NOT FOR FURTHER DISTRIBUTION
PRE-DECISIONAL

Costs of Cyber Incidents

Olga Livingston, NPPD Office of the Chief Economist, DHS (Olga.Livingston@hq.dhs.gov)

Matthew Shabat, NPPD Office of Cybersecurity and Communications, DHS

Tony Cheesebrough, NPPD Chief Economist, DHS

May 4, 2017

Homeland Security

Objectives

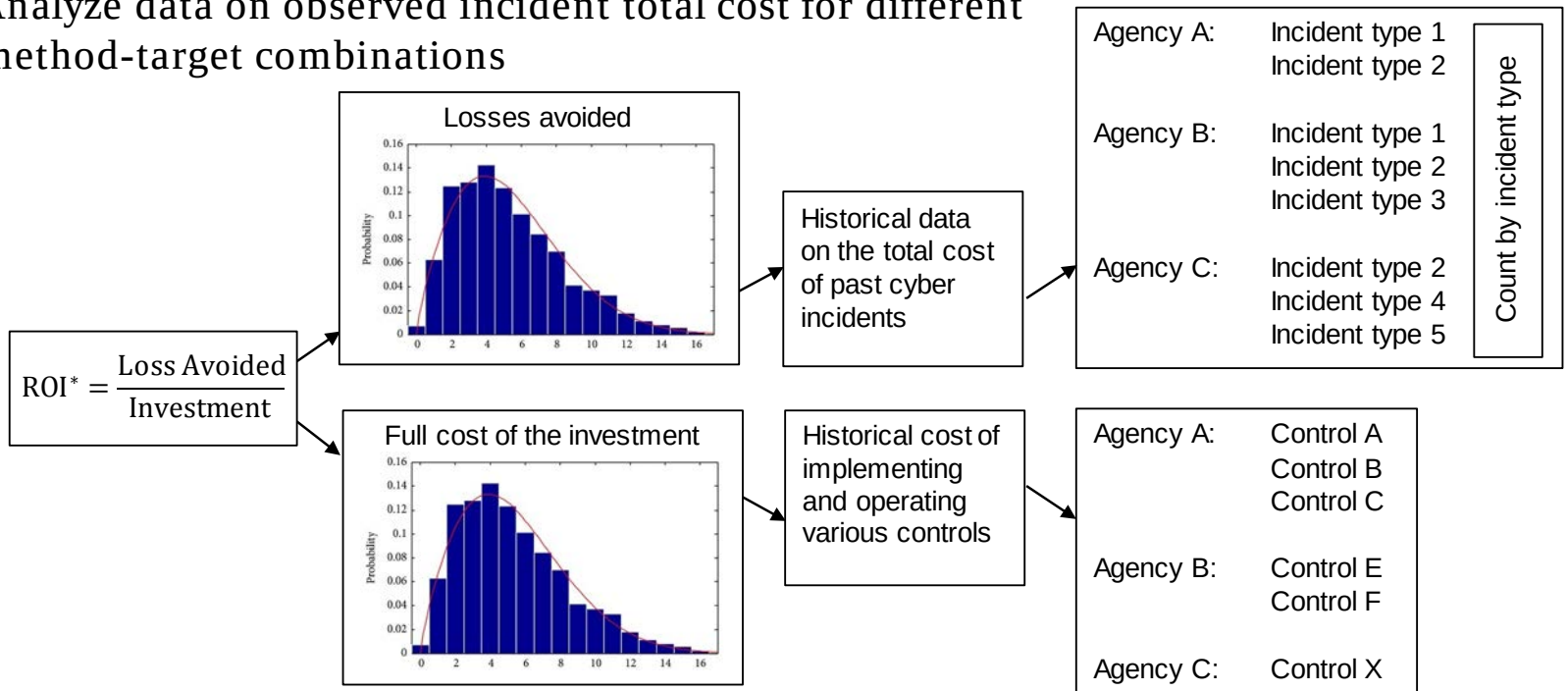
1. Estimate the benefits of cybersecurity investments as a performance metric.

2. Inform resource allocation decisions through an activity-based approach to bottom-up cost estimation.

3. Estimate the total macroeconomic impact of cyber incidents, as a function of the direct cost, to inform cyber risk management priorities.

Analysis

- Estimate savings to represent the benefits of cybersecurity investments
  - Losses prevented or reduced (costs avoided)
  - Time to detection
  - Time to containment, eradication and recovery
  - Progression down the cyber kill chain[1]
- Analyze data on observed incident total cost for different method-target combinations



1 Hutchins E.M., Clopperty M.J., Amin R.M. 2011. *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains.* Lockheed Martin Corporation.

