Yesterday
Today
Tomorrow

PROF. DR. JUAN CARLOS BARRERA

CYBER-SECURITY (BC6)

July 2020

Online Germany

Broadcasting from USA

Strategic Framework

Agenda:

1) Cyber-event Recovery Management

2) Videos: Discussion & Reflection

3) Fourth Lab

4) The Digital Age

5) In Closing: Debriefing for Cases 01 – 02 – 03 – 04

1) Cyber-event Recovery Management

- **1) Planning for Cyber Event Recovery**

- NIST Special Publication (SP) 800-61 defines an ***event*** as ***"any observable occurrence in a system or network"***, while an ***incident is defined as a violation of acceptable policies, or security policies and best practices***. Nowadays, **Event** = **Incident**.

- Recovery is one part of the enterprise risk management process lifecycle; for example, the Framework for Improving Critical Infrastructure Cybersecurity, better known as the **Cybersecurity Framework (CSF),** defines five functions: ***Identify, Protect, Detect, Respond, and Recover***. These functions are all critical for a complete defense.

Pre-requisites for a Recovery Plan

The Cybersecurity Framework (CSF) provides a high-level mechanism for an organization to understand and improve its security posture by building upon capabilities that have already been implemented. The framework functions *Identify, Protect, Detect, Respond, and Recover* all work together in a concurrent manner and directly inform the Recover function.

- Much of the planning and documentation for recovering from a cybersecurity event needs to be in place before the event occurs. The *Identify* function of the CSF suggests that the organization must identify critical systems which are central to the organization’s mission, and that must be recovered first, as part of the Response activity.

- Planning may be informed by threat modeling. The fundamental principle underlying ***threat modeling*** is that there are always limited resources for security and it is necessary to determine how to use them.

Pre-requisites (Cont’d)

- Due to the sensitive information that may be included in a recovery plan, an organization should treat it and protect with the same due care as an information system security plan. *[Confidential]*
- Other proactive recovery assessments should help identify and enable the understanding of security dependencies, for instance:

- a) Organizations should have a good understanding of the system boundaries, trust relationships, and identities that exist in their environment.

Pre-requisites (Cont’d)

- b) Once an organization has a handle on the identities in its environment, it must ensure that it has the proper access controls applied to them, especially in regards to the management and control of the infrastructure.

- c) Data integrity is the key driver and leads to confidence of the data. The organization has implemented sound processes and tools to protect the integrity of the mission-critical data and the control and management of the infrastructure data. This will include mechanisms to validate, backup, and replicate the data, and monitor and detect changes based on the organization-defined frequency.

RECOVERY PLAN

- Recovery planning includes the development of *processes and procedures* that are flexible enough to ensure timely restoration of systems and other assets affected by future cyber events, and also comprehensive enough to have modular components for *frequently used procedures represented in a* ***PLAYBOOK***, such as reestablishing control of accounts and systems from advanced adversaries.
- While the details of a recovery plan need to be developed by each organization, a typical recovery plan includes the following topics:

- **Service level agreements** – Relevant service/operational/organization level agreement details – Information about existing written commitments to provide a particular level of service (e.g., availability percentage, maximum allowable downtime, guaranteed bandwidth provision).

Recovery Plan (Cont'd)

- **Authority** – Documented name and point of contact information for two or more management staff members who may activate the plan.
- **Recovery team membership** – Point of contact information for designated members of the team who have reviewed, exercised, and are prepared to implement the plan.
- **Specific recovery details and procedures** – Documented system details that apply to the given information system, with diagrams where applicable. These details may prescribe specific recovery activities to be performed by the recovery team, including application restoration details or methods to activate alternate means of processing (e.g., backup servers, failover site).

Recovery Plan (Cont’d)

- **Out of band communications** – Ability to communicate with critical business, IT, and IT security stakeholders, including external parties like incident response and recovery teams, without using existing production systems, which are frequently monitored by advanced adversaries.
- **Communication plan** – Any specific notification and/or escalation procedures that apply to this information system. As an example, some systems impact users outside of the organization, and legal, public relations, and human resources personnel may need to be engaged to manage expectations and information disclosure about the incident and recovery progress.
- **Off-site storage details** – Details regarding any arrangement for storing specific records or media at an offline or offsite location. This is particularly critical given the credible threat of ransomware that encrypts data and holds the decryption key hostage for payment.

Recovery Plan (Cont'd)

- **Operational workarounds** – Approved workaround procedures if the information system is not able to be restored within the recovery time objective (RTO).
- **Facility recovery details** – Information relevant to resilience of a physical facility such as an office location or a data center. Such details might include personnel notification processes, alternate location information, and communications circuit details.
- **Infrastructure, hardware, and software** – Details regarding access to the infrastructure, hardware, and software to provide intermediary services used during the recovery process. Examples include an identity management system, a recovery network, a messaging system, and a staging system to validate the integrity of recovered data from backups and restore the system in order to instantiate trust in the infrastructure.

