EXTENDED ENTERPRISE

NEBRASKACERT'S CYBER SECURITY FORUM

AUGUST 21, 2019

DISCLAIMERS AND LEGALESE

- The views and opinions expressed by the presenter are not necessarily those of the companies I have worked for…and maybe not even myself
- I will cover just a fraction of what you really need to know
- No laughing matter…but laughter is the best medicine

Legal Disclaimer

ME → JOSHUA MAUK

- 23 Years experience with a focus in Security and IT Audit
- Director of Security and Information Protection at OPPD
- Adjunct Instructor at UNO
  - CyberSecurity Policy and Awareness
- What Do I Do Now
  - CyberSecurity
  - Physical Security
  - Disaster Recovery & Business Continuity

WHAT IS THE EXTENDED ENTERPRISE (EE)

- The Extended Enterprise is the concept that an organization does not operate in isolation, because its success is dependent upon a complex network of third-party relationships

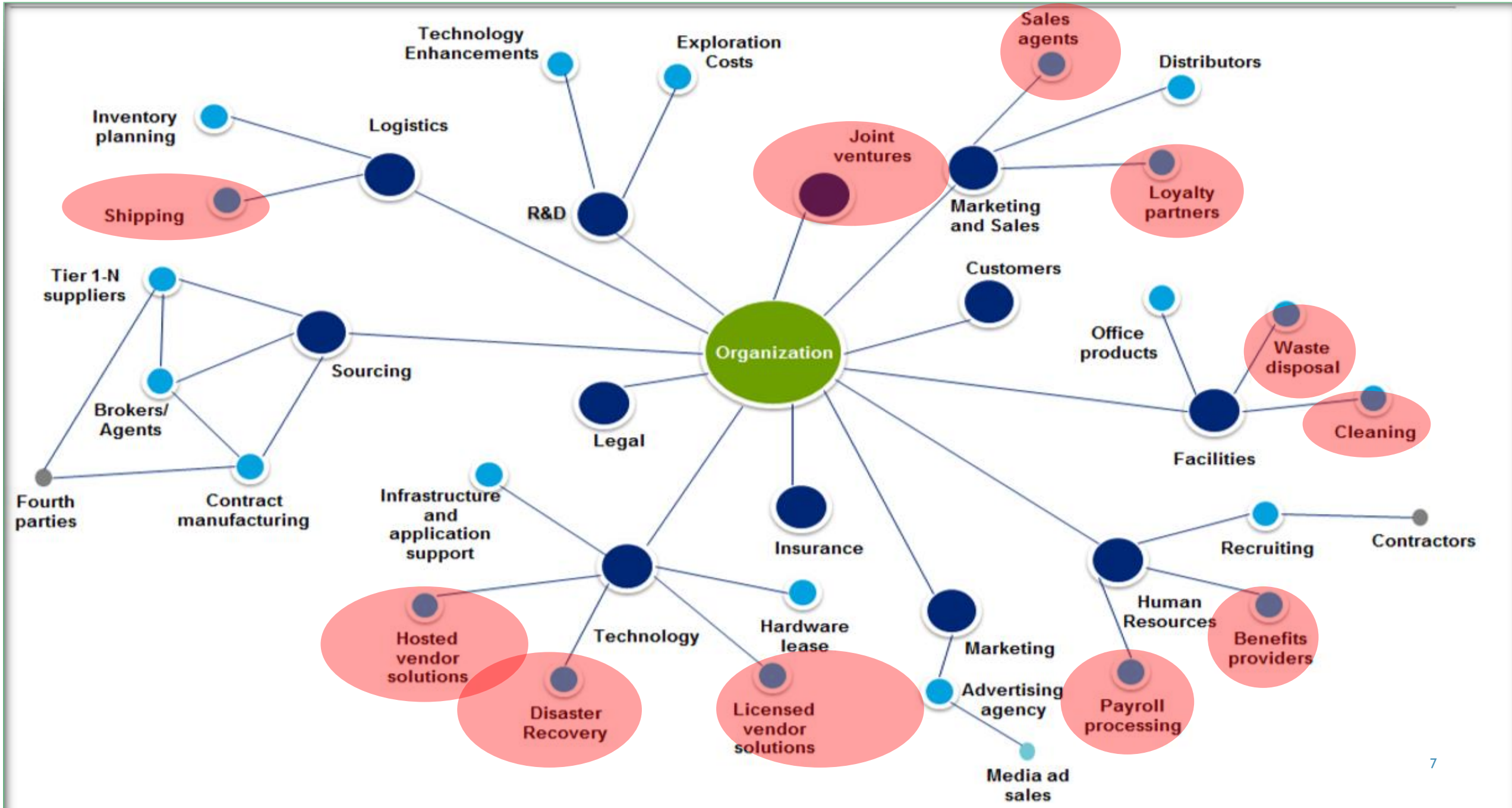
DEFINITIONS

- **Third Party** is any entity not under direct business control of a given organization.
  - Many people equate third parties with vendors, but that's not always the case; consider suppliers of products or services, Business partners (JV partners, alliances, etc.), Marketing partners, Strategic consultants, Government agencies, Regulatory bodies, and **Technology Suppliers**
