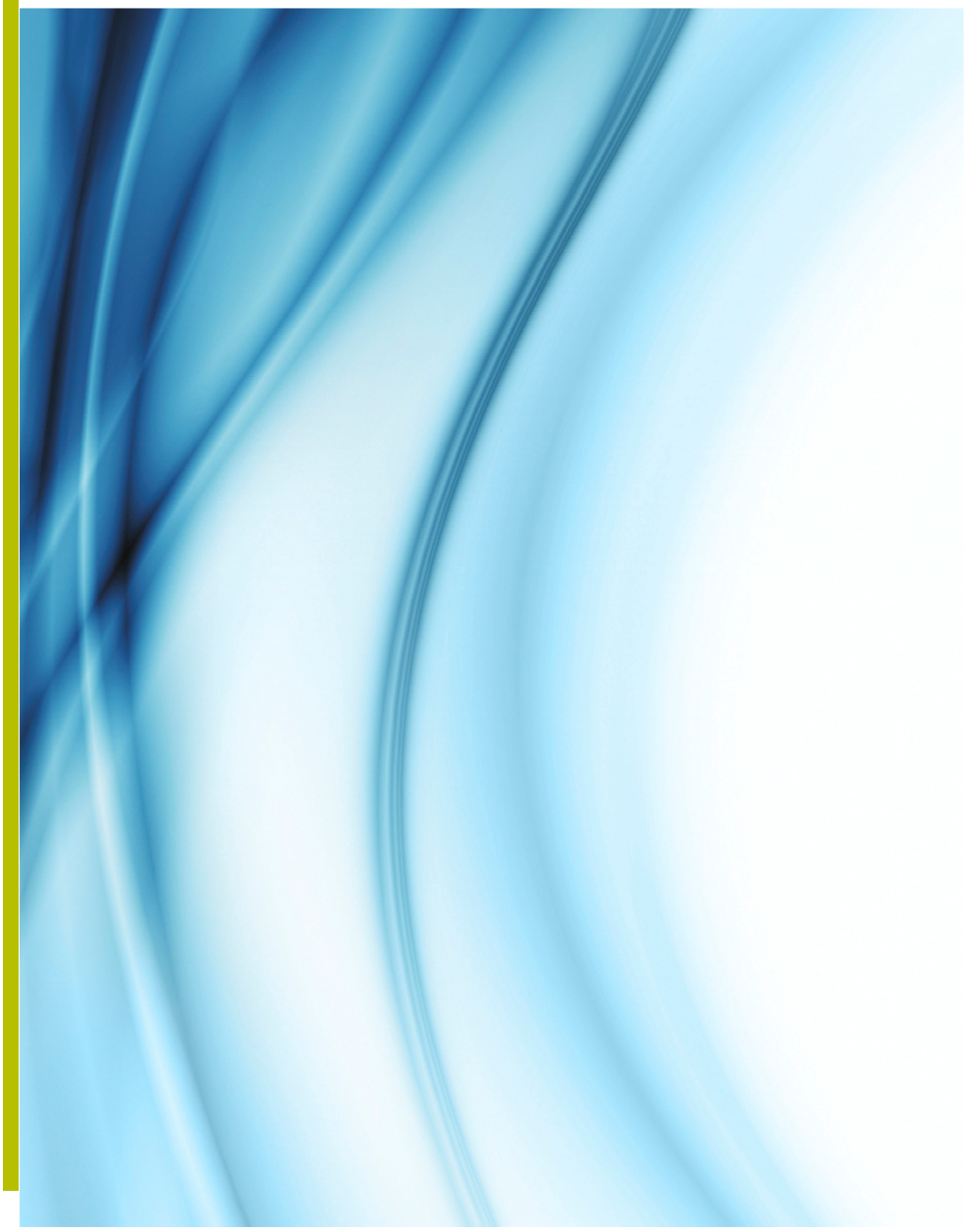
073011



Document Number: MTR170171
Authors: Suneel V. Sundar
Dr. David E. Mann

Location: Bedford, MA

November 2016

Effective Regional Cyber Threat Information Sharing

MITRE

This page intentionally left blank.

Table of Contents

List of Figures

List of Tables

Executive Summary

Cyber threat information sharing exchanges have traditionally formed within the context of industry sectors, either as direct peer-to-peer exchanges or within sector-based Information Sharing and Analysis Centers (ISACs).[1, 2] This has often been effective because organizations from the same sector tend to speak the same business language. They tend to have similar lines of business, hold similar digital assets, face similar cyber threats and have similar organizational practices. However, sector-based sharing organizations can face challenges to effective sharing. The Verizon 2015 Data Breach Investigations Report (DBIR) asserts that "our standard practice of organizing information sharing groups and activities according to broad industries is less than optimal." It then advocates "for more thoughtful and thorough research into risk profiles across various types of organizations."[3] This report contributes to that proposed body of research. Our assertions are based on two established MITRE research projects, Cyber Prep and Bilateral Analysis of Information Sharing Exchanges (BLAISE), and on empirical evidence of threat analysis and information sharing.

Our approach is to analyze the challenges to effective sharing in regional sharing organizations. Regional information sharing organizations, which are examples of Information Sharing and Analysis Organizations (ISAOs), offer the opportunity for face-to-face collaboration and the potential benefit of addressing threats that span sectors. [4] However, compared to sector-based, regional groups face additional challenges to effective sharing due to the diversity of the member organizations. Organizations from different sectors often have very different operating modes, hold very different digital assets, face different types of cyber threats, and have different organizational practices.

This report focuses on challenges to effective sharing in regional sharing organizations. Insights learned may also aid sector-based sharing organizations. In this way, this report seeks to provide managers and members of cyber threat information sharing organizations of both kinds with tools to manage the diversity among their membership in ways that maximize the benefits of diversity while minimizing the information sharing problems caused by that same diversity. To achieve this, we apply two MITRE-developed frameworks. The Cyber Prep Framework provides a way to describe how organizations differ from each other, both in terms of the threats they face and the defensive posture they employ, including operational practices, tools, priorities, and maturity.[5] The BLAISE methodology characterizes successful sharing strategies and matches strategies to exchanges, based on the operational diversity among the participants.[6] In particular,

---

[1] For the purposes of this report, we define cyber threat information to include information that exists relative to an attacker, including: threat actors; threat actor tactics, techniques, techniques and procedures (TTPs); indicators of compromise; exploit target; incidents; campaigns; and defensive courses of action.
[2] See https://www.isaccouncil.org/Home/Participation, accessed 2 November 2016.
[3] See 2015 Data Breach Investigations Report, Verizon. http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report_2015_en_xg.pdf, accessed 2 November 2016.
[4] See https://www.dhs.gov/isao, accessed 2 November 2016.
[5] See http://www.mitre.org/publications/technical-papers/cyber-security-governance, accessed 2 November 2016.
[6] See: Bilateral Analysis of Information Sharing Efforts: Determining the Expected Effectiveness of Information Sharing Efforts. By Mann, D., Shapiro, S. S., and Bodeau, D. (2014). *WISCS'14.* Scottsdale, AZ, USA: ACM.

BLAISE provides a structured approach to avoid two common mistakes in information sharing: first, to downplay the impact of social barriers such as non-aligned goals and lack of trust; and second, to rely on automation to overcome these barriers.

Applying Cyber Prep, we define and describe three categories of member organizations, which we refer to as preparedness groups, that are typically represented in regional sharing organizations:

- Vandalism: Members with a valuable Internet presence and who have capabilities to defend against adversaries who seek to embarrass or disrupt the organization or present the adversary's message publicly using simple attack tools.
- Theft: Members with monetizable digital assets and who have capabilities to defend against cyber criminals who seek to steal assets using known attacks with competent command and control capabilities.
- APT (Advanced Persistent Threat): Members with significant intellectual property or a specific mission. These members have capabilities to defend against advanced persistent attackers. Such attackers are motivated for the purpose of state-sponsored or industrial espionage, and have the ability to develop and use new attacks.

Applying BLAISE, we recommend three approaches for managing the diversity within regional sharing organizations:

1. Intentionally limit the diversity among its members by specializing membership to a single preparedness group (Vandalism, Theft, or APT). This approach has the potential of facilitating meaningful sharing of structured intelligence reports to increase situational awareness among the members who are "birds of a feather" and may be matured to support automated sharing.
2. Intentionally limit the detail to be shared. Refrain from attempts to facilitate automated sharing or the sharing of structured intelligence reports. Instead, facilitate effective collaboration among the diverse membership—provide human-to-human communication channels, build readiness and trust among the membership through mediated face-to-face meetings and tabletop exercises.
3. The third and most ambitious approach is to combine the two approaches above. Organize the membership into sub-groups, each organized according to threat. Then, facilitate the regular, high-detail sharing of threat intelligence among each of the groups separately. The sharing organization can also facilitate effective ad hoc collaboration across preparedness group lines by providing communication channels and through readiness and trust building activities which include face-to-face meetings and tabletop exercises.

We conclude by describing potentially feasible sharing activities for each of the three preparedness groups.

1 Overview

The sharing of threat and incident information has become a critical cybersecurity practice for organizations. It allows organizations to gain increased visibility and awareness of the cybersecurity threats they face. This creates greater situational awareness, which in turn, engenders better informed risk decision making.

Cybersecurity threat information sharing is often facilitated through involvement in sector-based consortiums. Information Sharing and Analysis Centers (ISACs) are one prominent type of such sector-based information sharing organizations. For example, there is an Aviation ISAC (A-ISAC) and a Financial Services ISAC (FS-ISAC). The sector-by-sector organization of ISACs has the advantage of facilitating information sharing among organizations that tend to have similar missions, similar needs, and that face similar threats. However, not all members of an ISAC face the same kind of threats. Additionally, sector-based sharing agreements face the myopia of deep insight on domain-specific threats but failure to see trends that cut across sector boundaries.