Root Cause Determination

- Identifying the root cause(s) of a cyber event is important to planning the best response, containment, and recovery actions. While knowing the full root cause is always desirable, adversaries are incentivized to hide their methods, so discovering the full root cause is not always achievable.
- Before execution of recovery efforts start in earnest, **the investigation** should achieve **two key objectives** to be considered sufficient:

- ***a) Basic knowledge of the adversary's objective*** (e.g., gain access to intellectual property, financial data, customer and partner data, disrupt organization business functions for monetary gain, etc.) or incident response subject matter expert (SME) confirmation that the adversary's objective is not apparent.

Root Cause Determination (cont’d)

- ***b) It is imperative that the full extent of the cyber event*** is understood and strong containment mechanisms are in place to detect that the attackers are no longer present or in control of the IT resources. Most targeted attacks that are part of a large campaign involve multiple types of well-concealed persistence mechanisms.

Recovery Communications

- Planning for and implementing effective recovery communications are critical success factors for achieving organization resilience. These are included in **CSF category Recovery Communications (RC.CO),** which has the following described outcome: *"Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs [computer security incident response teams], and vendors."*
- Recovery communications includes non-technical aspects of resilience such as management of public relation issues and organizational reputation.

Recovery Communications (cont'd)

Effective communications planning is important for numerous reasons, including:

- *Statements made* in the heat of recovery may have significant legal and/or regulatory. Understanding, from a legal perspective,
- *Key stakeholders* need to know sufficient information so that they understand their responsibilities during the recovery stage and can maintain confidence in the recovery team's abilities.
- *Individual members of the recovery team* may not have sufficient information to provide accurate and timely reporting of recovery status and activities.

Continuous Improvement

- Cyber event recovery planning is not a one-time activity. The plans, policies, and procedures created for recovery should be continually improved by addressing lessons learned during recovery efforts and by periodically validating the recovery capabilities themselves.
- **Validating recovery capabilities** refers to ensuring that the technologies, processes, and people involved in recovery efforts are well prepared to work together to effectively and efficiently recover normal business operations from disruptive cyber events. There are several ways to validate recovery capabilities.

Continuous Improvement (cont’d)

- a) ***FEEDBACK*** - The simplest method is to ask all of the individuals who may be involved in response efforts to provide input on the recovery plans, policies, and procedures.
- b) ***DRILLS*** - In some cases, recovery concerns can be addressed by conducting exercises or tests. Exercises and tests should be performed periodically to help the organization’s real-world recovery capabilities, building organizational “muscle memory” and identifying areas for improvement.
- c) Recovery teams should ***PRACTICE*** *a realistic scenario in a tabletop exercise* where at least one member of each team is part of the adversary group that provides realistic obstacles and complexities for the defense and recovery team to navigate.

Continuous Improvement (cont’d)

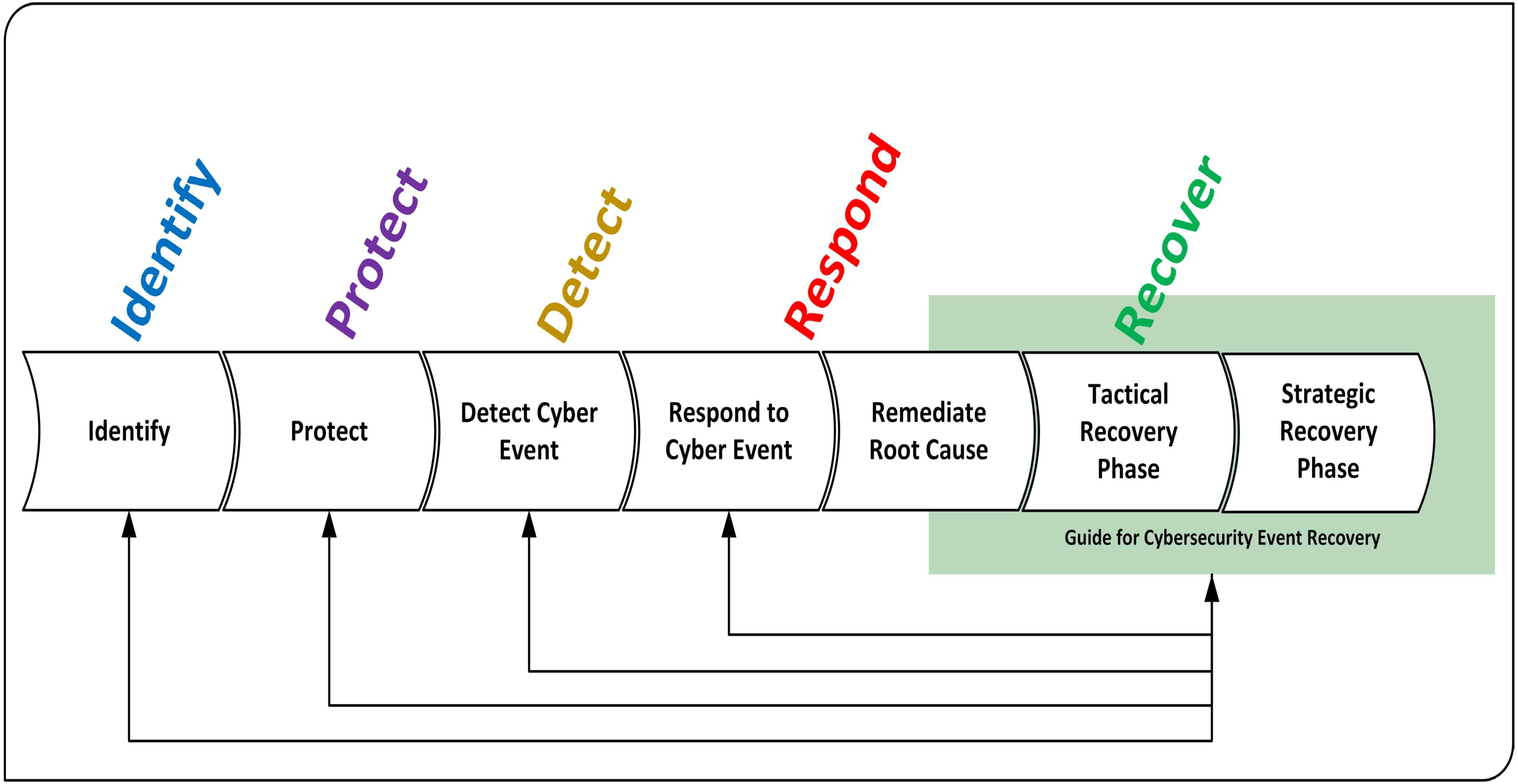
- d) Another practice is to use a newly discovered cyber event scenario described in the news to ***DEVELOP or CUSTOMIZE*** *a playbook exercising the recovery plan documentation*. Adding realism like this will proactively increase the visibility of gaps in the organization that can be resolved as part of continuous improvement to increase effectiveness in a real incident recovery.

