



# DIGITAL REAL-WORLD: WARGAMING CYBER EFFECTS ON SOLDIERS' DECISION-MAKING Surveying the Cyber Landscape

CSFI V1 Forum Final Report Summary

**3/15/2017**

Editors:

**Fenwick Gilroy, cyber analyst, lead editor**

**Robert Turner, software systems analyst and project manager**

Reviewers: **Jane Ohlmacher, Daniel Wood, Arvin Verma, James Yarnall, Chuck Williams, Christine de Souza**

**[www.csfi.us](http://www.csfi.us)**

The Cyber Security Forum Initiative (CSFI) is a non-profit organization headquartered in Omaha, NE and in Washington DC with a mission "to provide Cyber Warfare awareness, guidance, and security solutions through collaboration, education, volunteer work, and training to assist the US Government, US Military, Commercial Interests, and International Partners."

## CSFI PROJECT TEAM PARTICIPANTS

We thank all of the participants that volunteered their time, effort and expertise in contributing to this effort. Our diversified team of leaders, information security professionals, intelligence analysts, engineers, and project managers volunteered and collaborated in the CSFI portal contributing to this deliverable. We thank them for their contribution and hard work. Special thanks and credit to our CSFI volunteers:

Ohlmacher, Jane	Lead Reviewer, Director, Security Operations (RET)	USA
Carroll, Noelle	Federal Cyber Security	USA
Chesmore, Michael	State Government Cyber Security	USA
Cooper, Robert	Threat Analyst	USA
Crass, Torry	Senior Level Security Professional	USA
de Souza, Paul	CSFI Founder	USA
de Souza, Christine	CSFI Chief Information Assurance Officer	USA
Franke, Don	Security Architect	USA
Gironda, Andre	Threat Analyst	USA
Goth, William	IT Analyst	USA
Grech, Brandon	Information Security Specialist	USA
Jimenez Izquierdo, Jose Louis	Ethical Hacker, IT Cyber Security Trainer	Spain
Karedia, Rahil	SOC Analyst & Security Researcher	India
Klink, Mark	Cyber Operations Officer	USA
Lediju, Lola-Harry	Senior Security Analyst	USA
McKim, Dave	Cyber Security Engineer	USA
Mullinix, Michelle	Senior Forensic Analyst	USA
Overby, James	President/CEO	USA
Paulet, Mary	NSF Funded Analyst	USA
Richey, Hobart	Project Analyst	USA
Smith, Robert	Solutions Architect	USA
Stechyshyn, Alina	Information Security Analyst	USA
Stoneburner, Gary	Senior Cyber Security Engineer	USA
Sullivan, Lane	Director IS Security & Compliance	USA
Tarandach, Izar	Security Development	USA
Taylor, Bill	Software Developer	USA
VanKleeck, Steve	Lead Security Engineer, VAPT	USA
Verma, Arvin	Senior Cyber Security Consultant	USA
Williams, Chuck	Assistant Director of IT	USA
Wingo, Michael	Student CSIA	USA
Wisniewski, Brian	Cyber Security	USA
Witcher, Calvin William	Senior IT Manager/Cyber Security	USA
Wood, Daniel	Cyber Security	USA
Yarnall, James	Senior Information Security Analyst	USA

We also thank our sponsors at Army TRADOC Analysis center and other Defense participants; without their support this effort would not have been possible.



# Contents

- CSFI PROJECT TEAM PARTICIPANTS ..... i
- KEY FINDINGS ..... 1
- About This Report ..... 1
- ATTACK CATEGORIES..... 2
  - Nature of Cyber Attacks ..... 2
  - Insider Threat ..... 4
  - Supply Chain and Third Party Related Attacks ..... 5
  - Deny ..... 5
  - Deceive..... 6
    - Deception to Disrupt, Divert, and Delay ..... 6
    - An Example of Deception to Gain Entry ..... 7
    - Deception Vectors..... 7
  - Exploit ..... 8
  - Targeted and Random Attacks ..... 8
  - Combined Attack Categories..... 9
- DETECT ..... 10
  - Detection Approach ..... 10
  - Detecting Advanced Threats ..... 11
  - Lag Times..... 12
- DEFEND ..... 12
  - Network Monitoring ..... 12
  - Mitigation..... 12
    - Defense Approach ..... 13
    - Defense Effectiveness ..... 13
    - Best Practices ..... 14
- FORENSICS and ANALYSIS ..... 16
  - Reliability of Analysis..... 16
  - Priority for Forensics ..... 17
    - Analysis Tools and Third Party Assets ..... 17
  - Analysis of a Successful Attack..... 17
  - Post-Attack Analysis ..... 17
  - Attribution..... 17
- POST-OPERATIONS..... 17



Adapting Operations .....	18
Organizational Changes.....	18
RECOVERY .....	19
Short-Term Incident Response (IR) and Recovery.....	19
Advances in IR Technology .....	19
Importance of Incident Response .....	19
Operations Under Stress .....	20
Best Practices .....	21
Recovery Problems.....	21
Recovery Action Plans .....	22
VULNERABILITIES.....	23
Identifying Vulnerabilities .....	23
Third Parties and Acquired Organizations.....	23
Network Access Vulnerabilities.....	24
TRUST RESTORATION .....	25
Activities to Restore Trust .....	25
Priorities in Establishing Trust.....	26
Cost and Consequences of a Breach .....	27
Time to Restore Trust.....	28
ARTILLERY EXAMPLE .....	28
OTHER RELEVANT INSIGHTS.....	28
DATA GAPS .....	29
APPENDICES .....	31
A. Cyber Attack Categories Table .....	31
B. Cyber-Attack Types Table.....	32
C. Cyber Questions .....	34
DEFENSES .....	37
DETECTIONS .....	38
FORENSICS AND ANALYSIS .....	39
POST OPERATIONS .....	39
RECOVERY .....	40
TRUST RESTORTION .....	41
VULNERABILITIES.....	42
D. ACRONYMS.....	44



## KEY FINDINGS

The cyber domain is very dynamic as threats and threat actors are constantly evolving, new vulnerabilities and attack vectors are discovered, and defense technologies quickly emerge to protect networks and today's warfighter.<sup>1</sup> Cybersecurity experts are developing new ways to detect and defend against these attacks (from signature-based to heuristic). While there are thresholds to threat-actors' capabilities, there is a comparatively low barrier to entry in cyberspace to physical domains, which allows for a wider variety of actors to successfully operate.

Cybersecurity is both a technological and policy challenge. Cyberspace is fundamentally a technological domain that humans access through devices, and cyber-attacks are only instructions sent to those devices. While technology, such as anti-virus and intrusion prevention systems (IPS), can address many of the threats, there is an organizational policy dynamic that is still emerging. Organizations are beginning to adapt their operations and culture to cybersecurity and must ensure all employees have some level of cyber-awareness to protect the organization at large. In some instances, the human-made decisions may have a greater effect on cybersecurity than the technologies.

Raw quantitative data is difficult to obtain. Despite over 50 unique contributors from a variety of areas in cybersecurity (including government, private sector, and academia), most did not provide solid numbers or statistics to quantify cybersecurity challenges. Although some contributors recommended pre-compiled statistics from commercial threat reports, the research in this report is primarily based on qualitative evidence.

## About This Report

The Cyber Security Forum Initiative (CSFI)<sup>2</sup> engaged to bring to bear the full power of interested cyber security expert volunteers to provide input for a new initiative, broad based survey of the cyber landscape. This report provides the results of the project including a broad overview of cyber-attacks and how organizations view cyber threats and how they react after a network penetration. The project volunteers and management team reviewed current attack tactics and techniques; common defense and detection approaches; and how organizations remove threat actors from their network, implement improvements in security posture, and restore trust with their clients and customers. The questions posed for consideration are provided in Appendix C. The Forum collected comments from early-June 2016 through January 2017.<sup>3</sup> Verbatim Comments are documented in Volume 2.

The Forum received a total 280 comments (Posts, Table 1); with the highest number of contributions addressing attacks (101 posted comments) and defenses (37 posted comments). The heavy skew towards attack was not surprising, as most open-source literature and media reporting focus on attacks. Additionally, as cybersecurity experts, the volunteers are likely particularly interested in new threats and

---

<sup>1</sup> [https://www.defense.gov/Portals/1/features/2015/0415\\_cyber-strategy/Final\\_2015\\_DoD\\_CYBER\\_STRATEGY\\_for\\_web.pdf](https://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf).


<sup>2</sup> CSFI MISSION: "To provide Cyber Warfare awareness, guidance, and security solutions through collaboration, education, volunteer work, and training to assist the US Government, US Military, Commercial Interests, and International Partners."

<sup>3</sup> The CSFI Forum remains open for volunteers to continue to comment.



attack vectors. Additionally, the Forum’s backend design forced all topics into alphabetical order. The prominent position this algorithm gave to “Attack Categories.” Conversely, the artillery topic area received the fewest comments (6). This is likely due to a lack of military (especially artillery) expertise among many contributors. “Recovery” received the second fewest comments (7), which could be due to volunteers not having worked through a real-world recovery operation or recovery operations (and their company’s efforts) being proprietary information.

DIGITAL REAL-WORLD: WARGAMING CYBER EFFECTS ON SOLDIERS’ DECISION-MAKING PROJECT	Posts	Topics
<a href="#">Cyber Discussions Forum Intro</a>	17	2
<a href="#">Artillery Example</a>	6	3
<a href="#">Attack Categories</a>	101	5
<a href="#">Defenses</a>	37	5
<a href="#">Detections</a>	19	3
<a href="#">Forensics and Analysis</a>	7	5
<a href="#">Post Operations</a>	23	4
<a href="#">Recovery</a>	8	5
<a href="#">Trust Restoration</a>	27	4
<a href="#">Vulnerabilities</a>	35	4



The resulting posts of comments from the CSFI Forum are divided into 10 topics, each with several sub-sections and multiple questions within each sub-section, totaling 103 questions.

TABLE 1 CSFI COMMENTS BY CATEGORY

This report is part of a larger effort to map current and near-future cybersecurity trends, analyzing both threats and defenses as well as how organizations react and operate after a successful cyber-attack.

## ATTACK CATEGORIES

### Nature of Cyber Attacks

The threat landscape is dynamic and prone to significant shifts as advances in technology and human experimentation in the domain create both new threats and defense measures. Cyber actors are varied in organizational structure, capabilities, and objectives, and specific cyber-attacks as well as the attack cycle will vary based on these factors.<sup>4</sup> Also, types of cyber-attacks seem to ebb and flow in popularity<sup>5</sup> among attackers and profile. However, the proliferation of malware, ability to reverse engineer, and general interconnectivity allow different actors to access cyber capabilities that may “punch above their weight” and lowers the barrier of entry for all actors into the cyber domain. Therefore, any cyber

<sup>4</sup> A common breakdown is: 1) nation-state, which has the most capability but may be constrained by laws or geopolitical objectives; 2) criminal group, which has significant capabilities and less restrictions but are primarily motivated by profit (note: a nation-state could use these criminals as contractors for its operations); 3) hacktivists, who have fewer capabilities but have very little constraints beyond their own philosophy and operate in loose collectives, making them difficult to find; 4) terrorists, who have the least internal capabilities but may have access to funds to pay free-lance/criminal hackers.

<sup>5</sup> Ransomware was a very popular attack method in 2015 and early 2016, being used in a number of high-profile breaches. However, a combination of technical controls and employee education/awareness seem to have decreased its popularity and effectiveness for the time being.



landscape models on which this report will inform must be adaptable and allow for multiple actors, each with a variety of capabilities, in order to provide an accurate representation of cyber threats.

Additionally, classifying attacks as "targeted" and "untargeted" is not necessarily a clear indicator of risk. While organizations must be aware of threat actors who would target them, untargeted or random attacks can be just as damaging if an organization finds itself as collateral damage.

Malware can be modified based on intended target, which suggests artillery systems could be faced with a wide variety of attacks depending on how those systems connect to the broader Internet.

Attribution is a continuing challenge, especially for some of the more advanced attacks. Attackers can leverage a variety of obfuscation techniques, such as Internet Protocol (IP) address forgery, using anonymity networks (e.g. TOR), or encrypted or armored code.<sup>6</sup> Attribution is further complicated if attackers purchase malware from elsewhere, as some of the key indicators (malware writer’s language, compile date/time, known malware families, etc.) may mislead investigators. However, the shift over the past six years from blind defense against all attacks and purely perimeter defense to attribution and cyber-deterrence (leveraging new subject areas such as threat intelligence) represents a mind-shift as security professionals recognize that even generalized attribution can significantly improve cybersecurity decision-making.

Fundamental to a cyber-attack is the attacker’s objective (deny, deceive, exploit, etc.). The objective will determine what kind of attack is used, how long it will take to execute (reconnaissance, selecting/designing appropriate malware, gaining the needed access and persistence), how damaging it could be, and how difficult it can be for defenders to mitigate. However, generally speaking, the order of difficulty is as shown in Table 2 below:<sup>7</sup>

	Type	Difficulty Rating	Explanation
1	Degrade	Very simple	Requires some access to target network and coordinated effort.
2	Deny	Simple	Requires some access to target network and coordinated effort.
3	Exploit	Moderately Difficult	Requires ability to circumvent target’s security controls and persistence to exfiltrate relevant data.
4	Deceive	Difficult	Requires access to target network and information on target’s network/systems and applications to manipulate data or processes.
5	Destroy	Most Difficult	Requires significant access (possibly physical) and detailed information on target’s network/systems, as well as high, targeted malicious intent.

**TABLE 2 CYBER-ATTACK CATEGORIES COMPARATIVE DIFFICULTIES**

<sup>6</sup> The Onion Router (TOR) is a voluntary network of servers that allows users to hide their identities by obscuring the transaction between the user and destination, protecting them from traffic analysis and other forms of Internet surveillance. TOR routes the user’s Internet traffic through a random pathway of relays. No individual relay ever knows the complete path that a data packet has taken and different encryption keys are used at each relay. This approach prevents an eavesdropper to link the connection’s source and destination by monitoring traffic. TOR provides security through obscurity or obfuscation.

<sup>7</sup> Provided by CSFI Volunteer.



There are a number of attack cycles for cyber-attacks, based on the attack category a threat actor uses, each with its own timeline for the variables. Depending on the threat actor's objective (exfiltrate data, disrupt target's operations, destroy target's infrastructure, etc.), they may leverage attacks from any category. Therefore, a given attack may or may not immediately present indications or warnings before it goes into operation (stealing, corrupting, destroying data, etc.). Attack success rate depends on the threat actor's attack capabilities, what attack category they leverage in a given attack (and its aforementioned attack cycle), and whether the target's defense posture can absorb that category of attack.