A new generation of cybersecurity threat information sharing organizations has emerged in recent years to expand and build upon the sharing done in sector-based organizations. For example, the U.S. Department of Homeland Security (DHS) has been actively promoting the development of new Information Sharing and Analysis Organization (ISAOs).[7] In particular, the recent emergence of region-based cybersecurity sharing organizations represents a fundamentally different approach. As the name implies, regional sharing organizations are first and foremost regional, which makes regular face-to-face meetings and collaboration feasible. Additionally, since membership is based on geography instead of commercial sector, regional sharing organizations break down some of the institutional barriers imposed by sector-based approaches. In particular, locality may facilitate face-to-face interaction among members, which can engender trust. This promotes the cross-fertilization of ideas and approaches and can help defend against sector-biased "group-think." Examples of regional sharing organizations include the New England area Advanced Cyber Security Center (ACSC), the Mid-Atlantic Cyber Center, the Rocky Mountain region Western Cyber Exchange, and the California Cybersecurity Information Sharing Organization (CalCISO). [8, 9, 10, 11]

The sector diversity among participating organizations is a key resource and advantage for regionally-based sharing organizations. However, this sector diversity can undermine information sharing efforts. Organizations from different sectors often have different business processes, face different types of threats and as a result, tend to have different cybersecurity practices. Thus, to get the benefits of sector diversity in regional sharing organization, managers and members alike need to manage that diversity in ways that facilitates effective sharing.

---

[7] See https://www.dhs.gov/isao, accessed 2 November 2016.
[8] See http://www.acscenter.org/, accessed 2 November 2016.
[9] See "Mid-Atlantic Cyber Center Services & Programs Founding Partners", The MITRE Corporation, PRS 16-4014, 2016.
[10] See http://www.wcyberx.org/, accessed 2 November 2016.
[11] See http://www.californiatechnology.org/calciso/, accessed 2 November 2016.

This is the challenge facing managers and members of regional sharing organizations: how can they effectively manage the organizational diversity among their membership in a manner that a) realizes the benefits of sector diversity without b) running afoul of the communication roadblocks that greater diversity can create?

The purpose of this report is to provide managers and members of regional sharing organizations with tools to manage the diversity found in regional sharing organizations so as to achieve and sustain more effective cybersecurity threat sharing. Additionally, while we focus our attention on regional sharing organizations, we hope the approaches described can aid sector-based sharing organizations in recognizing and managing diversity among their membership. We do this by applying two MITRE-developed frameworks—the Cyber Prep Framework, which gives us a way to describe the diversity seen in the membership in regionally based sharing organization and the Bilateral Analysis of Information Sharing Efforts (BLAISE) methodology, which gives us ways to optimize information sharing efforts based on the diversity of participants.

The Cyber Prep Framework provides two central insights. First, different organizations face different kinds of cyber threat. Some primarily need to defend against cybercriminals who seek to steal monetizable digital assets while others must defend against nation-state attackers who seek to establish long-term campaigns of digital espionage. The second insight of Cyber Prep is that an organization's cyber-defensive strategy should be commensurate to and optimized for the kind of threat the organization faces. Different types of threat demand different types of cyber preparedness. The full Cyber Prep Framework discusses a comprehensive set of aspects of both attackers and defensive cybersecurity management program.

In Section 2, we give a short overview of the Cyber Prep Framework, which defines five Cyber Prep classes. We then synthesize Cyber Prep with findings based on interviews with stakeholders from regional sharing efforts which leads us to define three "preparedness groups" that can be expected to be found in regional sharing organizations—the Vandalism group, the Theft group, and the Advanced Persistent Threat (APT) group.

In Section 3, we apply Cyber Prep directly to threat information sharing. We focus on the most prevalent preparedness groups in regional sharing organizations, the Theft and APT groups, and establish that the associated defenders and attackers are fundamentally different. Based on these differences, we identify several differences in their motivations and goals with respect to cyber-threat information.

In Section 4, we give a brief overview of MITRE's BLAISE methodology, which was created to assist designers of information exchange systems. BLAISE defines four kinds of exchanges: automated machine level information sharing, structured human expert-level information sharing, ad hoc organizational-level collaboration, and indirect mediated translation. A central insight of BLAISE is that there is a tradespace relationship between the level of automation and detail that can be supported in an information exchange and the amount of diversity among the participants. We use this to discuss how information sharing efforts tend to fail and the conditions required to achieve successful sharing efforts.

In Section 5, we apply the BLAISE information sharing insights to the three preparedness groups derived from the Cyber Prep Framework to provide recommendations on structuring information exchanges in regional sharing groups. We describe three basic approaches for structuring successful regional sharing efforts:

- Accept members from all three preparedness groups and limit exchanges to collaborative efforts.
- Accept members only from either the Theft or APT preparedness groups and structure the sharing efforts to optimally support that group.
- Accept members from all three groups and concurrently offer separate sharing capabilities for the Theft and APT groups while also providing support for collaboration and mediated translation efforts to the whole membership.

We conclude by giving specific recommendations for information publication and sharing activities for each of the three groups that are potentially feasible and sustainable.

In Section 6, we provide a short concluding discussion and discuss possible extensions to this approach to other types of sharing groups as future work.

Finally, Appendix A describes a set of metrics that organizations can use to determine which preparedness group is the best way to describe their organization relative to threat information sharing efforts.

2 Cyber Prep and Regional Sharing Organizations

The key for constructing feasible and effective information sharing is identifying organizations that have operational practices that are similar enough to sustain the exchange. Industry sector, on its own, is not particularly helpful in this regard. While it is true that most organizations in the same sector may be able to communicate effectively, it is also true that some organizations from other sectors may also have cybersecurity practices that are close enough to be able to effectively share information. To realize the potential of facilitating effective cross-sector sharing, managers and members of regional sharing organizations need ways of recognizing organizations that have a high potential for effective sharing.

MITRE's Cyber Prep Framework provides us with a way of categorizing organizations based on the similarity of the cyber-defense strategy and posture; what we refer to as the organization's cyber-preparedness.

MITRE's Cyber Prep Framework asserts that organizational processes and preparedness can be understood according to the level of threat that the organization faces. It describes five levels of threat and five corresponding appropriate types of cyber defense posture, which is summarized in Figure 1.

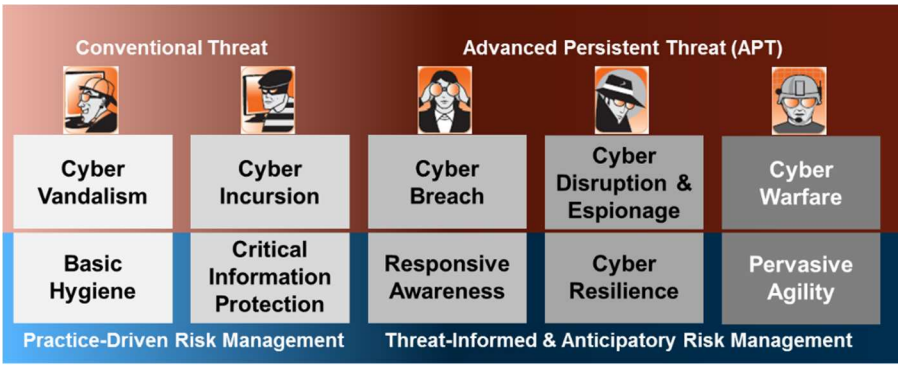


Figure 1. Cyber Prep Framework

Cyber Prep asserts that these defensive postures should be matched to the corresponding level of threat. It is possible to have too much of a good thing. A defensive posture that is not warranted by the level of threat actually faced by the organization imposes an unwarranted financial burden, which is a business risk. And of course, it is possible (and more common) to have a security posture that is inadequate for the threat.

Based on a series of interviews and qualitative research, we observe that organizations participating in regional sharing organizations can be grouped into three major groups, which can be mapped directly onto the Cyber Prep categorization. While these initial results need to be further validated through ongoing engagement with organizations involved in cyber-threat information sharing, we believe the initial results are strong enough to warrant the categorization.

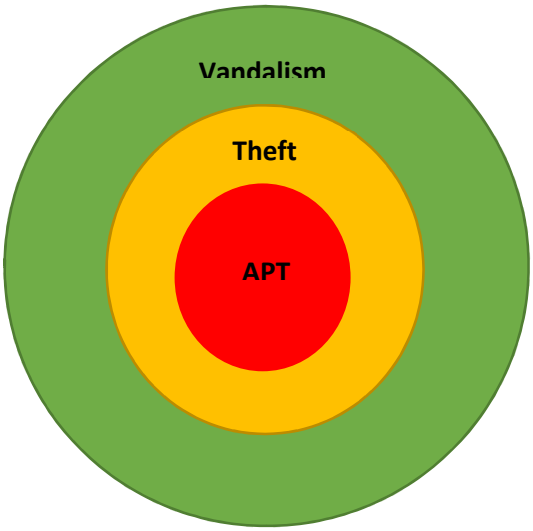


Figure 2. Preparedness Groups

The first group is the Vandalism group, which corresponds directly to the Cyber Prep Cyber Vandalism group. The highest threat faced by members of this group are to their Internet-accessible assets. They face attacks resulting in denial-of-service, including ransomware, and website defacement. Such attacks require comparatively little skill to execute. We believe that this group remains relevant for regional sharing organizations but we also believe that countermeasures to Vandalism acts are well-shared across the community. First, the greater adoption of standard security best practices, also called Cyber Hygiene, such as the Center for Internet Security (CIS) Critical Security Controls, ameliorate the majority of the threat posed by the Vandalism attacker.[12]

[12] See https://www.cisecurity.org/critical-controls.cfm, accessed 2 November 2016.

Second, monetizable information assets are more ubiquitous in organizations, so more sophisticated Theft attackers threaten more organizations. That is, basic cyber hygiene is no longer sufficient for many organizations. Third, there is a self-selecting aspect to membership in regional sharing organizations. Namely, organizations who commit resources to threat information sharing have typically already moved beyond basic cyber hygiene and conversely, organizations that correctly limit their cybersecurity investments to basic hygiene may be unlikely to commit significant resources to engage in sharing organizations.

