

Threat Based Cybersecurity Investments



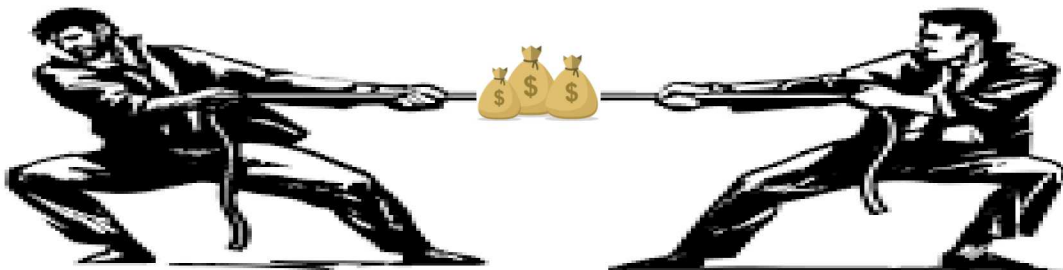
PRESENTED BY

ANITA BHAT

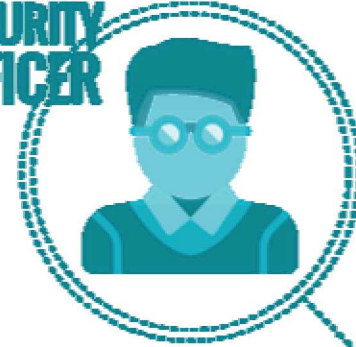


Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

The Unfortunate Reality



**CHIEF
INFORMATION
SECURITY
OFFICER**



CISO VS. CIO



**CHIEF
INFORMATION
OFFICER**

Current Trends

Cybersecurity spending seems to be sky rocketing

According to Gartner, companies will spend \$124 Billion on cybersecurity in 2019¹

Data from Strategic Cyber Ventures²:

VC funding for 2018 was 5.3 billion

20% higher than 2017

80% higher than 2016

Predicted to exceed ONE TRILLION DOLLARS by 2021!!!

¹ <https://www.gartner.com/en/newsroom/press-releases/2018-08-15-gartner-forecasts-worldwide-information-security-spending-to-exceed-124-billion-in-2019>

² <https://scvgroup.net/2018-cybersecurity-venture-capital-investment/>

Cost of Breaches

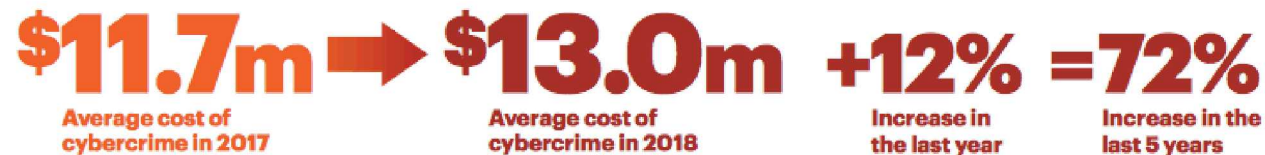
According to the Ninth Annual Cyber Crime Study by Accenture and the Ponemon Institute published on March 6, 2019³:

The **average cost** of cybercrime for an organization is now **\$13.0 million**.

