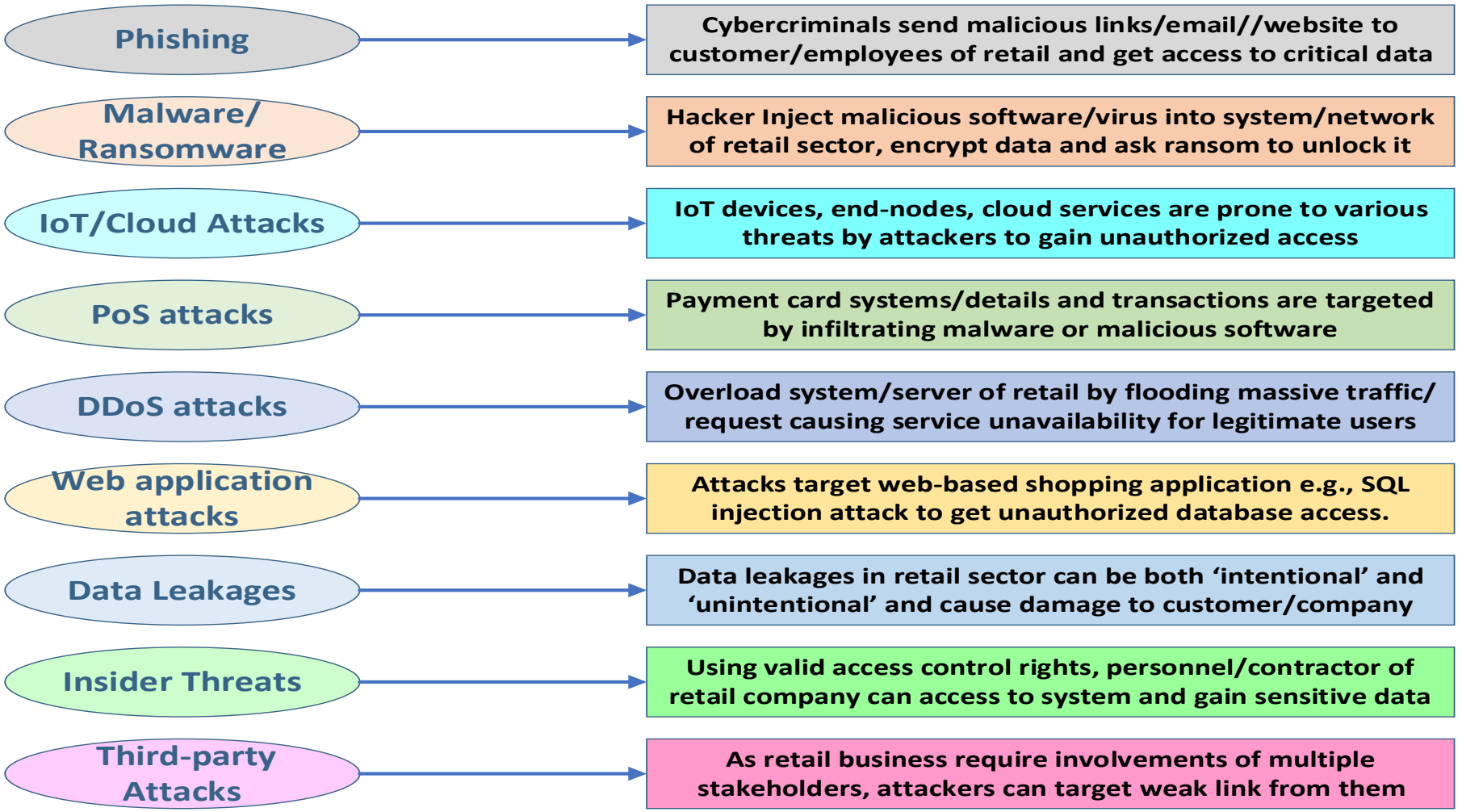
A!

