Unit #8

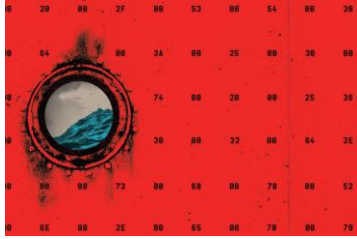
MIS 5214

Case Study 2 – Cyberattack: The Maersk Global Supply-Chain Meltdown

Agenda

- Timeline
- NotPetya
- Zero-Day Vulnerabilities
- Why attack was successful
- Mitigations
- Cybersecurity Capability model
- Team project implications…

Timeline



2016 – Maersk shipping company's senior system administrators warn company that its network of 80,000+ computers was vulnerable to attack

- Windows 2000 servers and Windows XP computers overdue for replacement
- Leadership approved upgrades, but systems administrators not motivated to implement the upgrades (due to bonuses based on "uptime" and not security)

2017, March – Microsoft issues emergency patch to update systems and protect from NotPetya

2017, June – NotPetya encryption attack

- IT availability loss
  - Active directory domain controllers (network of 150 of them) providing centralized store of usernames and passwords and access control authorization information all wiped out
  - Fall-back to manual business continuity activities
  - 1 domain controller in Ghana protected by power outage and served as a source for restoring domain control and access to restore systems
- 10-days of lost business ($300,000,000 in expenses and lost earnings)
  - **Note: 60% of small companies are unable to sustain their businesses over 6 months after a cyber attack!**

2017, July – System upgraded (4,000 new servers, 45,000 new PC's, with 2,500 applications) and computer-based business processes restored

NotPetya

- Arrives as infected e-mail attachments
- Designed to spread automatically, rapidly, and indiscriminately
- Propelled by two powerful hacker exploits working in tandem:
  1. EternalBlue
     - Penetration tool stolen from US NSA that takes advantage of a Windows Server Message Block (SMB) protocol vulnerability (CVE-2017-0144) which allowed hackers free rein to remotely run their own code on any unpatched machine
  2. Mimikatz
     - Windows left users' passwords lingering in computers' memory
     - Once hackers gained initial access to a computer, Mimikatz would pull those passwords out of RAM and use them to hack into other machines accessible with the same credentials. On networks with multiuser computers, it could even allow an automated attack to hop from one machine to the next
  3. Encryption of disk drives (no decryption offered)

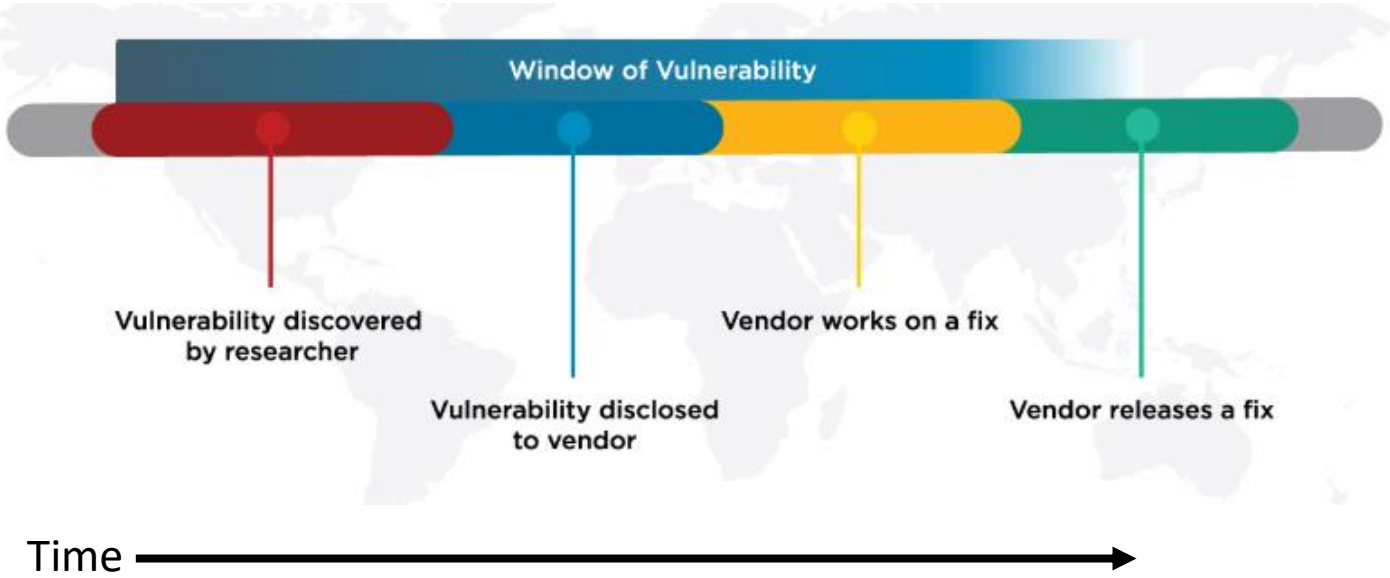
Note: Petya is a family of encrypting ransomware that was first discovered in 2016. The malware targets Microsoft Windows–based systems, infecting the master boot record to execute a payload that encrypts a hard drive's file system table and prevents Windows from booting.

