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
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

- Analyze data on observed incident total cost for different method-target combinations

\[ \text{ROI}^* = \frac{\text{Loss Avoided}}{\text{Investment}} \]


* Slide “Limitations” contains overview of the ROI analysis issues associated with estimating the baseline level of cyber risk and the anticipated effects of proposed cybersecurity 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), $I_1 = I_0 + I^*$

Cyber insurance:
- Only for a covered subset of loss categories $K$
- $K < N$
- Only up to a set limit for each category $TTT$
  
$TTT \leq $XXX

Actual Losses:
- Category 1 – $XYZ$
- Category 2 – $XYZ$
- Category 3 – $XYZ$
- ………………………
- Category N – $XYZ$
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:
  
  \[
  \text{Potential Losses Avoided} \div \text{Cybersecurity Investment}
  \]

* 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

Incident Characteristics:
- TTPs, attack progression, breach anatomy, breach size, etc.

Cleanup & Recovery Costs and Losses
- Fixed Cost
- Variable Cost

Other Induced Impacts
- Fixed Cost
- Variable Cost
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**
---|---|---|---|---|---|---|---|---|---|---|---|---
Websites | OS Vulnerability (Accessed Locally or Remotely) | In Memory Malware | Appln DLLs | Appln 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 | Custom Cryptographic Protocol
Component Object Model Hijacking | Exploitation of Vulnerability | 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
DLL Search Order Hijacking | Legitimate Credentials | DLL Search Order Hijacking | Network Sniffing | Peripheral Device Discovery | Remote File Copy | Regsvcs/Regasm | Email Collection | Exfiltration Over Other Network Medium | Data Obfuscation | Fallback Channels
Local Port Monitor | DLL Side-Loading | Two-Factor Authentication | 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](https://attack.mitre.org/wiki/Main_Page)
Copyright © 2016, The MITRE Corporation. ATT&CK and ATT&CK Matrix are trademarks of The MITRE Corporation
# Intrusion Set Example

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

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

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

<table>
<thead>
<tr>
<th>ID</th>
<th>Phase</th>
<th>Kill Chain Phase</th>
<th>ID</th>
<th>TTP</th>
<th>Capability/Tools/Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Recon</td>
<td>1</td>
<td>Enumeration/Identification of services (e.g. nmap, port scans, inventory)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Recon</td>
<td>1</td>
<td>Enumeration/Identification of services (e.g. nmap, port scans, block unnecessary ports and protocols)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Recon</td>
<td>1</td>
<td>Enumeration/Identification of services (e.g. nmap, port scans, centralized logging)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Recon</td>
<td>1</td>
<td>Enumeration/Identification of services (e.g. nmap, port scans, block unnecessary ports and protocols)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Recon</td>
<td>1</td>
<td>Enumeration/Identification of services (e.g. nmap, port scans, penetration testing)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Recon</td>
<td>2</td>
<td>Profiling browsers/clients/end points through data collection</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Recon</td>
<td>3</td>
<td>Requests for content from known infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Recon</td>
<td>3</td>
<td>Requests for content from known infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Recon</td>
<td>3</td>
<td>Requests for content from known infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Recon</td>
<td>3</td>
<td>Requests for content from known infrastructure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Recon</td>
<td>4</td>
<td>Scouring online content for news relating to org (e.g. Google)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Recon</td>
<td>5</td>
<td>Spidering of web content (e.g. proactively looking for new web)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Recon</td>
<td>5</td>
<td>Spidering of web content (e.g. proactively looking for new web)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Recon</td>
<td>5</td>
<td>Spidering of web content (e.g. proactively looking for new web)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Recon</td>
<td>5</td>
<td>Spidering of web content (e.g. proactively looking for new web)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Recon</td>
<td>5</td>
<td>Spidering of web content (e.g. proactively looking for new web)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Recon</td>
<td>5</td>
<td>Spidering of web content (e.g. Centralized Logging)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Recon</td>
<td>5</td>
<td>Spidering of web content (e.g. security awareness training)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Recon</td>
<td>5</td>
<td>Spidering of web content (e.g. security awareness training)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Recon</td>
<td>5</td>
<td>Spidering of web content (e.g. security awareness training)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Recon</td>
<td>5</td>
<td>Spidering of web content (e.g. security awareness training)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>22</td>
<td>Recon</td>
<td>5</td>
<td>Spidering of web content (e.g. security awareness training)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>23</td>
<td>Recon</td>
<td>5</td>
<td>Spidering of web content (e.g. security awareness training)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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
- Data Loss Prevention
- Disable Robots.txt
- Disallow Removable Media
- Disaster Recovery Plan
- Secure Baseline Web Configurations
- Multi-Stage Chain
- Low Impact

---

**Fixed Cost**

- 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
- Data Loss Prevention
- Disable Robots.txt
- Disallow Removable Media
- Disaster Recovery Plan

**Variable Cost**

- Secure Baseline Web Configurations
- Multi-Stage Chain
- Low Impact

---

**Fixed Cost**

- Secure Baseline Web Configurations
- Multi-Stage Chain
- Low Impact

**Variable Cost**

- Secure Baseline Web Configurations
- Multi-Stage Chain
- Low Impact

---
ROI* = \[
\text{Potential Losses Avoided} / \text{Investment in Blue}
\]

* 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.