Resisting and Recovering from a Ransomware Attack – Are You Ready?

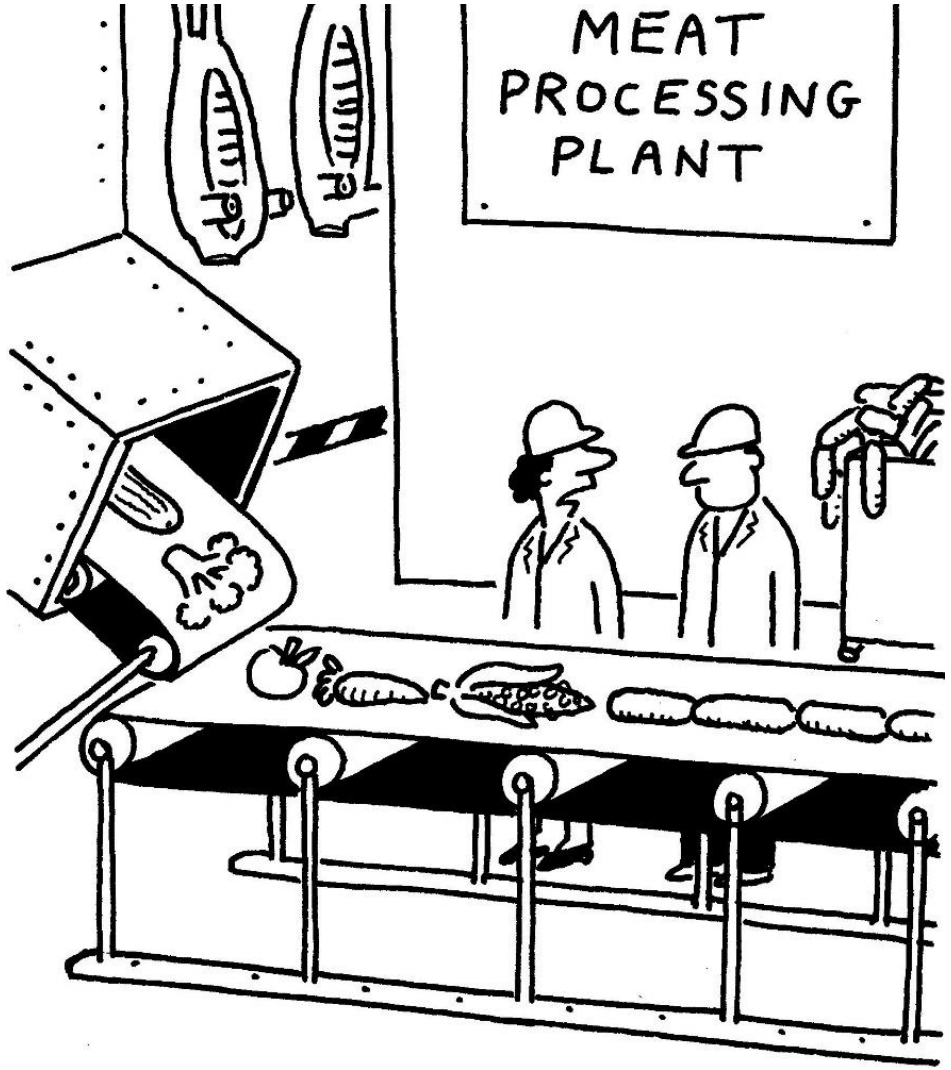
Dr. Sarbari Gupta, CEO, Electrosoft

8.8 Andina Computer Security Conference

July 16, 2021

Computer Security Conference

Malware Spares No One!



"I THINK WE'VE BEEN HACKED"

Electrosoft

Recent Ransomware Attacks

May

2021 May - Colonial Pipeline

- U.S. energy company shut down its entire fuel distribution pipeline
- Threatened gasoline and jet fuel distribution across the U.S. east coast
- DarkSide responsible. Paid $5M ransom

July

2021 July - Kaseya

- Remote Monitoring and Management Platform
- REvil ransomware spread from MSPs to ~1500 businesses worldwide
- Supply Chain attack - Authentication bypass vulnerability used to upload malicious payload