Many cyber-attacks rely on stealing and leveraging legitimate system and network credentials to both persist and increase access to the target network (both laterally and vertically). This information is often stored in Active Directory (AD) or web-facing servers and can be relatively easy to access. Depending on the network design, an attacker will often target web-facing credentials first (often using an application-based attack, such as SQL injection) to dump the stored credentials (web attacks and social engineering attacks being the most prevalent)<sup>8</sup>. The attacker can then use those credentials to access the target network. They actually cannot dump the credentials directly from AD because they are hashed. Instead, they were getting credentials from memory in hashed form and just reusing them. With Windows 10, the memory that supports passing of the credentials is walled off with a feature called Credential Guard. Upgrading to Windows 10 is recommended to prevent credential stealing.<sup>9</sup>

## Insider Threat

Insider threat was discussed at length. Insider threat is a security concern for any organization. Cyber means could be used as both a direct or indirect method to conduct an insider attack, with a hostile agent installing malware on the target network or the opposing force using the Internet to contact and corrupt personnel.

Many of the Forum's insider threat comments suggest that disillusioned or otherwise compromised personnel can be a threat. An employee could become disillusioned with the overall mission, a specific incident, or act in anger over personal disputes with colleagues. Depending on motivation, this insider could release confidential information to embarrass the target, compromise operation security, or sabotage equipment to achieve their goal.<sup>10</sup>

While insider threat is commonly thought of as malicious (perpetrated by a disgruntled employee), insider threats can also come from inadvertent actions or mistakes by employees. Forum commenters

---

<sup>8</sup> Example is what happened with Ukrainian soldiers when their social app was compromised for targeting purposes – see: <http://foreignpolicy.com/2016/12/22/in-a-hacked-ukrainian-app-a-picture-of-the-future-of-war/> for Ukrainian artillery forces being targeted by Russia.

<sup>9</sup> Subverting the Credential Guard and exploiting Windows 10 has been proven to still be possible (see: <https://www.cyberark.com/blog/cyberark-labs-research-stealing-service-credentials-achieve-full-domain-compromise/>).

<sup>10</sup> Malicious insiders often steal data they have legitimate access to from their immediate area of operations before expanding into other areas. Therefore, depending on their role and access in the organization and what their objectives are, an insider may need to unwittingly use other employees (such as asking for their credentials) to access the information they want. An organization can limit potential damage by enforcing separation of duties. Additionally, behavioral changes, such as asking for information a user does not normally need, can indicate malicious activities.





had a considerable discussion over the definition of insider threat, specifically whether or not to include inadvertent activities.

In a military context, one scenario describes how an opposing force (OPFOR) could use social media or other means to subvert service members with either direct blackmail or spreading general fear (if they or a loved one is compromised by a cyber or physical attack).<sup>11</sup> After compromise, the OPFOR could coerce a service member to provide information or conduct malicious activity in the same way an intelligence service would turn and pressure a foreign asset.

A continuing challenge for the military is balancing security (via separation of duties and data or system segmentation) with current efforts to give service members a better common operating picture and increasing interoperability between systems (such as through the Command Post Computing Environment).<sup>12</sup>

Technical security controls (e.g. least privilege policies, access controls, and network segmentation) can mitigate many risks from insider threat. However, insider threat is also a personnel issue. Unit leadership needs to be cognizant of those under them in order to identify and report suspicious behavior to proper authorities.

### Supply Chain and Third Party Related Attacks

Malware can be put on hardware in advance, lying dormant until activated by a malicious actor, which makes detection more difficult. Additionally, acquisition teams purchasing this equipment may not be familiar with the variety of cyber risks from the supply chain and could inadvertently purchase malicious hardware. As computer parts are built increasingly overseas in competitor countries or countries where security is harder to enforce, the supply chain is also a potential source of risk. Comments also noted that additional risks of design flaws exist in both foreign and domestic hardware development.

Third party users, such as coalition partners and downrange contractors, are also a concern. Depending on how these users are deployed and utilized, they may have access to valuable information or the networks in an administrator or information technology (IT) support role. Like service members, they are also vulnerable to psychological manipulation and changing loyalties (due to blackmail, financial gain, or other incentive). Personnel from third parties represent a grey area between insider threat (depending on the user's access to the primary organization's network) and supply chain.

### Deny

While many organizations fear a cataclysmic cyber-attack, project commentators noted that cyber-attackers are more likely to use the least amount of force to achieve their objectives, possibly preferring

---

<sup>11</sup> While unlikely, it is conceivable that an OPFOR could leverage social media to identify and "corrupt" artillery commanders by attacking their families with cyber (e.g. identity theft) or physical (kidnapping, murder, etc.) attacks. Fear for their family might convince a Service Member to turn over classified material or sabotage artillery systems. The Islamic State Hacking Division (aka Cyber Caliphate) attempted to create this type of fear by publishing personal information for 1,400 US military and civilian government personnel in 2015, and has released a number of other "kill lists" since. Although there is no evidence any violent acts were perpetrated as a result of the lists, an OPFOR that has a sympathetic criminal element already established in the US may be more willing or effective at this kind of tactic.

<sup>12</sup> [https://www.army.mil/standto/archive\\_2016-03-30](https://www.army.mil/standto/archive_2016-03-30)



to “deny” a system with a Denial of Service (DoS) attack, rather than destroy it.<sup>13</sup> A DoS attack is relatively easy to launch and has immediate effects. DoS attacks (especially Distributed Denial of Service) will also become more viable as more devices, namely from the Internet of Things, are connected to the Internet and provide attackers with more “zombies” to add to botnets.<sup>14</sup> Additionally, criminal actors are renting their botnets out to third parties as a commercial service. In a military context, DoS would be able to disrupt fires operations in real-time and possibly delay activity/nullify the battery on the battlefield. The proliferation and availability of botnets would allow a seemingly unsophisticated OPFOR to leverage this cyber capability. A DoS attacks could disrupt networks, call for fires decision-cycles, as well as the Global Positioning System.

Commentators also focused on ransomware, which could be considered a cousin of DoS attacks. While it does not crash or flood a service directly, it encrypts data, making it inaccessible to the user without the decryption key (which often only the attacker can provide). If leveraged against artillery systems, ransomware would lock systems and prevent access or use which would greatly reduce, if not eliminate, an artillery unit’s effectiveness until the systems are restored.

Deny attacks can also serve as a diversion. Depending on objective, an OPFOR may also use a variety of attack methods, such as DoS attacks, and honeypots to study how cyber defenders mitigate cyber-attacks or misdirect resources prior to a more significant cyber (or kinetic) attack elsewhere.

## Deceive

Deceive as used in this effort includes “manipulation, distortion, corrupt, or falsification of data; altering the message content, the intended recipients, etc. to persuade the victim to react, study victim behavior, or otherwise cause detrimental effect.” Deceive can occur at various stages and for a variety of purposes. Many attackers conduct deception campaigns within the noise while defenders are focusing elsewhere. In addition, attribution is difficult and exacerbated by the consideration that the use of command and control (C2) profiles contributes to the false attribution issues.

## Deception to Disrupt, Divert, and Delay

For example, a CSFI report explored a scenario where an OPFOR deceived Air Traffic Control (ATC) with a cyber-attack; fooling ATC into thinking an OPFOR aircraft had penetrated US airspace.<sup>15</sup> This kind of deception operation would at least cause confusion and delay decision-making or, at worst, encourage unwitting attacks on friendly or neutral forces.

This type of cyber-attack could also be leveraged as a diversionary/delaying tactic in a tactical combat scenario, reducing the target’s efficiency and effectiveness, thus allowing an OPFOR additional time for their own operations.

---

<sup>13</sup> While there is a variety of methods to launch a DoS attack, Denial of Service is an umbrella term that covers a variety of specific attacks that can either crash or flood a service. These include Distributed Denial of Service (DDoS) Advanced Persistent Denial of Service (APDoS).

<sup>14</sup> Leveraging the Internet of Things for botnets is a significant concern as it allows botnets to become far larger, and thus send more malicious traffic, than in the past. The Mirai botnet attack on Dyn’s DNS service in October 2016 illustrated that IoT devices are vulnerable to malicious actors and can serve as effective botnets.

<sup>15</sup> CSFI ATC (Air Traffic Control) Cyber Security Project (<http://www.csfi.us/pubdocs/?id=47>)



## An Example of Deception to Gain Entry

One commenter identified an event where the attacker leveraged both email and telephone as attack vectors to access the target network.

This deception attack began with phishing emails being sent to the victim. Often these emails request the target to click on a link or attachment, which covertly downloads malware or performs other malicious activity, such as opening backdoors into the target system. However, another approach includes more general social engineering, such as communicating with the target directly and convincing them to provide user or network information. For example, an attacker could carry on an email correspondence with the target or call them on the phone (a form of phishing called “vishing”). Through this email or voice correspondence, the attacker can build credibility in the target’s mind and glean information about the target’s network.<sup>16</sup>

In this example of a phishing/vishing combination, the target user realized the deception when the attacker did not have information a legitimate user should have had. When the attacker was unable to further manipulate the target, he ended the direct engagement and moved to another vector.

Another variant involves using a real event in the victim’s life to add credence to the deception. In this scenario, an attacker tracks a target individual, monitoring movements, family, activities, etc. The attacker waits for a real-world event to occur (often an emergency or significant life event [marriage, buying a home, birth of a child, etc.]) and sends a spear-phishing email related to the event and encouraging (or insisting) the target to take an action (open a file, click on a link, etc.). This scenario capitalizes on a real-world event that the target can validate, thus adding more credence to the phishing scam and leading the victim leading to be more trusting. Additionally, if that event is an emergency or somehow threatening to family, loved-ones, or personal safety, then the victim’s judgement may be impaired and more willing to take what they would then consider nominal risks such as links and attachments that they may not under normal circumstances.

## Deception Vectors

As Internet devices increasingly leverage wireless signals, there is a possible confluence with traditional electronic warfare. An OPFOR could target an Army network and broadcast malware for any number of purposes. The 2007 Israeli attack on Deir ez-Zor leveraged an electronic warfare capability to deceive or take over Syria’s Integrated Air Defense System (IADS), allowing their aircraft to slip into Syrian airspace undetected.<sup>17</sup> As nations integrate cyber capabilities into lower command echelons, operational and tactical cyber-attacks could become more common on the battlefield.

Many attacks rely on deceiving humans as an initial intrusion vector, such as phishing. Phishing attacks are often emails that appear genuine and request the recipient to perform an action, such as clicking on a link or opening an attachment. As described earlier, that action often triggers malware, which infects

---

<sup>16</sup> The attacker would use this information to infiltrate the target network by using stolen legitimate credentials or learning enough about the network (e.g. server type, Operating System version, and applications) to tailor malware or other intrusion vector.

<sup>17</sup> There is some debate as to whether this incident actually leveraged a cyber weapon or not. Some experts claim Israel leveraged a “Suter” network attack system, which could have allowed Israel to change the radars’ scanning positions or hide radar contacts from operators. If Israel transmitted actual data (bits and bytes) as opposed to only electronic signals to achieve those results, it would likely be considered a cyber weapon (and a targeted deceive/deny attack).



the target system or collects information about the target system.<sup>18</sup> The attacker can use that information to tailor other malware, gain direct access to the target network, or otherwise impersonate the target user.

An OPFOR could inject a message into the fire control decision cycle and pass up false orders that target friendly/allied units or civilians, miss targeted OPFOR units, or otherwise reduce artillery effectiveness. Relatedly, an OPFOR could just monitor these networks to gain early alert (and possibly move their ground forces) when a bombardment is incoming.<sup>19</sup>

Conversely, effects on Army artillery units could be a secondary or tertiary effect from an attack on a different part of the Army's network.

## Exploit

Exploit attacks (commonly as a result of exfiltrating data from the target) can be used for operational and tactical intelligence collection. An OPFOR could exploit exfiltrated data to determine an order of battle and capabilities in-theater, determine supply schedules and routes to inform their own attack planning, or otherwise discern the target's intentions.

For example, in December 2014, security experts observed a malicious variant of a Ukrainian military Android application (app). The app supports Ukrainian artillery units by conducting targeting calculations to reduce firing time. The malicious version of the app sends the Android device's approximate location (via cellular towers), device contacts, Short Message Service (SMS) data, and call logs. This data allowed the attacker to determine the Order of Battle, intentions, and approximate location of Ukrainian artillery units. Possibly using the location data, Russian forces dispatched unmanned aerial vehicles (UAVs) to identify precise targets and destroy Ukrainian artillery with counterbattery fires.<sup>20</sup>

Exploit attacks may place a heavier emphasis on persistence than other attack categories (deny or destroy attack, for example), as attackers will need time to move throughout the network to find the data they seek. As a result, an attacker may attempt to find multiple back doors into a system to maintain their persistence.

## Targeted and Random Attacks

None of the volunteers commented directly on targeted attacks. However, based on comments in other sections and conversations with other sources, targeted attacks are more prevalent than random attacks and are often more high-profile in the media.<sup>21</sup> These targeted attacks often begin with

---

<sup>18</sup> This could include personal information about the target (such as username and password) or information about the architecture or applications on the network.

<sup>19</sup> Moving an OPFOR unit in the time it takes for soldiers to call back for artillery and fire rounds maybe difficult depending on the size of OPFOR unit. However, a small OPFOR unit could scatter in a reasonable amount of time. Other alternatives for the OPFOR could be to "hunker down" or "grab the enemy by the belt" to reduce artillery fire effectiveness (both tactics used against US forces in Vietnam). Gaining extra time (whether minutes or seconds) could allow OPFOR to survive.

<sup>20</sup> <https://www.crowdstrike.com/wp-content/brochures/FancyBearTracksUkrainianArtillery.pdf>

<sup>21</sup> This could be due to malicious actors developing more specific objectives in cyberspace and wider adoption of basic cyber defenses over time. A notable exception is likely creating botnets, where the goal is to capture as many different devices as possible.



extensive reconnaissance on the target using social media or other open-source information and launching small-scale probes (such as port scans) to determine possible means of entry. Examples of targeted attacks include Lockheed Martin (2011), Target (2013), Sony (2014), Anthem Insurance (2015), United States Office of Personnel Management (2015), United States Democratic National Committee (2016), and DynCorp (2016).