- **Third Party risk management** encompasses vendor risk management, but is more broadly focused on gaining a understanding of organizational risks and understanding which of those risks may be either positively or negatively affected by third-parties
- **Supply Chain Risk Management (SCRM)** is the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of information and communications technology (ICT) product and service supply chains
  - NIST Special Publication 800-161

EXTENDED ENTERPRISE MATTERS TO ALL OF US

- outsourcing entire business functions to third parties, such as tax, legal, audit, or information technology operations
- outsourcing lines of business or products (i.e. logistics)
- relying on a single third party to perform multiple activities, often to such an extent that the third party becomes an integral component of the company's operations
- working with third parties that engage directly with customers (e.g., customer support)
- contracting with third parties that subcontract activities to other foreign and domestic providers (4th Party Risk????)
- working with a third party to address deficiencies in operations or compliance with laws or regulations

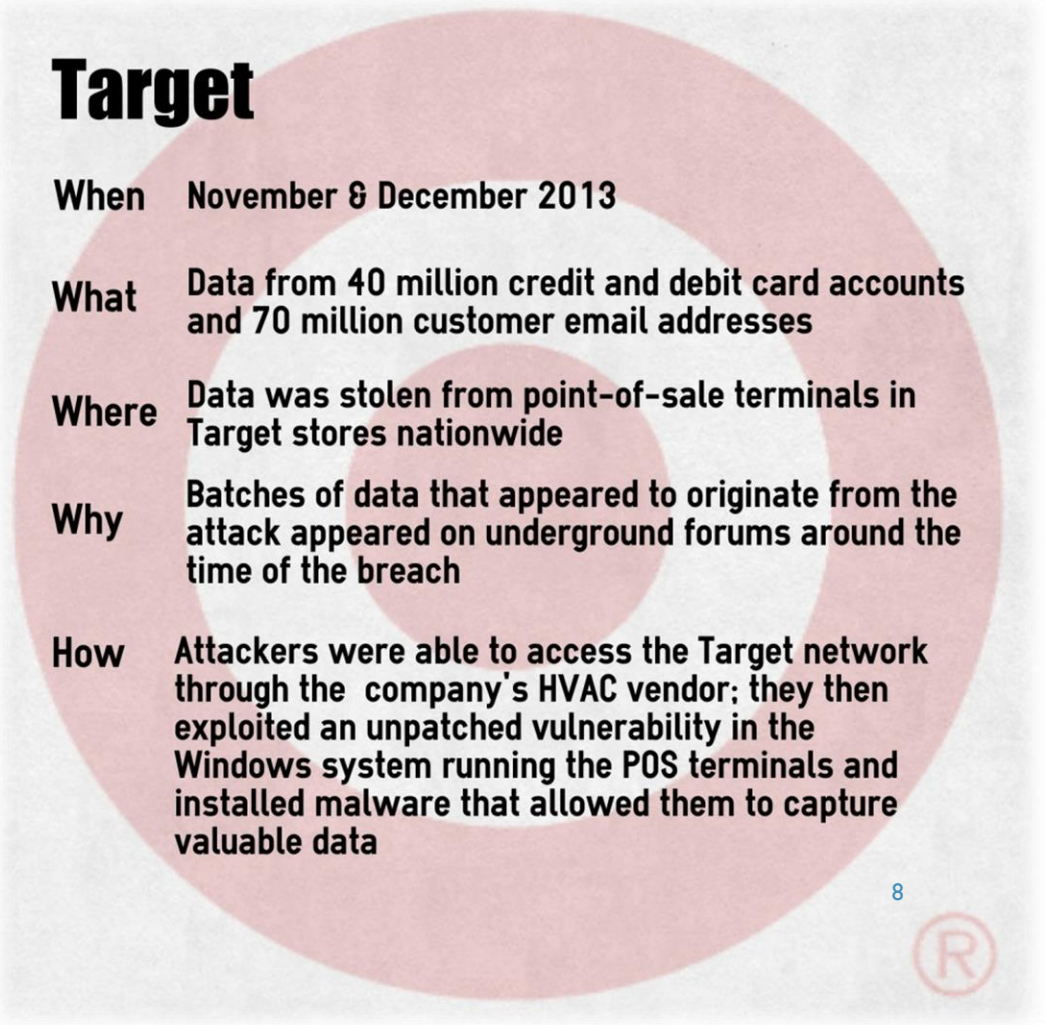
* Deloitte Tech Trends 2017
** Bomgar 2018 Privileged Access Threat Report