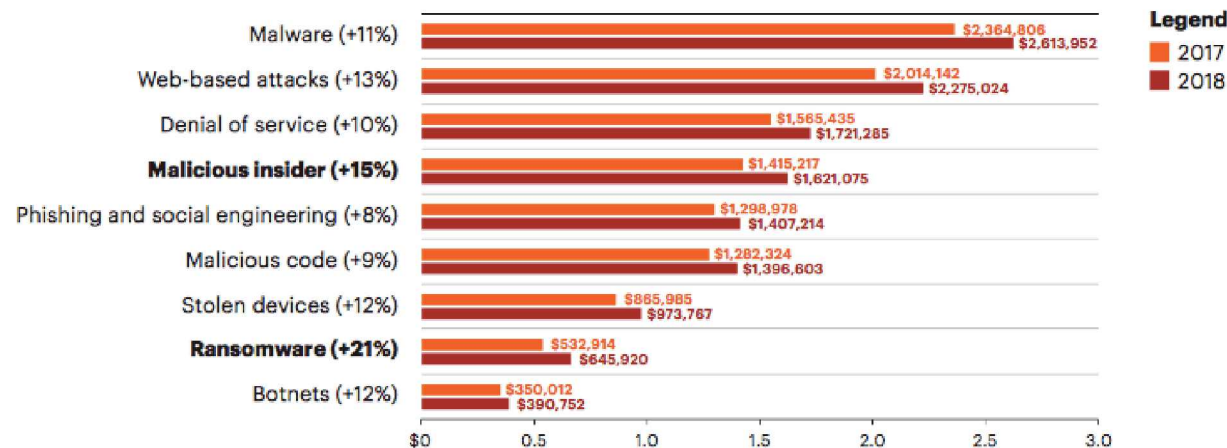
³ <https://www.accenture.com/us-en/insights/security/cost-cybercrime-study>

ORGANIZATIONS SPEND MORE THAN EVER DEALING WITH THE COSTS AND CONSEQUENCES OF INCREASINGLY SOPHISTICATED ATTACKS

Cost of cybercrime is rising



People-based attacks have increased the most



Business consequences are expensive

\$4.0m
Cost of business disruption

\$5.9m
Cost of information loss

36%
Proportion of spend on discovering attacks in 2018



WHAT HAVE WE BEEN DOING?

Compliance-Based Cybersecurity!!!





WHAT DO WE NEED TO DO?

Think like the Adversary!



Move from Compliance to Threat-Based Risk Management

Compliance



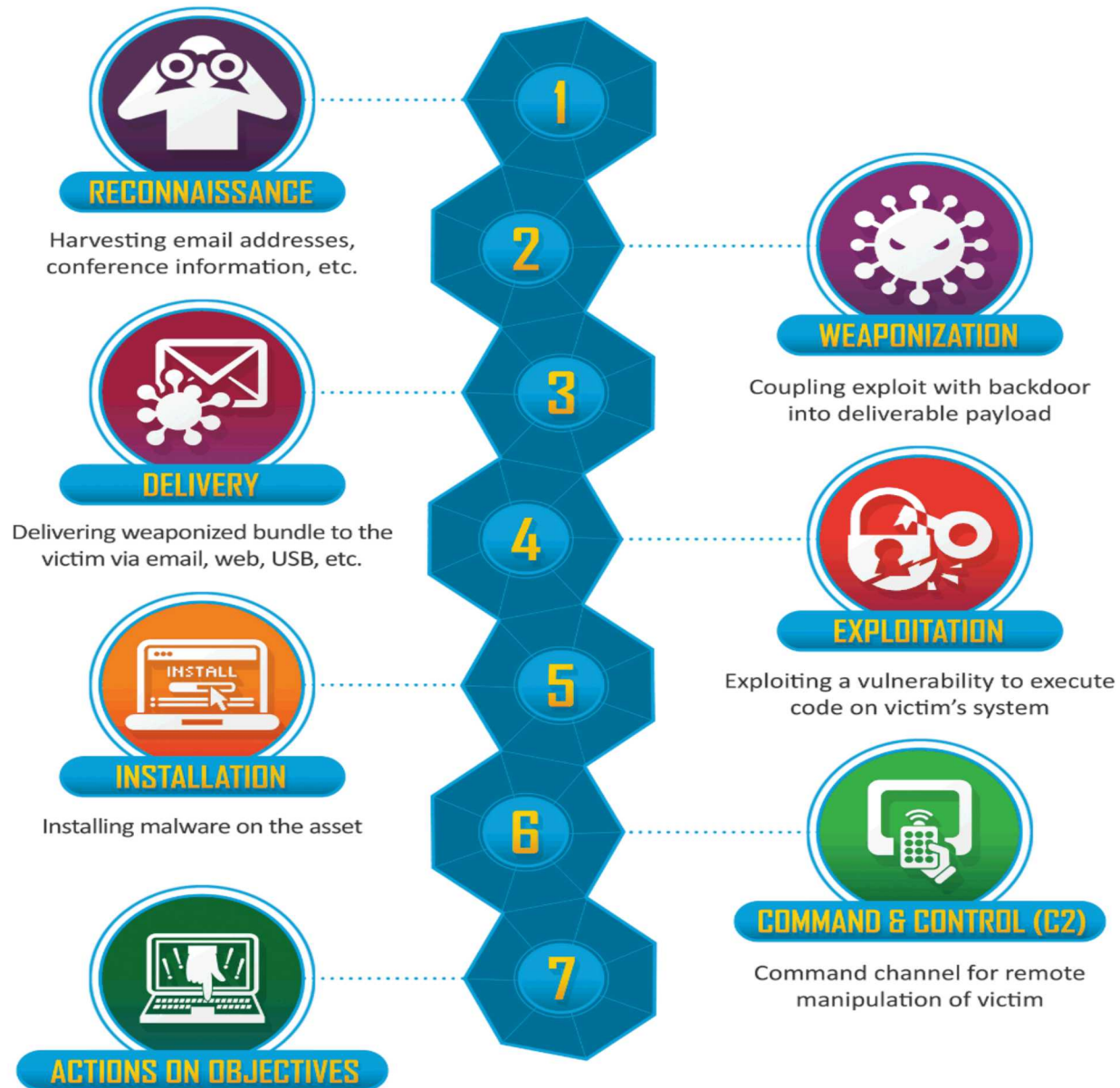
Here Are Several Threat Frameworks to Choose From