While random attacks, especially against military assets, are becoming less likely, there is a chance of malware unintentionally infecting Army systems either because Army runs similar platforms to the hackers' target or the target itself is otherwise related to Army products (i.e. Defense Industrial Base).<sup>22</sup> Additionally, if Army chooses to use a public data storage (such as cloud) provider, an attacker may gain access to Army data while targeting a different user.<sup>23</sup> Reported random attacks include SQL injection, HTTP/HTML tag injection, and Cross-Site Request Forgery.

Drive-by or watering hole attacks are traps laid on the open Internet and often require the user to click an infected link on a website. Sometimes these attacks are targeted or semi-targeted (as attackers may target users in a specific field or industry, selecting websites that those users are known to frequent to lay their traps). However, drive-by tactics and techniques are generally more aligned with random attacks.

### Combined Attack Categories

Advanced cyber actors often use multiple vectors and combine categories to achieve their objectives. Contributors focused on attackers' leveraging social media to either inform or complement their attacks.<sup>24</sup> Social media can support an OPFOR's operations by providing Intelligence, Surveillance, and Reconnaissance (ISR)-like information about targets (e.g. a target's pattern of life or the network stack). As stated by Forum contributors, this 'open-source intelligence' (OSINT) collection (especially leveraging social media sites) has a very low barrier of entry and is a common vector for both state and non-state cyber actors.<sup>25</sup> OSINT can provide an adversary the ability to mine information on their target to better understand their technology stack while preparing weaponized payloads during the exploitation phase of the killchain.

Social media platforms can also transmit malicious code or instructions through links and attachments directly, such as the Hammertoss malware.<sup>26</sup> Social Media Intelligence (SOCINT) provides an adversary

---

<sup>22</sup> Stuxnet was initially discovered by Kaspersky after a number of civilian Siemens systems were compromised. Although Stuxnet did not create any adverse effects for those systems, it still spread far beyond the Natanz reactors. A less carefully-designed code could bring malicious effect to unintended targets.

<sup>23</sup> The Department of Defense is unlikely to use a public cloud provider; storing any data on public clouds presents a significant risk. If they were to do so, they might follow other agencies' approaches such as using Amazon Web Services (AWS) or other FedRAMP certified cloud service provider (CSP).

<sup>24</sup> Although social media can help attackers tailor and otherwise improve their attacks, and in some cases may be considered a "combined attack," this is not the only form of combined attack.

<sup>25</sup> Although Service Members' online presence can be an attack vector, social media is also an important lifeline to family and loved ones. Cutting Service Members' access to social media is not feasible or likely worth the cost. Therefore, Service Members must manage this risk by understanding how malicious actors could use their information and limiting what they display on social media platforms.

<sup>26</sup> <https://www2.fireeye.com/rs/848-DID-242/images/rpt-apt29-hammertoss.pdf>



the ability to research their target(s) at will and paint the attack surface at their leisure based on the people instead of the technology.

Ransomware could be used as part of a combined attack, such as with a DoS attack, by blocking access to necessary data or workstations as a diversion while a more advanced cyber-weapon works within the target's systems.

These attack vectors are most often used in either deceive or exploit attacks to develop more convincing spear-phishing emails, refine a search for viable targets within Department of Defense (DoD) networks, or discern login credentials (i.e. passwords) to gain initial access into a target system. Other possible ways to combine attack vectors include the following:

- 1) A DDoS attack on a specific network egress point to distract security personnel coupled with a breach-style attack in another part of the network (e.g. for data exfiltration or corruption).
- 2) A simple attack intended to spam logs so they overwrite logs and other actual breach style attacks where tracks are covered on log overwrites.
- 3) A disable or destroy attack against infrastructure (e.g. electrical grid) and a DDoS against telephone systems to slow reaction time and increase infrastructure attack's effectiveness.<sup>27</sup>

## DETECT

### Detection Approach

Based on the received comments, cybersecurity teams utilize continuous monitoring to detect threats. Vulnerability scanners and signature analyses using Common Vulnerabilities and Exposures (CVE) lists are common methods of detecting network infiltrations. Packet analyzers (that break down individual packets) and traffic analyzers (that look at traffic trends) can detect malicious activity and actors.

As malware evolves, anomaly detection (which alerts to unusual activity after establishing a baseline of normal operations) is superseding signature analysis. The change in security tools has been dynamic and impressive over the past several years as more organization are moving their reliance away from rule-based or signature-based tools and utilizing newer methodologies. The fact that legacy signature-based tools are becoming obsolete is a major shift in cybersecurity. Newer methods of malware, virus, and threat detection leverage un-supervised machine learning, heuristics, and predictive forms of mathematics to find these threats and alert on them appropriately. The likelihood of catching an Advanced Persistent Threat (APT) or Nation-State actor using signature-based tools is, and has in many cases, already diminished beyond an acceptable level of confidence. This is not to say signature-based tools do not still have their place in cybersecurity, as they can still prove useful when deploying a defense-in-depth strategy; however, they should not be the primary tool used to safeguard an organization.

As well as the new aforementioned security tools, cybersecurity firms are beginning to focus on cyber threat intelligence (CTI), blending endpoint data with broader trends and non-cyber information to help

---

<sup>27</sup> Ukraine power grid, December 2015



them identify attacks and attackers.<sup>28</sup> The concept of cyber threat intelligence is taking a proactive approach to cybersecurity, rather than the normal reactive approach that has been taken traditionally. Detecting and acting on indicators of compromise (IOC) or indicators of attack (IOA) is the basis of threat intelligence with the goal being able to prevent or significantly reduce the impact an attacker will have on the organization. Threat intelligence is complementary to Security Information and Event Management (SIEM), giving organizations the ability to correlate known threats to real-time activity in their network. Integrating other tools like intrusion prevention systems along with CTI data in an organization's SIEM can really boost the ability to be proactive and reduce the impact of a cyber-attack.

Along with CTI, the idea of threat hunting has been gaining traction amongst cybersecurity minded organizations and is proving to be a valuable effort in safeguarding data and assets. Threat hunting is going a step further than CTI and actively searching, or "hunting" for indicators of compromise or indicators of attack. Sifting through the organization's data and logs, in this case the more data the better, can be easily achieved with a SIEM that is configured to receive endpoint logs, network device logs, and any/all other critical logs from the organization. Utilizing a Cyber Kill Chain framework for threat hunting can aide the hunter in identifying events in the different phases of an attack and proactively look for them or similar events in the future.

Both cyber threat intelligence and threat hunting rely heavily on data/log collection, as well as the newer methods of threat detection as mentioned earlier. Newer detection technologies, called behavior-based detections look for evidence of possible compromise rather than the malware itself. Several key indicators of compromise are increased network traffic; slow response time; specific IP addresses associated with a known malicious actor; and unusual files, hashes, or web addresses on the network. Currently, these technologies are useful for large Security Operations Centers, which can process the volume of false-positives that result from this approach. Importantly the more eyes, whether machine or human, looking through the network, the better the chance of stopping an attack before it starts.

## Detecting Advanced Threats

Advanced persistent threats (APT) are often considered to be the most capable cyber actors and are difficult to detect. These APT groups are often comprised of highly-skilled hackers and are very well-resourced (many APTs have some connection to a nation-state). While individual APTs and single APT groups each utilize a specific technique or narrow skillset, APTs are collectively thought of as often having access to both the highest quality and largest inventories of malware. These capabilities allow them to move more carefully in cyberspace, infiltrating and persisting on a target network until they complete their mission.

In general, APT malware is difficult to detect and mitigate. Depending on the malware, basic system users may not detect a compromise for some time. Conversely, basic users, who are most familiar with how their own systems operate, may realize there is a problem before cyber experts, who may have a

---

<sup>28</sup> Cyber intelligence combines endpoint data and indicators on a specific attack, broader trends within cyberspace, general attacker profiles, and non-cyber information on potential adversaries (objectives, support structure, and known member profiles).



very large area of responsibility on a variety of networks. While traditional detection methods can identify known malware through signatures or obviously anomalous behavior, those methods may not work against an APT using more advanced techniques.<sup>29</sup>

## Lag Times

Lag times between penetration and detection can vary widely depending on the OPFOR's attack vector and skill and the network defenders' attentiveness. In training exercises, when defenders are actively monitoring the network, detection time is small (minutes or hours, according to one contributor). However, other organizations, as well as media releases of publicized attacks, often report an attacker persisted for months or even years on a compromised system prior to detection.<sup>30</sup> Additionally, technical fixes may take time, especially if the fix requires developing and implementing patches. Thus even if a vulnerability or penetration is discovered, end users may have to operate in the degraded environment for some time before it is mitigated.

## DEFEND

Coupled with detection, organizations have a host of defense measures they can utilize to reduce the risk or consequences of a cyber-attack. The most common defense technologies include anti-virus software, intrusion prevention systems, firewalls, and access controls. Additionally, policies of network monitoring, defense-in-depth, and other protections are needed. Additionally, all of these defensive measures need constant updates to keep up with new attack vectors and tactics. One commenter noted: "the [security] staff at a firm [or] organization must be vigilant regarding possible threats and be proactive about possible weakness reports on web application infrastructure."

## Network Monitoring

Many organizations set up a Security Operations Center (SOC) and leverage multiple tools to monitor networks. Some are commercially-available and off-the-shelf. However, larger organizations also develop proprietary tools to tailor defense to their specific needs.

## Mitigation

Backups are helpful (especially when air-gapped or sub-netted, being connected only to the main network when data is backed-up) to mitigate short-term deception attacks as well as ransomware. Leveraging backups, security personnel can mitigate security breaches more aggressively (e.g. reimaging an operating system) without fear of losing data. However, long-term attacks could mean the backups are compromised, thereby rendering them useless in mitigating a DoS-style attack.<sup>31</sup>

Basic encryption may be a viable option for tactical communications. Some of the data (such as specific fire orders) may be short-lived (aside from archiving/record-keeping) and thus does not need heavy security (just enough to confound the OPFOR until the mission is complete). If possible, modifying

---

<sup>29</sup> For example, zero-day vulnerabilities.

<sup>30</sup> If ARCYBER continues with plans to integrate cyber elements within operational units, this on-site support could reduce lag time for lower-level cyber-attacks, especially if the attack effects are readily apparent.

<sup>31</sup> In case of a DoS attack, load-balancing and traffic-blocking practices are more effective.





security procedures, such as encryption keys, on a regular basis will also help by forcing hackers to devote more time to reconnaissance to find viable attack vectors rather than tailoring attacks to increase effectiveness.

One commenter developed a virtual local area network (VLAN) on a separate, dedicated switch for senior leadership to access sensitive data. Access control is based on hard-coded media access control (MAC) address, only allowing those devices to connect to the switch. Additionally, the switch only allows one device to access a port on the switch at a time and leverages Dynamic Address Resolution Protocol (ARP) Inspection (DAI) to reduce the probability of spoofing or man-in-the-middle attacks.<sup>32</sup>

## Defense Approach

An organization must ensure both cyber- and physical security to adequately protect its data and systems. Many organizations focus on monitoring, segmenting networks (with VLANs, network architecture of switches and routers, access control list, separation of duties, etc.), and controlling remote access (often with virtual private networks [VPNs]) to minimize lateral movement or privilege escalation on the network. Some commentators isolate their sensitive data on internal local area networks (LANs), thereby not connecting to the Internet at all. This significantly reduces the attack surface and entry points that security personnel need to monitor. Additionally, system administrators set up group-based access controls, which only allow users in a specific group to access particular data. Organizations also leverage encryption, especially for data at rest. Organizations also maintain physical security measures (such as locks on gates and doors) at office sites and data centers to prevent unauthorized access.

For some types of real-time high sensitivity data, the directive is to leave no electronic footprint: no discussions over email/text and no general electronic documentation. If and when electronic artifacts are necessary, such as for project tracking and mitigation of high Risk Priority Number (RPN) vulnerabilities, strict access control is enforced, files are encrypted and stored on encrypted servers, topics are not discussed on speakers, and artifacts are kept on file using dedicated, non-general purpose storage areas and servers so that deny by default is more easily enforced.<sup>33</sup>

Consideration now needs to be given to authenticating computer programs that ask for services. Typically, a service will be called by computer programs instead of by a browser, which can ask a human for credentials. The gap lies in the need for an effective way for a service program to authenticate a calling program.

## Defense Effectiveness

Although any defense is generally better than no defense, defense effectiveness can vary widely. Defense software (anti-virus, firewalls, IDS/IPS) effectiveness depends on how the software is developed and vetted, leveraging System Development Life Cycle (SDLC) principles. The cybersecurity community is

---

<sup>32</sup> Dynamic ARP Inspection (DAI) inspects incoming packets and compares the sender's MAC and IP addresses, dropping the packets if the addresses do not align in a database of trusted sources.

<sup>33</sup> Risk Priority Number is determined by the following: (Effect Severity)\*(Probability of Occurrence)\*(Probability of Detection) Failure Modes and Effects Analysis (FMEA) Standard ISO 27001 Security.



also acknowledging that defending networks requires a combination of technology and policy.<sup>34</sup> However, sometimes organizational leadership does not provide sufficient guidance or appropriate funding to support the policy. Leaving policies open to interpretation runs the risk of the policy not being implemented properly or effectively.

There is no single technology or policy to ensure an organization's cybersecurity. Therefore, security personnel apply the "defense-in-depth" principle, utilizing multiple policies and technologies to reduce attack surface, block malicious traffic, and defend against (or at least detect) intrusions. Disabling unused ports, using firewalls, anti-virus programs, and User Account Control (UAC) (used to prevent automatic changes to user accounts) all contribute to network defense and, in combination, block a wide variety of cyber-attacks.

IP filtering/blocking can help against random attacks, as it prevents IP addresses from specific countries from connecting to a network. While this will not dissuade highly-skilled attackers who would utilize The Onion Router (TOR) and other obfuscation techniques, it can block script-kiddies and botnets, which might be randomly attacking networks.

When possible, application whitelisting should be used to help eliminate the need for specific IP or IP range blocking, which could be an ongoing effort. IPs are easy to spoof that simply "blocking an IP" is not an ideal mitigation tactic. Furthermore, having a long, running Access Control List (ACL) can eventually do more harm than good, where the list contains names and privileges that are no longer correct.

Hackers take the path of least resistance and often use the most basic attack they can to achieve their objective. Therefore, security personnel can block a significant number of cyber-attacks by following basic cybersecurity best practices (known as the "Golden Oldies"), such as multi-factor authentication, patching systems, and closing unnecessary ports. These fairly rudimentary security measures can assure older techniques are not able to breach systems security.