Benefits of Continuous Improvement

Exercises and tests which are executed at an organization-defined frequency can provide several benefits related to recovery, including the following:

- The exercise or test itself will remind participants of known risk scenarios and help them consider what actions they might take in a real cyber event.
- Exercise and test results will help confirm or refute assumptions that were made in planning, particularly regarding how realistic the recovery targets are.
- Exercises and tests will spotlight gaps and inefficiencies in the processes that should be addressed to ensure smooth responses in real-world cyber events.
- Personnel, especially those with new recovery-related responsibilities, will receive training through exercises and tests in recovery practices.

Cybersecurity Event Recovery Relationships



Sample Metrics for Recovery

Recovery Area

- Assessing Incident Damage and Cost

Consider both direct and indirect costs; recovery damage and costs may be important evidence as part of a legal action.

Example Metrics

a) Costs due to the loss of competitive edge from the release of proprietary or sensitive information [dollar]

b) Legal costs [dollar]

c) Hardware, software, and labor costs to execute the recovery plan [dollar]

d) Costs relating to business disruption such as system downtime; for example, lost employee productivity, lost sales, etc. [time in hours, days, or weeks]

e) Other consequential damages such as loss of brand reputation or customer trust from the release of customer data [number of current or future business partner, advertiser, and customer losses in dollars]

Sample Metrics for Recovery (cont'd)

Recovery Area

- Organizational Risk Assessment Improvement

Example Metrics

a) Frequency and/or scope of recovery exercises and tests [number of times per year]

b) Number of significant IT-related incidents that were not identified in risk assessment [number of incidents]

c) System dependencies accurately identified [number of assets not identified]

d) Identified gaps during the recovery exercises or tests that help inform and drive the improvement in the other functions of the CSF [number of gaps]

Sample Metrics for Recovery (cont'd)

Recovery Area

- Quality of Recovery Activities

Example Metrics

a) Number of business disruptions due to IT service incidents [number of business functions]

b) Percent of business stakeholders satisfied that IT service delivery meets agreed-upon service levels [customer satisfaction]

c) Percent of IT services meeting uptime requirements [service level agreement]

d) Percent of successful and timely restoration from backup or alternate media copies [number of systems and times]

e) Number of recovery events that have achieved recovery objectives [number of successful recovery events]

A PLAYBOOK

- The tactical recovery phase will depend on performing the following actions before and during the cyber event:
- Create and maintain a list of the people, process, and technology assets that enable the organization to achieve its mission (including external resources), along with all dependencies among these assets. The creation of a map or diagram of the dependencies will help in planning the order of restoration.
- Document and maintain categorizations for all assets based on their relative importance and interdependencies to confidently prioritize recovery efforts.
- Identify and document the key personnel who will be responsible for defining recovery criteria and associated plans, and ensure these personnel understand their roles and responsibilities.

A Playbook (Cont’d)

- Ensure that the correct underlying assumptions (e.g., availability of core services, trustworthiness of directory services, adversary’s motivation is well understood) are made during the initiation of the recovery in order to prevent an ineffective recovery.
- Define and document the conditions under which the recovery plan is to be invoked, who has the authority to invoke the plan, and how recovery personnel will be notified of the need for recovery activities to be performed. Additionally, define key milestones, intermediate recovery goals, and criteria for finalizing active recovery efforts.