** Slide "Limitations" contains overview of the ROI analysis issues associated with estimating the baseline level of cyber risk and the anticipated effects of proposed cyber security measures on that risk.*

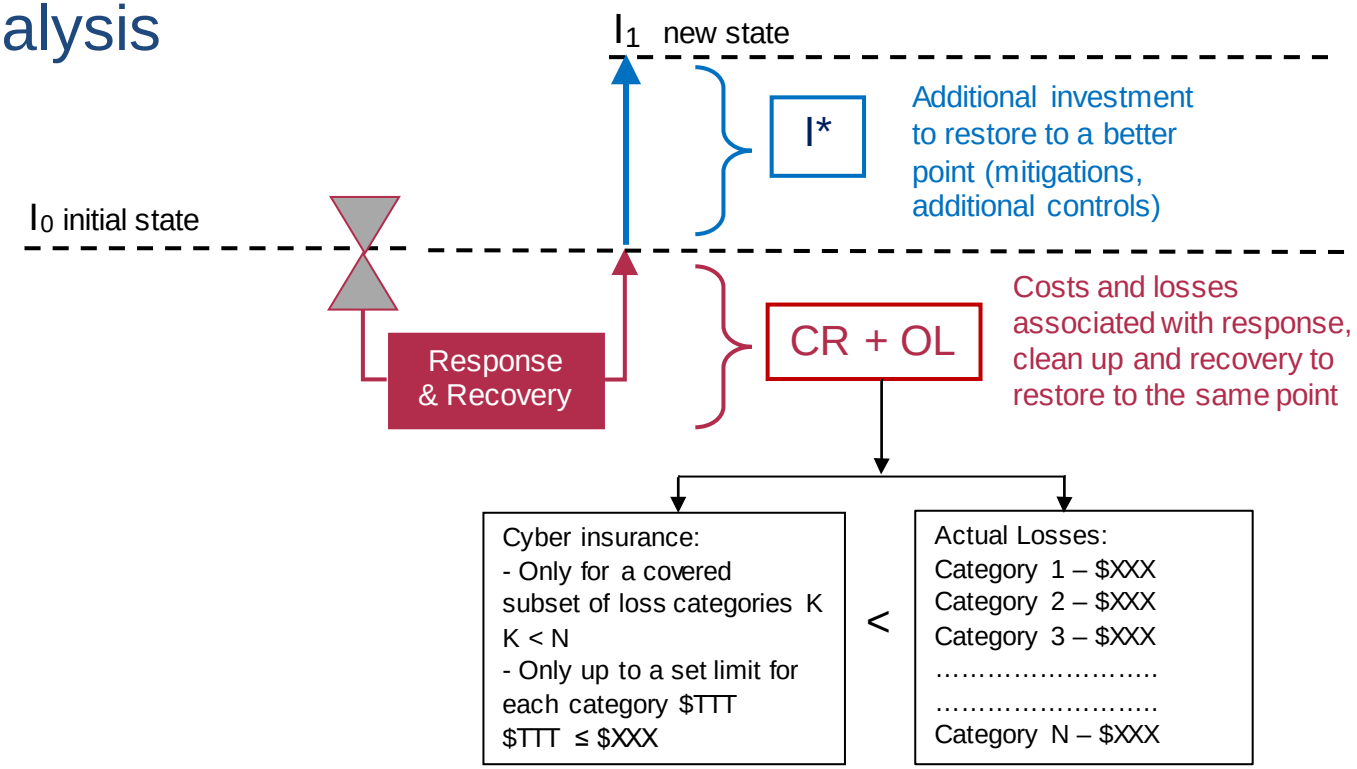
Limitations

- Benefit-cost analysis has yet to overcome two analytical challenges associated with estimating the baseline level of cyber risk and the anticipated effects of proposed cyber security measures on that risk:
  - a lack of data with which to estimate cyber risks, and
  - an inability to anticipate how adversaries will adapt to changes in the cybersecurity environment.

- Rather than attempt to estimate benefits directly, break-even analysis identifies the conditions necessary for the benefits of the investment to exceed the costs.

- Threshold or break-even analysis answers the question, “How small could the value of the non-quantified benefits be (or how large would the value of the non-quantified costs need to be) before the investment would yield zero net benefits?”