- NIST – Special Publication 800-30 (Guide for conducting Risk Assessments) - Appendix E
- Lockheed Martin's Kill Chain
- MITRE's Adversarial Tactics, Techniques, & Common Knowledge (ATT&CK)
- NSA Technical Cyber Threat Framework (NTCTF) v2

Appendix E lists Threat Events

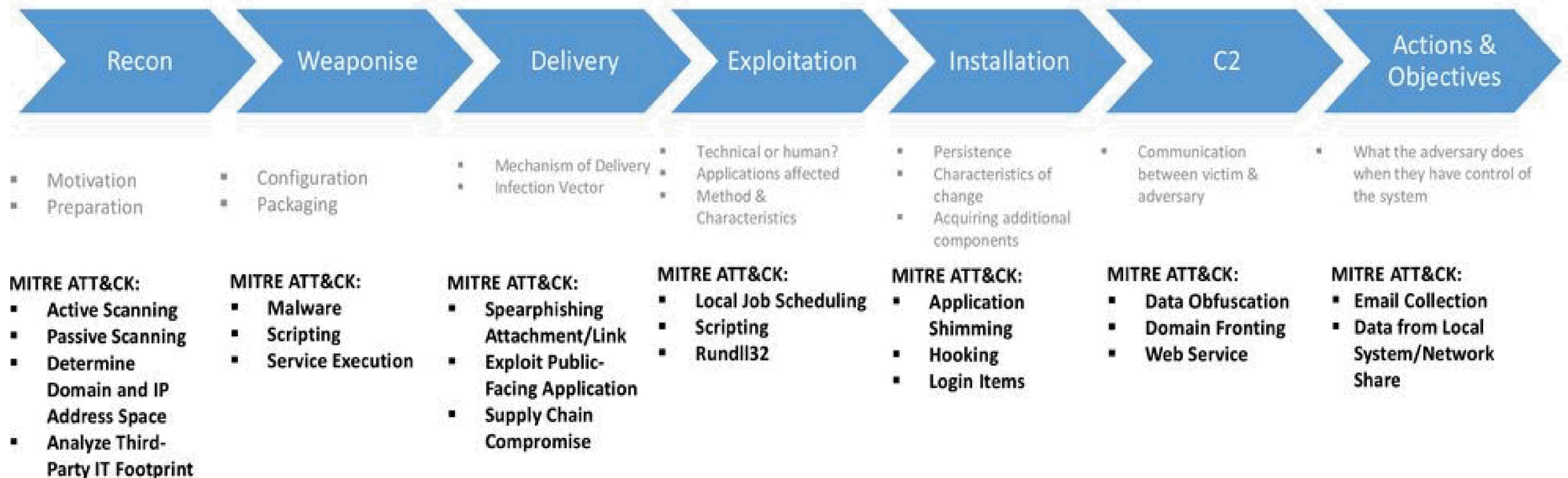
- Perform perimeter network reconnaissance/scanning.
- Perform network sniffing of exposed networks.
- Craft phishing attacks.
- Craft counterfeit certificates
- Deliver malware to information systems
- Exploit split tunneling
- Conduct wireless jamming attacks
- Conduct Denial of Service attacks
- ...
- ...
- ...