A Playbook (Cont’d)

- Ensure initial restoration planning addresses the need for the recovery efforts to be tactical in nature in order to prevent recovery from negatively affecting the incident response (e.g., by alerting an adversary or by erroneously destroying forensic evidence).
- Examine the cyber event to determine the extent that recovery must be carried out, and initiate the corresponding plan for recovery.
- Develop a comprehensive recovery communications plan while clearly defining recovery communication goals, objectives, and scope, including information sharing rules and methods. Based upon this communications plan, consider sharing actionable information about cyber threats with relevant organizations, such as those described in **NIST SP 800-150.**

A Playbook (Cont’d)

- Gather feedback for the recovery plans and capabilities from those stakeholders that will have a role in recovery activities.
- Formally implement cyber event recovery exercises and tests at a frequency acceptable for the organization. These events should include realistic objectives, with specific roles and responsibilities, for exercising and testing recovery capabilities. Based on the results of these recovery activities the organizations should update cyber event recovery plans, policies, and procedures. They should also use the information learned from recovery activities to improve the organization’s cybersecurity posture, ensuring the ability to meet its mission.

A Playbook (Cont'd)

- Vet recovery capabilities by soliciting input from individuals with relevant responsibilities and conducting exercises and tests.
- Execute the tailored playbook that has been created during the cyber event.
- Continually document issues during recovery so that there is enough information to expand on documentation and improve capabilities later in the recovery process or immediately after recovery is achieved.
- Implement monitoring for events, signatures, etc. to alert the organization about known malicious behavior. Monitor the artifacts and evidence found during detection and response. This monitoring will extend into the strategic phase.

A Note on Strategic Recovery

Strategic recovery phase depends on performing the following actions before/during the cyber event:

- **Develop and implement** an improvement plan for the organization’s overall security posture based on tactical phase results.
- **Continually execute communications plans** to inform appropriate internal and external stakeholders of the progress of the recovery effort. Internal stakeholders should be notified of any improvements that need to be made to people, processes, and procedures, while external stakeholders will need to be notified of any impact to them.
- **Review defined milestones, goals, and metrics gathered** throughout the tactical phase. This information can help quantify the effectiveness of the recovery effort, as well as identify areas that need improvement.

Recovery Scenarios

Please locate the following documents in the seminar platform. Read them carefully, and be ready to discuss them in class.

- NIST.CSF2018
- NIST.SP800 – 150
- Playbook Elements
- 3rd party Outsourcing ISA Questionnaire
- Recovery Scenario 01
- Recovery Scenario 02

2) Videos: Discussion & Reflection

- Quick Tips to Improving Your Board's Cyber Security Literacy
- National Cybersecurity Strategy Guide
- The promise and peril of active cyber defense

Go to the virtual room, and complete the activity thread.

3) Fourth Lab

Please go to the Virtual Room for Instructions\\

4) The Digital Age

Business Issues in the Digital Age

Supply Chain Attacks:

- A supply chain attack, also called a value-chain or third-party attack, occurs when someone infiltrates your system through an outside partner or provider with access to your systems and data.

2 Brief Examples:

- Uber - Date: Late 2016
  Impact: Personal information of 57 million Uber users and 600,000 drivers exposed.
- Adobe - Date: October 2013
  Impact: 38 million user records

Supply Chains at Risk

Common attacks to Supply Chains

- Malware
- Compromised Credentials
- Distributed Denial of Service (DDoS)
- SQL Injections