Analysis

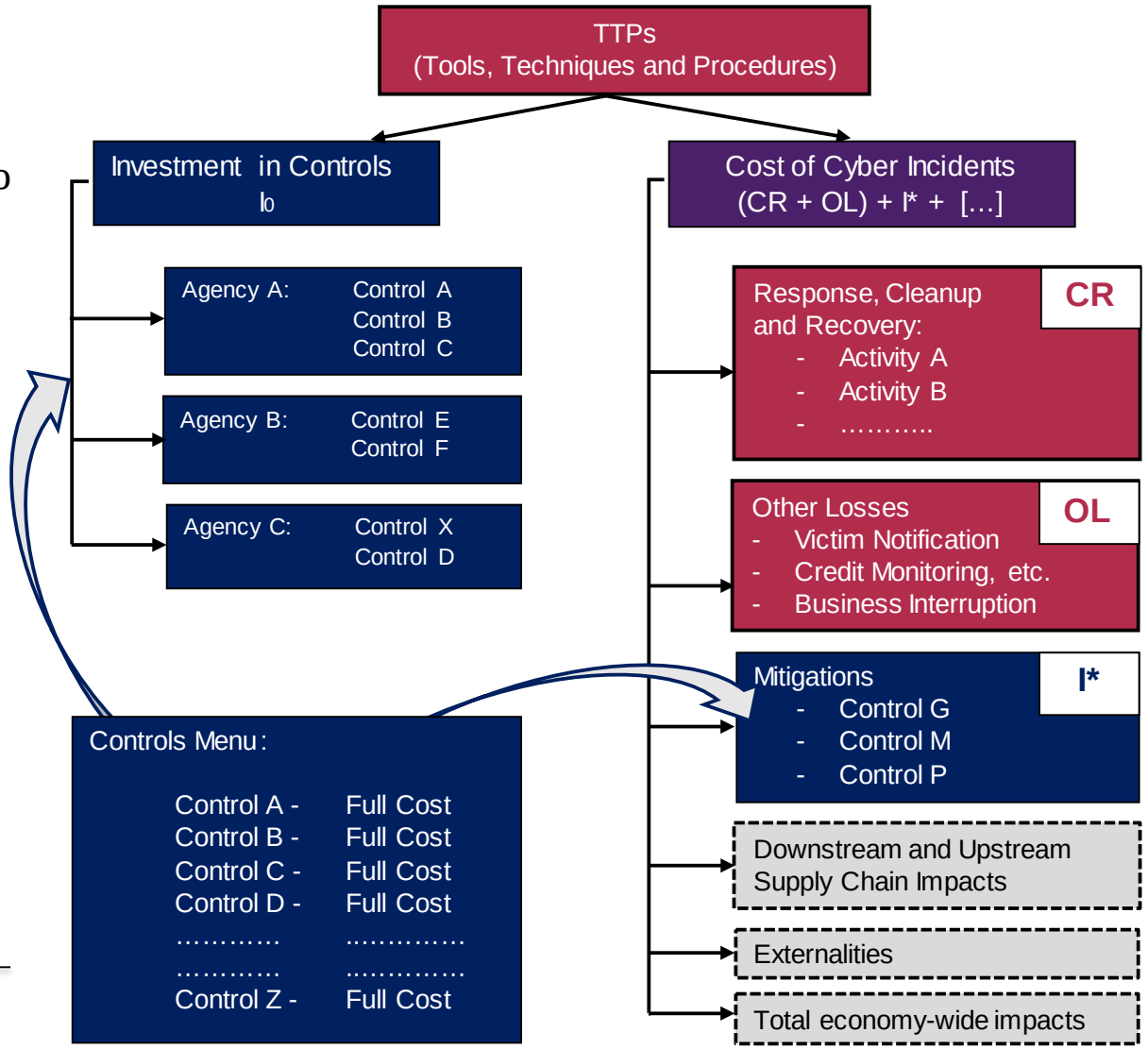


I_0	initial level of cybersecurity investment
CR + OL	cost of response and recovery, as well as other losses associated with the incident response, cleanup and recovery to the same point
I*	additional/incremental investment associated with recovering to a better point (improved security posture)
I_1	new state (recovery to a better point), $I_1 = I_0 + I^*$

Analysis

- Map specific response and recovery activities to tactics, techniques and procedures (TTPs) by kill chain phase
- Map defensive capabilities to the TTPs by kill chain phase
- Analyze ROI* by comparing investment into cybersecurity capabilities with the losses avoided:

$$\frac{\text{Potential Losses Avoided}}{\text{Cybersecurity Investment}}$$



** Slide "Limitations" contains overview of the ROI analysis issues associated with estimating the baseline level of cyber risk and the anticipated effects of proposed cyber security measures on that risk.*

Desired Input and Feedback

1. Data on observed incident-specific total cost
2. Actual estimates for the incident-specific total cost from past malicious cyber activity
3. List of relevant cost categories
4. Characterization of impacted assets
5. Review and validation of the intrusion sets
6. Methodology for quantifying the losses from the cyber incidents in the activity-based framework