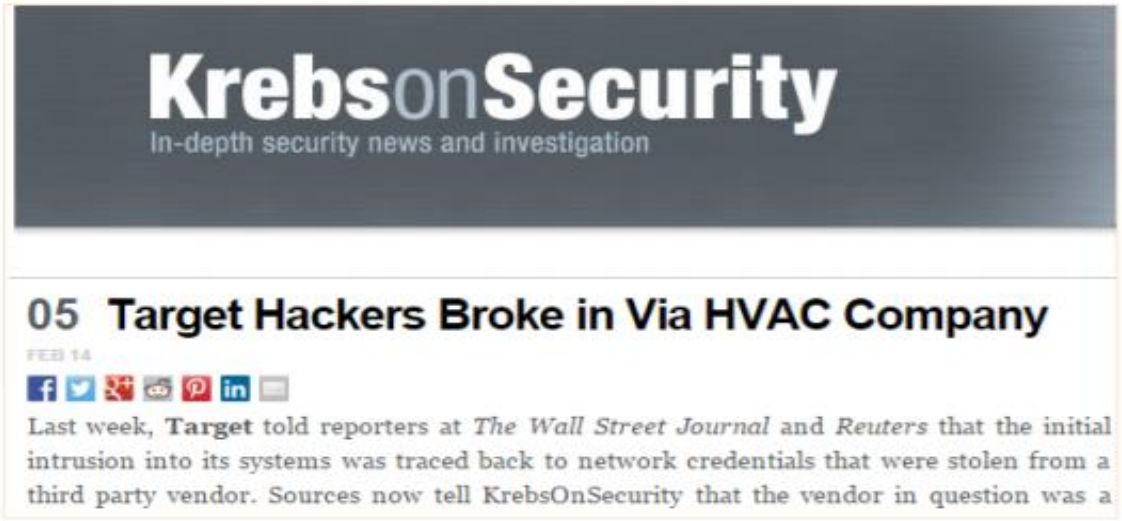


Illustrative example of the extended enterprise

THE EXTENDED ENTERPRISE: WHAT COULD GO WRONG

- Who knows the name of the vendor that led to the compromise for Target??





"...the source of the Target intrusion traces back to network credentials that Target had issued to **Fazio Mechanical**, a heating, air conditioning and refrigeration firm in Sharpsburg, Pa. Multiple sources close to the investigation now tell this reporter that those credentials were stolen in an email malware attack at Fazio that began at least two months before thieves started stealing card data from thousands of Target cash registers."

- 40 million customer credit cards stolen
- 70 million customer records (name, address, email, phone)
- 46% decrease in Q4 2013 profits vs Q4 2012

http://krebsonsecurity.com/tag/target-data-breach/

Fazio Mechanical was a 100-staff, $12M revenue HVAC company

The following correlates significant third party risks to the assessments utilized by organizations to evaluate the effectiveness of third party controls in place to mitigate risks.

Reputational:
Assesses the impact to the organizations reputation based on services provided by a third-party.

Compliance:
Assesses the third-party's ability/control framework in place to comply with laws/regulations.

Legend:
- Assessment
- Risk

https://www.pwc.com/us/en/services/consulting/cybersecurity.html

Operational Competency:
Assesses the ability of the third party to deliver the contracted products/services.

Subcontractor:
Assesses the risk management processes surrounding the use of subcontractors by third parties.

Technology:
Assesses the adequacy and appropriateness of the third parties systems and applications to provide the product/service.

Information Security & Privacy:
Assesses third party controls over the availability, confidentiality, and integrity of third party data .

Physical Security:
Assesses facility access and security measures implemented by the third party.

Financial:
Assesses financial stability for the third party to continue provide the product/service.

Country Risk:
Assesses political, geographic, regulatory, legal, and economic risks of sourcing to a country or region.

Business Continuity & Resiliency: Assesses the third parties ability to perform in the event of a process failure or catastrophic event.

EXTENDED ENTERPRISE = TPRM + SCRM

THIRD PARTY RISK MANAGEMENT + SUPPLY CHANGE RISK MANAGEMENT

TPRM

- The process of analyzing and controlling risks presented to your company, your data, your operations and your finances by parties OTHER than your own company.