We refer to the second group as the Theft group, which corresponds to Cyber Prep's Cyber Incursion and Cyber Breach groups. Members of the Theft group are actively attacked by competent attackers who are primarily interested in stealing information assets that can be monetized. While these attackers have a high degree of competence, they differ from more advanced attackers in that long-term presence on the victim's network is not required to accomplish the Theft actor's ends. We believe that a significant number of potential members of regional sharing organizations are in this preparedness group.

The third group is the APT group. This is a union of the Cyber Disruption and Espionage and Cyber Warfare groups in Cyber Prep. While we recognize the meaningful differences in these Cyber Prep categories, we believe that the operational practices among them are close enough to make effective sharing feasible. We also believe that it is currently impractical for regional sharing organizations to attempt to facilitate sharing across five groups.

We emphasize a point made in Cyber Prep. These groups (either Cyber Prep's five groups, or our proposed three) should not be viewed as levels. In Cyber Prep, it is not assumed that members of Cyber Incursion group should aspire to be in the Cyber Breach group. In like manner, in our simplified model, members of the Theft group should not aspire to be in the APT group. Instead, organizations should correctly invest in cybersecurity at levels that are commensurate to the threat they face. Overspending on cybersecurity in ways that can't be justified by the threat is a business risk, just as underspending is. However, attackers will use less sophisticated exploits whenever they can to penetrate a target; consequently, APT defenders must be able defend against Theft and Vandalism tools, techniques and procedures (TTPs), and Theft defenders must be able to defend against Vandalism TTPs. It is also an operational risk when organizations divert finite resources away from programs that are critical to defend against their real threat and towards cyber capabilities that can only be justified by a more aggressive threat.

We encourage information sharing organizations to embrace the distinctions between the three preparedness groups within their members as something that is to be expected, appropriate, and even as best practice. Information sharing organizations should explicitly describe the different levels of cyber preparedness and work with their membership to identify which preparedness group makes the most sense for them from the perspective of

managing their risk and then to consider constructing different sharing programs for the different groups.

With the basic differences of the three preparedness groups described, we now consider the differences in these groups in more detail.

3 Cyber Prep Analysis of Regional Sharing Organizations

Cyber Prep is informed by the National Institute of Standards and Technology (NIST) Cybersecurity Framework and correspondingly recognizes a broad range of threats and defensive controls. Given our observation that the Theft and APT groups tend to be more prominent in regional sharing groups, we emphasize distinctions between their associated defenders and attackers.[13] We then discuss how these distinctions inform different sharing practices for the Theft and APT groups.

3.1 Key Differences between APT and Theft Preparedness Groups

Defender organizations in the APT group possess proprietary intellectual property (IP) assets that are specifically targeted as the subject of espionage. The attackers who steal this IP are typically nation-states or large corporations who are motivated to obtain a long-term strategic advantage over the defender. The attacker does this by establishing a long-term and persistent capability to find and exfiltrate the targeted IP; hence the name, Advanced Persistent Threat.

In contrast, defender organizations in the Theft group have monetizable digital assets. The attackers who target organizations in the Theft group are criminals who are motivated by money, ranging from loosely organized criminals of opportunity to robust organized crime organizations. Because money is money no matter who holds it, the attackers associated with the Theft group target their victims according to a straight-forward cost/benefit decision, seeking the biggest return for the least effort and risk. The goal of the attacker is to steal the monetizable assets, with minimal expense and without being caught.

The attackers associated with the APT group are very well-funded, as the nation or corporation who supports them is highly motivated to obtain the targeted IP. They have the strategic discipline to take a long-term view of their attack and to develop and manage complex, multi-stage coordinated attacks referred to as campaigns. Their attack tactics are complex, often revealing aspects of tradecraft that are recognizable and attributable to the specific attacker. The APT attacker has the ability to develop or obtain previously unpublished "0-day" attacks and often tailors the exploit to the victim. Defenders in the APT group will typically track the campaigns and tactics used by the APT attacker and will strive to tailor their defenses to counter the specific campaign tactics used by the specific attackers who are trying to steal their specific IP. However, the APT attacker is sophisticated enough to have significant counter-intelligence capabilities and works hard to determine if their tactics have been discovered by the victim. As a result, the defenders

[13] See http://www.nist.gov/cyberframework/, accessed 4 November 2016.

in the APT group are motivated to closely protect their knowledge of the attacker's tactics for fear that the attacker will change their tactics, making it harder to defend against them.

In contrast, the funding level of the cybercriminals associated with the Theft group varies but is considerably lower than nation or large corporate funded espionage attackers. They have enough strategic discipline to execute technically difficult attacks but they do not aspire to maintain a persistent presence on the defender's network. Instead, they tend to reuse proven "smash and grab" attacks on multiple victims. The technical sophistication of their attack tactics require competence but they typically lack the ability to develop or acquire 0-day exploits. Instead, they rely on tactics that are well known and exploits that are publicly available on hacker sites and they typically only minimally adapt them to a defender's context, if at all. The Theft group defender's strategy might be described as "commercial-grade," as they typically rely primarily on commercially provided defenses that are designed to defend against known attacks and exploits. In response, the attackers do not invest in any significant amounts of counter-espionage, as they can assume that both their attacks and exploits are known. Instead, they primarily rely on the defender having inadequate defenses.

Table 1. Differences between the APT and Theft Threat Groups

		APT	Theft
Defender Motivation	Primary Assets	Specific intellectual property or mission	Monetizeable assets
Attacker Motivation	Targeting	Specific victim holding specific IP assets	Any victim with monetizable assets
	Identity	Nation state or large corporation	Organized crime or opportunistic criminals
	Goal	Persistent exfiltration of IP	Steal monetizable assets while avoiding prosecution
Attacker Capability	Funding	Millions of dollars	Thousands of dollars
	Exploits	Tailored to victim (including 0-day attacks)	Known and publicly available
	Counterintelligence	Yes	No
	Tactics	Complex and distinct to attacker	Routine and used by many attackers
	Strategic Sophistication	Multi-stage, coordinated campaign	Single attack technique used on multiple victims
Defender Capability	Strategy	Threat informed	Commercial grade

3.2 Implications for Sharing

The differences between the Theft and APT preparedness groups lead to very different goals for cyber threat information sharing. Defenders in the APT group are motivated to enter into sharing agreements in the hopes of learning about specific campaign techniques and tactics used by the specific nation state or corporately-backed attacks who target the

specific IP held by the defender. They seek to obtain machine-consumable detection signatures and suggested courses of action (COAs) associated with new, 0-day exploits, as these are not available from their commercial vendors. They seek to improve situational awareness for their threat analysts and other risk-oriented decision makers by obtaining information about campaign tactics that are attributed to specific attackers. They seek opportunities to collaborate directly with peer organizations to develop campaign information and to coordinate on incident response activities on campaigns that span multiple victims. Because APT attackers are known to have competent counterintelligence capabilities, APT group defenders demand an extraordinarily high degree of trust with their sharing peers to prevent the attacker from learning that their current tactics have been discovered.

In contrast, the goal of defenders in the Theft group is to stay informed of publicly known exploits. They seek to obtain trustworthy machine-consumable signatures for known exploits to augment their commercial defenses. They seek to improve situational awareness by staying abreast of time-sensitive criminal attack trends, including "be on the lookout" (BOLO) alerts and reports of confirmed sightings of attack of interest. They seek to collaborate with peer organization in learning about trends in cybercrime and in incident response activities involved with attacks that involve multiple defender organizations. While Theft group defenders are less concerned with disclosure, since the attacks and tactics of the attacker are already known. The defenders are motivated by effective quid pro quo in the sharing relationship. Generating shareable information costs both money and labor.

Table 2. Examples of Differences in Sharing between the APT and Theft Groups

	APT	Theft
Knowledge Goals	Specific campaign TTPs for specific attackers	State of art of publicly known exploits
Trust	"Classified" to prevent leaking information to attacker	Requires quid pro quo
Machine Sharing	Signatures and COAs for unknown 0-day exploits	Signatures for commoditized exploits
Human Sharing	Campaign TTPs attributed to relevant identified attackers	"Crime wave" situational awareness, specifically BOLOs and confirmed sightings
Organizational Collaboration	Campaign development and "classified" incident response	Cybercrime trends and "non-classified" incident response

4 BLAISE and Regional Sharing Organizations

Operators of regional sharing organizations must make three core decisions—who will share information with each other (diversity), what will they share (detail), and how will they share it (mode)? These questions of who, what, and how are closely related and

understanding these relationships is critical in shaping successful sharing efforts. In particular, the most common form of failure of information sharing efforts occurs when groups who are too diverse in terms of their operational practices attempt to share information that is too detailed. A primary success factor for successful information sharing efforts is achieving the appropriate balance between the amount of detail of what is shared and the diversity of those who are involved. Once this balance is achieved, the question of how they share is straight-forward.

The question of what is shared can be characterized in terms of the amount of "detail" captured in the shared information. By detail, we primarily mean the amount of formal structure which ranges from fully structured database transactions, to semi-structured reports (e.g., medical records, police reports), to unstructured reports enhanced with shared ID schemes (e.g., directions typically refer to standard street names and route numbers), to entirely unstructured exchanges (e.g., conversations). Detail also includes the amount of professional jargon that is used. A cyber threat report can be as inscrutable as any professional document for a niche audience: a legal brief, a medical journal, or an end-user license agreement (EULA).