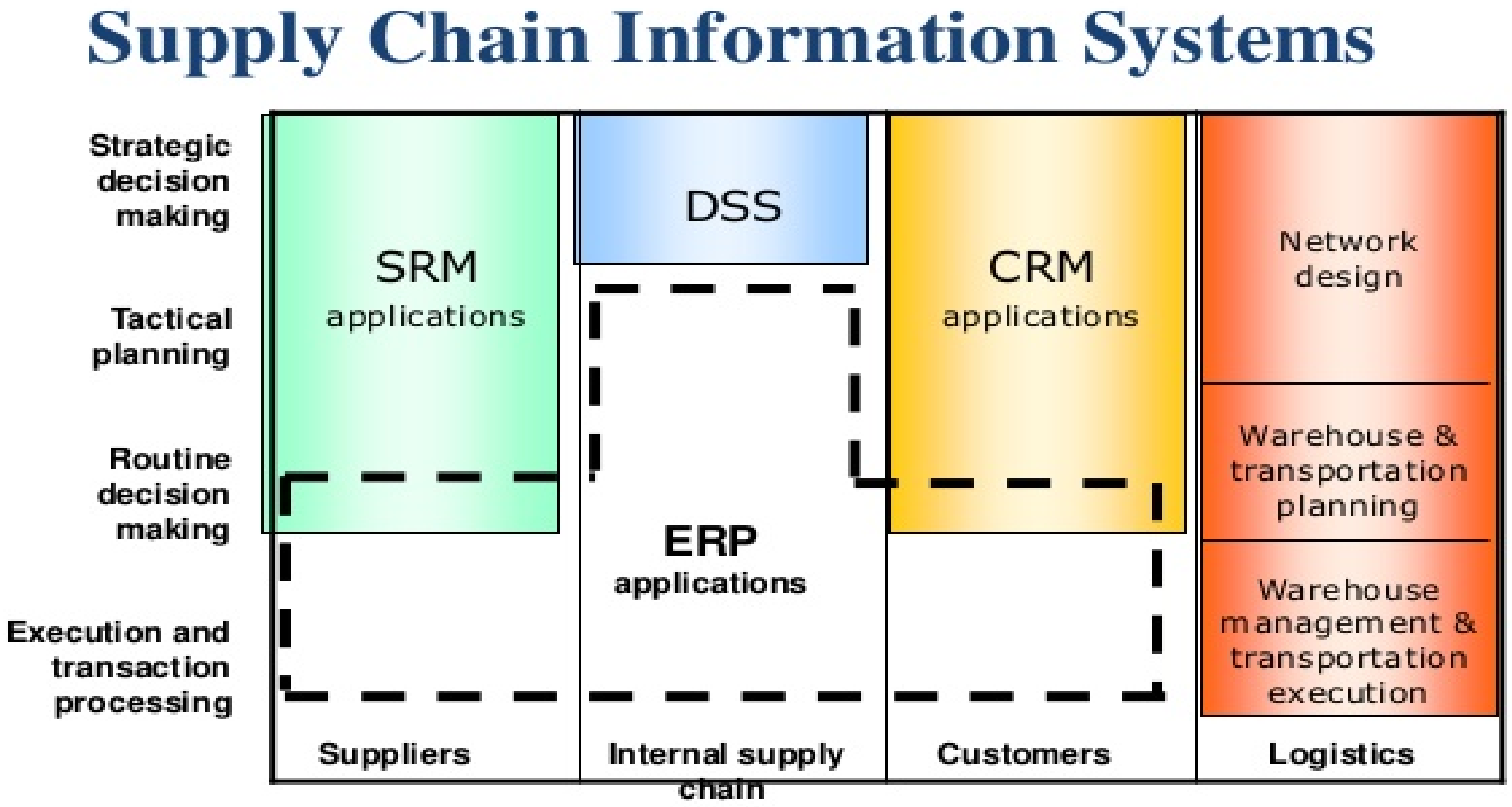
Risk Areas

- Vendor relationships and global information transmission
- Open access to data rather than "need to know" access
- Frequent changes in suppliers and products
- Lack of standardization of security protocols across vendors and other partners
- Infected devices on a corporate network
- Obsolete security infrastructure or outdated hardware/software