Zero-Day Vulnerabilities

- Zero day (0-day) is a vulnerability for which there is no software patch available

  Bug > Vulnerability > Proof of concept > weaponized exploit

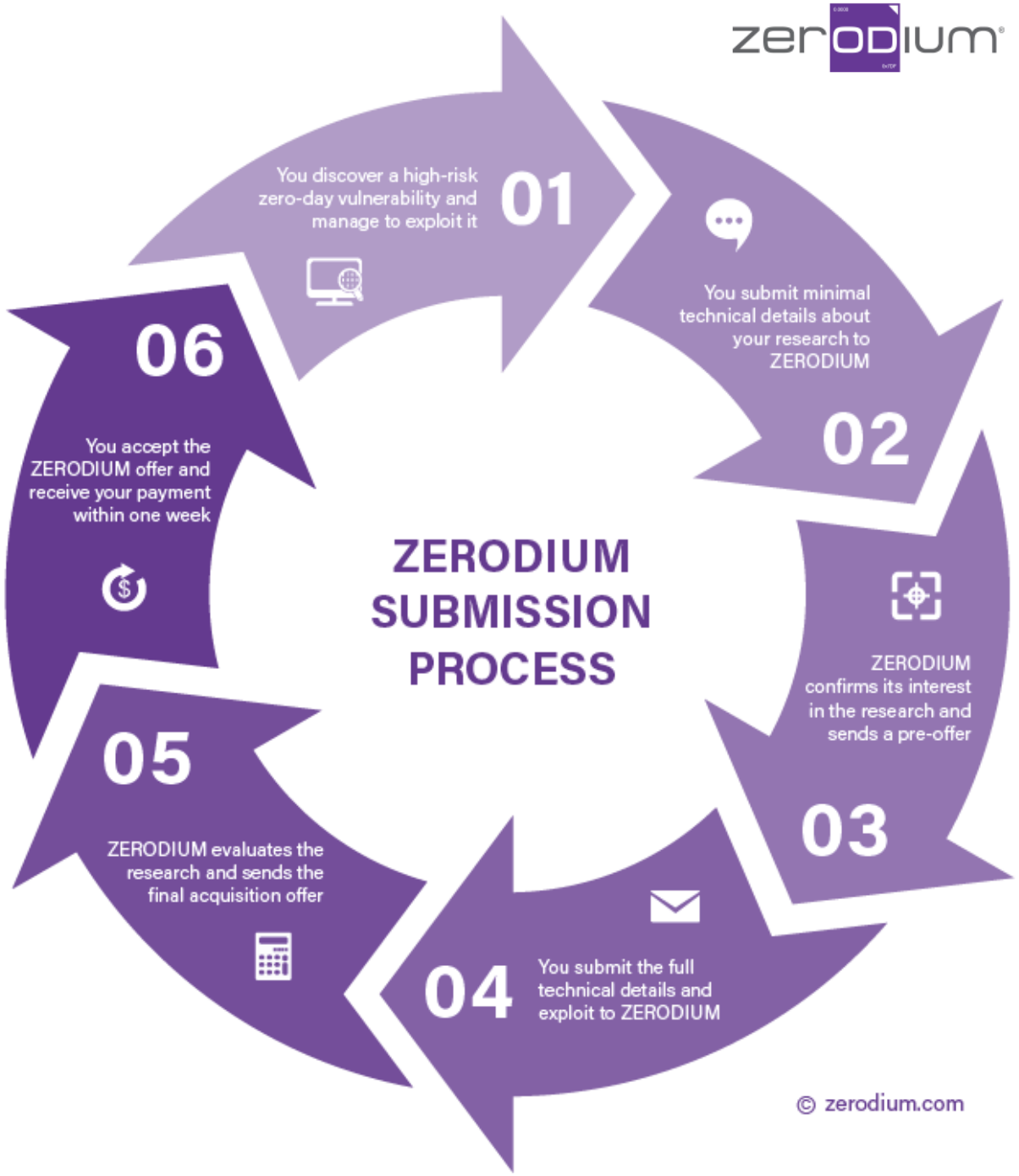
- First day a software patch is released, is Day 1 of the patch
- **Day 0 - no patch available**