One commenter discussed homomorphic encryption to both segment files from and enhance security within a network. Homomorphic encryption is a form of encryption that allows computations to be carried out on cipher text, thus generating an encrypted result which, when decrypted, matches the result of operations performed on the plain text. Traditional encryption schemes do not allow for data computations without first decrypting data, exposing the plaintext to potential attackers. Homomorphic encryption, by contrast, allows computations to be performed without decrypting the data. The results of the computations remain encrypted, and can only be read and interpreted by someone with access to the decryption key.

## Best Practices

The following is a current (February 2017) list of common best practices for familiar vulnerabilities:

---

<sup>34</sup> Technology is insufficient to ensure security. Many penetrations (especially spear phishing and brute force attacks) are due to human mistakes. Therefore, an organization must develop policies and procedures to ensure personnel adhere to good cyber hygiene practices and reduce the probability/effectiveness of these types of attacks.



1. Develop and maintain a list of business and control systems. Ensure that control systems are separated from business systems and are not communicating through your network. This includes military, industrial control systems, and Internet of Things (IoT) devices. When risk assessments are conducted, include analysis and checks for these items to ensure that separation continues. Eliminate extra pathways for vulnerabilities.
2. Analyze all systems functions, and segment the network in logical use units. Keep firewalls between these segments. Do not rely on perimeter security or a single set of firewalls at Internet gateways. If the network is segmented, and one segment is compromised, the attack will not be able to progress to other parts of your internal network.
3. Maintain current patch levels on all externally developed software, including and especially the operating systems of each box. Test the updated patches in a test environment before implementing them on production assets. Where possible, include automation the update process to ensure you are at the most current level. Many systems are compromised by old versions of software and long existing vulnerabilities. Highly skilled and motivated hackers are quick to use newly discovered vulnerabilities, so speed of updates is a priority. Likewise, if software is developed in your organization, use good security practices in software development and maintain change control systems. Do not run compilers, interpreters nor any unused software on your web servers. Software development networks should be segmented from production systems.
4. Practice role based access control. Ensure that as much as possible, employees access only what they need to perform their duties. When duties change or there is a termination, remove access as soon as possible. For very sensitive applications, require separation of duties and dual access so that an important change may require two employees. Limit the number of employees who have administrative access. Implement logging systems with individual accountability so an employee's actions can be traced if need be. Access to sensitive systems should require multi-factor authentication. These may include something you know (password or phrase), something you have (CAC, PIV, or other smart card), or something you are (biometric). Using Global Positioning System (GPS) technology, some systems only allow access from certain secure locations. If passwords are used, have enforced password policies that promote the longest, strongest passwords that are practical for the organization, and limit the number of failed tries. Encourage employees to use different passwords for each application and for their personal use.
5. If remote access is required into the network, make sure this is done securely through the use of Virtual Private Networks (VPNs) or other secured communications networks. Make sure VPNs use encryption algorithms that are approved for your sensitivity level and also have good authentication methods. Ensure the remote device is not connected to the Internet through a second channel that can also provide a pathway into the network and that the remote device is not running malware. If possible, maintain the remote devices within your organization so that all software packages, updates, and control remain in your domain. Do not use remote control software, file transfer protocol, telnet, or simple network monitoring protocol (versions 1 and 2). Make sure the standard ports for these functions are closed, and monitor the use of other protocols that are essential to operations.



6. Develop and maintain policies and procedures for cyber security. There should be policies for all topics pertinent to your operations. Implement these policies, including consequences for non-compliance. Some pertinent topics include email usage, social media, personal mobile devices, removable media, choosing passwords, and the use of organizational network resources for personal objectives. If possible, mobile devices should be owned and controlled by your organization. They should be password, token, or biometrically protected, and there should be a policy for reporting lost devices with immediate disablement remotely of any lost or stolen devices.
7. Develop and implement an end-user cyber-security employee training and awareness program. This training program should focus on cyber hygiene best practices, your organization's specific policies and procedures, and other pertinent topics such as not clicking on links received through email, observing your fellow employee (see something, say something), employee counseling for financial or emotional problems that might lead to insider threat for internal compromise of networks. Have new employee orientation classes and periodic recurring classes to renew cyber security awareness.
8. Monitor online services for new vulnerabilities. Many free and low cost services will provide the latest known vulnerabilities to systems, some of which may require network configuration changes rather than relying on vendor patches. One free service is Cyber Daily by Recorded Future. Furthermore, US-CERT keeps a current list of the top 30 high risk vulnerabilities: <https://www.us-cert.gov/ncas/alerts/TA15-119A>.
9. Protect your system by using intrusion detection devices and/or intrusion prevention devices, antivirus software, and log monitoring systems. If possible, deploy a security information and event management (SIEM) system for continuous monitoring and evaluation. As with other vendor products, keep all updates and versions current.
10. Develop an incident response plan according to scenarios that may cause loss of availability of your systems, loss of integrity of your data, or exposure of confidential information. Assign employees roles to implement the plan, and perform a tabletop walkthrough of the completed plan with proposed scenarios and players. Update your plan with findings from this walkthrough. Review your plan regularly and keep it up to date. Be sure to store the plan in a safe place externally so that the same compromise that may cause the problem does not block access to the plan.
11. Include upper command in major security decisions and get buy-in for expenditure of resources.

## FORENSICS and ANALYSIS

### Reliability of Analysis

Despite regular alerts from both government and private security experts, some firms have not yet taken cybersecurity seriously, while others have difficulty evaluating the variety of both threats and security tools currently available in the market. Additionally, contributors noted that security report templates are sometimes too rigid in either formatting or what data should be included, which suggests reporting could be incomplete and decision-makers may miss key details that could help inform their decisions.



Even if the analysis is accurate, another concern is how (or whether) it is acted upon. While Defense Department leadership considers cyber-attacks a priority threat, mid/low-grade commanders may not be aware of their role in cybersecurity and require extra training or awareness to carry out tactical incident response, such as acting on security reports and new threats.

## Priority for Forensics

### Analysis Tools and Third Party Assets

Organizations often use a variety of third-party or commercial tools to protect their networks. Larger firms with the resources to develop their own proprietary network-tailored tools will often use those as well. The DoD at large uses a number of commercial products and contracts with private cybersecurity firms to complement in-house capabilities. It is likely that some of these third-party tools will be used to help defend tactical networks during military operations. If the Army continues with its efforts to embed cyber experts with non-cyber units, those experts will likely use these commercial products.

### Analysis of a Successful Attack

A cyber-attack's severity depends on the effects (disrupt, destroy, etc.), the target (a DoD public-facing website, a single military unit, the Joint Chiefs of Staff, a COCOM [Combatant Command], etc.), and the degree to which the attack affected military operations. Assessing all three factors holistically gives the best analysis on how severe and significant a cyber-attack is.

Similarly, a cyber-attack's effectiveness depends on the target's direct defense (e.g. intrusion prevention systems, firewalls, antivirus, etc.), system maintenance (e.g. patching, continuous monitoring), system architecture (e.g. access control lists, separation of duties, subnets), and employee awareness (e.g. training, general cyber hygiene, etc.).

### Post-Attack Analysis

See the [Recovery Action Plans](#) section, which covers post attack analysis.

### Attribution

As one contributor describes it, the most important aspect is to resist the urge to turn it into a blame game. Do not target employees unnecessarily while still accurately assessing the factors (both human and machine) that contributed to the attack...

## POST-OPERATIONS

Aside from the immediate consequences of a cyber-attack (such as data loss, exposure, and loss of services or capability), organizations often go through a variety of changes after suffering a cyber-attack.

Gain insights into attacker's tactics, techniques, and procedures (TTPs), the vulnerabilities they used to gain access, and potentially their identity. The organization tends to become more sensitive to security issues (from employees to the Boardroom), especially if the breach is made public. However, this



sensitivity can reduce productivity and degrade efficiency if an organization invests in too much security.<sup>35</sup>

## Adapting Operations

An organization can adapt both policies and technologies based on the OPFOR's observed TTPs, reducing the OPFOR's ability to infiltrate again. The best security controls (both technical and procedural) are developed using in-depth knowledge of both the defender's network architecture and the attacker's TTPs. While both private sector and government experts share information, learning the right lessons from being breached can be an opportunity to more appropriately tailor security measures to the threats.<sup>36</sup>

Based on contributor comments, technological changes include basic computer maintenance and security tasks, such as removing outdated operating systems, developing application patching procedures, and enhancing password standards. After reviewing the attacker's tactic and intrusion vector, an organization may also change their network architecture or where data is stored (move data to the Cloud or to a central server or network drive to prioritize defenses in a single area). Image endpoints to ensure all devices are using the same, approved settings. As indicated in the Forum, one Defense Industrial Base firm reportedly virtualizes their desktops and wipes/reimages them every night. According to another contributor, a Federal agency developed automated notifications to alert system administrators or security personnel to data or system changes.

## Organizational Changes

Organizational changes also often occur after a cyber-attack. Many firms reallocate funds and human capital into cybersecurity programs, which could include hiring new personnel or contracting cybersecurity consultants, creating new positions (e.g. Chief Information Security Officer), or purchasing cyber insurance. An organization may also integrate cybersecurity or information technology offices within operational components to improve coordination in case of future attacks and increase general cybersecurity awareness throughout the organization.

Additional changes can include organizational culture or leadership changes. Leadership may encourage employees to learn about cybersecurity through training or incentive programs or requiring reports on cyber risk from components, changing the culture to include cybersecurity in everyone's mindset.<sup>37</sup> The attack could also force changes in leadership. In both private and public sector breaches, leaders have

---

<sup>35</sup> Investing in too many security products can slow both endpoint systems and networks, while new security procedures and permissions can slow decision-making.

<sup>36</sup> Some private sector firms have complained that the Federal government's information-sharing efforts are insufficient. These firms say the government data is too generalized or not released in a timely-enough fashion. Additionally, some legal and policy roadblocks continue to hinder widespread information-sharing among private companies. Efforts to bring government and private companies together through Information Sharing Analysis Centers (ISACs) have had mixed results, as a number of companies choose not to participate and claim that government representatives do not always have appropriate authorities or information to provide (although the Financial Sector and Defense Industrial Base are notable exceptions).

<sup>37</sup> This training may need to be tiered or otherwise tailored for the different stakeholder groups that leverage the system. For example, a casual user will not need to identify abnormal traffic flows, whereas a system administrator will. Additionally, leveraging all employees to watch their own applications for unusual activity and quickly report issues to security personnel would significantly reduce the time between detection and response.



been removed or asked to resign after publicized cyber-attacks.<sup>38</sup> Military personnel, especially senior leaders, could be held accountable for breaches they personally are involved in or that are of sufficient scale to compromise their operations. Several high-profile inquiries into both civilian and military leaders for mishandling sensitive data established a precedent to consider cybersecurity (and cybersecurity failures) as grounds for organizational change.<sup>39</sup>

## RECOVERY

### Short-Term Incident Response (IR) and Recovery

After detecting an infiltration, security personnel triage the most important systems or high value assets.<sup>40</sup> Personnel identify and isolate the infected systems to contain the attack, determine and evaluate the damage (data taken, services disabled, etc.), collect forensic evidence, and repair the infected systems to restore operations. While these efforts primarily involve the Information Technology Department, other parts of the organization, such as Finance, Legal, and general management are also involved in the effort.<sup>41</sup> If security personnel cannot remove the malware from the infected systems, they reimage those systems and use saved backups to restore the lost data.

### Advances in IR Technology

While new tools and technologies are continuously enhancing Incident Response (IR) capabilities, some contributors pointed out an increasingly tech-savvy workforce that not only results from the number of “digital-natives” entering the workforce but the increasing availability of computer education. As personnel become more technically inclined, even if at a rudimentary level, they could identify issues more quickly and possibly fix lower-tier computer problems or attacks, freeing security engineers to defend against more advanced threats.<sup>42</sup> Despite ARCYBER’s plans to integrate cyber subject matter experts (SMEs) into non-cyber units, these “non-cyber” soldiers will need (and possibly will have) some level of cyber education so they can identify (if not address) a cyber incident in a more timely manner.

### Importance of Incident Response

The most important element of an incident response program is timeliness, specifically the time between detection and response. Although it is a misconception that all cyber-attacks occur “at the speed of light” (or “network speed”), certain elements of an attack can operate very quickly.<sup>43</sup>

---

<sup>38</sup> Some well-known examples include Target CEO Gregg Steinhafel, OPM Director Kathrine Archuleta, and Sony Pictures head Amy Pascal.

<sup>39</sup> This could include a variety of punitive measures depending on the specifics of an investigation, including reprimand, hold-up for promotion, demotion, removal from leadership post, dishonorable discharge, or jail time.

<sup>40</sup> System importance could be determined by the data it stores, the capabilities/application it provides for business operations, or otherwise designated by the organization. System value and priorities are usually determined beforehand and found in the organization’s Continuity of Operations Plan.

<sup>41</sup> A Finance office may determine direct monetary effects of the breach and monitor ongoing costs of recovery and reallocate appropriate funds to cover expenses, the Legal department may determine the organization’s resultant liability, and general management would coordinate efforts among the various offices.

<sup>42</sup> A “lower-tier” computer problem could be user errors that require only basic IT support; a “low-level” attack could be rudimentary spear phishing.

<sup>43</sup> Examples could include a virus spreading through a network, specific instances of data exfiltration, or privilege escalation.



Therefore, it is paramount that information security personnel react quickly to contain and remediate the malicious activity when a network is penetrated.

Part of that timeliness comes from having the right detection and mitigation technologies and practicing incident response procedures (such as through security exercises or penetration testing). Another part is having a clear Incident Response Plan (IRP) in place to provide direction to the various offices within the organization. One commenter recommended breaking an overall Incident Response Plan into specialized sub-plans based on the type of attack or attack effects (e.g. ransomware, data breach/exfiltration, Denial of Service, disaster recovery, etc.) to further reduce response time.

Timeliness is essential during all phases of military operations, as equipment and personnel must act in concert over a wide Area of Responsibility (AOR) to ensure victory. Adding cyber risk to that equation only increases the need for timely responses when military systems are compromised or degraded. Service members must periodically drill their Incident Response Plans and know what to do when their system is attacked or compromised so they can react quickly to limit mission disruption.

## Operations Under Stress

Given that cyber-attacks are inevitable and some amount of down-time or service reduction is very likely while security personnel address the problems, organizations develop back-ups and policies to continue operations while under stress.<sup>44</sup> These “Primary, Alternate, Contingency, and Emergency” (PACE) programs provide three distinct back-up communication methods in the event the primary method fails.<sup>45</sup> An organization’s PACE program should ensure reliable communications in a wide variety of circumstances and have the necessary infrastructure in place to activate on short notice.