Source: https://www.trendmicro.com/en_se/business/retail-cybersecurity.html
Source: https://docs.broadcom.com/doc/cybersecurity-retail-en
Source: https://link.springer.com/chapter/10.1007/978-981-13-7139-4_18

Overview of Cybersecurity Threats

Analyzing Cybersecurity Procurement: Retail Companies

Analyzing Cybersecurity Procurement: Threat Landscape



Source: https://www.nwcrc.co.uk/post/what-cyber-threats-do-retailers-face
Source: https://www.forbes.com/councils/forbestechcouncil/2023/08/15/19-common-cyberthreats-to-retailers-and-how-to-defend-against-them/
Source: https://link.springer.com/chapter/10.1007/978-981-13-7139-4_18

Areas/Operations to consider for Cybersecurity Procurement

Analyzing Cybersecurity Procurement: Retail Companies

Areas/Operations to consider for Cybersecurity Procurement: Retail

Protection of Sensitive Data

Customer personal information, credentials, payment card data,

Securing E-commerce Platform

Platform protection e.g., websites/mobile Apps

Supply Chain Security

Protection against various risk in entire supply chain/ third-party vendors.

Point of Sale (POS) Security

Ensure strong security measures for PoS systems

Regulatory Compliance

Industry specific standards & regulations (PCI DSS)

Staff Training and Awareness

Training/awareness about some specific cybersecurity solution

Securing Clouds Services

Ensure overall cloud security management

Security of IoT Devices/OT Systems

Protection of smart devices, cameras, mobile & OT

Securing IT systems & networks

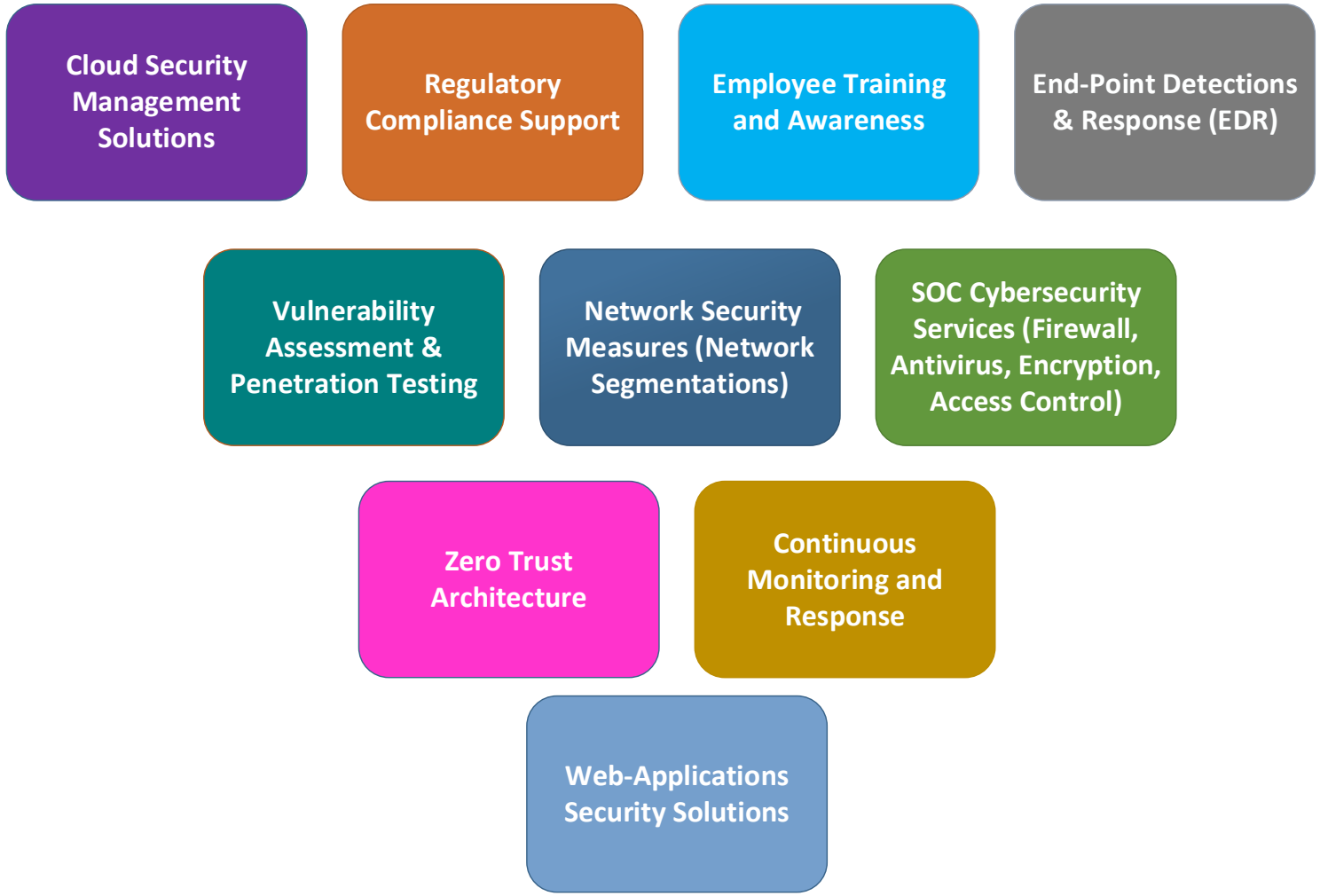
Ensuring protection of overall IT infrastructure & network