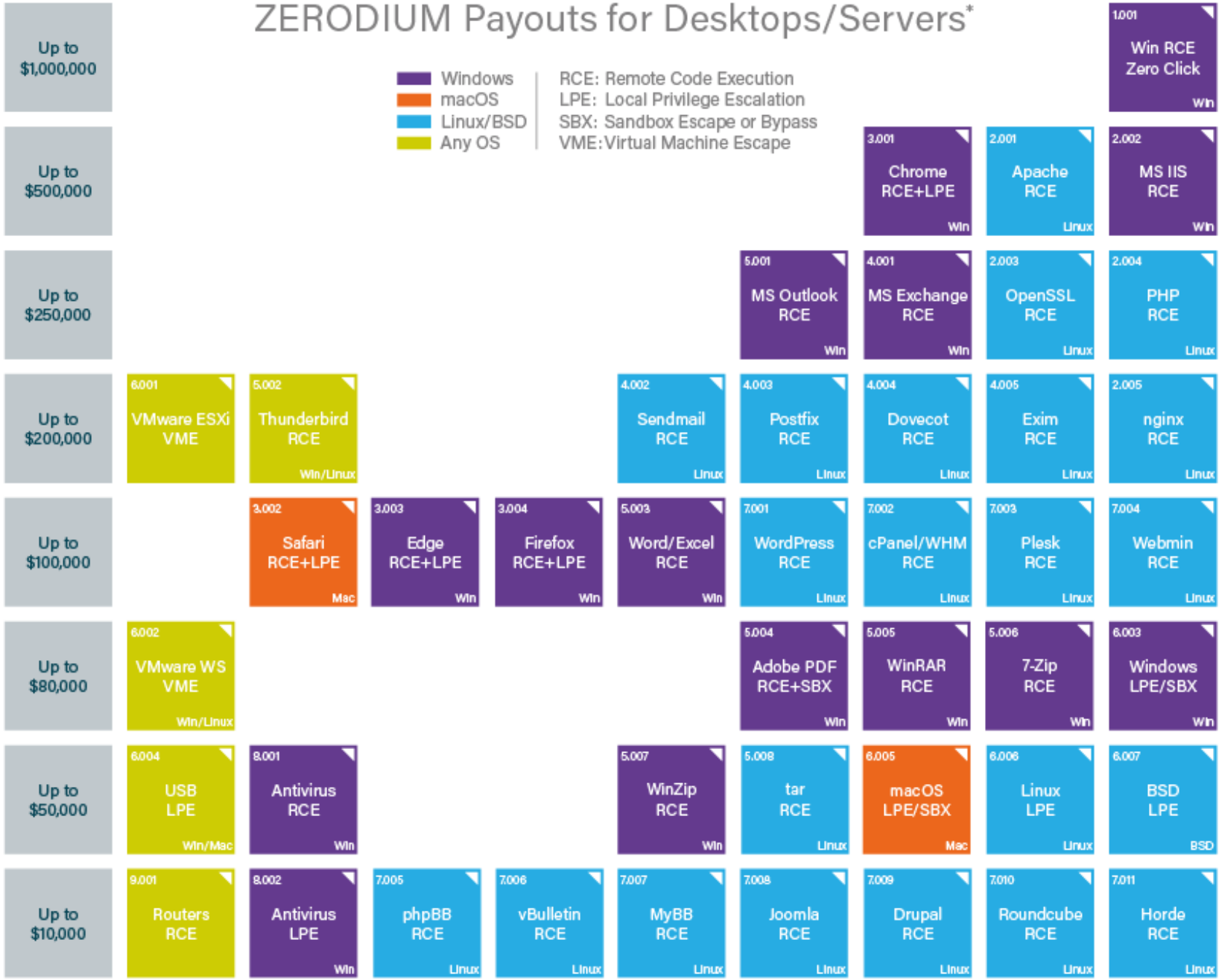
Zero-day exploit market

- 1st Exploit sold in-public was a Microsoft Excel exploit posted on eBay in 2005
  - Subsequently discontinued
    - It violated eBay's policy against encouraging illegal activity

Today: Zerodium is a zero-day reseller, kind of an arms dealer



ZERODIUM Payouts for Desktops/Servers*



** All payouts are subject to change or cancellation without notice. All trademarks are the property of their respective owners.*

Why was the NonPetya attack on Maersk successful?