Cost Categories

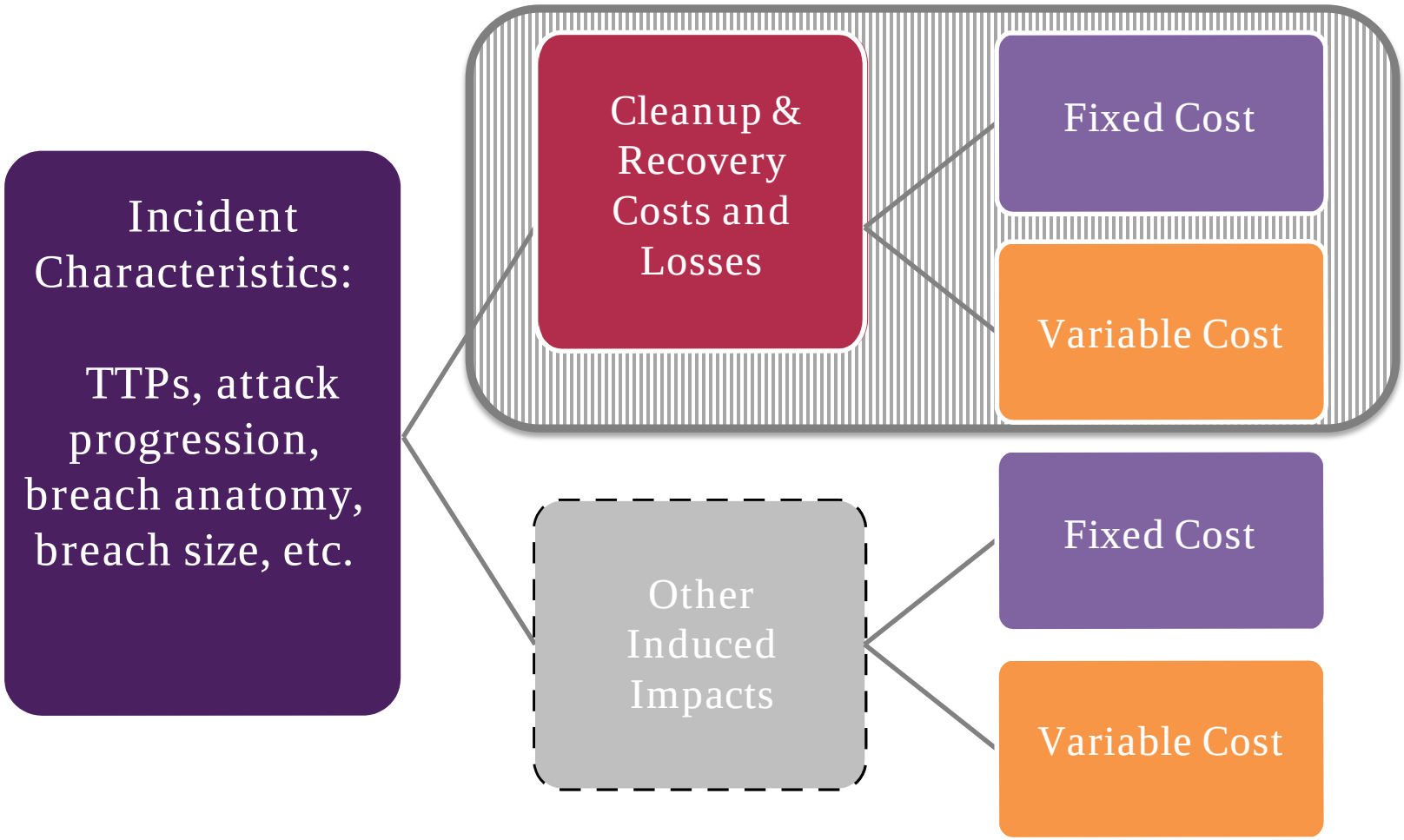
Examples of clean up and recovery costs

- Incident detection
- Investigation and analysis
- Clean up/removal
- Network countermeasures and reconfiguration
- Installation of additional authentication and security solutions
- New hardware, software/security solutions and protocols
- Data restoration from backup
- Patching and updates
- Data management to upgrade privacy policy changes

Examples of other losses and indirect impacts

- Downtime
- Loss of productivity
- Legal fees and regulatory fines
- Liability Claims/Restitution
- Denial of service from an IT provider
- Purchase of credit monitoring for customers or employees
- Loss of sales due to dissatisfied customers and negative publicity
- Relationship and reputational losses
- Decrease in market value of the company

Cost Breakdown Structure



Cleanup and Recovery Costs

- **Incident investigation and forensic analysis**

- **Incident response and containment (direct response, clean-up and recovery costs):**
  - Patching and updates
  - Clean up/removal of artifacts
  - Network countermeasures and reconfiguration
  - Network mitigation
  - Installation of additional authentication and security solutions
  - Other IT and cyber services to clean up the breach
  - Data management to upgrade privacy policy changes
  - Data restoration from backup
  - Documentation and reporting
  - Other contracted third party services for incident response and recovery including staff augmentation
  - Hardware upgrade or replacement
  - Software upgrade or replacement

- **Incident-induced additional training (staff time and acquisitions for development and implementation)**

- **Management, General Council, Public Affairs, etc.**

Other Costs and Losses

Lost Revenue or Productivity:

- Business Interruption/Downtime
- Lost Transactions/Sales/Revenue
- Cost of PR campaign
- Other Mission Disruptions _____

Theft/Fraud/Direct Financial Loss:

- Financial Theft and Fraud
- Extortion Demands and Costs
- Credit Card and Account Losses
- Other _____

Legal Fees and Regulatory Fines:

- Legal Fees/Individual Litigation/Class Action
- Liability Claims/Restitution
- Regulatory Fines, Fees and Assessments
- Additional Reserve Requirements
- Other Fees and Fines _____

Victim Notification and Protection Services:

- Victim Notification
- Credit Monitoring
- Other Third Party Services

Other Losses:

- Loss of IP
- Physical asset damage
- Bodily injury
- Loss of life
- Environmental damage
- Other _____

Additional Indirect and Induced Impacts

- Relationship and Reputational losses
- Increase in cyber insurance premium
- Decrease in market value of the company following the breach
- Damage to the perception of the product quality and reliability to result in the loss of market share to a competitor
- Overall financial performance
- Loss of IP undermining the victim's revenue and disincentive investment in research and development
- Market manipulation, subversion of sales
- Loss of competitive position/market share
- Potential for a duress liquidation sale as a result of corporate devaluation attack
- Opportunity cost
- Theft of IP to result in unnatural business growth of a competitor
- Ripple costs from the disruption of supplies and services to consumers
- Erosion of public confidence in the reliability of the networks in question, the relocation of businesses to unaffected areas
- Costs of curtailing the use of ICT in critical infrastructure management and business operations
- Global shifts in competitiveness at the industry level
- Access to control of natural resources
- Impact on national economy
- Changes in economic growth rate and patterns