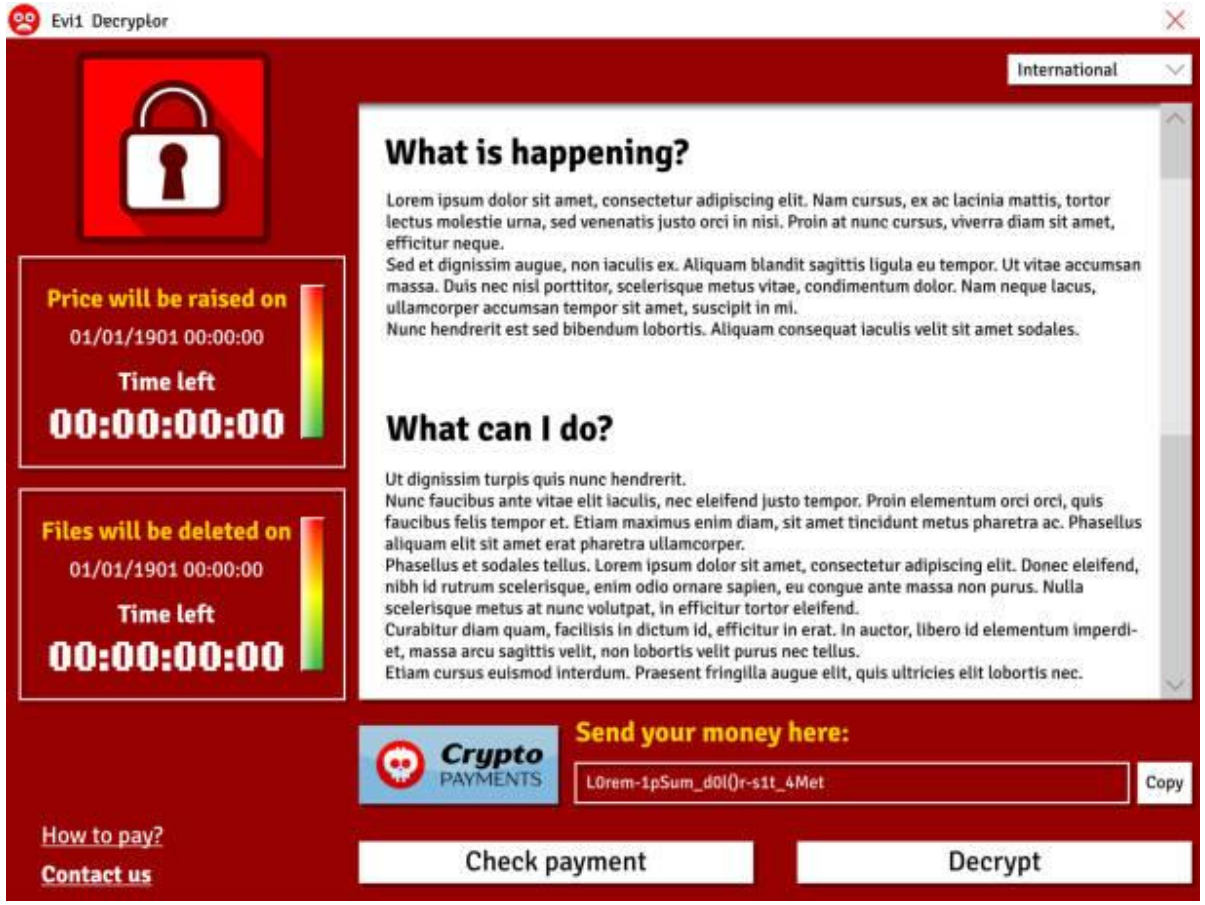
June

2021 June - JBS

- Largest meat supplier
- Took systems offline and stopped work
- Russian cyber gang REvil
- Paid $11M in bitcoin

Ransomware - What is it?

- A type of malware that compromises data or systems with the single goal of extorting a ransom payment from the victims.
- The attack can be used to steal, corrupt or scramble data, hijack systems, disrupt operations or threaten exposure.
- Typically, a ransom note is left on the system, demanding payment to restore the data or keep the data confidential.



Malware vs. Ransomware

Malware

- *Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. [NIST SP 800-53 Rev 4]*
- *Many types – Spyware, Keylogger, Rootkit, Virus, Worm, Trojan, etc. [https://www.thepcinsider.com/malware-types-explained/*
- *Most malware tries to evade detection!*