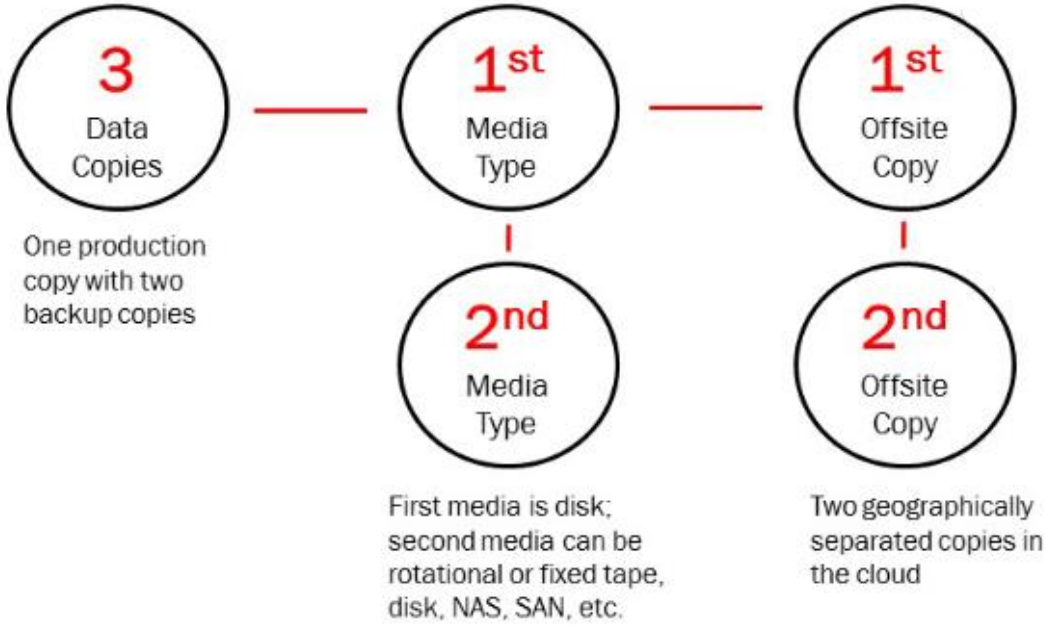
- Systems not upgraded nor patched to protect from NotPetya virus/malware
- All data, backups and systems accessible on the Internet (except Ghana Active Directory server)
- No contingency planning (Business Continuity Plan / Disaster Recovery Plan)