The US military has access to a number of possible backup systems, including radio and satellite phones, and likely already has PACE-like programs in place. The US Naval Academy has resumed teaching cadets celestial navigation to provide a backup navigation capability to GPS and other electronic methods, which are vulnerable to jamming and cyber-attacks.<sup>46</sup> DoD training centers could consider conducting coursework on using Morse Code<sup>47</sup> for communication, exercises with human runners, or other low-tech methods of communication to give service members experience using these back-up tools as well. Service members should practice operations using the full range of PACE options to reduce the learning curve during combat operations, if they do not do so already.

---

<sup>44</sup> Planning ahead for both mitigation and adapting operations will reduce response time after a cyber-attack. Determining whether a data or communications loss was due to malicious activity or a necessary action by administrators (e.g. maintenance) is essential for determining a proper course of action.

<sup>45</sup> A sample “PACE” program could be as follows: Primary: Voice-over IP, Alternate: radio, Contingency: personal mobile device, Emergency: human messenger.

<sup>46</sup> <https://www.washingtonpost.com/news/the-switch/wp/2016/02/17/why-naval-academy-students-are-learning-to-sail-by-the-stars-for-the-first-time-in-a-decade/>

<sup>47</sup> Various Military Basic Training courses, including Army and Air Force, include lessons on tap code (aka knock code), which is an alternative to Morse Code and is known for its use for communication among Prisoners of War (PoW).





## Best Practices

One commenter noted that the Information System Audit and Control Association (ISACA) monitors and gathers information, including Business Continuity-Disaster Recovery Planning.<sup>48</sup> Another identified that Veracode.com has recovery best practices specifically for incident response.<sup>49</sup> Furthermore, Cisco identifies a method summarized here.<sup>50</sup>

A key factor is to have an existing recovery plan. Chapter 3 summarizes the phases for disaster recovery: “1. Activation Phase: In this phase, the disaster effects are assessed and announced. 2. Execution Phase: In this phase, the actual procedures to recover each of the disaster affected entities are executed. Business operations are restored on the recovery system. 3. Reconstitution Phase: In this phase the original system is restored and execution phase procedures are stopped.” One highlight is from Chapter 3.2 Execution Phase. “Recovery operations start just after the disaster recovery plan has been activated, appropriate operations staff have been notified, and appropriate teams have been mobilized. The activities of this phase focus on bringing up the disaster recovery system. Depending on the recovery strategies defined in the plan, these functions could include temporary manual processing, recovery and operation on an alternate system, or relocation and recovery at an alternate site.” Section 3.2.1 Sequence of Recovery Activities continues: “The recovery procedure reflects priorities previously analyzed during the activation planning phase. For instance, if a server room has been recovered after a disruption, the most critical servers should be restored before other, less critical servers. The procedures should also include instructions to coordinate with other teams when certain situations occur, such as:

- An action is not accomplished within the estimated time frame.
- A key step has been completed.
- Items must be procured.

If a system must be recovered at a different location, specific items related to that service need to be transferred or obtained. Recovery procedures should delegate a team to manage shipment of equipment, data, and vital records. Procedures should explain requirements to package, transport, and purchase materials required to recover the system.”

## Recovery Problems

Often times, many organizations that are in a state of recovery face a multitude of challenges when bringing their organization back to a fully operational state. One major challenge is implementing the necessary controls to mitigate any further attacks, both new and repeating. The key challenge with this is having a strong forensics team in place to understand the security incident thoroughly, often taking months before the cause is identified.

Another challenge faced during recovery is the restoration of data as well as understanding the criticality of that data. Many organizations have some understanding of the data they utilize within their

---

<sup>48</sup> <https://www.isaca.org/Groups/Professional-English/business-continuity-disaster-recovery-planning/Pages/ViewDiscussion.aspx?PostID=72>; <http://www.isaca.org/Journal/archives/2012/Volume-1/Documents/12v1-Key-Issues-Challenges.pdf>

<sup>49</sup> <https://www.veracode.com/blog/2014/08/5-best-practices-in-data-breach-incident-response>

<sup>50</sup> [http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/white\\_paper\\_c11-453495.html](http://www.cisco.com/en/US/technologies/collateral/tk869/tk769/white_paper_c11-453495.html)



organization and some requirements around the recovery point and recovery time objectives for systems and data. Organizations that do not understand these aspects face extreme difficulty when recovering data, backups, and systems from failure. Some organizations have spent significant sums of funds to recover data only to realize that data recovery priorities were wrong, and critical business data required for day to day business operations were not recovered.

Furthermore, a most recently discovered recovery problem, which results from newer technology, is the failure of hardware and its ability to be restored, repaired, and/or replaced within a timely and cost effective manner. With the rise of interconnected systems, hardware failure is now more likely a result of a combined attack against systems and/or organizations.

## Recovery Action Plans

Key action plans and activities for recovery are to first identify key systems, data, and their recovery point and recovery time objectives. Often times, this can be determined by conducting a business impact analysis (BIA) of the organization and especially within key, critical business/operating groups.

Once the BIA has been completed as well as proper classification and prioritization of data has been determined, the implementation of recovery controls can begin.

Having a defined business continuity plan (BCP) and/or a disaster recovery plan (DCP) in place within the organization is critical, as it defines the process steps required to keep the organization and key critical systems up and running with little, if any, disruption to end services being received. These plans include details from the BIA such as RTOs (Recovery Time Objectives), RPOs (Recovery Point Objectives), and other details that help support and justify recovery priorities. Additionally, contingency aspects should be regularly updated, such as call trees, points of contact (POC), delegated responsibilities, and more. Having a strong BCP/DR plan in place within an organization with details provided can be one of the factors that help will keep an organization afloat instead of sinking during an emergency.

There are several frameworks that provide guidance of implementing recovery based controls, such as the National Institute of Standards and Technology (NIST) special publication (SP) 800-53, the NIST Cybersecurity Framework, the Control Objectives for Information and Related Technologies (COBIT), and the International Organization for Standardization (ISO) 27001. For all US Federal Government agencies, implementing NIST SP 800-53 would be the required mandate and provides numerous controls guidance across a wide spectrum of areas, from enterprise-wide to application/hardware specific. As a result, utilizing the business impact analysis in this space is imperative in order to identify the proper controls required at the enterprise level as well at the hardware/software level.

Once controls are implemented, monitoring for effectiveness and enhancing/optimizing is next. This provides the organization the best capabilities along with technical tools to actually recover from a disaster. Monitoring also helps evaluate the robustness as well as the need for a particular control or group of controls. Effectively, this reports into the overall cybersecurity program management office, which will then handle the necessary related projects to bring controls management up to par.

The next steps focus on what to do in the event of a recovery situation. The primary goal is to continue to keep operations supported and running. This is where the BIA and BCP/DR plans come into play. The



goal is to keep essential systems up and running as safely as possible. Human safety is always first. After critical and business essential systems are up and running smoothly, non-priority systems can be brought back up until the organization is back to full strength.

Once the organization is back up and running, forensics can begin across the environment to understand the details around what prompted the recovery and activation of the BCP/DRP. While this process will take time and resources, it is a valuable part of the recovery process as it exposes any threats and vulnerabilities that may have never been seen or uncovered during other tests and/or assessments.

The final step is remediation, which links back to the monitoring and enhancing of program controls but more at the operational level than at the remediation level. As processes of the organization evolve, so will the various technologies and trends in that space. As a result, it is vital that the security processes, controls, and security programs continue to improve. Plans, processes, and technologies should be evaluated each year for any changes and should be enhanced as the organization continues to grow.

## VULNERABILITIES

### Identifying Vulnerabilities

Vulnerabilities come from a variety of sources, including insecure coding practices or coding mistakes (prioritizing usability or functionality over security, coding error, etc.), interaction of different software and/or hardware components, or idiosyncrasies in the programming language.<sup>51</sup> Additionally, vulnerabilities can persist if system administrators do not properly update and maintain their systems. A large group of persistent vulnerabilities develop due to missing operating system (OS) or application patches, security misconfigurations, and poor network maintenance.

While not all vulnerabilities are equal in risk on their own, small (or seemingly low-priority) vulnerabilities can allow attackers an initial entry point that opens more significant vulnerabilities. For example, a Cross-Site Scripting inject could affect web-based applications to bypass access controls (which would be especially damaging if the target uses a same-origin policy or single sign on).

In addition to technological vulnerabilities, human end users will always introduce vulnerabilities by uninformed or inadvertent actions and mistakes. Even the most sophisticated endpoint and network security tools cannot make up for an uninformed user or a mistake by that user. As previously discussed, regular training is the current approach to reduce vulnerabilities from human user error.

### Third Parties and Acquired Organizations

Acquiring or partnering with another firm means connecting with their network and, by extension, accepting the vulnerabilities that exist with that network. Therefore, some organizations are looking at a potential network as part of the evaluation on whether to acquire or partner with another firm. An organization's security experts will study the network and test security measures and, if possible, review their supply chain and research vendors. Additionally, an organization could look at a potential partner's

---

<sup>51</sup> <https://www.veracode.com/sites/default/files/Resources/Whitepapers/how-vulnerabilities-get-into-software-veracode.pdf>



reputation and history. Bad press or reckless behavior within their market could suggest increased risk and vulnerabilities.<sup>52</sup>

Contributors also suggested that organizations should be mindful of third-party products (hardware or software). Despite a firm's reputation, it is good practice to conduct a security assessment (i.e. vulnerability scans, research the product, and test in development environment) before putting it on the network. One commentator stated that if a device or software is not developed completely in-house, the organization should assume it has vulnerabilities.<sup>53</sup> Currently, many public and private organizations use legal contracts and stipulations to enforce third party cybersecurity without conducting full assessments of the third party's environment. Having insight into an organization's cybersecurity posture can assist in not only identifying gaps within their environment but also the requesting organization's environment. Evaluation of particular products and/or services adds one more level of visibility to the requesting organization, consistent with a defense-in-depth approach, and can ultimately reduce possible attack vectors against the primary organization.

Third parties or acquired companies are analogous to military allies or coalition partners, who may need some access to US networks to coordinate operations or share intelligence. Vulnerabilities and any potential compromises in partner networks can transfer to US military networks and produce new holes in US cybersecurity. The DoD has developed various cybersecurity standards and likely compartmentalizes or isolates networks for allied or partner use.

Once agreeing to partnering with or acquiring the other firm, Forum contributors recommend the organization establish clear roles of accountability and obligation to determine who is responsible for remediating vulnerabilities and maintaining good cybersecurity practices.<sup>54</sup> Some organizations are asking vendors to provide Service Organization Control (SOC) 2/3 reports, ISO 27001 Attestation Certifications, and/or Statements on Standards for Attestation Engagements (SSAE) 16 reports as well as various security policies, threat and vulnerability management standards. Further success is reported from the use of basic agreements, tools, legal contracts, and non-disclosure agreements (NDAs). Additionally, many security firms are now providing scanning tools.

## Network Access Vulnerabilities

Network access is a key element of cybersecurity. All cyber-attacks require some level of network access to be effective, and proper access management can significantly curtail a cyber-attack's effect on a network. Organizations must manage current user access but must also diligently address on-boarding and off-boarding personnel and third party organizations. This effort can be helped with user account auditing on a regular basis. Depending on how often there is rollover should help determine how often this audit is executed. Keeping user accounts for former personnel or leaving unnecessary ports open

---

<sup>52</sup> If an organization has a reputation for data breaches, poor leadership, or other negative indicators, a partnering or acquiring firm may wish to take additional security measures or potentially walk away from the partnership/acquisition.

<sup>53</sup> Vulnerabilities can exist even on in-house devices (programmer mistake, lapse security procedures, etc.). Therefore, even those devices should go through a vulnerability evaluation before connecting it to (or installing it on) the network.

<sup>54</sup> In the private sector, these responsibilities are notated in an Interconnection Security Agreement or Service-Level Agreement. This document should lay out roles and responsibilities for all concerned parties and articulate the cybersecurity standards to which the network is to be held.



increases the system’s attack surface and exposes it to more threats. Deployed service members should have some capability to disable user accounts and close unnecessary ports or protocols to reduce the attack surface and related vulnerabilities.

Additionally, adding unauthorized software to increase capability (such as a Domain Name System “jumper” to quickly access firmware) opens up new vulnerabilities. While Federal networks have policy standards in place (such as Security Technical Information Guides and Federal Information Processing Standards), these best practices are not always followed.<sup>55</sup> Moreover, when end users can change a system or endpoint without security review, this change can also introduce a new vulnerability.<sup>56</sup>

## TRUST RESTORATION

### Activities to Restore Trust

After an organization has recovered from a cyber-attack, it must quickly restore the trust it has lost with its user base. Private firms risk losing customers and market share. In a worst-case scenario, the company could fail. Additionally, depending on the attack, employees may leave the company. While the US military does not have the ability to “take their business elsewhere” in a combat situation, computer technologies provide the military with many tactical and operational advantages that are increasingly essential in modern combat.<sup>57</sup> If Service members lose confidence in those systems and choose to not use them, they give up those advantages and could risk mission success.<sup>58</sup>

Restoring trust is both a technological and public perception challenge. The organization must take appropriate steps to curtail its losses and make reparations to those affected. However, making those changes is not enough. As trust is a belief predicated on emotion, the organization must appeal to users’ emotions and exude confidence to encourage customers to return. The organization must ensure its user base knows that effective changes were made and that there is little (or at least minimized) risk of another cyber-attack in the future. Depending on the breach’s effects, the organization may choose to provide additional services to affected customers or employees (e.g. free credit monitoring or broader identity theft protection) as well.

Transparency is a major factor in maintaining and regaining trust. In the case of a breach, transparency may include conducting an open and transparent dialog with both employees and external stakeholders to explain the breach, the consequences, and how it is being addressed.<sup>59</sup> Additionally, the organization

---

<sup>55</sup> One contributor noted that unapproved software is often added and then removed just prior to an audit. This could be due to a slow Federal acquisition and approval process for software, as employees may feel they cannot wait the weeks or months for approval.

<sup>56</sup> Adding or changing an application, for example, could introduce a new current vulnerability into the network. Additionally, if security personnel do not know an application is on the network, they do not know to download patches for it, thus potentially allowing future vulnerabilities to persist on the network.

<sup>57</sup> Certainly, from an acquisition standpoint, the military could choose to stop using a particular system or company after a significant cyber-attack on their systems. However, that is beyond the scope of this project.

<sup>58</sup> Advantages include, but are not limited to, precision targeting and timely communication.