SCRM

- Supply chain risks are associated with an organization's decreased visibility into, and understanding of, how the technology that they acquire is developed, integrated, and deployed
- Processes, procedures, and practices used to assure the integrity, security, resilience, and quality of the products and services.

GOVERNANCE AROUND EXTENDED ENTERPRISE

- Companies must have effective risk management regardless of whether the company performs the activity internally or through a third party
- A company's use of third parties does not diminish the responsibility of its board of directors and senior management to ensure that the activity is performed in a safe and sound manner and in compliance with applicable laws
- Companies need to adopt risk management processes commensurate with the level of risk and complexity of its third-party relationships

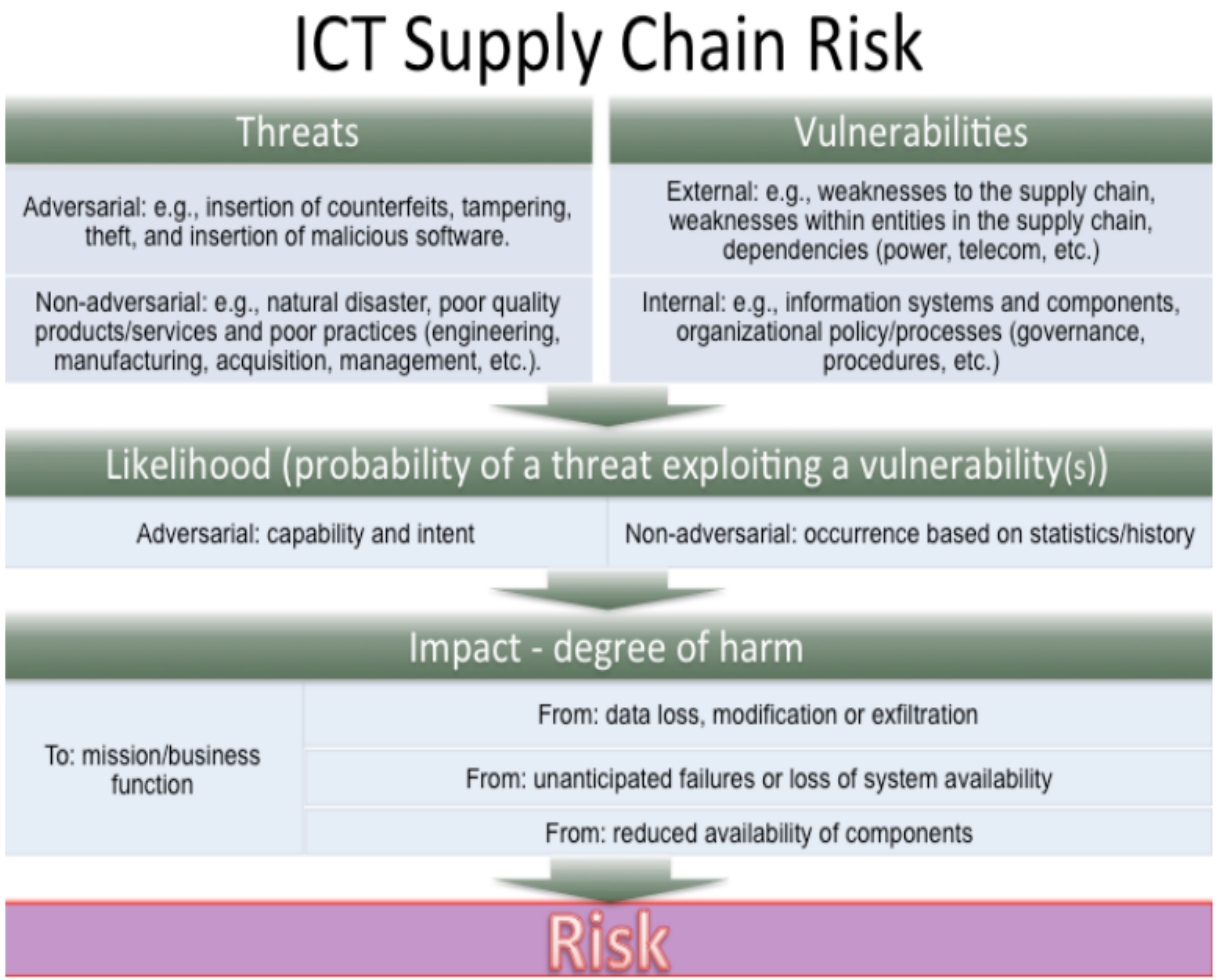
HAS BEEN REGULATED FOR AWHILE

OCC 2013-29 Expectations

- A bank should adopt **risk management processes** commensurate with the level of risk and complexity of its third-party relationships
- A bank should ensure **comprehensive risk management and oversight** of third-party relationships involving critical activities
- An **effective risk management process throughout the life cycle** of the relationship includes:
  - Plans that outline the bank's strategy, identify the **inherent risks** of the activity, and detail how the bank **selects, assesses, and oversees** the third party
  - Proper **due diligence** in selecting a third party