Mitigation – Best Practice

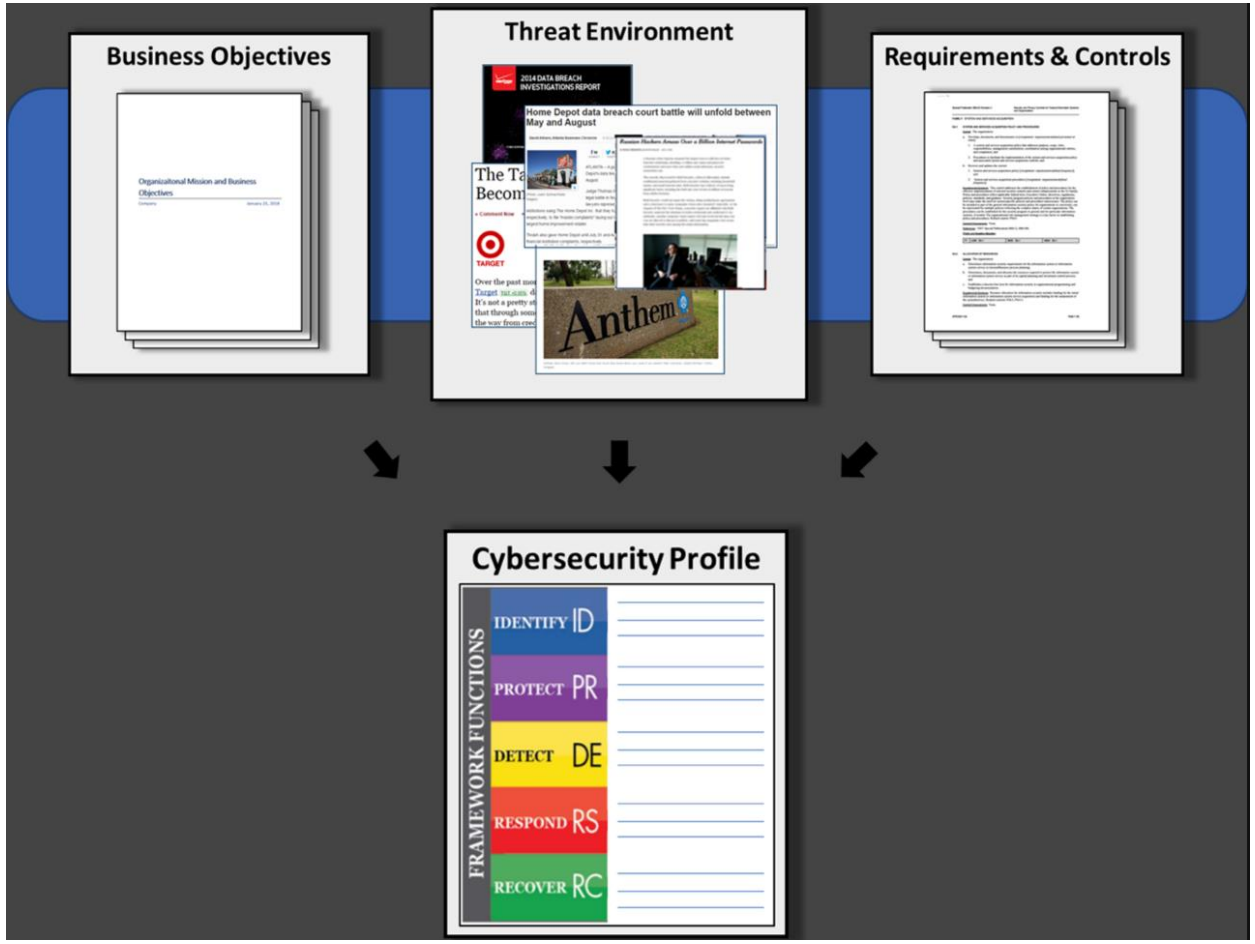
Three-Two-One rule

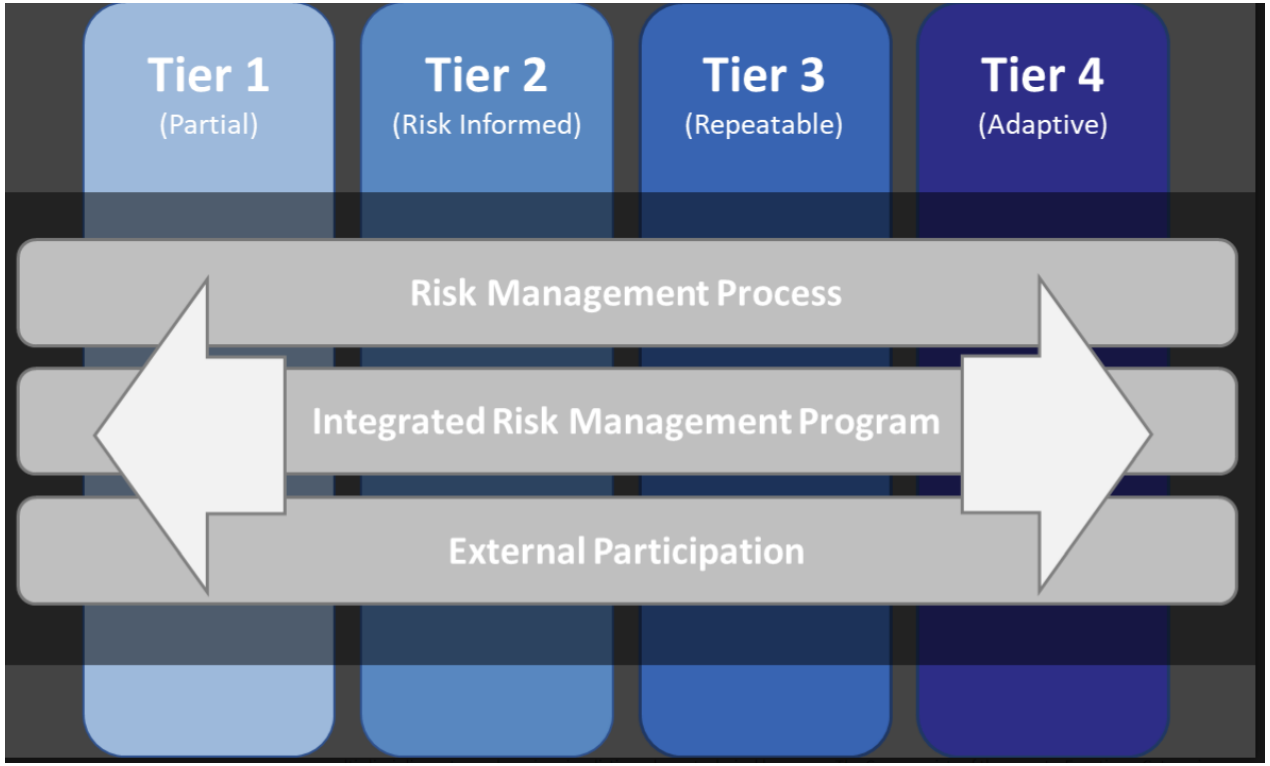
- Make 3 copies of all mission critical software and corresponding data in 2 different formats (to run on Linux and Windows machines), with 1 copy stored off-site not connected to any network

Maersk had 50 copies of their mission critical software and corresponding data – all in the same format, all on the network



How would you rate Maersk's InfoSec Maturity?