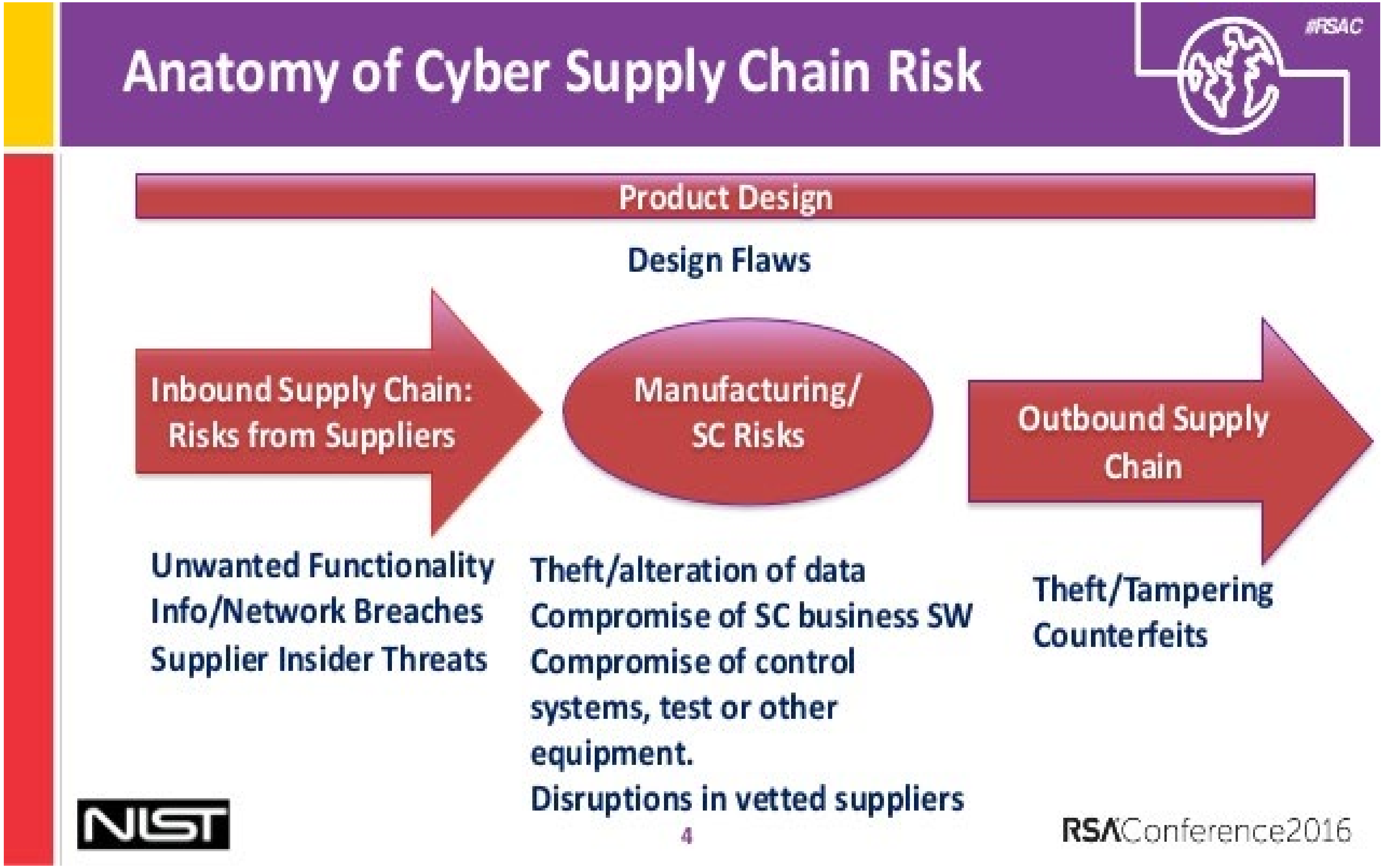
Vendor Assessment

- Please locate the document titled “3rd party outsourcing InfoSec Assessment”…..in the seminar website.
- Read it
- Let’s discuss it in class

Supply Chain Information System


Supply Chain Information Systems
Strategic decision making
Tactical planning
Routine decision making
Execution and transaction processing
SRM applications
DSS
CRM applications
Network design
Warehouse & transportation planning
Warehouse management & transportation execution
ERP applications
Suppliers
Internal supply chain
Customers
Logistics

Supply Chain Attack



#RSAC

Anatomy of Cyber Supply Chain Risk

Product Design

Design Flaws

Inbound Supply Chain: Risks from Suppliers

Manufacturing/ SC Risks

Outbound Supply Chain

Unwanted Functionality
Info/Network Breaches
Supplier Insider Threats

Theft/alteration of data
Compromise of SC business SW
Compromise of control systems, test or other equipment.
Disruptions in vetted suppliers