The relationship between the detail of what is shared and how information is shared is direct—the more highly structured the information is, the more that automation technologies can be used to facilitate the information exchange. We identify three primary modalities of information sharing:

- Automated Machine-to-Machine Information Sharing
    - Information Products - Machine consumable
    - Level of Automation - Automated transfer, ingest and processing
    - Examples - Actionable indicators of compromise (IOCs) such as machine consumable signatures
- Structured Human Expert Information Sharing
    - Information Products - Structured but human readable, like medical records
    - Level of Automation - Digital capture and transport
    - Examples - Cyber threat event alerts, malware threat event alerts, analytic recipes
- Human and Organizational Level Collaboration
    - Information Products - Diverse written notes and communications; may be augmented with shared vocabularies
    - Level of Automation - Supported by digital communication channels such as email or chat
    - Examples - Round-table meetings, joint exercises, ad hoc incident response activities

There is a fourth modality of information sharing called Mediated Translation, which we motivate by example: Doctors create medical records. Claims are processed by insurers, who produce Explanation of Benefit (EoB) reports for patients. The work of insurance claims processors is based on information produced by doctors and captured in medical records. But doctors do not share medical records with insurance companies. Instead, the

doctor's office has a medical billing office, which takes the medical records and translates the information into a form that can be used by insurance claims processors. We refer to capabilities such as medical billing as "mediating translators" because their work facilitates an information exchange between two groups that cannot be sustained through direct information sharing. The 2013 white paper, "APT1: Exposing One of China's Cyber Espionage Units" written by the private cybersecurity firm Mandiant (since acquired by FireEye) is an example of mediating translation, as the authors of the paper took information that was only comprehensible to elite cyber analysts and translated it in a manner that would be comprehensible to other audiences such as policy makers.[14]

The relationship between what is shared (detail) and how it is shared (mode) is direct and straightforward. The more detail that can be agreed upon, the more automated technologies can be used to facilitate the information exchange. Achieving agreement on automation and technologies does take work but it is generally achievable provided the parties involved agree on the level of detail to be shared. What is to be shared (detail) drives the discussion of how (automation).

However, the relationship between what is to be shared (detail) and who will be sharing (diversity) is typically much more contentious and most often the reason that information sharing efforts fail. BLAISE is based on a sociologically based understanding of communication. It defines five related but separable factors that are related to how people work and their ability to trust another group. The factors of diversity are:

- Factors related to workplace practice
    1. Professional Ambiguity: Measures the amount of ambiguity in the group's professional work
    2. Internal Diversity: Measures the degree to which the work practices in each group are the same or different
    3. Comparative Diversity: Measures the degree to which work practices of the groups are the same or different from each other
- Factors related to trust and value
    4. Cooperative Resistance: Measures the degree to which a group supports or resist the collaboration with the other group
    5. Process Novelty: Measures the degree to which the information exchange and the processes that support it are new, or conversely, the degree to which they have been codified in the group's work practices.

The relationship between what is shared and who is sharing is that groups can only agree on high levels of shared detail (and highly automated sharing) if their operational work practices are similar – that is, if they have: little professional ambiguity in their work, little diversity in how they work, a strong commitment to share, and established sharing practices. Conversely, if groups are diverse in terms of their operational practices or if they don't trust the sharing relationship, they cannot agree on high levels of detail and thus cannot sustain automated sharing.

[14] See https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf, accessed 29 November 2016.

The BLAISE framework for understanding work practice diversity provides us with a means of understanding the root cause of sharing problems reported participants in sharing groups. First and most importantly, the three groups face different threats and correctly have different defensive priorities. For example, members of the APT group track threat actor campaigns and members of the Theft do not (and should not, as doing so diverts resources from their primary threat). In BLAISE terms, the groups have a high degree of Comparative Diversity. As a result, they cannot agree on what kind of information is the most important to share with each other.

The Theft and APT preparedness groups also display a high degree of Cooperative Resistance. Members of the APT group correctly distrust the operational security practices of the Theft group and resist sharing information with them for fear of information leaking out to the APT threat actors.

We describe these relationships in the following diagram. Optimal information sharing efforts occur along the diagonal boundary and appear only if the proper balance between what is shared (detail) and who is sharing (diversity) is maintained.

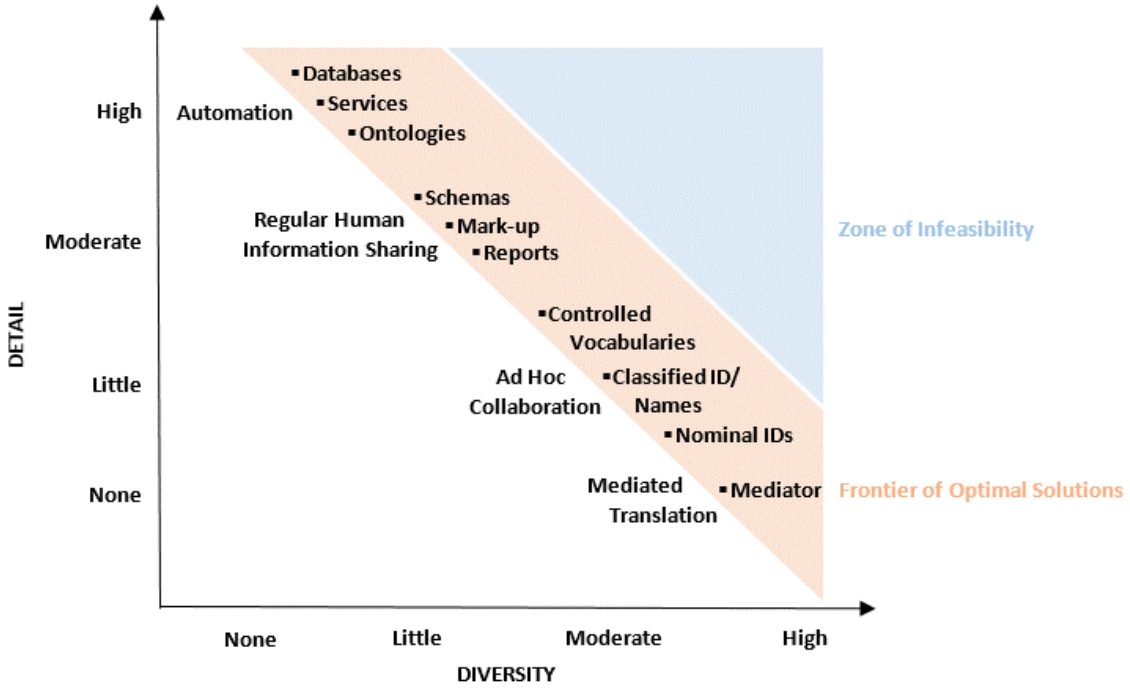


Figure 3. The Diversity/Detail Tradespace

There are two primary implications of this characterization of information sharing modalities for regional sharing organizations. First, this characterization makes clear the primary mode of failure in information exchanges; namely trying to share too much detail among stakeholders who are too diverse. Failure is not only an option; it is commonplace among sharing efforts.

Second, this characterization highlights the two primary methods for making an information sharing initiative work. Limit the amount of detail shared, or limit the amount

of diversity (in terms of operational practices) of those involved. And even then, this characterization makes clear that there are some professional groups that cannot effectively share information directly.

Initial engagements with regional sharing organizations indicate that it is common for them to have members from all three preparedness groups. This means that the operational diversity among the membership is higher than various "birds of a feather" type of sharing organizations that tend to form along industry sector lines. The diversity of opinions and experiences found in regional sharing organizations can be a resource, but designers of the sharing efforts must find ways to define and manage that diversity so as to make sharing effective.

A primary approach, therefore, is to define subgroups within the sharing organizations based on preparedness group, as this helps ensure that operational practices are more closely aligned. If subgroups of this nature can be identified, then more detailed sharing within these groups can be facilitated and more detailed forms of sharing among the groups can be considered.

5 BLAISE Analysis of Regional Sharing Organizations

The first and most important recommendation for regional sharing organizations is to recognize that their members (or pool of potential members) can be grouped into three groups—the Vandalism group, the Theft group, and the APT group. With respect to information sharing, these preparedness groups should be considered to be distinct. These differences, if left unrecognized and thus unmanaged, can easily place a regional sharing organization deep in the zone of infeasibility; the hallmark of which is irreconcilable differences on what and how to share.

There are two ways to get out of the zone of infeasibility: reducing diversity or reducing detail. This leads to three primary recommended strategies for regional sharing organizations. The first is to intentionally reduce the amount of diversity among its members by focusing on a single preparedness group (Vandalism, Theft, or APT) and restricting membership in the sharing organization to organizations in that preparedness group. This approach will facilitate meaningful sharing of structured intelligence reports to increase situational awareness among the members. With effort, this approach may mature to support automated sharing.

The second approach is to intentionally reduce the level of detail to be shared. This can be achieved by focusing on providing (human-to-human) communication channels and building readiness and trust among the membership through face-to-face meetings and table-top exercises. Defer on automated sharing and even ongoing sharing of structured intelligence reports. Instead, focus on facilitating effective collaboration among the diverse membership.

The third and most ambitious approach is to combine the above. Organize the membership into three (or two, depending on the membership) subgroups, each organized according to preparedness group. Then, facilitate the regular, high-detail sharing of threat intelligence among each of the groups separately. Additionally, the sharing organization can facilitate

effective ad hoc collaboration across subgroups by providing communication channels and through readiness and trust building activities like face-to-face meetings and tabletop exercises.

We raise an important caveat regarding our categorization into preparedness groups. An organization's defensive capabilities should directly and accurately match the level of threat that they face. In practice, this is not always the case. On the one hand, as financial and human resources are typically too precious to permit unjustified cybersecurity expenditures, it is relatively uncommon for an organization's defensive posture to be significantly greater than the threat it faces. It is more common for organizations to underspend on cybersecurity and for their defensive capabilities to be inadequate to defend against the threat they face. In these latter cases, we recommend that the organization raise its level of cybersecurity preparedness so that it can effectively be peer in sharing activities with others who face similar threats. Until that time, the organization will be an ineffective member of the preparedness group, and detrimental to threat information sharing. For this reason, we recommend that organizations be grouped primarily based on the capabilities they demonstrate, not on the threat they face, as a means of enabling better sharing. In particular, we do not recommend placing an organization into a preparedness group in a sharing organization in the hopes that the experience will help educate them. Education and improvement may result from involvement in a sharing organization, but education is not the primary goal of a sharing organization. Sharing is.