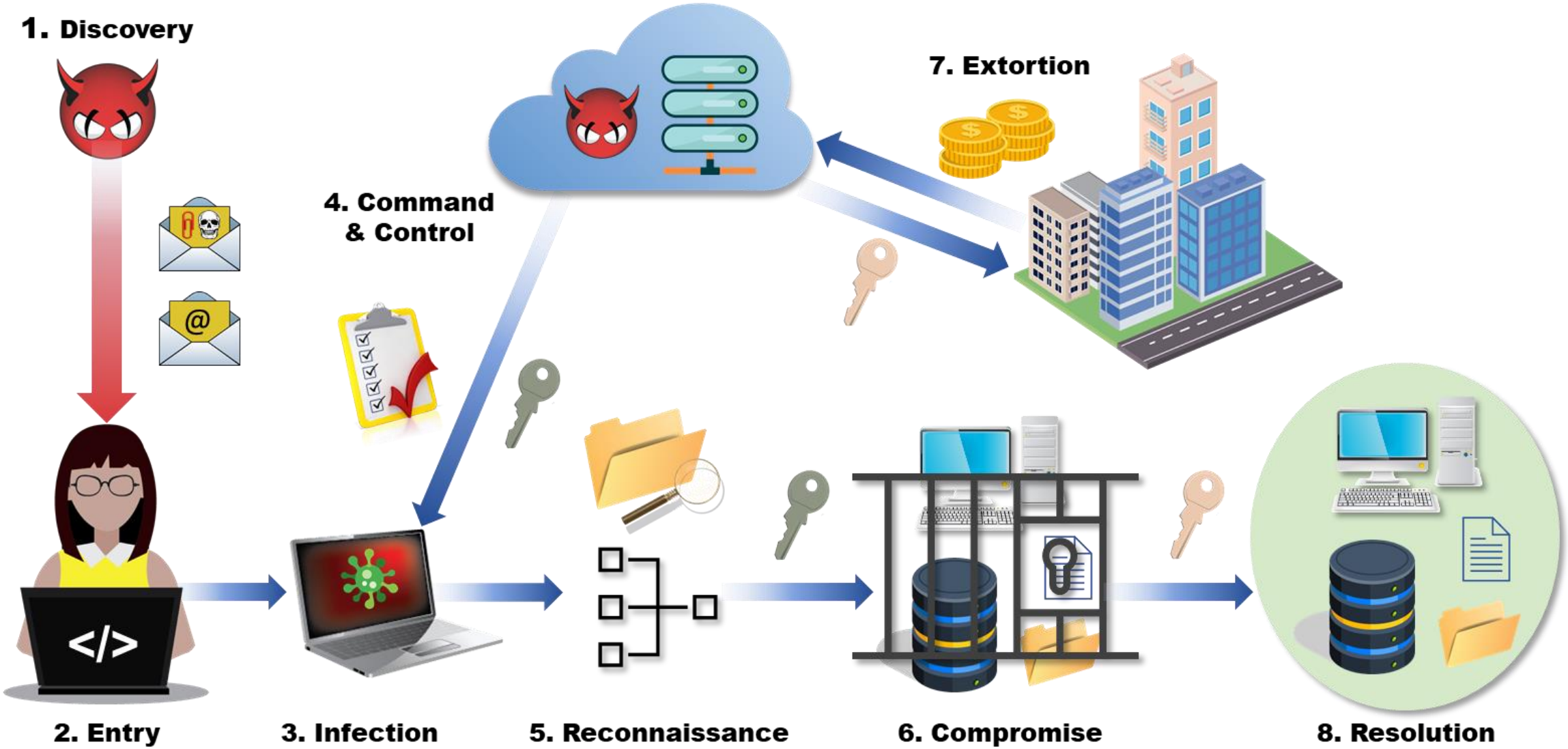
Ransomware

- *A type of malicious attack where attackers encrypt an organization's data and demand payment to restore access. [Courtesy NIST IR 8374 draft]*
- *Attackers may also steal an organization's information and demand payment for not disclosing the information*
- *Ransomware does not try to HIDE!*

Ransomware (RW) Kill Chain

- **Discovery – Attacker tries to collect information about Organization or Users**
- **Entry – Injection of RW to corporate network**
- **Infection – RW installs on local platform**
- **Command & Control – RW client establishes connection with C&C Server**
- **Reconnaissance – Leveraging initial foothold, scan for high value targets**
- **Compromise – Identify and compromise target files, processes and systems**
- **Extortion – Demand ransom through threat**
- **Resolution - Restore the targets to enable normal operations**