Cybersecurity Maturity Models (Enterprise Strategy Group)

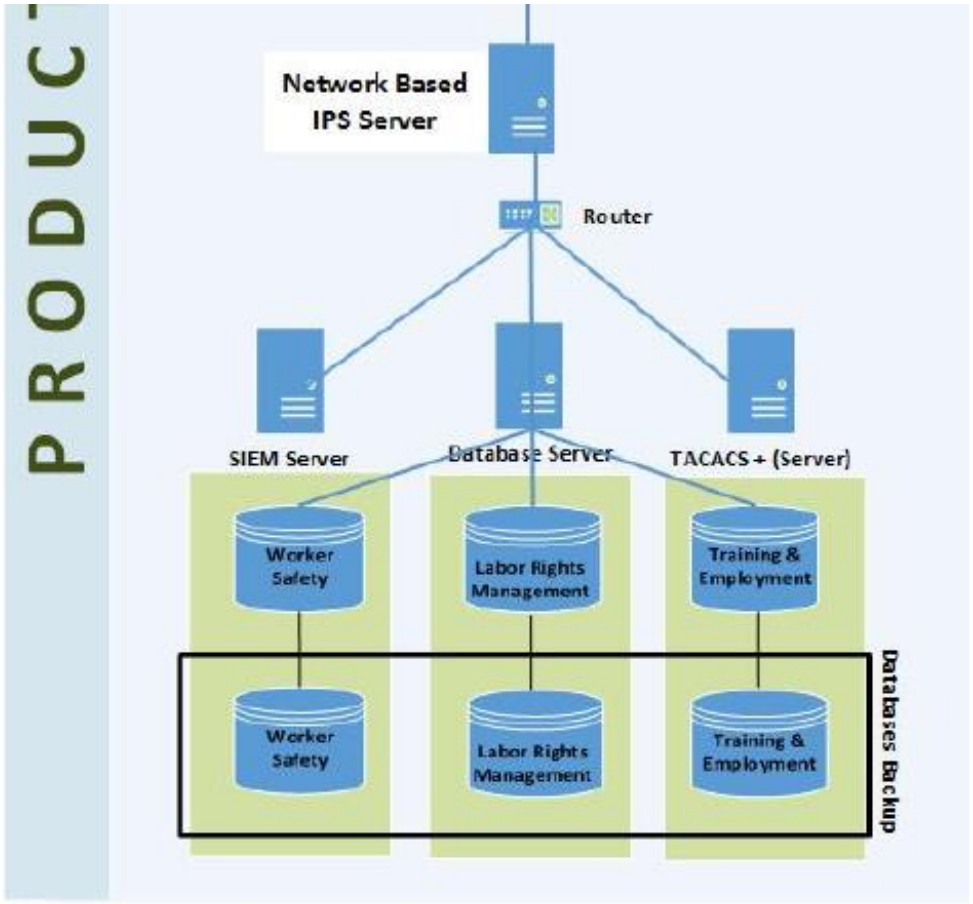
Category	Basic Organizations	Progressing Organizations	Advanced Organizations
Philosophy	Cybersecurity is a "necessary evil."	Cybersecurity must be more integrated into the business.	Cybersecurity is part of the culture.
People	The CISO reports to IT. Small security team with minimal skills. High burnout rate and turnover.	The CISO reports to the COO or to another non-IT manager. Larger security team with some autonomy from IT. Remain overworked, understaffed, and under-skilled.	The CISO reports to the CEO and is active with the board. The CISO considered to be a business executive. Large, well-organized staff with good work environment. Skills and staff problems persist due to the global cybersecurity skills shortage.
Process	Informal and as necessary. Subservient to IT.	Better coordination with IT but processes remain informal, manual, and dependent on individual contributors.	Documented and formal with an eye toward more scale and automation.
Technology	Elementary security technologies with simple configurations. Decentralized security organization with limited coordination across functions. Focus on prevention and regulatory compliance.	More advanced use of security technologies and adoption of new tools for incident detection and security analytics.	Building an enterprise security technology architecture. Focus on incident prevention, detection, and response. Adding elements of identity management and data security to deal with security for cloud computing and mobile computing.