Intrusion Sets – Based on ATT&CK Matrix™

Delivery	Initial Compromise	Installation	Persistence*	Privilege Escalation*	Defense Evasion*	Credential Access*	Discovery*	Lateral Movement*	Execution*	Collection*	Exfiltration*	Command and Control*
Spearphishing E-mail w/ Attachments	Application Vulnerability (Accessed Locally or Remotely)	Write to Disk	Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Automated Exfiltration	Commonly Used Port
Websites	OS Vulnerability (Accessed Locally or Remotely)	In Memory Malware	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed	Communication Through Removable Media
Removable Media	Trojan	Interprated Scripts	Basic Input/Output System	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted	Connection Proxy
	Social Engineering		Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	InstallUtil	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
			Change Default File Association	DLL Search Order Hijacking	Component Object Model Hijacking	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	PowerShell	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
			Component Firmware	Exploitation of Vulnerability	DLL Injection	Input Capture	Network Service Scanning	Remote Desktop Protocol	Process Hollowing	Data from Removable Media	Exfiltration Over Command and Control Channel	Data Obfuscation
			Component Object Model Hijacking	Legitimate Credentials	DLL Search Order Hijacking	Network Sniffing	Peripheral Device Discovery	Remote File Copy	Regsvcs/Regasm	Email Collection	Exfiltration Over Other Network Medium	Fallback Channels
			DLL Search Order Hijacking	Local Port Monitor	DLL Side-Loading	Two-Factor Authentication Interception	Permission Groups Discovery	Remote Services	Regsvr32	Input Capture	Exfiltration Over Physical Medium	Multi-Stage Channels

* Only a subset of TTPs shown on the slide.

Source: ATT&CK Matrix. The MITRE Corporation. https://attack.mitre.org/wiki/Main_Page

Intrusion Set Example

Delivery	Initial Compromise	Installation	Persistence*	Privilege Escalation*	Defense Evasion*	Credential Access*	Discovery*	Lateral Movement*	Execution*	Collection*	Exfiltration*	Command and Control*
Spearphishing E-mail w/ Attachments	Application Vulnerability (Accessed Locally or Remotely)	Write to Disk	Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Automated Exfiltration	Commonly Used Port
Websites	OS Vulnerability (Accessed Locally or Remotely)	In Memory Malware	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed	Communication Through Removable Media
Removable Media	Trojan	Interprated Scripts	Basic Input/Output System	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted	Connection Proxy
	Social Engineering		Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	InstallUtil	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
			Change Default File Association	DLL Search Order Hijacking	Component Object Model Hijacking	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	PowerShell	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
			Component Firmware	Exploitation of Vulnerability	DLL Injection	Input Capture	Network Service Scanning	Remote Desktop Protocol	Process Hollowing	Data from Removable Media	Exfiltration Over Command and Control Channel	Data Obfuscation
			Component Object Model Hijacking	Legitimate Credentials	DLL Search Order Hijacking	Network Sniffing	Peripheral Device Discovery	Remote File Copy	Regsvcs/Regasm	Email Collection	Exfiltration Over Other Network Medium	Fallback Channels
			DLL Search Order Hijacking	Local Port Monitor	DLL Side-Loading	Two-Factor Authentication Interception	Permission Groups Discovery	Remote Services	Regsvr32	Input Capture	Exfiltration Over Physical Medium	Multi-Stage Channels

Source: ATT&CK Matrix. The MITRE Corporation. https://attack.mitre.org/wiki/Main_Page
Source: FireEye, Inc. Threat Intelligence Report "APT 30 and the Mechanics of a Long-Running Cyber Espionage Operation". https://www2.fireeye.com/rs/fireye/images/rpt-apt30.pdf

Response Actions by TTP

Delivery	Initial Compromise	Installation	Persistence*	Privilege Escalation*	Defense Evasion*	Credential Access*	Discovery*	Lateral Movement*	Execution*	Collection*	Exfiltration*	Command and Control*
Spearphishing E-mail w/ Attachments	Application Vulnerability (Accessed Locally or Remotely)	Write to Disk	Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Automated Exfiltration	Commonly Used Port
Websites	OS Vulnerability (Accessed Locally or Remotely)	In Memory Malware	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed	Communication Through Removable Media
Removable Media	Trojan	Interpreted Scripts	Basic Input/Output System	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted	Connection Proxy
	Social Engineering		Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	InstallUtil	Data from Local System		and Control Protocol
			Change Default File Association	DLL Search Order Hijacking	Component Object Model Hijacking	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	PowerShell	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
			Component Firmware	Exploitation of Vulnerability	DLL Injection	Input Capture	Network Service Scanning	Remote Desktop Protocol	Process Hollowing	Data from Removable Media	Exfiltration Over Command and Control Channel	Data Obfuscation
			Component Object Model Hijacking	Legitimate Credentials	DLL Search Order Hijacking	Network Sniffing	Peripheral Device Discovery	Remote File Copy	Regsvcs/Regasm	Email Collection	Exfiltration Over Other Network Medium	Fallback Channels
			DLL Search Order Hijacking	Local Port Monitor	DLL Side-Loading	Two-Factor Authentication Interception	Permission Groups Discovery	Remote Services	Regsvr32	Input Capture	Exfiltration Over Physical Medium	Multi-Stage Channels