Lockheed Martin's Kill Chain



MITRE ATT&CK MATRIX

- Builds on the Kill Chain
- Provides deeper level of granularity



NSA Technical Cyber Threat Framework (NTCTF) v2 *

(13 November 2018)

NSA/CSS Technical Cyber Threat Framework (NTCTF v2)

Administration	Engagement	Presence	Presence	Effect	Ongoing Processes
Planning	Delivery	Execution	Credential Access	Monitor	Analysis, Evaluation, and Feedback
Analyze operation	Access via wireless	Create scheduled task	Add or modify credentials	Activate recording	Abandon infrastructure
Determine strategy and goals	Alter communications path	Execute via service controller	Conduct social engineering	Collect passively	Conduct effects assessments
Issue operational directive	Compromise supply chain or trusted source	Execute via third-party software	Crack passwords	Enable other operations	Refine potential victims
Produce operational plans	Connect removable media	Inject into running process	Dump credentials	Log keystrokes	Command and Control
Receive approval to execute operations	Connect rogue network devices	Leverage authorized user	Hijack active credential	Maintain access	Beacon to midpoints
Select intended victims	Infect via websites	Replace existing binary	Locate credentials	Take screen capture	Establish peer network
Resource Development	Inject database command	Run commands in shell	Log keystrokes	Exfiltrate	Relay communications
Acquire operational infrastructure	Leverage device swapping	Run fileless payload	Lateral Movement	Collect crosstalk	Send commands
Build alliances and partnerships	Send malicious email	Use interpreted scripts	Exploit peer connections	Collect from local system	Use botnet
Create botnet	Transport via common network infrastructure	Use OS APIs	Logon remotely	Collect from network resources	Use chained protocols
Develop capabilities	Traverse CDS or MLS	Use remote services	Pass the hash	Compress data	Use peer connections
Obtain financing	Use chat services	Use trusted application to execute untrusted code	Pass the ticket	Disclose data or information	Use remote shell
Seed supply chain	Use compromised host	Write to disk	Replicate through removable media	Position data	Use removable media
Staff and train resources	Use legitimate remote access	Internal Reconnaissance	Taint shared content	Run collection script	Evasion
Research	Use physical network bridge	Enumerate accounts and permissions	Use application-deployment software	Send over C2 channel	Access raw disk
Gather information	Exploitation	Enumerate file system	Use remote services	Send over non-C2 channel	Avoid data-size limits
Identify capability gaps	Abuse protocols	Enumerate local network connections	Write to remote file shares	Send over other network medium	Block indicators on host
Identify information gaps	Access virtual memory	Enumerate local network settings	Write to shared webroot	Throttle data	Block indicators on host
Preparation	Conduct social engineering	Enumerate OS and software	Persistence	Transfer via physical means	Degrade security products
Reconnaissance	Defeat encryption	Enumerate processes	Create new service	Traverse CDS or MLS	Delay activity
Conduct social engineering	Exploit firmware vulnerability	Enumerate windows	Create scheduled task	Modify	Employ anti-forensics measures
Gather credentials	Exploit local application vulnerability	Map accessible networks	Edit boot record	Alter data	Employ anti-reverse-engineering measures
Identify crosstalk	Exploit OS vulnerability	Scan connected devices	Edit file-type associations	Alter process outcomes	Employ rootkit
Map accessible networks	Exploit remote application vulnerability	Sniff network	Employ logon scripts	Cause physical effects	Encode data
Scan devices	Exploit weak access controls	Privilege Escalation	Leverage path-order execution	Change machine-to-machine communications	Encrypt data
Scrape websites	Hijack	Exploit application vulnerability	Modify BIOS	Change run-state of system processes	Impersonate legitimate file
Select potential victims	Impersonate or spoof user	Exploit firmware vulnerability	Modify configuration to facilitate launch	Deface websites	Manipulate trusted process
Survey devices	Launch zero-day exploit	Exploit OS vulnerability	Modify existing services	Defeat encryption	Mimic legitimate traffic
Use social media	Leverage exploit packs	Inject into running process	Modify links	Deny	Modify malware to avoid detection
Staging	Leverage trusted relationship	Use accessibility features	Modify service configuration	Corrupt files or applications	Obfuscate data
Add exploits to application data files	Replay	Use legitimate credentials	Replace service binary	Degrade	Remove logged data
Allocate operational infrastructure			Set to load at startup	Disrupt or denial of service	Remove toolkit
Create midpoints			Use library-search hijack	Encrypt data to render unusable	Sign malicious content
Establish physical proximity				Destroy	Store files in unconventional location
Infect or seed website				Brick disk or OS (full delete)	Tailor behavior to environment
Pre-position payload				Corrupt disk or OS (partial delete)	Use signed content
				Delete data	
				Destroy hardware	