Theft/Tampering
Counterfeits

NIST

4

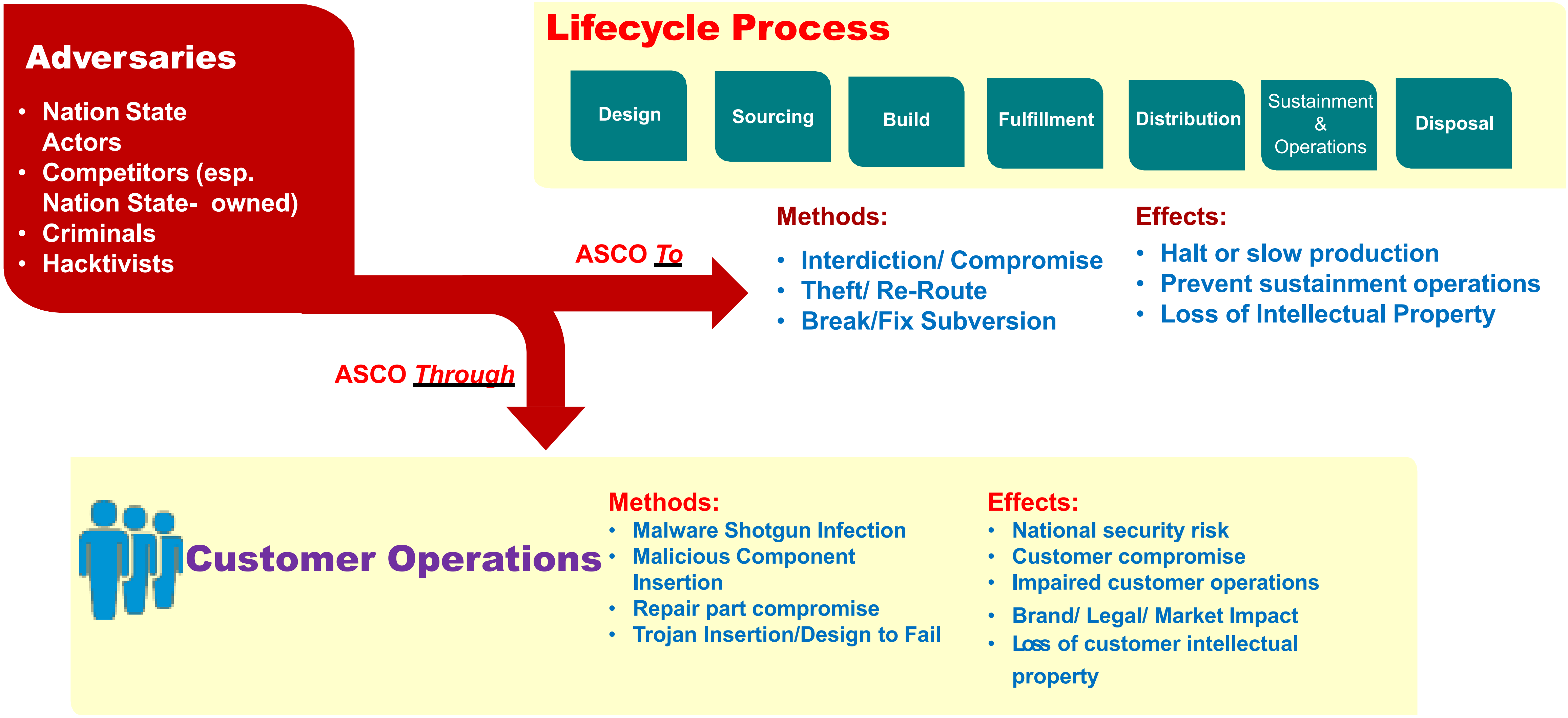
RSAConference2016

Supply Chain as an Attack Chain

Please locate the short reading about Supply Chain (Case 02) and answer the following questions. Be ready to debrief your answers in class.

- What is a Supply Chain Ecosystem?
- Why is it critical to protect a Supply Chain?
- What is ASCO To attack and ASCO Through attack?
- What is a Maturity model – In Supply Chain Cybersecurity Program?

Adversarial Supply Chain Operations (ASCO) To vs. ASCO Through



Adversaries

- Nation State Actors
- Competitors (esp. Nation State- owned)
- Criminals
- Hacktivists

ASCO *To*

ASCO *Through*

Lifecycle Process

Methods:

- Interdiction/ Compromise
- Theft/ Re-Route
- Break/Fix Subversion

Effects:

- Halt or slow production
- Prevent sustainment operations
- Loss of Intellectual Property

Customer Operations

Methods:

- Malware Shotgun Infection
- Malicious Component Insertion
- Repair part compromise
- Trojan Insertion/Design to Fail

Effects:

- National security risk
- Customer compromise
- Impaired customer operations
- Brand/ Legal/ Market Impact
- Loss of customer intellectual property

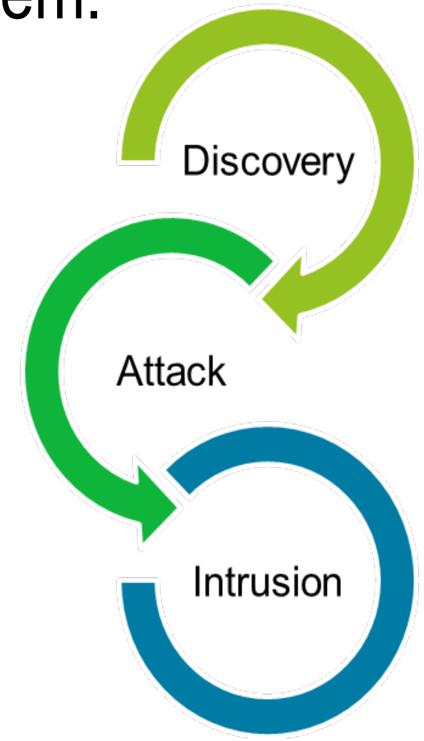
Anatomy of a Cyber-attack (SCM)

- A cyber attack generally follows a process allowing the attacker to perform reconnaissance or discovery of the targeted business, then develops and executes the attack, and finally uses the attacker’s command and control presence to extract data and/or achieve the attacker’s goals on the target system.

Discovery:
Characterize Systems and Find Vulnerabilities

Attack:
Exploit vulnerable people, Components, and Processes.

Intrusion: Data exfiltration, Denial of Service, Command and Control of Operations.



Anatomy (Cont’d)

- In the discovery phase, a threat agent performs reconnaissance by probing the network perimeter to characterize the system, that is, determine if there is a firewall (and what type), what types of web or other Internet facing servers are used, and whether there are any open communication ports. The goal is to find any way possible to get into the system. They may also harvest publicly available corporate information (company principal’s names and email addresses, photos that may show physical security barriers, sup- port personnel names and numbers) to gain any advantage they can for social engineering or email-based attacks.

Anatomy (Cont’d)

- Asset discovery allows a potential intruder to decide what systems to target, to gauge how easy it will be to launch an attack on a particular entity, and to find weaknesses in the target’s security, which allows them to determine the best method for launching a successful attack
- Attack: Once the attacker has determined potential intrusion vectors, they determine what weaknesses and vulnerabilities are inherent in the targeted system. Poor configuration management is one of the most common ways that an attacker can find an opening into the control system domain. General purpose OS platforms provide numerous processor and network services that automatically run by default. The result is unmonitored, open ports that are vulnerable to network exploits and actively executing code that may be subject to attacks such as buffer overflows.

Anatomy (Cont'd)

Attack Methods in Supply Chains

- Weak authentication, Network scanning/probing, Removable media, Brute force intrusion,
- Abuse of access authority, Spear phishing, and (SQL) injection.
- Black Energy: is a crimeware toolkit that has evolved significantly since it emerged in 2007. Recent versions of the toolkit use social engineering to trick a user into opening an email or a document attach- ment that drops a Trojan or infected legitimate executable file on the target computer which results in the installation of a malicious software component. The malware can infect a system by exploiting a standard feature in Windows that elevates the user privilege of a system file, allowing execution of the command executable with administrative privilege—even if the user is not a member of the administrator group.