Delivery TTP	Response Actions
Spearphishing E-mail w/ Attachments	Reconfigure perimeter filters/sensors User training
Websites	Reconfigure perimeter filters/sensors User training
Removable Media	Reconfigure endpoint security configuration User training

Initial Compromise TTP	Response Actions
Application Vulnerability (Remotely or Locally)	Patch application
OS Vulnerability (Remotely or Locally)	Patch OS
Trojan	Disinfect Reconfigure endpoint security configuration
Social Engineering	User Training

Response Action Details

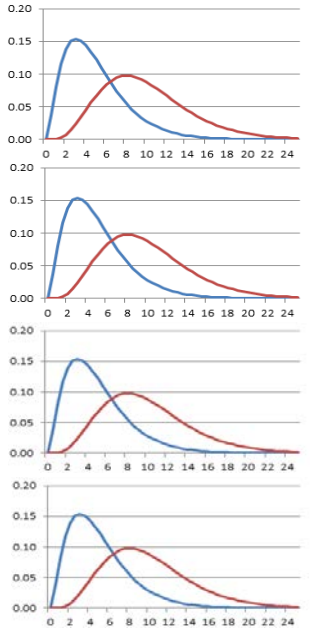
Reconfigure perimeter filters/sensors	May include	Changing the configuration of existing filters/sensors Adding a new filter/sensor capability Adding new log/data collection from filters/sensors Adding new filter/sensor log/data analytics
User Training	May include	End user training Sysadmin training
Reconfigure endpoint security configuration	May include	Changing the configuration of security settings in the operating system Changing the configuration of security settings in the applications Changing the configuration of the policy of installed security software Adding new endpoint security capabilities Adding new log/data collection from endpoint Adding new endpoint log/data analytics

Fixed Cost

Variable Cost

Fixed Cost

Variable Cost



Example

If an attack proceeded to the execution phase and the TTPs employed at this stage included Windows Remote Management, the response to that TTP could be:

1) reconfiguration of the endpoint security; and

2) reconfiguration of credential trust/privilege structure.

In turn, action (1) may include the following:

1. Reconfigure endpoint security configuration
    a. Changing the configuration of security settings in the operating system
    b. Changing the configuration of security settings in the applications
    c. Changing the configuration of the policy of installed security software
    d. Adding new endpoint security capabilities
    e. Adding new log/data collection from endpoint
    f. Adding new endpoint log/data analytics

Functionality and Capabilities by TTP

Delivery	Initial Compromise	Installation	Persistence*	Privilege Escalation*	Defense Evasion*	Credential Access*	Discovery*	Lateral Movement*	Execution*	Collection*	Exfiltration*	Command and Control*
Spearphishing E-mail w/ Attachments	Application Vulnerability (Accessed Locally or Remotely)	Write to Disk	Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Automated Exfiltration	Commonly Used Port
Websites	OS Vulnerability (Accessed Locally or Remotely)	In Memory Malware	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed	Communication Through Removable Media
Removable Media	Trojan	Interpreted Scripts	Basic Input/Output System	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted	Connection Proxy
	Social Engineering		Bootkit	DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery	Pass the Hash	InstallUtil	Data from Local System	Data Transfer Size Limits	Custom Command and Control Protocol
			Change Default File Association	DLL Search Order Hijacking	Component Object Model Hijacking	Exploitation of Vulnerability	Local Network Connections Discovery	Pass the Ticket	PowerShell	Data from Network Shared Drive	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
			Component Firmware	Exploitation of Vulnerability	DLL Injection	Input Capture	Network Service Scanning	Remote Desktop Protocol	Process Hollowing	Data from Removable Media	Exfiltration Over Command and Control Channel	Data Obfuscation
			Component Object Model Hijacking	Legitimate Credentials	DLL Search Order Hijacking	[illegible]	Peripheral Device Discovery	Remote File Copy	Regsvcs/Regasm	Email Collection	Exfiltration Over Other Network Medium	Fallback Channels
			DLL Search Order Hijacking	Local Port Monitor	DLL Side-Loading	[illegible]	Permission Groups Discovery	Remote Services	Regsvr32	Input Capture	Exfiltration Over Physical Medium	Multi-Stage Channe[illegible]