  - **Written contracts** that outline the rights and responsibilities of all parties
  - **Ongoing monitoring** of the third party's activities and performance
  - **Contingency plans for terminating** the relationship in an effective manner
  - Clear **roles and responsibilities for overseeing and managing** the relationship and risk management process
  - **Documentation and reporting** that facilitates **oversight, accountability, monitoring, and risk management**
  - **Independent reviews** that allow bank management to determine that the bank's process aligns with its strategy and effectively manages risks

- Comptroller of the Currency (OCC) publication 2013-29 Third Party relationships sets the expectations for banks and provides a good example of what should be included in an effective TPRM program
- NIST Special Publication 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations

SUPPLY CHAIN RISKS



NIST Special Publication 800-161

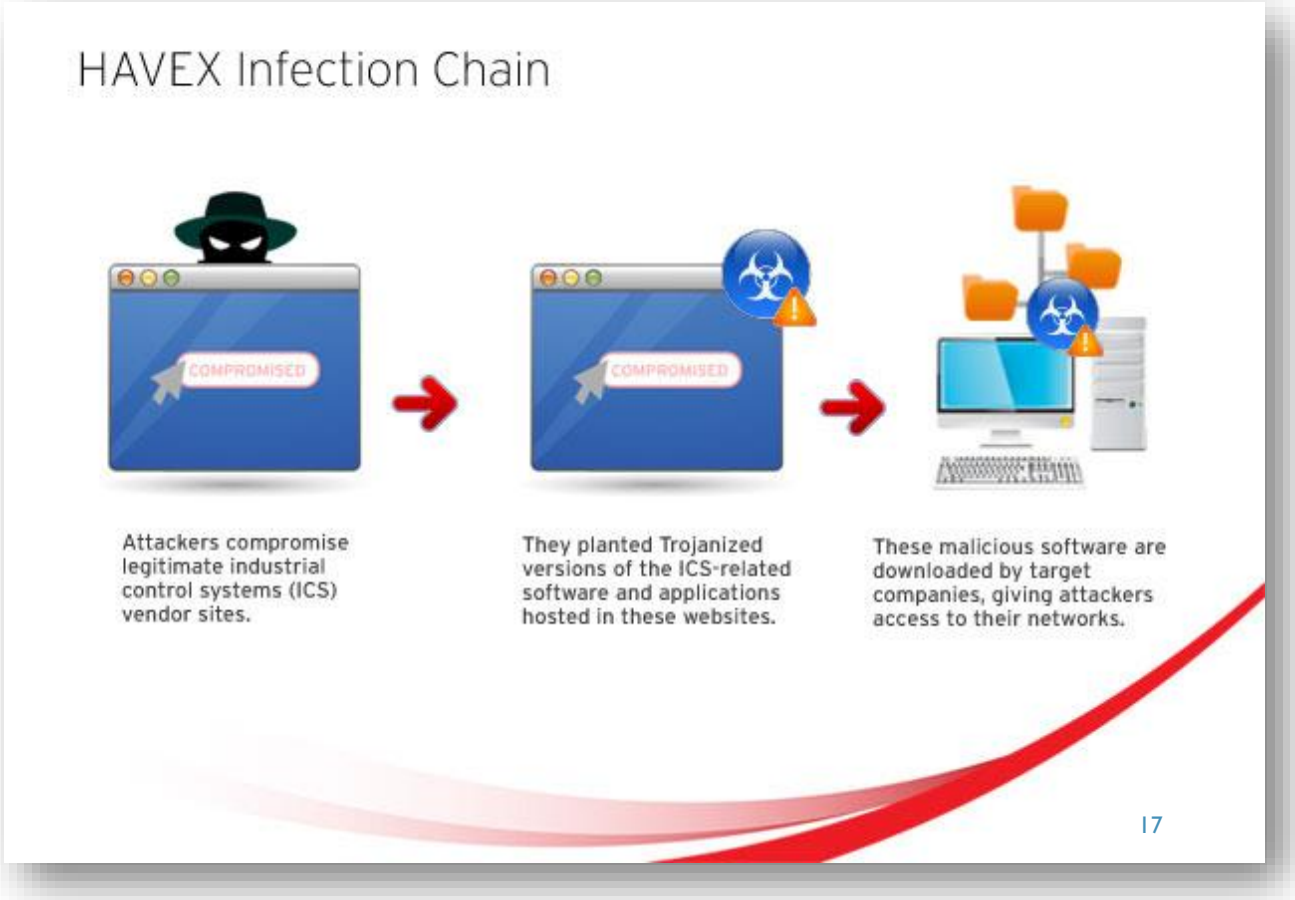
- What steps are taken to "tamper proof" products? Are backdoors closed?
- What physical security measures are in place? Documented? Audited?
- What security practice expectations are set for upstream suppliers? How is adherence to these standards assessed?
- How does a vendor assure security through product their lifecycle?
- Component purchases are tightly controlled; component purchases from approved vendors are prequalified. Parts purchased from other vendors are unpacked, inspected, and x-rayed before being accepted.
- Secure Software Lifecycle Development Programs are used to evaluate externally-provided software