Legend

Stage
Objective
Action

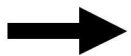
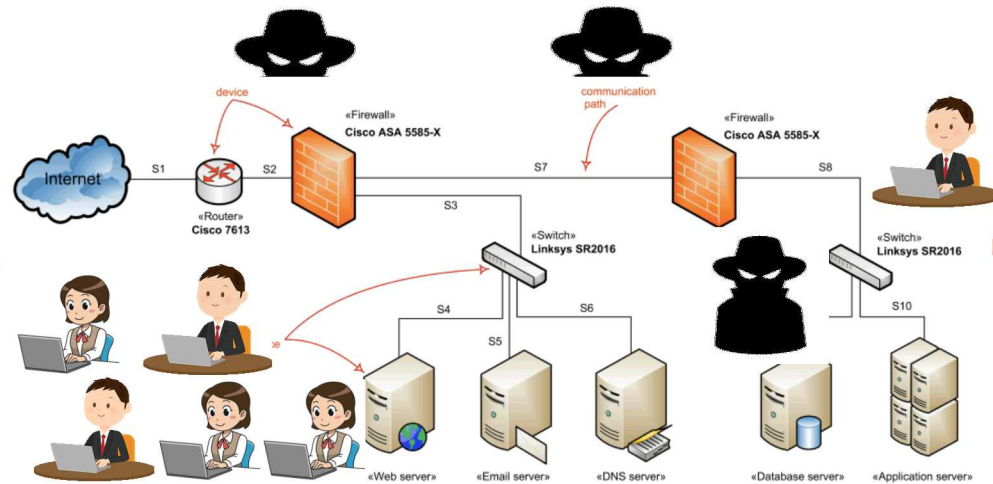
Lifecycle of a Threat