With the above caveat noted, recognizing the differences in the preparedness groups (assets, attackers, defensive strategies, and operational capabilities) provides the basis for developing more detailed concepts of operations (CONOPS) for information sharing efforts among members of the same group. Thus, our final recommendation is to develop these CONOPS, particularly for the Theft and APT groups.

As a first step towards developing more formal CONOPS, we provide recommended sharing strategies for each of the preparedness groups in the following sections. For each preparedness group, we describe the recommended information exchanges in terms of publication or participation and not in terms of consumption. Experience shows that publication of shareable information is the most important first step. Because sharing within a single preparedness group is fundamentally different than sharing across preparedness group boundaries, we consider both separately. Note, successful participation in automated machine sharing and structured human sharing is dependent on the participation of competent staff within particular operational capabilities.

5.1 APT Preparedness Group: Recommended Information Sharing

Sharing information about the APT threat carries a large risk that the information will be leaked, which will allow the APT attacker to learn they are known and being monitored, which in turn will cause them to change their behaviors. For this reason, members of the APT group will only share with established, trusted partners. With this noted, a member of the APT group may be able to publish and share the following with other members of the APT group:

- Automated Machine Sharing
  - Validated indicators of compromise associated with potential 0-day attacks (e.g., Intrusion Detection System [IDS] signatures)
  - Recommended COA
- Structured Human Sharing
  - Malware analysis results
  - Event alerts associated with suspected 0-day attacks
  - Attacker analysis (e.g., identity and techniques)
  - Analytic recipes
  - Campaign information
- Ad Hoc Collaborations
  - APT-oriented joint incident response activities
- Mediated Translations
  - State of the art best practices (e.g., active defense techniques, advanced malware analysis).

Members of the APT group do not have established trust with members of the Theft and Vandalism groups. However, there will be circumstances in which the APT group members will determine that the benefits of promiscuous sharing will outweigh the potential risks; the aforementioned "APT1" white paper is an instance. In such a case, a member of the APT group may publish and share the following with members of the Theft and Vandalism groups:

- Automated Machine Sharing
  - Validated indicators of compromise associated with known attacks
- Structured Human Sharing
  - BOLO requests
  - Requests for information (e.g., Have you seen this?)
  - Malware analysis results associated with known malware
  - Event alerts associated with known attacks
- Ad Hoc Collaborations
  - None identified
- Mediated Translations
  - APT lessons learned out-briefs
  - Theft-oriented joint incident response exercises.

5.2 Theft Preparedness Group: Recommended Information Sharing

Theft attackers and Theft defenders are in a race situation when new vulnerabilities or attacks become known publically. Attackers attempt to develop or obtain attack tools to exploit the new vulnerabilities while defenders wait for patches to be developed, tested and deployed. Members of the Theft group are motivated to share with each other to augment their security products while they wait for their security product vendors to

respond with updates. Members of the Theft group may be able to publish and share the following with other members of the Theft group.

- Automated Machine Sharing
  - Validated indicators of compromise associated with known attacks (e.g., IDS signatures)
  - Recommended COAs (Consumers will never execute a COA without some approval process.)
- Structured Human Sharing
  - BOLO requests
  - Requests for information (e.g., Have you seen this?)
  - Malware analysis results associated with known malware
  - Event alerts associated with known attacks
- Ad Hoc Collaborations
  - Theft-oriented joint incident response activities
- Mediated Translations
  - State of the art Theft-oriented best practices
  - Theft-oriented joint incident response exercises.

Members of the Theft group will typically have no reservation with sharing information outside of their preparedness group with respect to divulging information to the attacker. However, they will have reservations about sharing if there is not enough quid pro quo. Which is to say that if they perceive that they are submitting useful information while others are not, they will be less motivated to continue the in the sharing relationship. This is more of an issue in sharing information with members of the Vandalism group who may not be able to share at the same level in return. Members of the Theft group may be able to publish and share the following with members of the APT and Vandalism groups:

- Automated Machine Sharing
  - Validated indicators of compromise associated with known attacks (e.g., IDS signatures)
  - Recommended COA (Consumers will never execute a COA without some approval process.)
- Structured Human Sharing
  - BOLO requests
  - Requests for information (e.g., Have you seen this?)
  - Malware analysis results associated with known malware
  - Event alerts associated with known attacks
- Ad Hoc Collaborations
  - Theft or Vandalism-oriented joint incident response activities
- Mediated Translations
  - State of the art Theft-oriented best practices
  - Theft or Vandalism-oriented joint incident response exercises.

5.3 Vandalism Preparedness Group: Recommended Information Sharing

A member of the Vandalism preparedness group may be able to publish and share the following with other members of the any preparedness group.

- Automated Machine Sharing
  - None identified
- Structured Human Sharing
  - Requests for information (e.g., Have you seen this?)
  - Event alerts associated with known attacks
- Ad Hoc Collaborations
  - Vandalism-oriented joint incident response activities
- Mediated Translations
  - Vandalism-oriented joint incident response exercises.

6 Conclusions and Future Work

We have applied two MITRE frameworks to the question of how to better manage regional sharing organizations to achieve more effective sharing. The first, Cyber Prep, asserts that organizations can be categorized according to the kinds of cyber threats they face. Organizations that face similar cyber threats tend to have similar cyber defensive postures. While Cyber Prep defines five different categories, interviews with threat analysts involved in sharing led us to simplify to three groups—the Vandalism group, the Theft group, and the APT group. Of these three, the most common are the Theft and APT groups. The second framework, BLAISE, asserts that there is a fundamental trade-off between the amount of diversity (in terms of organizational practices) among sharing partners and the level of detail they can effectively share. BLAISE further provides a categorization of four modes of sharing—automated, structured, ad hoc and mediated. Lastly, we've combined the two frameworks to make specific recommendations on modes of sharing that have a higher likelihood of succeeding.

We hope the work of this report can be expanded and extended in future work. We identify three possibilities.

- First, while our recommendations are based on input and guidance from operational subject matter experts and established MITRE frameworks, it would be worthwhile to conduct an in-depth case study of a regional sharing organization that implements the recommendations to validate that sharing efforts are made effective.
- Second, while our analysis focused on regional sharing groups and our recommendations are made specifically for them, we hope the insights and approaches described here will also benefit managers and members of sector-based sharing organizations.
- Third, while our study is focused on cyber threat information sharing, we believe that combining the insights of Cyber Prep (that organizations differ according to

their cyber threat and preparedness) and BLAISE (that sharing methodologies should be selected based on the similarities or differences of cyber defense capabilities) would be of benefit to cybersecurity information and collaboration efforts beyond cyber threat such as risk management, resiliency, and compliance.

Achieving and sustaining effective information sharing is an ongoing and iterative process. For this reason, we recommend further research to apply these approaches to regional sharing groups and to monitor their impact with the hope of further developing effective sharing best practices. We also recommend further research to determine the degree to which these approaches can be applied to sector-based sharing organizations, or more broadly to ISAOs in general.

Appendix A Metrics for Determining Preparedness Group Membership

In Section 5 of this report, we described differences among organizations from the three preparedness groups in four dimensions: defender motivation, attacker intent, attacker capability, and defender capability. In this appendix, we provide more detailed descriptions of the distinctions in these dimensions that are based on observable characteristics. An organization can assess itself against these observables to determine which group will best facilitate its sharing needs. Understanding which preparedness group an organization is a member of is a necessary first step in determining who it shares with and what is shared.

A.1 Defender Motivation Assessment

The type of highest value asset that an organization holds is one way to discriminate among the preparedness groups, as summarized in Table A-1.

Table A-1. Defender Assets

	APT	Theft	Vandalism
Highest Value Asset	IP or Mission	Money	Reputation

Highest Value Asset: Organizations in the three preparedness groups differ according to the highest value asset they seek to protect.

- APT (Advanced Persistent Threat): Organizations in the APT group hold some intellectual property (IP) or similar asset that is both valuable and unique to that organization.
- Theft: Organizations in the Theft group possess monetizable data such as credit card numbers or personally identifying information (PII). A Theft attacker would attack such an organization, and crucially, the Theft attacker does not target the organization, but the asset. So two banks or two PII databases are effectively indistinguishable for this attacker.
- Vandalism: The most valued digital assets for organizations in the Vandalism group include their public-facing Internet infrastructure, such as websites and other Internet-facing servers and databases.

Generally speaking, organizations that have monetizable digital assets have Internet-facing assets that need protection as well. And, organizations that have significant digital IP that could be targeted by APT attackers may have monetizable assets and Internet facing assets. Conversely, organizations in the Vandalism and Theft groups have no meaningful digital IP holdings. For such organizations, it would be unwise to invest in defensive practices to protect IP from the APT threat. In this way, the differences in digital assets to be protected lead to significant differences in the kinds of threat information that is of value across the three preparedness groups.

A.2 Attacker Intent Assessment

Attacker intent can be described according to the type of assets that are targeted as summarized in Table A-2.

Table A-2. Attacker Intent

	APT	Theft	Vandalism
Asset Targeted	Intellectual Property	Money	Reputation

Asset Targeted: Just as different types of organizations hold different kinds of digital assets, it is also true that different kinds of attackers are attracted to those different kinds of assets.