SCM RISKS

Threat Agent	Scenario	Examples
Counterfeiters	Counterfeits inserted into ICT supply chain	Criminal groups seek to acquire and sell counterfeit ICT components for monetary gain.
Insiders	Intellectual property loss	Disgruntled insiders sell or transfer intellectual property to competitors or foreign intelligence agencies for a variety of reasons including monetary gain. Intellectual property includes software code, blueprints, or documentation
Insiders	Malicious code insertion	Disgruntled employee of an Integrator company inserts malicious functionality into traffic navigation software, and then leaves the company
External (i.e., Nation State, Activists)	Unauthorized access	Activist group seek to penetrate ICT supply chain and may implant unwanted functionality (by inserting new or modifying existing functionality) or subvert system or mission operations.
External (Nation State)	Industrial Espionage	Industrial spies seek to penetrate ICT supply chain to gather information or subvert system or mission operations

WHAT IF YOU ARE PART OF THE SUPPLY CHAIN

- Don't forget to meet your own security responsibilities as a supplier
  - Ensure that you enforce and meet any requirements on you as a supplier
  - Provide upward reporting and pass security requirements down to sub-contractors
  - Welcome any audit interventions your customer might make
  - Know your requirements to disclose security incidents and vulnerabilities
  - Be proactive and ask your customers and seek assurance that they are they happy with the measures you are taking



SUPPLY CHANGE RISK MANAGEMENT

- Foundational Practices include:
  - Integrating information security requirements into the acquisition process
  - Using applicable baseline security controls as one of the sources for security requirements
  - Ensuring a robust software and hardware quality control process
  - Establishing multiple sources, e.g., delivery routes, for critical system elements

https://www.ncsc.gov.uk/collection/supply-chain-security?curPage=/collection/supply-chain-security/principles-supply-chain-security

KYTP → "KNOW YOUR THIRD PARTIES"

- How well do you know your third parties?
- How well do you continue to pay attention to them?
- Does the risk appetite of your third parties match those of your own?
- What data that is shared with/collected by/ accessible to the third party?
  - Customer, customer spouse, and prospective customer information
  - Employee, Employee Family, Applicant, and Contractor Information
  - Organization's Intellectual Property, Proprietary Information, and Financial Data
  - Technology Information

THIRD PARTY RISK MANAGEMENT LIFECYCLE

- Planning for the use of third parties
- Initial due diligence of third parties
- Contract negotiations with third parties
- Ongoing monitoring, re-assessment, and oversight of the third party relationships
- Disengagement of third parties

THIRD PARTY RISK MANAGEMENT

Identify and classify all Third Party Suppliers	• Comprehensive list of all third parties, what services they offer and what SLA's and contractual obligations have been set
Develop a security assessment process	• Leverage your security framework (NIST 800, ISO, etc.)
Continuously monitor risk between assessments	• Continuous Monitoring is now becoming a critical element of third-party risk programs with the most comprehensive services covering multiple risk domains including data, operational, financial, brand and regulatory risk.
Include downstream suppliers	• Many IT suppliers outsource their data processing, software development or platform support to Fourth and even Fifth Parties who may represent additional layers of risk. • Need to build accountability throughout the data supply chain within contractual terms and SLA's as well as adding subcontractor requirements into procurement processes.
Collaborate and build stronger peer networks	• Many industries have a common pool of third parties and suppliers who support numerous (often a substantial percentage) clients. • Can you leverage 'shared evidence networks'