Pre-event

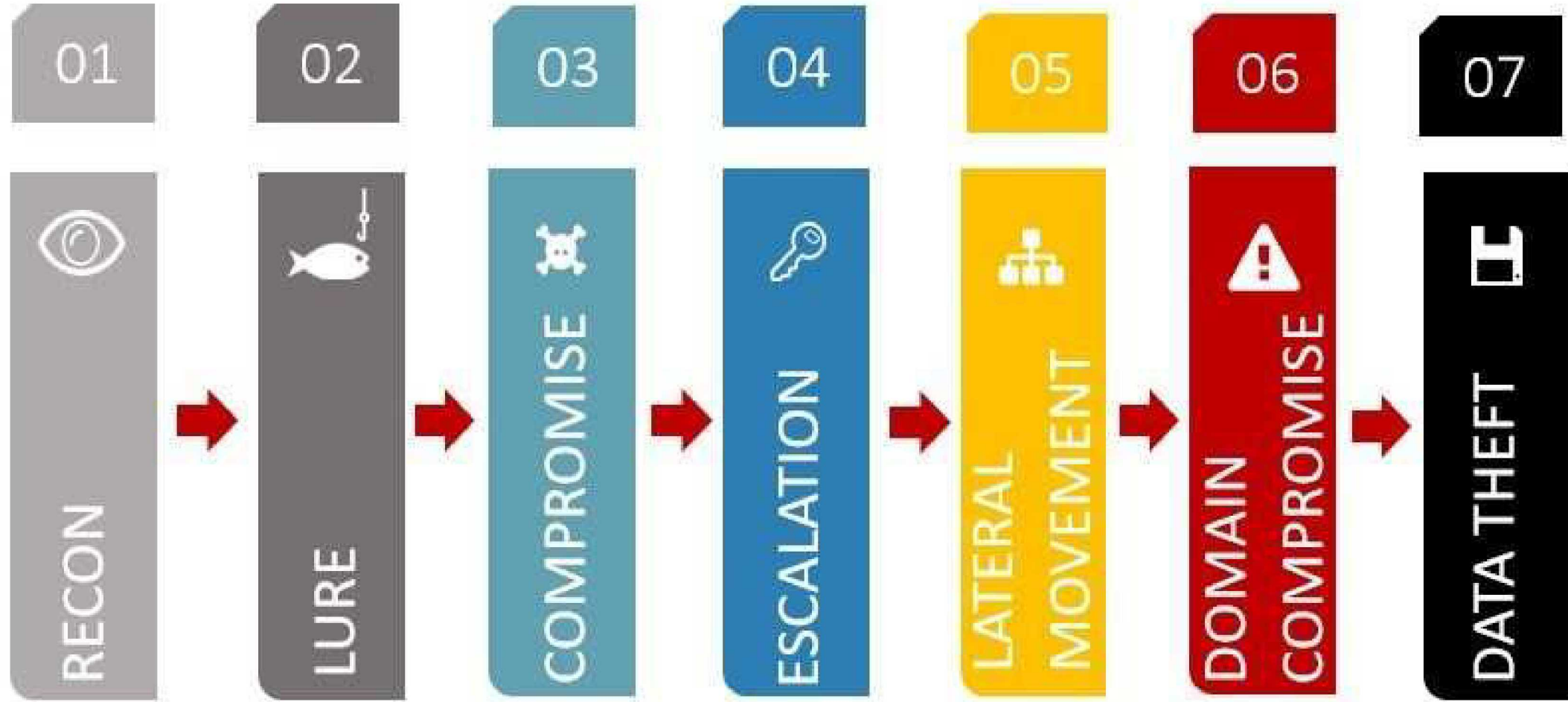
Get-in

Stay-in

Act



What Actually Happens



Anatomy of a Threat

The NSA Technical Cyber Threat Framework depicts threats in layers:

1. **Stages:** The progression of cyber threat actions over time to achieve objectives
2. **Objectives:** The purpose of conducting an action or a series of actions
3. **Actions:** and associated resources used by an threat actor to satisfy an objective
4. **Indicators:** Discrete cyber threat intelligence data (company x reported to have created malware y)

Layers of a Threat

The NSA Technical Cyber Threat Framework depicts threats in three layers:

1. Stages:
 - Pre-Event
 - Get-in
 - Stay-in
 - Act
2. Each Stage has different Objectives
3. Each Objective has several Actions used to fulfill the Objective
4. Indicators or intelligence data that can be specific about adversary actions

Pre-Event Stage

Objective: Intent / Resource Development

Action: Intent/Resource Development

Objective: Reconnaissance / Staging

Action: Crawling Internet Websites

Action: Network Mapping (e.g. NMAP)

Action: Social Media

Action: Mid-points

Action: Vulnerability Scans

Objective: Weaponization

Action: Add Exploits to Application Data Files

Get-In Stage

Objective: Delivery

Action: Spear-phishing Emails w/ Attachments or w/ Malicious Link

Action: Websites

Action: Removable Media (i.e. USB)

Action: SQL Injection

Action: Virtualization Attacks

Action: DNS/Cache Poisoning

Action: ...