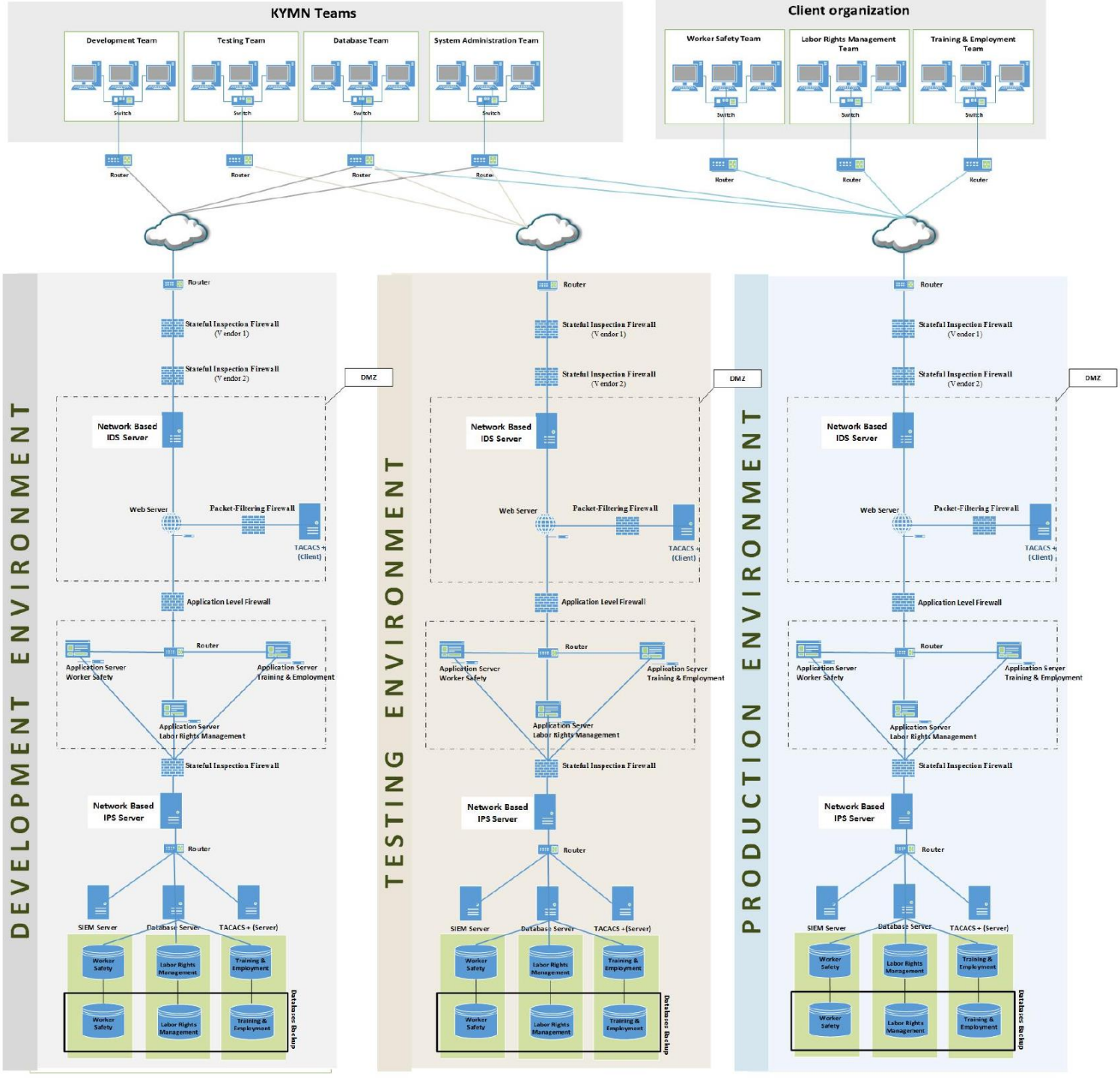
Cybersecurity Maturity ModelsPeople, Process, Technology

	LEVEL 1 PERFORMED	LEVEL 2 MANAGED	LEVEL 3 DEFINED	LEVEL 4 QUANTITATIVELY MANAGED	LEVEL 5 OPTIMIZED
PEOPLE	General personnel capabilities may be performed by an individual, but are not well defined	Personnel capabilities achieved consistently within subsets of the organization, but inconsistent across the entire organization	Roles and responsibilities are identified, assigned, and trained across the organization	Achievement and performance of personnel practices are predicted, measured, and evaluated	Proactive performance improvement and resourcing based on organizational changes and lessons learned (internal & external)
PROCESS	General process capabilities may be performed by an individual, but are not well defined	Adequate procedures documented within a subset of the organization	Organizational policies and procedures are defined and standardized. Policies and procedures support the organizational strategy	Policy compliance is measured and enforced Procedures are monitored for effectiveness	Policies and procedures are updated based on organizational changes and lessons learned (internal & external) are captured.
TECHNOLOGY	General technical mechanisms are in place and may be used by an individual	Technical mechanisms are formally identified and defined by a subset of the organization; technical requirements in place	Purpose and intent is defined (right technology, adequately deployed); Proper technology is implemented in each subset of the organization	Effectiveness of technical mechanisms are predicted, measured, and evaluated	Technical mechanisms are proactively improved based on organizational changes and lessons learned (internal & external)