<sup>59</sup> Freelance cybersecurity experts will likely conduct their own analysis based on publically-available data and any sources they can cultivate within the organization. If these expert’s reports differ from the organization’s statements, users or customers



may have to manage public perceptions through both traditional media and social media platforms to appropriately illustrate the changes being implemented.<sup>60</sup>

An important phase is publicizing the steps the organization is taking to both address the attack's effects and to proactively prevent future attacks. When dealing with civilians or military personnel, this step is vital to restoring trust. A detailed post-mortem, as well as 'lessons learned' report should be presented to all those impacted (sanitizing the reports per clearance level) so they have some level of confidence that it will not happen again. This includes any and all organizational and operational changes mentioned previously. Integration of IT security or Incident Response personnel with regular operations departments will help to reduce lag time between detection (by users) and response. Considerations may also include purchasing cyber insurance for attacks.<sup>61</sup> Address any resulting regulatory, legal problems or liabilities to reassure stockholders and employees.<sup>62</sup>

Despite an organization's best efforts, some customers will remain hesitant to return. Depending on the attack's scale and publicity surrounding it, it could take months or years to regain users' trust. Organizations must be patient and allow time for customers and other stakeholders to rebuild their trust in the organization.

### Priorities in Establishing Trust

The first priority in reestablishing trust with users is to stop the intrusion. If users believe the threat still exists, they will not trust the organization with their data or participation. Organizations with a strong incident response plan can quickly eliminate any infiltrations and remove malicious actors from their networks.<sup>63</sup> The sooner an organization can report an infiltration contained, the sooner the organization can begin rebuilding trust with its users. It is helpful to start with a high-level Incident Responses Plan.

The second priority is to establish a dialog with stakeholders. People often speculate the worst-case scenario and can make rash, damaging decisions in the event of an information vacuum. Regular and substantive communication with users will reduce this speculation and restrain some of the emotion-fueled reactions that could otherwise damage customer-relations and the organization at-large. In the

---

may suspect a cover-up or deception from the organization, which would further degrade trust. Therefore to the extent possible (within legal and security constraints), the organization must be candid and forthcoming.

<sup>60</sup> This could include regular updates and interviews from credible organization leadership on social media platforms and reaching out to news organizations. In 2015, Target posted an article on its corporate website to display its new cyber fusion center: <https://corporate.target.com/article/2015/07/cyber-fusion-center>.

<sup>61</sup> While cyber insurance will likely not help a current breach, publicizing its purchase will help illustrate the organization is being proactive against future attacks (some policies will retroactively cover breaches that occurred after purchasing the policy if the breach was not discovered until after the policy purchase date).

<sup>62</sup> If the organization is not liable, per contract or other legally-binding agreement, the organization should fight any unjustified lawsuit. However, the organization will likely restore trust with its customers and employees by being proactive and taking responsibility for any damages for which it is liable.

<sup>63</sup> This could require a "triage" approach depending on the scale of the intrusion, where organizations identify their critical systems or the most severe intrusion and focus efforts in securing that area first.



private sector, this often involves alerting stockholders and the public that a breach occurred and, to the extent possible, the type and scale of loss.<sup>64</sup>

Finally, the organization needs to initiate medium- and long-term changes to reassure users. These are most commonly the cybersecurity improvements and organizational or operational changes the organization makes. It also might include providing identity theft protection or other additional services at the organization's expense. A common example is free credit monitoring for a period of time (e.g. one to three years).

### Cost and Consequences of a Breach

Negative publicity from a cyber-attack often tarnishes an organization's brand and reputation. In the corporate world, this loss of trust could lead customers to take their business to competing firms.

Between any data lost, operations disrupted, and the cost of repair and recovery, a cyber-attack can have significant financial consequences. Breaches may cost an organization from \$3-75 million. These costs could easily curtail the organization's future projects, retard growth potential, and possibly result in bankruptcy. Additionally, a breach will be a red mark on the organization's stock value and could affect future investment or acquisition desirability.

While high-profile firings of C-suite leadership are often the ones most publicized, mid-level management and security personnel could also be fired or laid off, creating new holes in the organization's security structure and breeding an unstable office environment (especially among other security staff). Depending on the public perception of the breach, it may also affect future ability to hire talented employees. If IT workers believe the organization had an inattentive or negligent leadership or a bad organizational culture, they would be less likely to apply for positions within that organization.

In the medium-term, an organization's past failure (especially in the case of multiple incidents) might encourage future attacks. If the organization develops a reputation for inadequate security or inability to respond to attacks, other threat actors may see this as weakness and target that organization again, depending on their objective. For example, a large retail company with publicized poor cybersecurity would likely be a regular target for criminals, who often have financial motivations.<sup>65</sup> Attackers might target a known vulnerable firm to glean corporate secrets or to gain access to a third party organization that does business with the targeted firm.<sup>66</sup>

An organization could also likely face a number of regulatory and legal consequences from the Federal Trade Commission, State laws, or other oversight organizations. Business partners may sue if they believe a contract was violated (e.g. for not protecting shared data) or stop doing business with the compromised organization, leading to further loss of revenue and reputation.

---

<sup>64</sup> Most often this is related to answering the "what" and "how much" questions: what was compromised or stolen and how much/what was the volume lost?

<sup>65</sup> These criminals would likely hack the retail company to gain customer credit card information to either sell directly or perpetrate identity theft.

<sup>66</sup> Conversely, organizations that recently experience a security breach and have since upped their security measures tend to be more secure than an organization that has not yet suffered a public breach of security. So, having had a recent breach can also act as a deterrent against future attacks, as the attackers know the organization is now more alert.



In the military, the cost may be in human life, delay in completing a mission, or direct mission failure.

## Time to Restore Trust

The time it takes to restore trust in a system depends on the nature of the attack, the degree or extent of compromise within the network, and how the organization corrected the penetration (in terms of timeliness, effectiveness, and communicating with stakeholders). Another factor is the organization's importance to its users. If users rely on a product or service the organization provides (especially if they cannot easily migrate to a competitor), trust will be restored more quickly out of necessity.<sup>67</sup>

Trust is ultimately restored when users no longer believe the system is compromised (and that the organization is doing its due diligence to protect against further compromise). If a cyber-attack leaves obvious signs (a DDoS blocking traffic, webpage defacement, or recognizable data corruption) that users can easily identify, they can quickly determine for themselves when a system is compromised and when it has been restored. Once it has knowingly been restored, users will return knowing they can trust the data.<sup>68</sup> Conversely, if a cyber-attack is more difficult to identify and users cannot be sure it has been cleared from the infected system, they will be more hesitant to trust.

Additionally, users will likely trust a network more quickly if the compromise or infiltration affected a comparatively small part of the network and/or if the data compromised was relatively minor (e.g. external-facing servers). Users are more concerned, and less likely to trust a compromised network, with a more pervasive cyber-attack that affected a larger percentage of the network or compromised key information (such as personally identifiable information) or impeded key business operations.

Depending on the breach's severity and effects, trust might never be fully restored.<sup>69</sup>

## ARTILLERY EXAMPLE

The Artillery Example category was entered later than the other categories, partly as a test to see which participants would respond and determine which, if any, had military experience. Results from this category suggest the project team should develop a separate Forum directed at military experts.

## OTHER RELEVANT INSIGHTS

The rate of change in technology may be a challenge. While discussions generally focus on "digital natives" and "digital immigrants," typified by Millennials and Baby Boomers, respectively, there are also significant variations in tech savvy and preferences among Millennials (18-34 years old) and between Millennials and Generation Z (13-18 year-olds).

---

<sup>67</sup> Users may downplay the cyber-attack in their minds or be willing to forgive the organization as a coping mechanism to continue receiving what the organization provides. While some could argue this is not real trust, the effect of users continuing their activities with the organization is the same.

<sup>68</sup> This assumes the organization implements good cybersecurity practices after the fact. Otherwise, a law of diminishing returns may apply as repeated cyber-attacks and breaches steadily degrade users' overall trust of the system and move to other providers.

<sup>69</sup> If a cyber-attack fooled an artillery unit to kill friendly soldiers, guilt or other grave emotion may lead that unit to never fully trust the compromised system again.





Former National Security Agency Director Chris Inglis stated that Millennials may be more comfortable with using technology but do not necessarily understand how the technology works (hardware or software) below the surface.<sup>70</sup> They are not “digital natives” but “app natives,” who leverage technology far more effectively than other generations might, but do not understand the underlying architecture or appreciate either the vulnerabilities or the security implications. Several news reports and private sector surveys suggest a similar picture.<sup>71</sup>

Conversely, personnel assignment rotations (especially among officers) may prevent service members from developing an in-depth knowledge of the systems and networks they use. Some civilian cyber-experts can almost predict when a disruption is imminent by watching traffic patterns on the network. However, this level of understanding often takes years to develop and may take too long for military personnel to learn before they move to their next duty assignment.

An upcoming challenge will be the evolving human-computer interaction (HCI). The DoD’s Third Offset Strategy includes several elements related to different aspects of HCI. These include autonomous learning systems for big data and pattern detection, human-machine collaboration to reduce decision-making time, and advanced human-machine combat teaming.<sup>72</sup> How these technologies develop and are integrated into military operations will have a profound impact on what vulnerabilities develop and how an OPFOR can or would leverage cyber operations.

## DATA GAPS

There is a great deal of anecdotal evidence, but the project still lacks widespread quantitative data on attacks. High-level data (percentages, attack totals, general target data) is available in private sector reports, but the raw data behind those final numbers is often proprietary. Cyber insurance firms also report that there is insufficient actuarial data to precisely determine insurance premiums.<sup>73</sup> Thus, while the project team will continue to locate useable quantitative data, the group acknowledges collecting this data will likely be difficult for the foreseeable future.

Despite significant contributions by CSFI volunteers, the Forum has a number of topics that did not receive comments (Analysis of a Successful Attack, Post-Attack Analysis, Attribution, Long-Term IR and Recovery, and Recovery Action Plans). Many of these topics are under the Post Operations and Forensics sections. The project team will focus individual research efforts on these areas.

The project team would need a detailed understanding of Army network defenses (architecture, products used, and TTPs for continuous monitoring) to determine what attacks would truly be effective, as well as how the Army would detect and mitigate attacks.

To maintain relevance for DoD into the future, the project team will need to monitor new developments in Army systems, especially, but not exclusively, as related to the Third Offset Strategy. Cybersecurity,

---

<sup>70</sup> [https://www.youtube.com/watch?v=nOcqI8KYcHM&list=PL-bQ6\\_vfcE04DLtgJVTPFPkh6sGpFojxv&index=3](https://www.youtube.com/watch?v=nOcqI8KYcHM&list=PL-bQ6_vfcE04DLtgJVTPFPkh6sGpFojxv&index=3)

<sup>71</sup> <http://changetheequation.org/does-not-compute/>

<sup>72</sup> <http://www.defense.gov/News/Article/Article/991434/deputy-secretary-third-offset-strategy-bolsters-americas-military-deterrence>

<sup>73</sup> “Focusing on the Future: Prioritizing Security in the Digital Economy.” *Chertoff Group*. November 18, 2016. Washington, DC.



and the use of cyber at large, is growing into a regular concern on all operational levels. Additionally, the Third Offset Strategy relies heavily on cyber capabilities as well as other related capabilities (robotics and artificial intelligence) that indirectly influence cyber operations. Depending on how these strategic and technological developments evolve, the project team may need to update research findings to ensure the models that use this data are accurate.



## APPENDICES

### A. Cyber Attack Categories Table

**Cyberspace Attack:** Cyberspace actions that create various direct denial effects in cyberspace (i.e., degradation, disruption, or destruction) and manipulation that leads to denial that is hidden or that manifests in the physical domains; These specific actions are: (JP3-12)

Attack Category	Definition for purposes of this survey	Cyberspace Operations Definitions (JP3-12R) <small>Joint Publication 3-12 (R) Cyberspace Operations, 5 February 2013; Joint Publication 3-14, 29 May 2013 - Space Operations</small>
Deny	Any of delay, degrade, disrupt, destroy	To degrade, disrupt, or destroy access to, operation of, or availability of a target by a specified level for a specified time. Denial prevents adversary use of resources.
Deny/ Delay	Preventing access to or communication with other nodes in the networks (including denial of service)	Those measures designed to temporarily eliminate the utility of targeted adversary systems, usually without physical damage. (JP3-14)
Deny/ Degrade	Permanently impairing, either partially or totally, a system's or data's integrity	To deny access (a function of amount) to, or operation of, a target to a level represented as a percentage of capacity. Level of degradation must be specified. If a specific time is required, it can be specified.
Deny/ <u>D</u> isrupt	Temporarily impairing specifically targeted nodes within the network	To completely but temporarily deny (a function of time) access to, or operation of, a target for a period of time. A desired start and stop time are normally specified. Disruption can be considered a special case of degradation where the degradation level selected is 100 percent.
Deny/ Destroy	Making data or hardware permanently unusable	To permanently, completely, and irreparably deny (time and amount are both maximized) access to, or operation of, a target.
Deceive/ Manipulate	Manipulation, distortion, or falsification of data; altering message content, recipients, etc. to persuade the victim to react, study victim behavior, or otherwise cause detrimental effect	Those measures designed to mislead an adversary by manipulation, distortion, or falsification of evidence to induce the adversary to react in a manner prejudicial to their interests. (JP3-14) To control or change the adversary's information, information systems, and/or networks in a manner that supports the commander's objectives. (JP3-12)
Exploit	Accessing data to gain insight or operational advantage	Take advantage of measurement and signal intelligence, open source intelligence, and human intelligence JP3-12 (p I-3). Take advantage of vulnerabilities JP3-12 (p II-9).