Objective: Initial Compromise / Exploitation

Action: Targets Application Vulnerability

Action: Target Operating System Vulnerability

Action: Targets Web Application Vulnerabilities (ex. XSS, CSRF)

Action: Trojan

Action: Exploit Weak Access Controls

Action: Defeat Encryption

Installation

Action: Writing to Disk

Action: In Memory Malware

Action: Replace Legitimate Binary with Malicious

Stay-In Stage

Objective: Persistence

- Action: Legitimate Credentials
- Action: Automatic Loading at Startup
- Action: Path Interception
- Action: Link Modification
- Action: Hypervisor Rootkit
- Action: Modify Existing Services
- Action : ...

Objective: Privilege Escalation

- Action: Process Injection
- Action: Credential Access
- Action: Exploitation of Vulnerability (ex. XSS, CSRF, OS/Software)
- Action: ...

Objective: Defense Evasion

- Action: Binary Padding
- Action: Disabling Security Tools
- Action: Indicator Blocking
- Action: File Deletion
- Action: ...

Stay-In Stage

Objective: Credential Access

- Action: Credential Dumping
- Action: User Interaction
- Action: Network Sniffing
- Action: Password Recovery
- Action: ...

Objective: Host Enumeration

- Action: Account/File System/Permissions/Network/OS/Process Enumeration

Objective: Lateral Movement

- Action: Remote Services
- Action: Peer Connections
- Action: Remote Interactive Logon
- Action: Shared Webroot
- Action: ...

Objective: Command & Control

- Action: Commonly Used Port
- Action: Standard /Custom Application Layer Protocol
- Action: Peer Connections
- Action: Multiband Communications

Act Stage

Objective: Collection

Objective: Monitor / Exfiltration

- Action: Exfil over C2 Channel

- Action: Exfil over Network Resources

- Action: Scheduled Transfer

- Action: Exfil over Physical Medium

- Action: ...