IDphase	Kill Chain Phase	IDttp	TTP	Capability/Tools/Controls
2	Recon	1	Enumeration/Identification of se[illegible] (e.g. nmap, port scans,	Inventory
2	Recon	1	Enumeration/Identification of s[illegible]e.g. nmap, port scans,	Block Unnecessary Ports and Pro[illegible]
2	Recon	1	Enumeration/Identification of serv[illegible]s (e.g. nmap, port scans,	Centralized Logging
2	Recon	1	Enumeration/Identification of services (e.g. nmap, port scans,	HIDS
2	Recon	1	Enumeration/Identification of services (e.g. nmap, port scans,	HIPS
2	Recon	1	Enumeration/Identification of services (e.g. nmap, port scans,	NIDS
2	Recon	1	Enumeration/Identification of services (e.g. nmap, port scans,	NIPS
2	Recon	1	Enumeration/Identification of services (e.g. nmap, port scans,	Penetration Testing
2	Recon	1	Enumeration/Identification of services (e.g. nmap, port scans,	Vulnerability Management
2	Recon	2	Profiling browsers/clients/end points through data collection	Proxy Server
2	Recon	2	Profiling browsers/clients/end points through data collection	Scrubbing Policy
2	Recon	3	Requests for content from known infrastructure	Access Control
2	Recon	3	Requests for content from known infrastructure	Block Unnecessary Ports and Proto[illegible]
2	Recon	3	Requests for content from known infrastructure	HIDS
2	Recon	3	Requests for content from known infrastructure	HIPS
2	Recon	3	Requests for content from known infrastructure	Infrastructure Hardening
2	Recon	3	Requests for content from known infrastructure	NIDS
2	Recon	3	Requests for content from known infrastructure	NIPS
2	Recon	3	Requests for content from known infrastructure	Penetration Testing
2	Recon	3	Requests for content from known infrastructure	Restrictive Zone Transfers
2	Recon	3	Requests for content from known infrastructure	Vulnerability Management
2	Recon	4	Scouring online content for news relating to org (e.g. Google	Aware of Internet Footprint
2	Recon	4	Scouring online content for news relating to org (e.g. Google	Security Awareness Training
2	Recon	5	Spidering of web content (e.g. proactively looking for new web	Alerting
2	Recon	5	Spidering of web content (e.g. proactively looking for new web	Centralized Logging
2	Recon	5	Spidering of web content (e.g. proactively looking for new web	Disable Robots.txt
2	Recon	5	Spidering of web content (e.g. proactively looking for new web	Secure Baseline Web Configurations

Capability/Tools/Controls
Access Control
Account Lock Out
Account Management
Account Obfuscation
Alerting
Antivirus (AV)
Application and Directory Whitelisting
Application Firewall
Application Hardening
Autorun Disable
Block Uncategorized Traffic
Block Unnecessary Ports and Protocols
Centralized Logging
Code Signing
D[illegible]oss Prevention
[illegible]able Robots.txt
[illegible]isallow Removable Media
Disaster Recovery Plan

Overall Logic

Delivery	Initial Compromise	Installation	Persistence*	Privilege Escalation*	Defense Evasion*	Credential Access*	Discovery*	Lateral Movement*	Execution*	Collection*	Exfiltration*	Command and Control*
Spearphishing E-mail w/ Attachments	Application Vulnerability (Accessed Locally or Remotely)	Write to Disk	Accessibility Features	Accessibility Features	Binary Padding	Brute Force	Account Discovery	Application Deployment Software	Command-Line Interface	Automated Collection	Automated Exfiltration	Commonly Used Port
Websites	OS Vulnerability (Accessed Locally or Remotely)	In Memory Malware	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	Application Window Discovery	Exploitation of Vulnerability	Execution through API	Clipboard Data	Data Compressed	Communication through Removable Media
Removable Media	Trojan	Interpreted Scripts	Basic Input/Output	Bypass User Account Control	Code Signing	Credential Manipulation	File and Directory Discovery	Logon Scripts	Graphical User Interface	Data Staged	Data Encrypted	Connection Proxy
	Social Engineering			DLL Injection	Component Firmware	Credentials in Files	Local Network Configuration Discovery			Data from Local System	Data Transfer Size Limits	Custom Command and Control
				DLL Search Order Hijacking	Component Object Model Hijacking	Exploitation of Vulnerability	Local Network Connections Discovery					
				Exploitation of Vulnerability	DLL Injection	Input Capture	Network Service Scanning					
				Legitimate Credentials	DLL Search Order Hijacking	Network Sniffing	Peripheral Device Discovery					
				Local Port Monitor	DLL Side-Loading	Two-Factor Authentication Interception	Permission Groups Discovery					

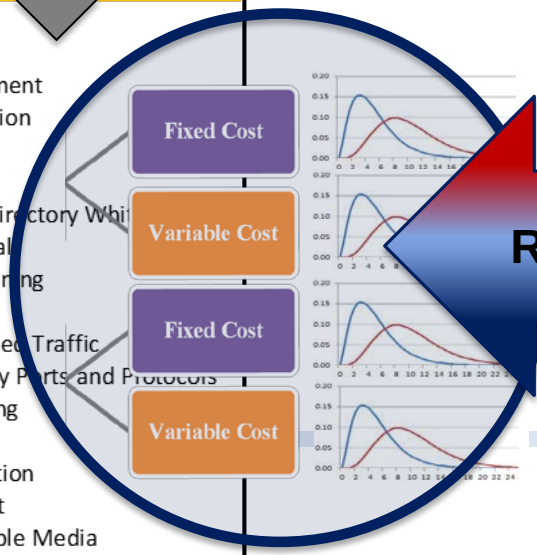
IDphase	Kill Chain Phase	IDttp	TTP	Capability/Tools/Controls
2	Recon	1	Enumeration/Identification of services (e.g. nmap, port scans,	Inventory
2	Recon	1	Enumeration/Identification of services (e.g. nmap, port scans,	Block Unnecessary Ports and Protocols
2	Recon	1	Enumeration/Identification of services (e.g. nmap, port scans,	Centralized Logging
2	Recon	1	Enumeration/Identification of services (e.g. nmap, port scans,	HIDS
2	Recon	1	Enumeration/Identification of services (e.g. nmap, port scans,	HIPS
2	Recon	1	Enumeration/Identification of services (e.g. nmap, port scans,	NIDS
2	Recon	1	Enumeration/Identification of services (e.g. nmap, port scans,	NIPS
2	Recon	1	Enumeration/Identification of services (e.g. nmap, port scans,	Penetration Testing
2	Recon	1	Enumeration/Identification of services (e.g. nmap, port scans,	Vulnerability Management
2	Recon	2	Profiling browsers/clients/end points through data collection	Proxy Server
2	Recon	2	Profiling browsers/clients/end points through data collection	Scrubbing Policy
2	Recon	3	Requests for content from known infrastructure	Access Control
2	Recon	3	Requests for content from known infrastructure	Block Unnecessary Ports and Protocols
2	Recon	3	Requests for content from known infrastructure	HIDS
2	Recon	3	Requests for content from known infrastructure	HIPS
2	Recon	3	Requests for content from known infrastructure	Infrastructure Hardening
2	Recon	3	Requests for content from known infrastructure	NIDS
2	Recon	3	Requests for content from known infrastructure	NIPS
2	Recon	3	Requests for content from known infrastructure	Penetration Testing
2	Recon	3	Requests for content from known infrastructure	Restrictive Zone Transfers
2	Recon	3	Requests for content from known infrastructure	Vulnerability Management
2	Recon	4	Scouring online content for news relating to org (e.g. Google	Aware of Internet Footprint
2	Recon	4	Scouring online content for news relating to org (e.g. Google	Security Awareness Training
2	Recon	5	Spidering of tent (e.g. proactively looking for new web	Alerting
2	Recon	5	Spidering of tent (e.g. proactively looking for new web	Centralized Logging
2	Recon	5	Spidering of tent (e.g. proactively looking for new web	Disable Robots.txt
2	Recon	5	Spidering of tent (e.g. proactively looking for new web	Secure Baseline Web Configurations