- APT: The APT attackers engage in some form of cyber espionage or warfare. Their goal is to establish a persistent and stealthy presence on the victim's network to prosecute a long-term campaign designed to steal IP and to stay abreast of the victim's proprietary plans. The motivations can be commercial or state-sponsored. It is worth noting that unlike the Theft attacker, monetizing stolen data is generally counter to the intent of the APT attacker, since the act of monetizing the stolen data increases the risk of alerting the victim that their network has been compromised.
- Theft: The attackers motivated by money are cybercriminals. They seek to maximize the financial return while minimizing the cost of an attack. Examples include a bank infiltrated for fraudulent ACH transfers or a hospital targeted for patients' PII or personal health information (PHI), which can be sold.
- Vandalism: The attackers attracted to assets associated with the victim's reputation seek to either damage the victim's reputation (e.g., a university website is defaced by a protest group or an online retailer is subject to a denial of service attack) or to enhance their own reputation (e.g., a hacker group defaces a website). While it may be the case that damage to the victim's reputation can impose direct or indirect financial costs, it is important to distinguish this type of attacker intent from the Theft threat. Attackers motivated by reputation don't directly gain financial benefit from their attack.

A.3 Attacker Capability Metrics

The organization or sharing group may use six different dimensions to evaluate the capability of the cyber adversaries it faces. We list them from the more objective and observable, or verifiable, to the least: resources, attacks, reconnaissance, persistence, expertise, and personnel.

We summarize the differences in the attackers' capabilities in Table A-3.

Table A-3. Capabilities Maturity Assessment

	APT	Theft	Vandalism
Resources	Significant	Moderate	Limited
Attacks	Multiple Coordinated	Multiple	Single
Reconnaissance	Yes	Sometimes	No
Stealth and Persistence	Advanced Stealth and Persistence	Some Stealth	Neither

Resources in this context include attack tools, and the financial and political resources to acquire new or tailored tools (e.g., 0-day exploits). Levels of available resources include:

- APT: If the attacker demonstrates that it can consistently develop or otherwise obtain exploits for unknown (0-day) vulnerabilities, its resources are rated as "significant," which is consistent with the APT-level attacker.
- Theft: If the attacker demonstrates the ability to maintain a command and control infrastructure for attack tools such as a large botnet, either for personal use or in a mercenary capacity, then its resourcing is rated as "moderate," which is consistent with the Theft-level attacker.
- Vandalism: If the attacker demonstrates the ability to use freely-available tools, including those from Metasploit, Exploit.db, then its resourcing is rated as "limited," which is associated with the Vandalism-level attacker.

It should be noted that expertise and resources are correlated but not identical. Expertise measures how the adversary obtains tools, and resources measures how they are used.

Attacks assesses the sophistication of the attacker's operations in the context of strategy.

- APT: If the attacker demonstrates the ability to conduct multiple coordinated attacks with distinct operations to achieve a larger, unified objective, then its attack sophistication is consistent with that of the APT attacker.
- Theft: If the attacker demonstrates the ability to repeat the same attack strategy against multiple targets or the ability to repeatedly attack the same target, then its attack sophistication is consistent with the Theft attacker.
- Vandalism: If the attacker demonstrates the ability to attack a single target at one time, then its attack sophistication is consistent with the Vandalism attacker.

Similarly, multiple personnel and multiple attacks are directly correlated. It is possible, but unlikely, that a team of hundreds would commit single attacks, and likewise that a lone attacker could carry out multiple coordinated attacks.

Reconnaissance in this context evaluates the attacker's ability and willingness to obtain information on the target.

- APT and Theft: If the attacker demonstrates the ability to conduct reconnaissance against its targets to the level of identifying and targeting individual employees of

the victim organization, then its reconnaissance ability is consistent with the APT attacker. However, some advanced Theft attackers also have the ability to perform reconnaissance too.

- Vandalism: If the attacker's attacks give no indication that the attacks are based on reconnaissance of any kind, then its reconnaissance ability is consistent with the Vandalism attacker.

A clear example of the use of reconnaissance is spear-phishing instead of phishing. An attacker that sends its emails to lure employees in a specific department, or a particular location, or with unique expertise clearly demonstrates that the attacker has completed some advance research. A generic phishing email to an organization's employees conversely indicates less preparation on the adversary's part.

Stealth and Persistence evaluates the difference between a "slow-and-low" intrusion and a "smash-and-grab" attack. Stealth measures efforts to avoid detection. Activities include the ability to modify logs and to create difficult to detect Trojans. Persistence is the ability for the attack to reconstitute a compromise despite efforts to remove the attack tools. Increased persistence indicates that the attacker has invested time and resources.

- APT: The attacker remains undetected on the network for a long time (months to years).
- Threat: If the attacks demonstrate moderate stealth capabilities, but not meaningful persistence capabilities, then their capabilities are consistent with that of the Theft attacker.
- Vandalism: The attacks are opportunistic and demonstrate no concern about detection.

Stealth and persistence on the part of the attacker are distinct from poor monitoring and response on the part of the defender. That is, days to detection measures stealth or persistence incompletely.

A.4 Defender Preparedness Metrics

The National Institute of Standards and Technology (NIST) Cybersecurity Framework defines five top level categories for cybersecurity capabilities: identify, protect, detect, respond and recover.[15] Restating one of the insights of Cyber Prep, the preparedness group that an organization is in necessitates different levels of resources to be expended across the five categories. That is, members of the Vandalism group typically focus most of their investments in the identify and protect areas, whereas members of the APT group typically have robust investments across all five areas. More deeply, the different type of assets to protect and the different types of threats make it reasonable for the focus of security investments to be different within each of these five areas across the three preparedness groups.

Different cybersecurity investments lead to different typical cybersecurity operational capabilities across the three preparedness groups, each tailored and appropriate to defend

[15] See http://www.nist.gov/cyberframework/, accessed 3 November 2016.

their different assets from their different expected attackers. The differences in operational capabilities across the preparedness groups has a direct bearing on what kinds of threat information sharing efforts the organization can participate in. For example, an organization cannot share findings from malware analysis if they don't have a mature, in-house malware analysis capability.

A.4.1 Operational Capabilities Defined

We briefly describe the major operational differences among the three major preparedness groups. We begin by making three observations. First, for the purpose of description, we organize the operational capabilities into three primary areas:

- Network Management: Operational management of tools and infrastructure involved in network operations, monitoring, blocking and routing
- Threat Awareness: Monitoring and analysis capabilities with the primary purpose of achieving and sustaining situational awareness of threats by attackers who are both inside and outside of the organization
- Incident Response: Capabilities involved in the recognition, declaration and management of cyber incident response activities.

We briefly describe the typical operational capabilities found within these three major areas in organizations participating in cyber threat-sharing organizations.[16] We note that this categorization of capabilities is notional, for purposes of highlighting the operational differences between the preparedness groups. We would not expect to find any member organization organized in exactly this way and would expect, in most cases, that there would be significant overlap in some capability areas.

The maturity of the operational capabilities can range from stable, to nascent, to outsourced, to entirely missing.

[16] We extracted these from our review of MITRE institutional knowledge including *Ten Strategies of a World-Class Cybersecurity Operations Center*, our experience with operational practices at various members of various Information Sharing and Analysis Organizations (ISAOs), the National Institute of Standards and Technology (NIST) Cyber Security Framework, and capabilities mentioned in Cyber Prep.

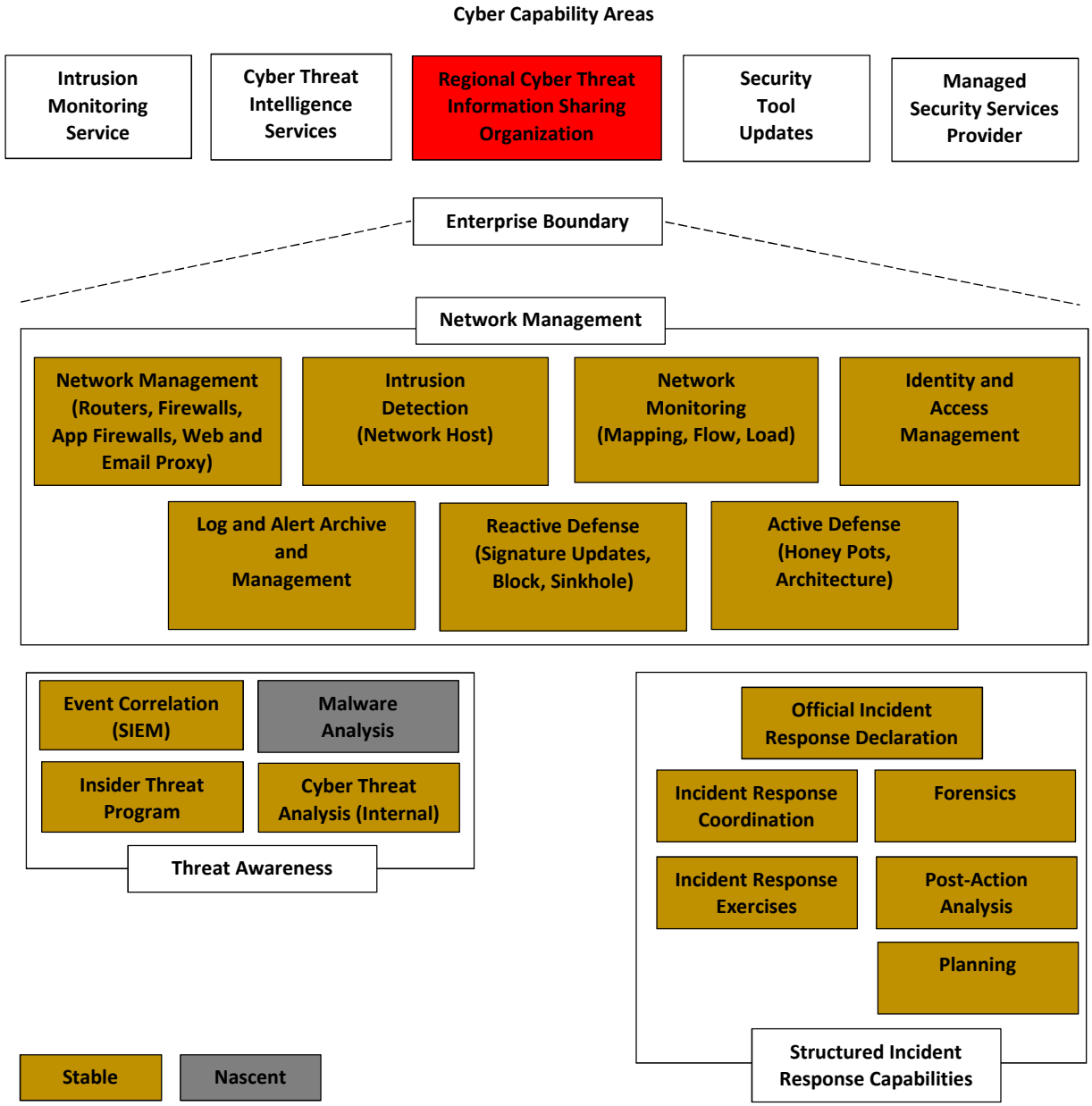


Figure A-1. Capabilities Related to Threat Information

Typical capabilities within the area of Network Management include:

- Reactive Defense: The updating and alteration of signatures and rules to produce alerts or to block or shape traffic. The Reactive Defense capability receives (or manages the receipt of) vendor published security tool signature updates such as Intrusion Detection System (IDS) or antivirus products. The Reactive Defense capability may also have the ability to author or modify signatures based on information relayed to it by the Cyber Threat Analysis capability.