Source: https://versprite.com/blog/major-threats-to-the-retail-industry/
Source: https://www.terranovasecurity.com/blog/ways-to-protect-retail-business-from-cyber-attacks
Source: https://link.springer.com/chapter/10.1007/978-981-13-7139-4_18/

Which Cybersecurity Services can be Outsourced?

Analyzing Cybersecurity Procurement: Retail Companies

Which Cybersecurity Services can be Outsourced?: Retail



Source: https://www.bluevoyant.com/knowledge-center/supply-chain-security-why-its-important-7-best-practices
Source: https://www.upguard.com/blog/cybersecurity-challenges-and-solutions-for-the-retail-sector/
Source: https://www.infosecurityeurope.com/en-gb/blog/guides-checklists/cybersecurity-challenges-and-solutions-in-retail-industry.html
Source: https://schneiderdowns.com/our-thoughts-on/fortifying-retail-security-essential-cybersecurity-tools-and-software/

Selecting the Vendor for Cybersecurity Procurement

Analyzing Cybersecurity Procurement: Retail Companies

Selecting the Vendor for Cybersecurity Procurement: Retail

Source: https://www.bocasay.com/cybercrime-protection-choose-a-cybersecurity-company/
Source: https://www.edendata.com/post/how-to-choose-a-cyber-sec-company
Source: https://www.creative-n.com/blog/how-to-choose-a-cyber-security-provider-for-your-business/
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: Retail

1. Need Assessment

- Assessing the current **cybersecurity posture** (existing security measures, gaps/threats)
- Comprehensive **risk assessment** (potential retail related threats, PoS threats, impact).
- Identify retail specific **cybersecurity requirements** (size, critical data/assets, online platforms)
- Specify the regulatory and **compliance requirements** e.g., PCI DSS standards
- **Budget** estimation

Source: https://www.edendata.com/post/how-to-choose-a-cyber-sec-company
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: Retail

2. Setting the Selection Criteria

- Industry **experience/expertise** in providing retail related cybersecurity solutions/POS System
- Range of **offered services** and relevant tools/ technology
- **Security measures** (capabilities of handling various retail vulnerabilities/Incident response plan)
- Alignment with **regulatory compliance** e.g., PCI DSS standards.
- Expertise in **online/E-commerce** security solutions.
- **Price structure** and **reporting/communication** protocols.
- **Scalability/Flexibility** of the solutions and options for **staff training and awareness**

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: Retail

- **Identify potential vendors** providing cybersecurity services in retail industry
- Consider **recommendation/referral** from peers/ professionals
- Review recent **industry reports/aricle, conference & events,** about potential vendors in retail sector
- **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: Retail

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
- **Evaluate industry expertise/experience,** PoSs/e-commerce security, third-party risks
- Analyze **security practices**/Incident response capabilities
- **Alignment with regulatory compliance** (e.g., such as PCI DSS and GDPR,)
- **Risk Assessment and Management**
- Assess **scalability/flexibility**, **ease of integration**, i.e., compatibility 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: Retail

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

- Clearly **define scope** cybersecurity services/ solutions roles, expectations, tools/technologies
- Determine **performance metrics**, e.g., incident response time/system availability
- Negotiate **Pricing and payment terms**
- Terms negotiation about **data protection and confidentiality**
- Discuss about **incident response, 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