Delivery TTP	Response Actions
Spearphishing E-mail w/ Attachments	Reconfigure perimeter filters/sensors User training
Websites	Reconfigure perimeter filters/sensors User training
Removable Media	Reconfigure endpoint security configuration User training

Initial Compromise TTP	Response Actions
Application Vulnerability (Remotely or Locally)	Patch application
OS Vulnerability (Remotely or Locally)	Patch OS
Trojan	Disinfect Reconfigure endpoint security configuration
Social Engineering	User Training

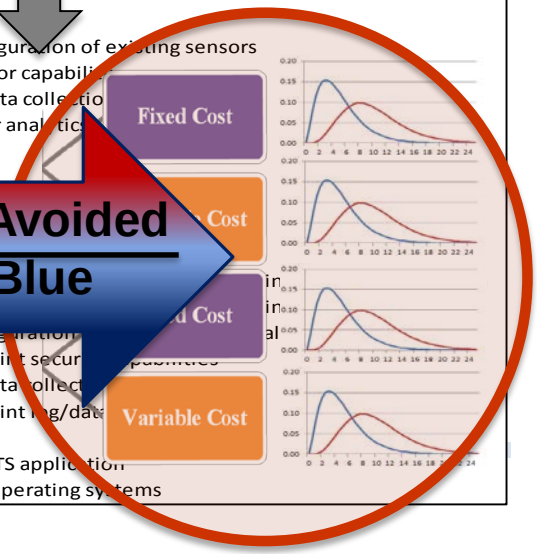
Capability/Tools/Controls

- Access Control
- Account Lock Out
- Account Management
- Account Obfuscation
- Alerting
- Antivirus (AV)
- Application and Directory Whi
- Application Firewal
- Application Harden ng
- Autorun Disable
- Block Uncategorized Traffic
- Block Unnecessary Ports and Protocols
- Centralized Logging
- Code Signing
- Data Loss Prevention
- Disable Robots.txt
- Disallow Removable Media
- Disaster Recovery Plan



Response Action Details

Reconfigure perimeter sensors	Changing the configuration of existing sensors Adding a new sensor capabili Adding new log/data collectio Adding new sensor anal tics
User Training	End user training
Patch management	Patching COTS/GOTS applic tion Pathing endpoint operating sy tems



$$ROI^* = \frac{\text{Potential Losses Avoided}}{\text{Investment in Blue}}$$

* *Slide "Limitations" contains overview of the ROI analysis issues.*

Interest in Data

To support the bottom-up cost analysis, we are continually seeking the following:

- Data or actual estimates for the incident-specific total cost from past malicious cyber activity
- Cost information (data or estimates) at that activity-specific level of granularity to capture the resources required for clean up and recovery (staff time, software and hardware acquisitions)
- Cost information (data or estimates) for mitigation activities and capability investment (staff time, software and hardware acquisitions to implement specific functionality)
- Intrusion set review and validation

Individual data will be anonymized by sanitizing and aggregating it into distributions in such a way that it will prevent identification of specific contributing parties or their security posture, agency-specific incident profiles, or individual incidents.

Status

1. Following up with individual agencies to obtain data on observed incident-specific total cost from past malicious cyber activity.
2. Extending review and discussion of the cyber cost categories with the focus on clean up and recovery costs as a lower bound.
3. Validating mitigation activities included in each response action for typical intrusion sets.
4. Validating mapping from TTPs to controls, functionality and capabilities.
5. Validating intrusion sets for various actor groups
6. Developing ICS counterpart for the bottom-up activity-based costing model.