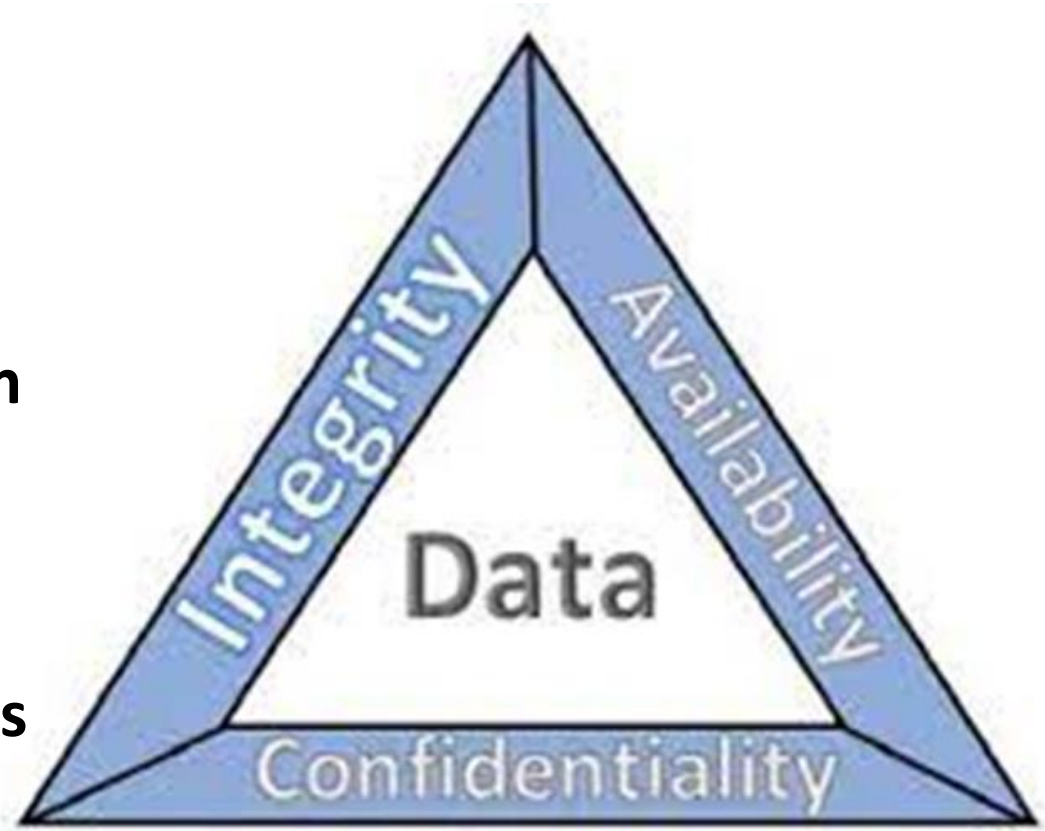
Ransomware Kill Chain!



Electrosoft

CIA of Ransomware

- **Confidentiality Attack – Steal sensitive data and threaten to reveal it unless ransom is paid**
- **Integrity Attack – Encrypt data to make it unusable and demand ransom to decrypt it**
- **Availability Attack – Compromise of data leads to applications and systems becoming unavailable for legitimate users**