## B. Cyber-Attack Types Table

Attack Type	Description	Attack Category	Desired Effects
Virus	Malicious code that attaches itself to a host application; the virus is activated when the infected application is executed (either by the user or the Operating System's automatic commands). Replicates by infecting other applications on the target host/computer.	Degrade, Disrupt, Destroy	Activates malware (which can cause any number of issues). Often used to destroy/corrupt data or open back doors into systems.
Worm	Self-replicating malware that travels through a network without the need of host applications or user actions. (note: a 'headless worm' takes advantage of Internet of Things (IoT), spreading through personal devices to reach the target)	Degrade, Disrupt, Destroy, Exploit	Activates destructive malware (encrypts files for ransom, destroy files), open back doors, degrade service (by slowing bandwidth), or joins the victim computer to a botnet.
Logic Bomb	Code that executes an action in response to an event (time/date, launched application, a change in a file/database, etc.).	Degrade, Disrupt, Destroy, Exploit	Disrupt service (by shutting down a device, rebooting system, etc.), destroy/corrupt data (add or delete content), open back doors.
Trojan	Malware that appears to be benevolent or beneficial software. Often poses as an antivirus program/patch, a popular application, and screen saver. Embedded in a website's code to automatically download when the victim visits the infected site (aka drive-by download) or intentionally downloaded by the user.	Degrade, Deceive, Disrupt, Destroy, Exploit	Creates a back door into the affected system to use for the following: identity theft, surveillance, exfiltrating/corrupting data, joining the victim computer to a botnet, injecting other malware.
Botnet	Computers slaved together and controlled by a malicious actor. A user may or may not realize their computer is part of a botnet, based on how the malicious actor uses the "bot." Botnets are often built by Trojan horse and rootkit malware. Botnets are commonly sold on the black market for either single-time or regular use.	Deny/Delay, Disrupt, Exploit	Often used as part of a DDoS attack against other computers or propagate spam messages; can spread other forms of malware within the botnet.
Rootkit	Modifies Operating System files and applications to hide the fact that malware is present on the victim computer.	Deceive, Exploit	Install back doors and hide other malware. Anti-virus is unable to detect a problem.
Spyware	Monitors a user's computer to send the information to a third party. Key loggers report what characters a user types. They are often installed as part of Trojan horse programs or separate drive-by downloads from infected web pages.	Exploit	Surveillance, data exfiltration, system crashes, degraded service.
Phishing	Tricking users via deceptive emails to encourage them to take an action. This could include providing sensitive information or carrying out incorrect orders. Phishing often includes impersonating someone of authority and/or suggesting an urgency to the request.	Degrade, Deceive, Disrupt, Destroy, Exploit	Installation of malware via infected link or email attachment, providing sensitive information to malicious actor, carrying out incorrect orders.
Smurf Attack	A malicious actor duplicates a victim's MAC address and broadcasts a directed ICMP ping (which asks all computers that hear it to respond). The attacker changes their MAC address back so the returned ICMP pings travel to the victim computer instead, resulting in a Denial of Service attack due to the flood of increased traffic.	Deny/Delay, Disrupt	Diminished system capacity, communication disruption.
SYN Flood	A denial of service attack where an attacker does not complete a sync/acknowledgement handshake. The attacker sends "SYN" request packets but disregards the victim's automated SYN acknowledgements. This forces the victim to expend bandwidth waiting to complete the handshakes and preventing other, legitimate users, from connecting.	Deny/Delay, Disrupt	Diminished system capacity, communication disruption.
Xmas	A malicious actors conducts a scan of active ports to learn details about the target's operating system. This is a recon attack used to gather intelligence and inform the malicious actor what categories of malware to use against the target.	Exploit	Reconnaissance conducted against system. No damage.



Man-in-the-Middle	An attacker intercepts all traffic between two users before forwarding the packets to their intended recipient. This serves as an eaves-dropping/intelligence-gathering attack as the attacker is reading the mail of both victims without their knowledge.	Deceive, Exploit	Reconnaissance conducted against organization and users. Could block communications, but this is unlikely as it would reveal the attacker's presence. Insert malicious code.
Replay	A malicious actor captures and replays traffic (and corresponding credentials) that was already sent in a communications session, attempting to impersonate a user and get information or credentials from those contacted with this old traffic.	Deceive, Exploit	Enables data exfiltration and surveillance of user communications. Could also inject malware into the correspondence before forwarding it to the victim.
Pharming	A malicious actor corrupts a Domain Name Service (DNS) server or client router, which redirects users to different, often malicious, websites instead of the website they typed in to their web browser.	Degrade, Deceive, Disrupt, Destroy, Exploit	Installation of destructive or surveillance malware on target computer. Prevents user from connecting to a particular website.
Watering Hole	A malicious actor places malware on a legitimate website that members of the target organization frequent (a news source, government website, online shopping, etc.), infecting machines (often via drive-by download or click downloads) when they visit the website.	Degrade, Disrupt, Exploit	Creates back doors, enables data exfiltration, disrupt service, destroy data.
Session Hijacking	A malicious actor learns a user's website session ID (often pulled from an Internet cookie) and uses it to impersonate the user.	Degrade, Deceive, Exploit	Enables data exfiltration, surveillance. Could also be used to upload incorrect instructions to other users or malicious attachments.
Buffer Overflow	A malicious actor submits more input to an application (often a web-based form) than the application can handle. This forces the computer to open up more areas of memory than the application was initially allotted.	Exploit	May degrade service (likely slowing the system down). Enables other malware to be planted within the system's exposed memory.
Integer Overflow	An attacker attempts to create a numeric value the application cannot handle, resulting in an error and inaccurate results. Similar to a buffer overflow attack.	Exploit	May degrade service (likely slowing the system down). Creates an error that provides inaccurate results to the system.
SQL Injection	An attacker inputs SQL statements into a web-based form in order to access and send commands to back-end SQL servers. Note that this approach can also access servers using other database languages (e.g. injecting Microsoft Access queries for Access databases).	Disrupt, Destroy, Exploit	Commonly used for data exfiltration but can also corrupt or delete data from the back-end database.
Cross-Site Scripting (XSS)	An attacker inputs malicious HTML or JavaScript code into an email, webpage messages, images, etc. The malware is activated when a user clicks on the infected element.	Disrupt, Deceive, Exploit	Infiltrate systems by bypassing access controls (elevated permissions), access sensitive data, pull web browser's cookies (potentially enabling more access), and redirecting users to malicious websites.
Ghostware	A specific attribute added to malware that, upon completing its mission, erases all traces before security measures can detect that a compromise has taken place.	Degrade, Deceive, Disrupt, Destroy, Exploit	Destroy evidence that an infiltration occurred to avoid triggering incident response and/or hinder digital forensic and attribution efforts.
Ransomware	A victim's data, computer, etc. is encrypted by a malicious actor who demands payment (ransom) to provide the key to unlock the data	Destroy, Degrade, Disrupt	Often used to extort money, but will certainly temporarily degrade or disrupt operations as the victim would be unable to access whatever has been encrypted (unless the data is backed-up externally).
Two-Faced Malware	A specific attribute added to malware where the malware activates a benevolent/innocent task while in a sandbox, tricking the security device into letting the packets through. The malicious code is activated once beyond the sandbox.	Degrade, Deceive, Disrupt, Destroy, Exploit	Deceives sandboxes, bypassing that security measure. Once beyond the sandbox, the malware can execute its code.
Blastware	A specific attribute added to malware where, upon completing the malware's initial mission, destroys its target or renders its host unusable if detected by security systems.	Degrade, Deceive, Disrupt, Destroy, Exploit	Destroy evidence that an infiltration occurred to avoid triggering incident response and/or hinder digital forensic and attribution efforts.



## C. Cyber Questions

### I. Topic: General

#### a) Identifying your business sector, size, and geographic region

For your organization(s) identify:

- Business sector: Consumer (discretionary or staples); Energy, Financial, Health Care; industrial (which); Information Technology; Materials, Telecommunication Services; Utilities; Federal Government/DoD; State Government/sector);
- Size: How many nodes do you defend (people/technical nodes) in your organization? (less than 1,000; 1,000-10,000; 10,000-100,000; 100,000-500,000; 500,000-1,000,000; 1,000,000+);
- Locations: US States (how many/which), countries (how many/Which), or General: provide a general description of your organizational experiences.

#### b) Select one or more topics below for comment.

- Objective: Identify considerations for cyber-attack related decision making including information needed at various stages of an attack, the decision criteria at that timeframe, and decision options available.
- Purpose: This request seeks to gather information on cyber-security statistics including: characterizing threats, defenses, data and criteria for decisions, time-frames for threat detection and attack recovery, and future trends in threats and defenses. The data will be used to ensure accurate narratives and injections for US Army simulations, studying how the loss of network components affects human behavior and decision-making. The primary objective is to make a parametric description of detection, defense, and ways to restore trust. Click to see more guidelines.
- Select a Category, and a Discussion Topic to drill down to the specific questions and comment block. You may also provide information in a more free-form mode of your choosing if the topics become too cumbersome for your input.

### II. Topic: Effective Decision Making Related to Cyber Operations, Your Industry's Point of View

#### a) Effective decision-making by non-expert network users for operations

- What information do they need to make effective decisions?
- What are the choices of decision options for/once you have this information?
- Can there be a threat condition identified for cyberspace attack (e.g., DEFCON, FPCON, THREATCON )?
  - What are the indicators for various levels of cyber alert?
  - Is there any value to putting non cyber expert personnel on alert?
  - Is there any time or way to put non cyber expert personnel (aka operators) on alert?
  - When chances of cyberspace attack are elevated, operators are on alert, what should be the things they should notice, identify, or look for to maintain vigilance?
- For messages/input for the operators mission:
  - What are the indicators of abnormality?
  - Can there be a measure of the extent or level of abnormality?
- Given that the operators systems are compromised:
  - How can the operator determine if the compromise is in the network or in their decision support systems?



- What are the decisions the operator needs to make to try to mitigate or analyze the compromise?
- If the operator is in the process of performing immediate critical functions for which delay could cause significant compromise, what information does the operator need to decide to deal with the cyber concerns, performing the operation, or moving to an alternate solution to perform immediate critical functions?
- b) What decisions are impacted by various cyberspace operations effects?
- c) What decisions/courses of action (COA) options are “lost” and what decisions/COAs emerge when impacted by cyberspace operations?
- d) How does the mission influence the impacted decisions?
- e) How does the operational environment influence the decisions? For instance mobile units in Urban and Non-Urban environments/terrain influencers.
- f) What changes in operation’s perceptions when impacted by various cyberspace operations?
- g) What impacts does reduced trust have on operational decision making?
- h) How is risk estimated and risk-aversion impacted by the effects of cyberspace operations?
- i) How is decision making speed impacted?
- j) What aspects of situational awareness are critical for effective COA decisions and resultant behaviors?
- k) What is the impact of the difference between having a single incident attack environment and having a continuous threat environment on decision making and messaging?

### III. Topic: What Information Does an Entity Need to Know to Make an Effective Decision and Situation-Dependence?

Identify an example of what information you would need to know to make an emergency decision when something went wrong related to a cyber-attack on your environment. What situation does this refer to? If you have no planned response, you may identify what you think the response should be and the information needed. The "entity" is the human, their hardware (computer) and their interface.

### IV. Topic: What Decisions/Courses of Action (COA) Options are “Lost” and What Decisions/COAs Emerge When Impacted by a Cyberspace Attack?

From your point of view, what is a (less obvious than network down?) example of cyber-attack that causes a change in the environment that a user has to deal with and what do you think they need to do now?

### V. Topic: The Nature of Cyber Attacks: Categories, Intentions, Effects

- What attacks types (attacks that destroy, disrupt, deny/delay, degrade, disrupt, deceive, or exploit data or systems) are most severe? Least severe? Why?
- What are the success rates of the different attack types above?
- To the best you can estimate, what are the attackers’ intentions based on the attack types above?
- Have you experienced Advanced Persistent Threats? What were some of the indicators of compromise?
- Can you identify the cost of attacks to your organization? Any lessons learned based on the costs?
- What other data should we collect on attack categories, vectors, or statistics? (Please add other relevant information as you find useful.)

### VI. Topic: Attack Categories: Insider Threat



- How does your organization address the risk from insider threat?
- Do you use technologies to monitor suspicious online behavior? If so, what kinds of technologies?
- Do you use non-technical means to gauge non-technical indicators (e.g. traumatic event or suspicious personal behaviors)? If so, what do you use?
- How often do insider-attacks occur in your organization (times per year)? What portion were the insiders acting alone as opposed to receiving external help?
- Which insider threat activities/events would you consider corporate espionage?
- In your experience, which attack category do insider threat actors attempt most: Deny (Destroy, Delay, Degrade, Disrupt); Deceive; or Exploit? Which is the second most prevalent?

## VII. Topic: Attack Categories: Random Attacks

- Are random attacks prevalent in your network environment or are you more frequently intentionally targeted?
- What percentage of attacks against your networks would you consider targeted versus random?
- What is the nature or any specific characteristics of random attacks?

## VIII. Topic: Attack Categories: Combined Attack Categories

- Of the attack categories Deny (Delay, Disrupt, Degrade, and Destroy); Deceive; and Exploit, which two (or more) are combined most often?
- Which combination have you found to be most detrimental, and what were the worst consequences of those combinations?

## IX. Topic: Attack Categories: Deny

Deny/Delay: Preventing access to or communication with other nodes in the networks.

Deny/Disrupt: Temporarily impairing specifically targeted nodes within the network.

Deny/Degrade: Permanently impairing, either partially or totally, a system's or database/data's integrity.

Deny/Destroy: Making data or hardware permanently unusable.

- In your organizations' experience, do attackers focus more on:
  - Denial of service (DoS)?
  - Delaying communications?
  - Disrupting, impairing systems functionality?
  - Degrading system integrity?
  - Destroying data or software?
  - Destroying hardware?
- What is the proportion of attacks in these categories compared to deceive and exploit?
- Which is more dangerous or detrimental to your organization: data theft or data destruction?
- What percentage of total cyber-attacks involves corrupting data as opposed to stealing data?

## X. Topic: Attack Categories: Exploit

Exploit: Accessing data to gain insight or operational advantage over a targeted victim.

- In your experience, have there been attempts to exfiltrate data from your systems? How frequently would you estimate these attacks occur (per month, per year)?
- What kinds of data were targeted (general categories only, e.g. PII, trade secrets, negotiation strategies, correspondence, etc.)?
- Are there any particular malicious actors that leverage exfiltration attacks against your organization?
- How could malicious actors exploit the data they access/steal against your organization?





- What is the worst case scenario for your organization if data is exfiltrated and exploited? How would stolen data damage your organization the most?
- What is the cost of a data breach?
- How do you define "cost" (e.g. man-hours, monetary cost of developing stolen information, price stolen data is sold for by attackers, effect on company stock if/when breach is made public, etc.)?
- Is there anything your organization does/can do to recoup those losses?

#### XI. Topic: Attack Categories: Deceive

Deceive: Manipulation, distortion, or falsification of data; altering message content, recipients, etc. to persuade the victim to react, study victim behavior, or otherwise cause detrimental effect.

- Have you experienced deception-type attacks? What was its purpose? What was its mechanism?