UNDERSTAND RISK OF YOUR 3RD PARTIES

- Evaluate the third party's inherent security and privacy risks against a primary set of qualitative and quantitative risk factors
  - IT systems and data sensitivity – Critical systems and sensitive data elements (based on the organization's data classifications) that are shared with, collected by, or accessible to the third-party organization
  - Type of sensitive data and information accessible to the third-party organization
- Based on the inherent risk assessment the third-party is risk rated against defined risk tiers
- The risk tiers define the due diligence requirements to be completed for each third-party

Risk Tier	Due diligence requirements	
	Nature	Timing
Tier 4 - High Risk	Onsite assessment	Annually
Tier 3 - Moderate Risk	Remote Assessment	Bi-Annually
Tier 2 - Low Risk	Self assessment	Tri-Annually
Tier 1 - Very Low Risk	Annual Recertification of TSP Profile	N/A

RISK BASED PROCESSES

- Where are you spending your focus and resources?
- Self-Assessment vs. Questionnaire vs. Hands-on
- How often do you re-classify your vendors?
- Who is responsible for monitoring changes in your vendor risk profile
  - Hopefully those closest to the vendor!

INFORMATION SECURITY & PRIVACY AREAS

- Your security framework, policies and standards become the basis of your 3rd Party Security Assessment
  - Data Security
  - Encryption
  - Logical access control
  - Monitoring
  - Communication and connectivity
  - Incident management & security logging
  - Application Security & System development

Try asking a SaaS vendor for their firewall logs to ingest into your SIEM

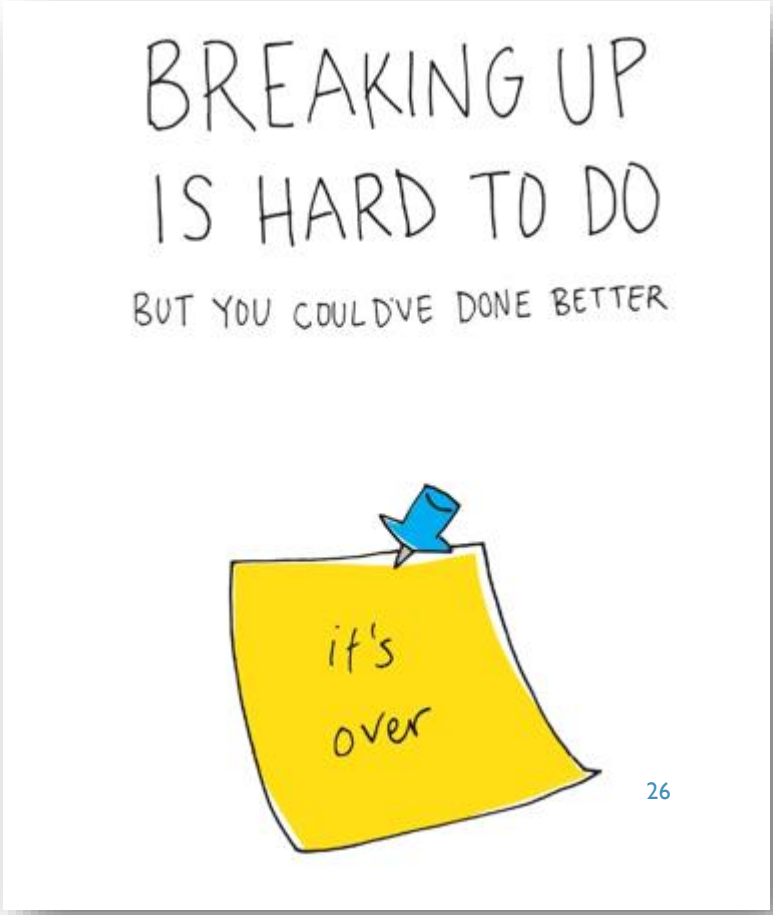
ONGOING MONITORING

- Ongoing monitoring for the duration of the third party relationship is an essential component of the a risk management process
  - More comprehensive monitoring is necessary when the third-party relationship is higher risk
- Includes a process for adjusting policies, procedures, and controls in response to changing threats and new vulnerabilities and material breaches or other serious incidents
- Reliance on, exposure to, or performance of subcontractors; location of subcontractors; and the ongoing monitoring and control testing of subcontractors

TERMINATION

- Need to ensure that relationships terminate in an efficient manner, whether the activities are transitioned to another third party or in-house, or discontinued.
- In the event of contract default or termination, the company should have a plan associated with data retention and destruction, information system connections and access control issues, or other control areas
- How do you ensure you get your data

  (or at least have confidence its deleted properly)