- Network Management: Routers, firewalls, application firewalls, web and email proxy servers. Network Management is responsible for the operation and monitoring of the network management components. It is typically not responsible for updating the security rules and signatures in the tools; instead, the Reactive Defense capability updates the security rules and signatures. Logs and alerts from the tools are sent to the Log and Alert Archive and Management capability. This capability may send an alert to the Incident Response Declaration capability if suspicious activity is detected.
- Intrusion Detection: Network-based IDS, host-based IDS, data protection monitoring. (May be combined with Network Monitoring.) Intrusion detection is responsible for the operation and monitoring of the components. It is not responsible for updating the security rules and signatures in the tools. The Reactive Defense capability updates the security rules and signatures. Logs and alerts from the tools are sent to the Log and Alert Archive and Management capability. This capability may send an alert to the Incident Response Declaration capability if suspicious activity is detected.
- Network Monitoring: Network mapping, network flow monitoring, network load monitoring. (May be combined with Intrusion Detection.) Logs and alerts from the tools are sent to the Log and Alert Archive and Management capability. This capability may send an alert to the Incident Response Declaration capability if suspicious activity is detected.
- Identity and Access Management: Identity management, directory management, Virtual Private Network (VPN), authentication, network access control. Logs and alerts from the tools are sent to the Log and Alert Archive and Management capability. This capability may send an alert to the Incident Response Declaration capability if suspicious activity is detected.
- Log and Alert Archiving and Management: The collection and storage of logs and alerts from the tools managed by the Network Management, Intrusion Detection, Network Monitoring and Identity and Access Management capabilities, as well as the ability to search and retrieve them. The Log and Alert Archiving and Management capability provides information access to the Event Correlation capability.
- Active Defense: The creation and management of honey pots and network obfuscation techniques. Includes security driven network architecture planning. This capability may send an alert to the Incident Response Declaration capability if suspicious activity is detected.

The typical capabilities within the area of Threat Awareness include:

- Event Correlation: Includes functions and products in the Security Information and Event Management (SIEM) category. Receives alerts from multiple IDS and network monitoring feeds via the Log and Alert Archiving and Management capability, correlates them and identifies relationships among them. In organizations in the Theft group, the focus of this activity is to identify an active penetration and breach.

This capability may send an alert to the Incident Response Declaration capability if suspicious activity is detected.

- Malware Analysis: Analyzes malware samples found on the organization's network. The focus of the analysis is to understand the malware's execution with the purpose of detection, eradication, and recovery.
- Insider Threat Program: Seeks to identify attackers who are members of the organization or who have legitimate access to the organization's systems.
- Cyber Threat Analysis: Seeks to identify threats that are external to the organization. When possible, the Cyber Threat Analysis capability provides input to the Reactive Defense Capability, so that signatures and firewall rules can be updated or adjusted to include new threat information. This capability identifies attackers who seek monetizable assets using commercial grade exploits, tracks APT threats that use 0-day based exploits, and learns of new, advanced tools, techniques and procedures (TTPs) that may become commoditized and used by the Theft attacker in the near future.

Typical capabilities with the area of Incident Response include:

- Official Incident Response Declaration: Has the recognized authority to declare that an incident has occurred. Takes inputs from many sources from the Network Management and Threat Analysis groups.
- Incident Response Coordination: Responsible for coordinating incident response activities. This capability typically coordinates response activities across a broad set of stakeholders across the organization including: cybersecurity, Information Technology (IT), business management, and executives. In smaller organizations, this capability may be merged with the Official Incident Response Declaration capability.
- Forensics: Is responsible for the technical analysis of affected systems. The goal of forensics is to determine the amount of impact of an incident, preserve evidence, and to make recommendations on response and improving the security posture.
- Post-Action Analysis: Is responsible for analyzing the incident response activities after the incident has been resolved. The goal is to improve future incident response activities. They typically provide the results to the Planning capability.
- Planning: Establishes incident response procedures and plans. In smaller organizations, this may be merged with the Incident Response Coordination capability.
- Incident Response Exercises: Coordinates the organization's participation in incident response exercises with outside organizations including partners, fellow regional sharing groups and law enforcement.

A.4.2 Defensive Capabilities in the Preparedness Groups

As discussed in the previous section, the sophistication and skills of the attacker increase as we move from the Vandalism group to the Theft group and then to the APT group. Correspondingly, and consistent with the Cyber Prep Framework, we should expect that

members of the Theft group to have more cybersecurity capabilities than members of the Vandalism group, and members of the APT group will have more than members in the Theft group.

We underscore that this does not imply that members of the Vandalism or Theft groups should aspire to have more complete sets of operational capabilities on par with members of the APT group. In fact, quite the opposite is true, as expenditures on cybersecurity capabilities not justified by the presence of a commensurate threat wastes resources, thus imposing other business risks. For example, it would be counterproductive for a typical member of the Theft group to attempt to stand up an effective malware analysis capability because the Theft attacker typically uses “commercial-grade” malware which is typically caught by commercial anti-malware.

With these observations in hand, the following are typical capabilities for the three preparedness groups:

- APT: Organizations in the APT group typically have mature, state of the art operational capabilities within the areas of Network Management, Threat Awareness, and Incident Response as shown in Figure A-2. The sole notable exception is malware analysis, which is typically a nascent growth area.

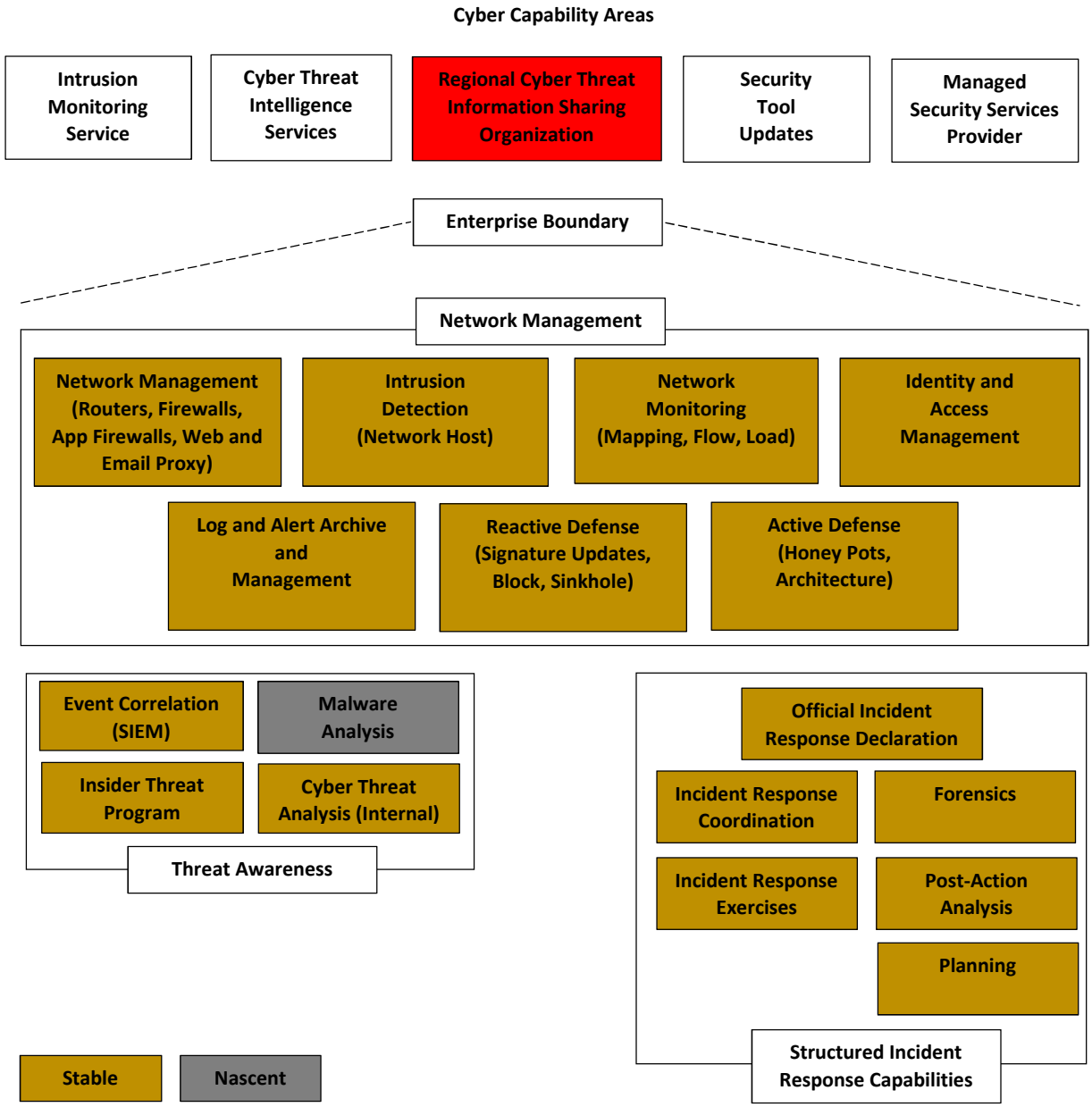


Figure A-2. Typical Threat-Related Capabilities in the APT Preparedness Group

- Theft: Members of the Theft group typically have mature capabilities in nearly all aspects of network management and in most aspects of incident response. It is common for Malware Analysis, Insider Threat and (External) Cyber Threat Analysis to be colocated in the same team. A well-established Event Correlation capability is necessary. Reference Figure A-3.