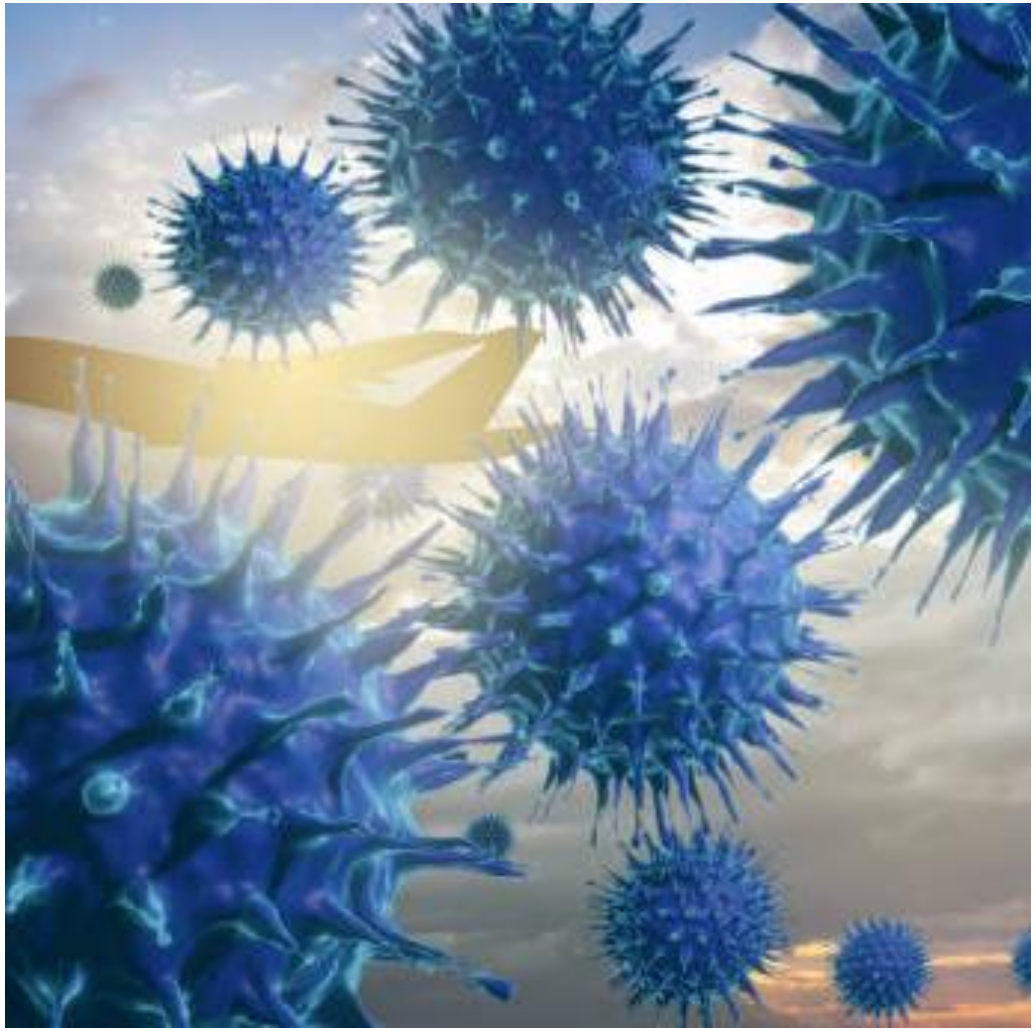


Courtesy NIST SPECIAL PUBLICATION 1800-25

How Ransomware Enters

- Malware-laden Email
- Web Browsing
- Downloading Rogue Applications
- Vulnerable Remote Connections
- Connecting Infected Systems to the network
- Connecting infected storage drives to a network computer

How Ransomware Spreads



- Identify and exploit vulnerabilities
- Leverage access to local and network/cloud files
- Delete backup copies
- Disable backups
- Disable system recovery

Protecting and Defending Against Cyber Attacks

Courtesy NIST SPECIAL PUBLICATION 1800-25

- **NIST Cybersecurity Framework V1.1**
  - ***Identify* – Develop understanding of enterprise cyber risk**
  - ***Protect* – Implement appropriate safeguards**
  - ***Detect* – Identify occurrence of cyber events**
  - ***Respond* - Take action on identified incident**
  - ***Recover* – Restore capabilities or services**

[https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf]

Defense Techniques - Good Cyber Hygiene

- **Maintain security posture of network/systems**
  - ***Secure Configurations***
  - ***Timely Patching***
  - ***Vulnerability Scanning and Remediation***
  - ***Strong Security Policies and Enforcement***
  - ***Minimize User Privileges (Least Privilege Principle)***
  - ***Network Segmentation***

Defense Techniques – User Awareness and Training

- **Train Users**
  - ***Security Policies***
  - ***Phishing***
  - ***Unsafe Browsing***
  - ***Downloading Applications***
  - ***Connecting Non-Work Devices to Network***
  - ***Securing Home Network***
  - ***Allow Patching***
  - ***Protect authentication credentials***

Defense Techniques – Border Control

- Endpoint Detection and Recovery (Anti-Virus)
- Scan Incoming Emails
- Block Access to Malicious Websites
- Multi-factor Authentication

Defense Techniques – Detection and Response

- **Security Monitoring**
  - ***Event Logs***
  - ***Network Activity***
- **Incident Response**
  - ***Maintain Incident Response (IR) Plan***
  - ***Test IR Plan regularly***
  - ***Forensic capabilities***

Defense Techniques – Backup and Restore

- **Maintain Working Backups**
  - ***Identify critical data/files/systems for continuity***
  - ***Implement online and offline backups***
  - ***Maintain multiple backups***
  - ***Test restoration from backups regularly***

Summary

- **Ransomware attacks can be highly disruptive!**
- **Any and every Organization can become a target**
- **Important to understand the Ransomware Kill Chain to develop defensive techniques**
- **Two lines of defense**
  - ***Proactive – resistance to attacks***
  - ***Reactive – resiliency in case of attack***
- ***Taking effective proactive and reactive steps can make us more resistant and resilient to ransomware attacks!***

Contact Information

- **Contact Info: Dr. Sarbari Gupta – Electrosoft**
  - *Founder and CEO*
  - *Email: sarbari@electrosoft-inc.com;*
  - *LinkedIn: https://www.linkedin.com/in/sarbari-gupta/*
- **Electrosoft**
  - *Web: http://www.electrosoft-inc.com*
  - *LinkedIn: https://www.linkedin.com/company/electrosoft/*
  - *Twitter: https://twitter.com/Electrosoft_Inc*
  - *HQ: 1893 Metro Center Drive, Suite 228; Reston VA 22066*