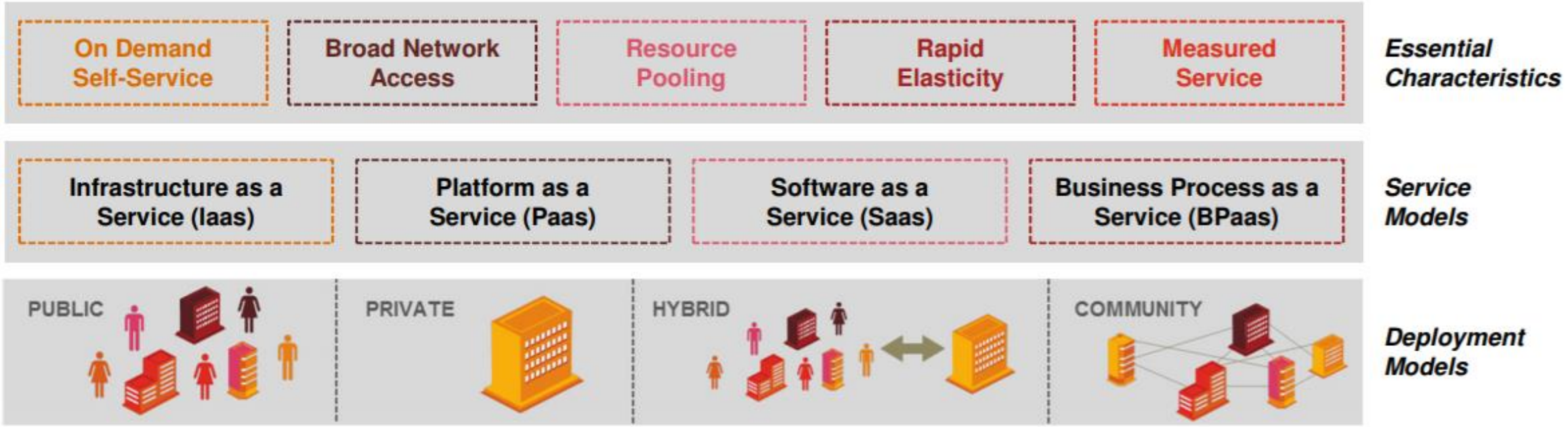


CLOUD COMPUTING

How to deal with security risk and compliance in Cloud Based Services

WHAT IS CLOUD COMPUTING?

Security impact: Driving new risks and security concerns that impacts all elements of the business ecosystem



* Source: "The National Institute of Standards and Technology (NIST) Definition of Cloud Computing (NIST Special Publication 800-145), Sept. 2011

CLOUD RISKS

- Cloud is a shared responsibility environment and requires a revised approach to manage risk and security
- Cloud services often involve multiple third party providers making responsibility for security controls unclear
- Lack of Cloud governance may lead to Cloud consumption with little governance, oversight and unapproved usage

CLOUD SECURITY KEY AREAS

- Access Control
  - Control access to sensitive data
  - Audit and report user access and data use
  - Provision and de-provision user access
  - Elevated access
- Compliance
  - Maintain regulatory compliance across cloud ecosystems
  - Right to audit
  - Contract and SLA compliance
- Data Security
  - Data classification scheme and processes for handling sensitive data
  - Prevent unauthorized data exposure, loss or corruption
  - Maintain data segregation in multi-tenet environment
  - Data flows across jurisdictions and zones with various regulatory and data protection requirements
  - Securely dispose of data no longer required
- Events – threats, response and investigations
  - Ability to log, monitor, and communicate events
  - Detect and correct security events
  - Cooperate during investigations and incident responses

IMPLICATIONS OF CLOUD MIGRATION ON SECURITY & RISK STRATEGY

- Migration readiness framework:
  - Need an integrated security and risk assessment framework to determine the "readiness" of applications to move to cloud
  - Readiness should be determined based on risk
- You are responsible for securing the gaps:
  - Outsourced/cloud providers do not solve all your risk and security problems (they take on some of them…and cause others)
  - Many technology, operations, contracting, and process controls are needed to operate securely
  - You must design, implement, operate, and manage these controls
- Third-party Risk Management:
  - Perform a TPRM risk analysis to understand the security capabilities of the third party, control integration points, and gaps as you work to migrate to a cloud service

THINGS TO MAKE YOU GO HMMMM

- How do we define technology-related third parties?
- Are we looking at going-forward only? What about contracts/relationships already in place?
- Are we going to re-write existing contracts that outline the rights and responsibilities of all parties from a cybersecurity perspective?
- Are we going to "require" compliance from our vendors/third parties if it "costs" us more?
- How (and who) is providing ongoing monitoring of the third party's activities and performance?
- Are we ready and have contingency plans for terminating a relationship if risks are unacceptable?
  - "They aren't secure, but they are too important to leave"

QUESTIONS?