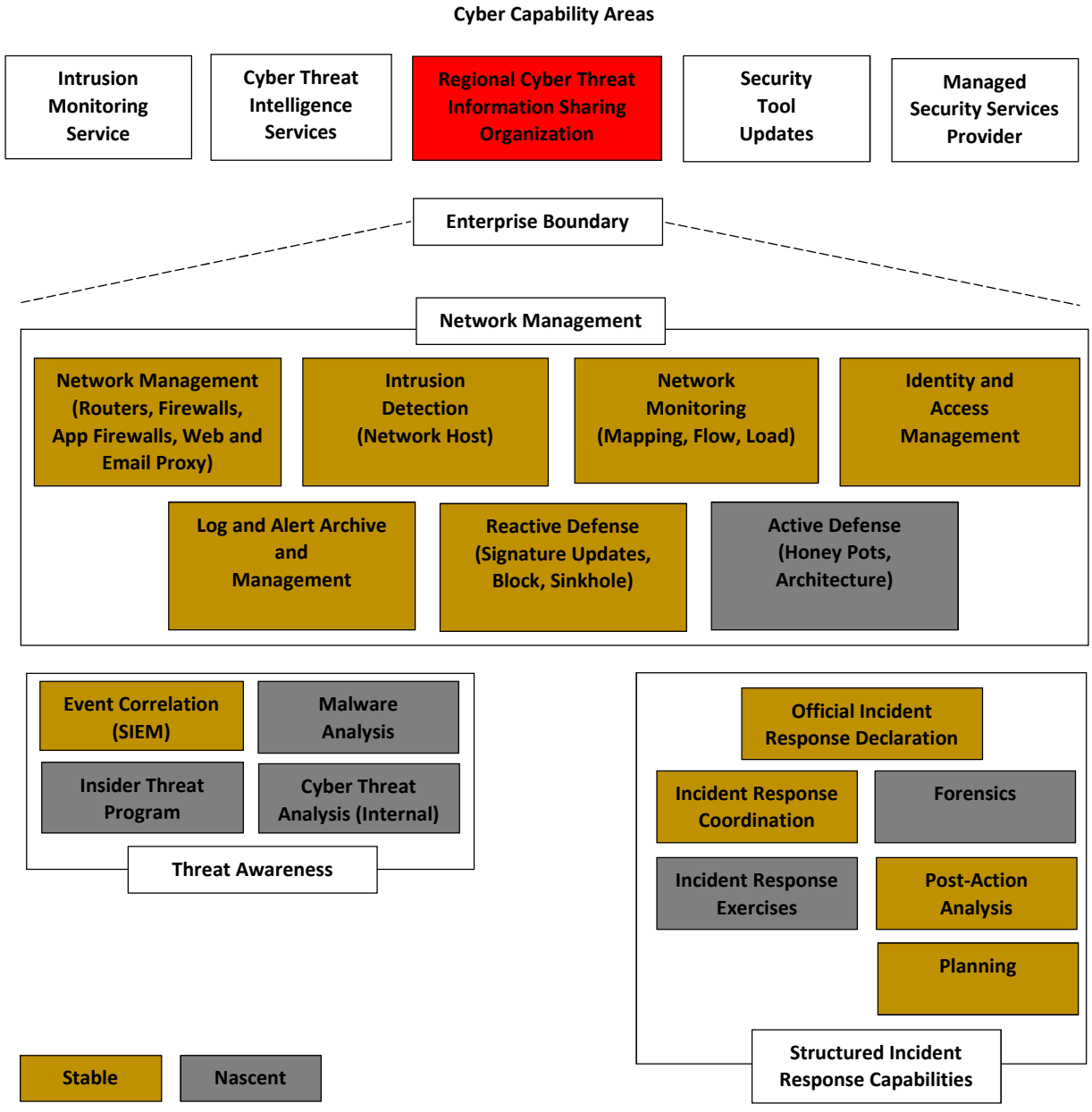


Figure A-3. Typical Threat-Related Capabilities in the Theft Preparedness Group

- Vandalism: Members of the Vandalism group typically have stable, well-established capabilities in most aspects of network management, and most other areas are nascent or absent. Reference Figure A-4.

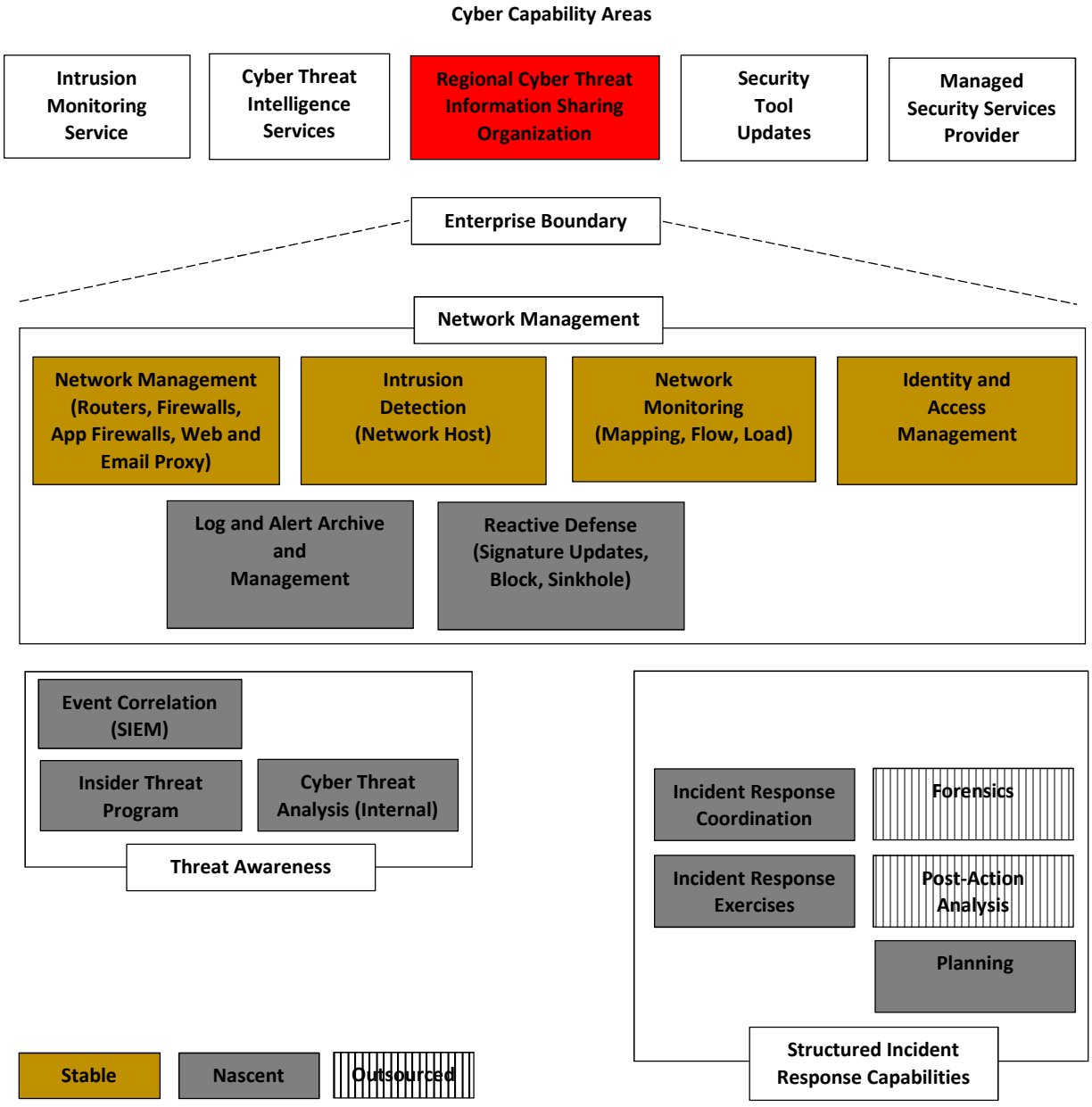


Figure A-4. Typical Threat-Related Capabilities in the Vandalism Preparedness Group

Appendix B Abbreviations and Acronyms

ACSC	Advanced Cyber Security Center
A-ISAC	Aviation-Information Sharing and Analysis Center
APT	Advanced Persistent Threat
BLAISE	Bilateral Analysis of Information Sharing Exchanges
BOLO	Be On the Lookout
CalCISO	California Cybersecurity Information Sharing Organization
CIS	Center for Internet Security
COA	Course of Action
CONOPS	Concept of Operations
DBIR	Data Breach Investigations Report
DHS	Department of Homeland Security
EOB	Explanation of Benefit
EULA	End User License Agreement
FS-ISAC	Financial Services-Information Sharing and Analysis Center
IDS	Intrusion Detection System
IOC	Indicators of Compromise
IP	Intellectual Property
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organizations
IT	Information Technology
NIST	National Institute of Standards and Technology
PHI	Personal Health Information
PII	Personally Identifying Information
SIEM	Security Information and Event Management
TTP	Tactics, Techniques, and Procedures
VPN	Virtual Private Network