Objective: Alter/Deceive

- Action: Full Data Deletion

- Action: Denial of Service

- Action: Cause Physical Effects

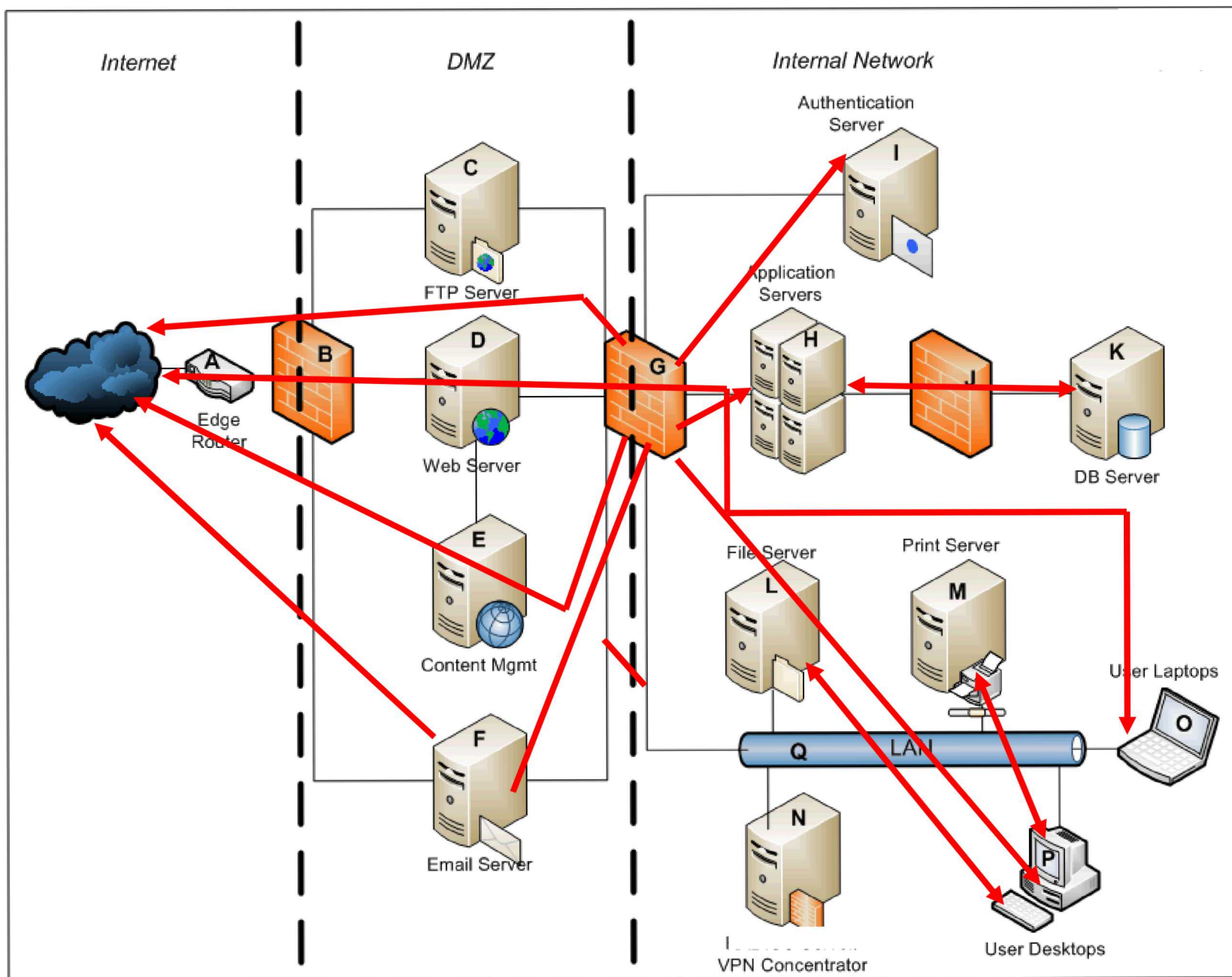
- Action: ...

Applying the Threat Framework to Target Architecture

How do you evaluate how these threats affect your architecture?

Architectural features to consider:

- Traffic Flows
- Security Capabilities along those Flows
- Enumerate Security Capabilities
- Score each Capability against each Threat Action for its ability to Protect / Detect / Respond to the threat action



Exemplar Security Capabilities

- Next Generation Firewall
- SIEM
- Web Content Filtering
- Sand Boxing
- Virtual Desktop Infrastructure
- Inbound/Outbound SMTP Proxy
- Use of a Content Delivery Network
- Remote Access VPN
- DNS Proxy for inbound Queries
- Network Segmentation
- Network Access Control
- Host IPS
- Device Health Check
- Application Whitelisting
- Etc

Scoring

				Stage					
				Objective					
	Detailed Capability Description	Enh	% Scores Done	Threat Action Y			Threat Action z		
				Protect	Detect	Respond	Protect	Detect	Respond
Capabilities	To create new Capabilities, select the entire row of an	Is Enhanc	% Scoring Comple	Threat Action Description			Threat Action Description		
Layer1									
A	Description			M	M	S	None	None	L
Rationale				P/D has some allowed paths. All actions are logged			Threat action is permitted but logged. Logs only persist 1 week		
Layer2									
B	Description			N/A	N/A	N/A	L	L	L
Rationale			0%				only covers one possible vector		
B (Enhancement)	Description			N/A	N/A	N/A	M	M	M
Rationale			0%				coverage include additional but not all vectors		

Coverage Map

The diagram is a complex, multi-layered flowchart or organizational chart. It consists of numerous small rectangular boxes connected by lines, forming a dense, interconnected network. The boxes are arranged in a way that suggests a flow from top to bottom, with many branches and sub-branches. The overall structure is highly detailed and appears to be a technical or organizational diagram.

So What?

2. We see where the gaps lie based on our own “Risk Tolerance”
3. Based on the scoring map we prioritize technologies
4. We calculate the cost of implementing the prioritized technologies

Cost of Technology + Cost of Labor

Further Considerations...

- Assessments
- Red Teaming



Questions