Other Attacks

- OPC/DCOM Attacks: A campaign called Operation Dragonfly utilized a multi-pronged intrusion chain to establish a presence on the network, perform reconnaissance, and establish a command and control capability to phone home to the intruder and allow them to launch other specific attack tools. It employed the "Havex" Re- mote Access Trojan (RAT) within targeted spear-phishing campaigns against industry asset owners, and it used a watering hole campaign to circumvent the normal practice of users accessing vendor resources.
- The next stage in the intrusion involves the enumeration of the asset owners' OPC servers, specifically targeting a vulnerability in the OPC Classic protocol. This provided the threat actor with the potential capability of performing deep discovery into the ICS,

Other Attacks (cont'd)

- OPC standards and application programming interfaces (APIs) that are common in control system environments are OPC Data Access, OPC Alarms, OPC Data Exchange, and OPC Data-XML. All OPC standards and APIs are widely supported and used in Windows editions, and there are a wide variety of security implications and vulnerabilities associated with the use of OPC services and standards.
- Vulnerabilities range from simple system enumeration and password vulnerabilities to more complex remote registry tampering and buffer overflow flaws. These vulnerabilities expose many ICSs to critical risks such as the installation of undetected malware, denial-of-service attacks, escalated privileges on a host, and/or the accidental shutdown of ICSs because of an overload flaw.

Scalating Supply Chains into Cyber-war: Is it real?

- Cyberwarfare is computer- or network-based conflict involving politically motivated attacks by a nation-state on another nation-state. In these types of attacks, nation-state actors attempt to disrupt the activities of organizations or nation-states, especially for strategic or military purposes and cyberespionage.

Evidence:

- Significantly increased over the last decade
- Frequency, scale, sophistication, and severity of impact
- Thousands of attacks daily
- ~240 New forms of Malware released each day
- Requires minimal cost and effort
- Malicious Tools easily found on the “DarkNet” at minimal cost
- Can impose a tremendous amount damage and confusion on a global scale.
- Reliant on technology, even minor attacks can be catastrophic and debilitating

What is Cyber Warfare? (IEEE View)

- Cyber warfare “is a combination of computer network attack and defense and special technical operations” (IEEE).

- **8 Principles:**

1) Lack of physical limitations
2) Kinetic effects
3) Stealth
4) Mutability & inconsistency
5) Identity & privileges
6) Dual use
7) Infrastructure control
8) Information as operational environment

Who is the Enemy?

- Individual Hackers
- Hacktivist Groups
- Criminal Organizations
- Corrupt Businesses
- Terrorists
- Foreign Military or Government

Cyberwarfare involves the following attack methods:

- Sabotage: Military and financial computer systems are at risk for the disruption of normal operations and equipment, such as communications, fuel, power and transportation infrastructures.

- Espionage and/or security breaches: These illegal exploitation methods are used to disable networks, software, computers or the Internet to steal or acquire classified information from rival institutions or individuals for military, political or financial gain.

Food for thought ! The Great Firewall of China (2011)

- The Great Firewall of China, also formally known as the Golden Shield Project, is the Chinese government's internet censorship and surveillance project. Initiated, developed, and operated by the Ministry of Public Security (MPS), the project is one of the most controversial subjects in the world. While many people of the Western world treat the project as a human right violation, some countries are actually adopting China's model. Below are some of the tricks China uses to censor its Internet:
- DNS Poisoning
- Blocking Access to IPs:
- Analyzing and Filtering URLs
- Inspecting and Filtering Packets
- Resetting Connections & Blocking VPNs

Food for thought ! Russia's new 'disconnect from the internet' law (Nov 01, 2019)

- a new "internet sovereignty" law entered into effect in Russia, a law that grants the government the ability to disconnect the entire country from the global internet.
- The Kremlin government cited the need to have the ability to disconnect Russia's cyberspace from the rest of the world in the event of a national emergency or foreign threat, such as a cyberattack.
- In order to achieve these goals, the law mandates that all local ISPs route traffic through special servers managed by the Roskomnadzor, the country's telecoms regulator.
- These servers would act as kill-switches and disconnect Russia from external connections while re-routing internet traffic inside Russia's own internet space, akin to a country-wide intranet -- which the government is calling RuNet.

A brief Survey of Issues!

• Point of Sale Attacks:	28.5%
• Crimeware:	18.8%
• Computer Espionage:	18.0%
• Privilege Misuse:	10.6%
• Web Applications:	9.4%
• Miscellaneous:	14.7%

SOURCE: Verizon Data Breach Investigations Report (DBIR) 2019

5) In Closing: Debriefings for Cases

- Debriefing for Cases 01 – 02 – 03 – 04
- Please go to the *Virtual Room* for Instructions
- Prepare your answers accordingly!

Thank you

Day 04

CLOSED

FOR BUSINESS