## DEFENSES

#### XII. Topic: Best Practices

#### XIII. Topic: New NIST password guidelines

#### XIV. Topic: Remove attack-data out of Office documents and images

#### XV. Topic: What are your or your organization's approaches to defenses?

- What defenses does your organization use?
- What defenses do you find most effective?
- How often do you update or change defense technologies/policies?
- Does your organization have specific approaches for different attacks (such as to avoid Zero Day attacks, countering denial of service, and/or countering breaches)?
- If your organization is looking into improving defenses, please identify your approach and in which areas you may be focusing. Please identify the magnitude of resources (investments, personnel) you apply for defense.
- If you provide cyber training to your staff, please identify the type and frequency. Any lessons learned?

#### XVI. Topic: Network Monitoring

- How does your organization leverage network traffic monitoring to support cyber-defense?
- Do you use multiple tools? If so, are they commercial or proprietary?
- How often do you update those tools?

#### XVII. Topic: Defense Effectiveness

- Describe your defenses' overall effectiveness against various attack types; provide a percentage of attacks blocked (e.g. virus: 85%). (A) With a typical defense approach and updated systems? (B) With legacy systems that have not been updated?

#### XVIII. Topic: Defense Categories

- What categories of defense you use: Preventative, Active, Passive? What technologies do you use from each category?



- **Preventive** (including but not limited to): input validation, firewall, delete cookies, whitelisting, hardening, delete cookies, strengthen passwords, maintain web browser, delete cookies, digital signatures, block suspicious IP addresses, block direct broadcasts, access controls.
- **Active** (including but not limited to): IPS, load balancer, failover cluster, packet inspection, flood guard.
- **Passive** (including but not limited to): antivirus/antimalware, IDS, detect RAM usage, reverse engineer virus, social engineering/threat training, only accept website with proper certifications, use only HTTPS for web browsing, time stamps and sequence numbers.

## XIX. Topic: Mitigations

- What are some mitigation techniques your organization uses to isolate most-sensitive data/capabilities from attacks?

## DETECTIONS

### XX. Topic: Detecting Advanced Threats

In your organization's experience, against a complex entity/Advanced Persistent Threat (i.e. nation state or sophisticated criminal group), identify below what is the average time to detect a cyber-attack for each of the following categories?

- Denial of Service attack? (Seconds... weeks...)
- Virus or Trojan-based malware? (Seconds... weeks...)
- Web-based attack (XSS, session hijacking, etc.)? (Seconds... weeks...)
- Exploit: Breach incident (Seconds... weeks...)

### XXI. Topic: Detection Approach? Is it successful?

- What types of attacks are the most difficult to detect (e.g. Trojan horse, XSS, CSRF, DoS, etc.)?
- What type of detection approaches/technologies do you use?
- Do you consider your detection approaches to be current based on best practices? If not, what would you change to improve your defenses?
- In many cases a third party may detect a specific attack; what is your experience with third party detection?
- What are the various methods of detection when communications and operations are disturbed? How long do those methods take to detect the issue?
- What is your typical approach for improving your system after a successful breach to detect continuing/similar breach in the future?
- Microsoft indicates that there are methods to follow the trail of a breach, and that they isolate breached systems after a "detection" (with reduced privileges) to determine if an attacker is continuing the exploit or if other attackers may try. If you have a similar process, please explain it and identify any statistics available. Any lessons learned?

### XXII. Topic: Lag Times

- What is the lag time or known average (Weeks) time from compromise to initial discovery/detection? Shortest time to detection? Longest?
- What is the typical time from detection to initial defense/mitigation (Weeks)?
- What is a typical time from detection to defense/mitigation to where permanent security improvements are?



## FORENSICS AND ANALYSIS

### XXIII. Topic: Reliability of Analyses

- How reliable, accurate do you believe the final forensics reports are?
- Have you had any experiences where the forensics/analysis reports have been inadequate or misleading?

### XXIV. Topic: Analysis Tools and 3rd Parties

- Does your organization use in-house or third party tools for cyber forensics? What tools do you use, what are their capabilities (generally)?
- Does your organization use only in-house security personnel or do you use third party experts/analysts as well?
- Are there specific tools that you have found to be most helpful in analyzing a successful cyber-attack? What capabilities (generally) did those tools leverage?

### XXV. Topic: Organizational Priority for Forensics

- How does your organization react/adapt to important findings in the forensic report?
- Is there a specific review process to address relevant findings? If so, what is it?
- On average, do you believe report findings more often result in purchasing new security products or changes in policy/procedures?
- In your opinion, are the organization's attempts to address report findings successful? Why or why not?

### XXVI. Topic: Analysis of a Successful Attack

- Please identify your organization's approach to analyzing a breach.
- What evidence do you collect when conducting forensics and attack analysis?
- Do you engage third-party or outside consultants? If so, are there specific vendors you turn to (identify them if possible)?
- Any lessons learned?

### XXVII. Topic: Post Attack Analysis

- Does your organization conduct computer forensics?
- What is your forensic/analysis experience for various types of attacks: Delay; Deny; Degrade; Disrupt; Destroy; Deceive; Exploit?
- Do you create reference documentation for the analysis? If so, what do you include in it? What datasets are you capturing?

### XXVIII. Topic: Attribution

- Does your organization attempt to identify the source of an attack? If so, how well are you able to attribute to a specific threat actor (home country, government vs. criminal, etc.)?

## POST OPERATIONS

### XXIX. Topic: Operations after a Cyber Attack: Useful Operational Changes

- After attempt(s) or successful cyber-attacks, did you make any operational changes? Please describe.



- What were the changes you implemented?
- What type(s) of attack were the changes addressing?
- What was the timeline for implementation?
- How successful have those changes been?
- Any lessons learned?

**XXX. Topic: Operations After a Cyber Attack: What Else, What All?**

Any other details or comments on what is lost, gained, or changed in your organization as a result of a cyber-attack?

**XXXI. Topic: Operations after a Cyber Attack: Useful Organizational Changes**

- After attempt(s) or successful cyber-attacks, did you make any organizational changes? Please describe.
- What were the changes you implemented?
- What type(s) of attacks were the changes addressing?
- What was the timeline for implementation?
- Any lessons learned?

**XXXII. Topic: Operations After a Successful Cyber Attack: Adapting Operations**

How did your organization modify business processes to mitigate the adverse effects of future cyber-attacks? Have these modifications been successful? Why or why not?

## RECOVERY

**XXXIII. Topic: Recovery Best Practices**

What are the best practices for system recovery following a cyber-attack?

**XXXIV. Topic: Immediate/Short-Term Incident Response and Recovery**

- For immediate incident response (IR), how do you do you prioritize vital systems, how they should be fixed (recover, clean, re-image, destroy and replace etc.), and in what order?
- What types of considerations and decisions do you make for immediate IR and mitigations after a breach or other attack (specify)?
- Related, how does your organization determine the most important (damaging) effects of a cyber-attack, which must be addressed, as opposed to less important effects which may not need an immediate response?
- Who or what groups are involved in IR for your organization?
- What is your approach to removing the threat once it is in the network?
- How do you assure the network has been re-secured?

**XXXV. Topic: Advances in IR (Incident Response) Technologies**

- What are the most important advances in computer/network security that will take place in the next decade?
- What are some emerging technologies that support incident response and recovery?

**XXXVI. Topic: Importance of Recovery**

- What do you see as the important aspects of successful Incident Response (IR) and recovery?



### XXXVII. Topic: Continuing Business Operations Under Stress

- During an identified, ongoing cyber-attack, how do you adjust business operations (communications, planning, etc.) to continue providing your goods or service to customers? For example, do you have a backup method for conducting business operations? Please describe how you would adjust your operations.
- What kinds of cyber-attacks can these “adjusted business operations” compensate for (DDoS, failed servers, corrupted data, etc.)?
- When are these “adjusted business operations” activated? What kinds of decisions (and at what level of responsibility, e.g. C-suite, on-site manager, etc.) need to be made to switch to the “adjusted business operations?”

### XXXVIII. Topic: Long-Term Incident Response and Recovery

- For long-term remediation/recovery after the initial IR process, how do you decide which groups within the organization are involved, what to do, priorities, and timing?
- What types of considerations and decisions do you make for long-term improvements in the environment?
- What are your resources/approach to downstream consequences and recovery?
- Any lessons learned?

### XXXIX. Topic: Recovery Problems

- What can go wrong during a system’s recovery phase?
- What would the results/effects be?

### XL. Topic: Recovery Action Plans

What are the important considerations when developing a recovery action plan? What aspects of Incident Response are generally the weakest/strongest when that plan is carried out?

## TRUST RESTORTION

### XLI. Topic: Trust Restoration: Activities to Restore Trust

- What sorts of activities would you conduct to rebuild trust within your organization? With outside partners/clients/customers? How do you prioritize these activities?
- How/what information or artifacts (e.g., new credit cards) do you disseminate to others to restore trust?
- What is your estimate of the associated costs of these activities to regain trust in your organization (note: this is different from the cost of Incident Response and shutting down an attack)?

### XLII. Topic: Trust Restoration: How Long Does It Take?

- How long (weeks, months, years) does it take to restore trust with partners, clients, other organizations?
- Have you found a way to measure how much and when trust is restored? Please explain.

### XLIII. Topic: Trust Restoration: How Does a Cyber Attack Compromise Trust

- In your organization’s experience, how is trust compromised by cyber-attacks?

### XLIV. Topic: Trust Restoration: Organizational Challenges



- What general challenges does a breakdown in trust create for your organization?
- How does that trust breakdown affect achieving your mission?
- How does that trust breakdown affect communicating within your organization?
- When a breach occurs, to what extent are security personnel blamed for the incident (e.g. for negligence)? Does this shake the organization's trust in security personnel? If so, how is that trust regained?

## VULNERABILITIES

### XLV. Topic: Three Emerging Innovations with the Same Security Issue

### XLVI. Topic: Identifying Vulnerabilities

- What is your organization's general experience with identifying and addressing software/system vulnerabilities (has your security or IT department found any systematic vulnerabilities? Any lessons learned?)
- What are some typical vulnerabilities you've encountered? Are there specific vulnerabilities you look for? Are they mostly in applications or the broader environment (operating system, for example)?
- How often does the organization itself identify vulnerabilities (or breaches) and how often are they discovered by the third party?
- Are vulnerabilities more often found before or after a malicious actor uses them to breach the network?

### XLVII. Topic: Cloud Implementation

- Are there any security drawbacks in using the Cloud? If so, what are they?
- Are you using a public Cloud provider or running a private Cloud? If a public provider, how does that provider assure you that your data/services are safe? Do you find the argument credible?
- Are there any data/services you will not put on the Cloud? Why (sensitivity, accessibility, logistically/technically complex, legal ramifications, something else)?
- Based on your current experience, what lessons have you learned about using the Cloud? What guidance would you give others about using it?

### XLVIII. Topic: Ease of Access to the Network

- How would you characterize the ease of access to your systems/networks, either in the past or currently? If you know of iterations of recent updates to your environment, please identify.
- Ease of access is the time and resources an attacker uses to breach a network. If you know of successful breaches on an organization's, how would you rate the ease of access of the environment at the time? What, if any, subsequent improvements were made to the network?
- What other factors can affect the ability of attackers to succeed?
- Any lessons learned?
- The media has reported several instances of suppliers/vendors having broad access to a client's information systems, which later led to a breach (a la Target). Other considerations include when a company acquires another with poor cybersecurity. Please describe your organization's experience with access by vendors and vulnerabilities of acquired companies and the effect on your organizations security?



#### XLIX. Topic: Acquired Companies

- How has absorbing/purchasing other organizations into your own affected overall security?
- Has absorbing/purchasing another organization or company that has less security in their environment compromises yours? If so, what was the source of the weakened security (unpatched applications, poor employee cyber hygiene, server-level issues, etc.?)
- If there was weakened security, how did you mitigate and overcome it?
- What process changes would you make to not let it happen again?



## D. ACRONYMS

ACL	Access Control List
AD	Active Directory
ARP	Address Resolution Protocol
APDoS	Advanced Persistent Denial of Service
APT	Advanced Persistent Threat
ATC	Air Traffic Control
AWS	Amazon Web Services
AOR	Areas of Responsibility
BCP	Business Continuity Plan
BIA	Business Impact Analysis
CEO	Chief Executive Officer
CSP	Cloud Service Provider
COCOM	Combatant Command
C2	Command and Control
CAC	Common Access Card
CVE	Common Vulnerabilities and Exposures
COBIT	Control Objectives for Information and Related Technologies
COA	Course of Action
CSFI	Cyber Security Forum Initiative
CTI	cyber threat intelligence
DoS	Denial of Service
DoD	Department of Defense
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DDoS	Distributed Denial of Service
DNS	Domain Name Service
DAI	Dynamic ARP Inspection
FedRAMP	Federal Risk and Authorization Management Program
GPS	Global Positioning System
HCI	Human-Computer Interaction
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IR	Incident Response
IRP	Incident Response Plan
IOA	indicators of attack
IOC	indicators of compromise
ISAC	Information Sharing Analysis Center
ISACA	Information System Audit and Control Association





IS	Information Systems
IT	Information Technology
IADS	Integrated Air Defense System
ISR	Intelligence, Surveillance, and Reconnaissance
ISO	International Organization for Standardization
ICMP	Internet Control Message Protocol
IoT	Internet of Things
IP	Internet Protocol
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
LAN	Local Area Network
MAC	Media Access Control
NIST	National Institute of Standards and Technology
NSF	National Science Foundation
NDA	Non-Disclosure Agreement
OPM	Office of Personnel Management
OSINT	Open-Source Intelligence
OS	Operating System
OPFOR	Opposing Force(s)
PIV	Personal Identification Verification
POC	Point of Contact
PACE	Primary, Alternate, Contingency, and Emergency
PoW	Prisoner of War
RPO	Recovery Point Objective
RTO	Recovery Time Objective
RPN	Risk Priority Number
SIEM	Security Information and Event Management
SOC	Security Operations Center
SOC	Service Organization Control
SMS	Short Message Service
SOCINT	Social Media Intelligence
SP	Special Publication
SSAE	Statement on Standards for Attestation Engagements
SQL	Structured Query Language
SME	Subject Matter Expert
SDLC	System Development Life Cycle
TTP	Tactics, Techniques, and Procedures
TOR	The Onion Router
TRADOC	Training and Doctrine Command (US Army)
US	United States



ARCYBER	United States Army Cyber Command
US-CERT	United States Computer Emergency Readiness Team
UAC	User Account Control
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VAPT	Vulnerability Assessment and Penetration Testing



Source <https://www.flickr.com/photos/ganatlguard/14399103762/>