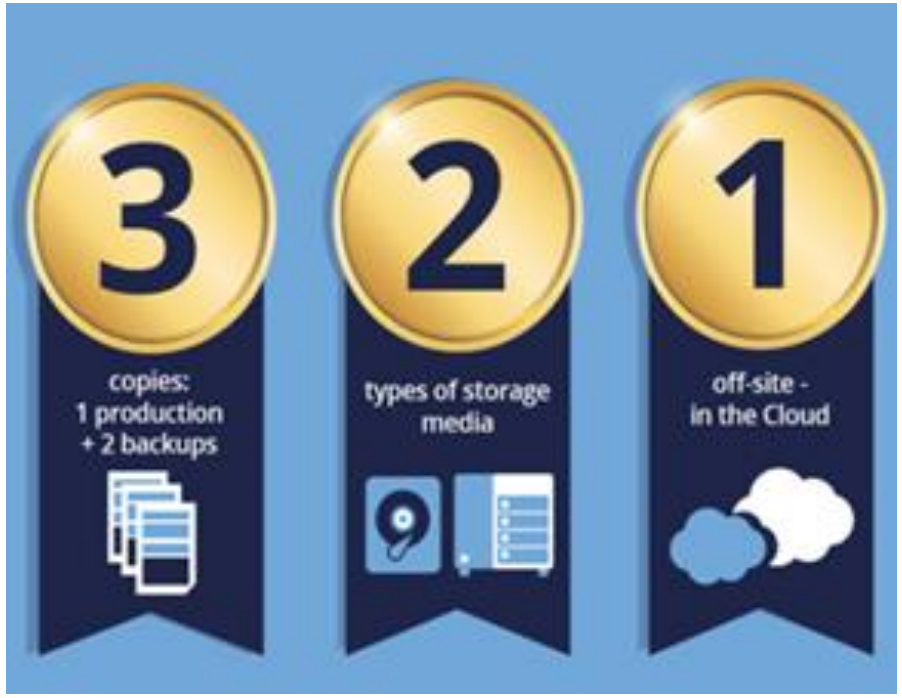
ISACA | CMMI Institute

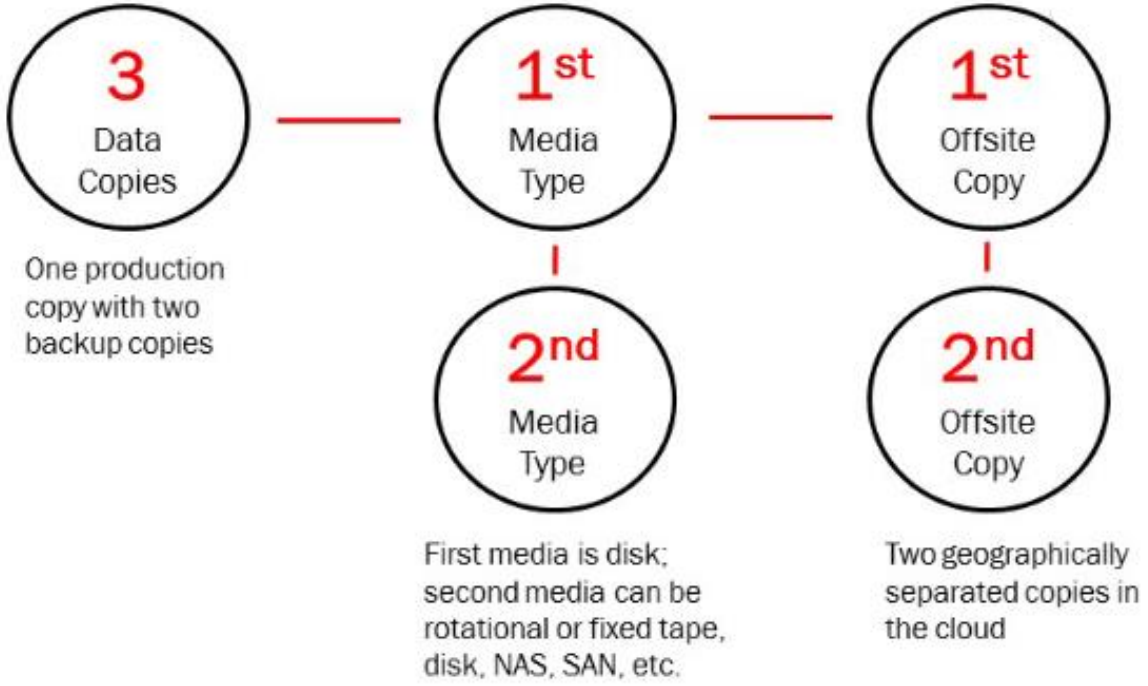
What Maersk case study relevant vulnerabilities do you see in this architecture?





Mitigation – What is the implication for your team's project?





Agenda

- ✓Timeline
- ✓NotPetya
- ✓Zero-Day Vulnerabilities
- ✓Why attack was successful
- ✓Mitigations
- ✓Cybersecurity Capability model
- ✓Team project implications…

Unit #8

MIS 5214

Case Study 2 – Cyberattack: The Maersk Global Supply-Chain Meltdown