A FRAMEWORK FOR CYBER INDICATIONS AND WARNING

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE
Presented by INSA's Cyber Council

October 2018

INSA

ACKNOWLEDGEMENTS

This paper was developed and written by members of a Cyber I&W working group collaborating under the auspices of INSA's Cyber Council. Thanks are due to:

Blake Moore, *Splunk**

Andrea Little Limbago, *Endgame*

Jeremy Erb, *Deloitte*

Kevin Zerrusen, *Goldman Sachs*

Cody Barrow, *Recorded Future*

Lonnie Garris

Terry Roberts, *Whitehawk*

**Blake Moore is currently serving as Chief of Staff to the Chief Information Officer of the Department of Defense. His work on this paper was conducted during his tenure at Splunk, which preceded his government position. His contributions to this paper reflect his personal research and analysis and do not necessarily represent the views of the Department of Defense.*

Appreciation is also due to INSA staff members who contributed to the publication:

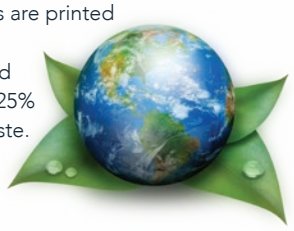
Chuck Alsup, *President*

Larry Hanauer, *Vice President for Policy*

Ryan Pretzer, *Senior Manager, Policy and Public Relations*

Ehrlich Alba, *Digital Marketing Manager*

Jean Cocco, *Intern*



EXECUTIVE SUMMARY

Malicious cyber activity continues to evolve rapidly, with an expanding set of tools available to a growing range of threat actors. The public and private sector have yet to fully evolve their threat models, defenses, and courses of action in line with this landscape. While frameworks for indications and warning (I&W) – and "warning intelligence" – have matured in other intelligence domains, cyber I&W remains nascent and ill-defined. The lack of such a framework has resulted in an absence of best practices and lessons learned. It also contributes to many of the resource challenges and reactive defensive postures put in place today. To address this gap, INSA conducted a survey of industry, academia, and government experts to elicit best practices for cyber I&W, share lessons learned, and help evolve the community toward a common cyber I&W framework.

Survey results show that the absence of a framework hinders an organization's ability to prioritize resource allocation, data acquisition, and incident response. Respondents also have difficulty developing a skilled workforce and modernizing defenses with constrained resources. Lengthy and confusing technology acquisition processes further complicate defensive preparations. In fact, organizations are prone to over-estimate their capability maturity, lack insight across their IT infrastructure, and maintain too narrow a focus on known threats to their organizations.

INSA has developed a framework to help organizations address many of these problems and take a more proactive defensive posture. The I&W framework is based on the definition of cyber I&W as an analytic process where an anticipated scenario in cyberspace is "decomposed," or broken down, into indicators that can be continuously monitored to provide warning of the scenario coming to fruition. We recommend implementing this framework, which consists of seven steps: 1) identify and prioritize assets; 2) prioritize the threat; 3) assess threat courses of action; 4) decompose scenarios into indicators; 5) plan and exercise countermeasures; 6) align to the intelligence cycle; and 7) execute proactive measures. This framework can then be hardened through red and blue team exercises to help ensure it works both in theory and in practice.

Organizations should also complement this framework with renewed focus on both the talent pipeline and retention and the implementation of a nuanced understanding of threats and internal defenses. Information sharing working groups should also be leveraged to collect the insights of other organizations and to contribute to a broader collective security that benefits all organizations.

The intent of this framework is to give government, academic, and industry professionals a practical analytic process in which an anticipated attack scenario is decomposed into indicators that can be continuously monitored to warn of an actual attack. With an I&W framework in place, and subsequent efficiencies gained through a customized threat model and resource allocation, organizations will gain greater defensive efficiencies and resilience, while moving away from the whack-a-mole approach that fosters the current complexities in the security and IT stacks. Importantly, this is not a one-time process. Organizations must reiterate and update their I&W framework to stay relevant with the changing threat landscape. Even basic I&W initiatives have the potential to foster greater resilience and preparedness, while the transparency and information sharing supports enhanced defenses and can help the broader community proactively counter cyber threats.

INTRODUCTION

Given the increasing velocity, complexity and magnitude of malicious cyber activity by a disparate range of threat actors, the private and public sectors are challenged to stay ahead of and prepare for the breadth of attacks encountered on an hourly basis. While intelligence frameworks for indications and warning (I&W) have matured in other intelligence domains, cyber I&W concepts remain nascent and ill-defined. Accordingly, the Intelligence and National Security Alliance (INSA) conducted a survey at the request of several government agencies to identify the current state of cyber I&W across industry, academia, and the public sector. Aiming to capture and share best practices and current gaps, the survey highlights key pain points including talent gaps, budget constraints, and a limited understanding of the potential range of threats. Most respondents pointed to the necessity for a comprehensive I&W framework, with a focus on staying ahead of the threat rather than constantly reacting. To that end, INSA proposes an I&W framework that can enable organizations to proactively anticipate and prepare for threat scenarios prior to potential compromise.

DEFINITIONS & TERMINOLOGY

The Department of Defense Joint Publication (JP) 2-0, "Joint Intelligence," defines "warning intelligence" – a term DOD now uses in lieu of "indications & warning" – as "those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that forewarn of hostile actions or intention against United States entities, partners, or interests."[1] Older definitions of I&W specified a litany of threats that I&W could be employed to address: "enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied and/or coalition nations; hostile reactions to U.S. reconnaissance activities; terrorists attacks; and other similar events."[2]

This definition, although robust and explicit, is appropriately focused on hostile foreign actions against U.S. national interests. It does not address unique challenges within the cyber domain; take into account cyber activities originating inside the United States (e.g., U.S.-based cyber criminals); envision hostile activities by non-state actors other than terrorists; or consider non-state U.S. actors, such as industry and academia. The definition does not encompass industry and academia's need to establish warning indicators within their own networks of nefarious actors. Consequently, the definition fails to provide a framework for how government and non-governmental entities can approach this problem.

In an attempt to apply I&W more directly to cyberspace, DoD JP 3-12R elaborates on what the end result of I&W should be and what it can do within intelligence contexts in cyberspace operations. The JP states, "cyberspace intelligence on nation-state threats should include all-source analysis in order to factor in traditional political/military I&W. Adversary cyberspace actions will often occur outside, and often well in advance of, traditional military activities. Additionally, cyberspace I&W may recognize adversary triggers with only a relatively short time available to respond."[3] This elucidation makes clear that all-source intelligence analysis is important for effective analysis of adversary capability and intent in cyberspace. This insight, while useful, focuses on what I&W should include and what it can provide – *not how to do it.*

Thus, at its most basic level, cyber I&W remains a fairly vague construct open to a variety of interpretations. This is unsurprising given the concept's roots in the government space. (Indeed, the specific call by DoD JP 3-12R to factor "traditional political/military" factors into cyber I&W leaves out economic and commercial factors, further highlighting that the discipline of I&W generally excludes hostile activities by, or targeting of, non-government actors.)

As validation of just how widespread these inconsistencies are, almost a third of our survey respondents conceptualized cyber I&W as a methodology for monitoring information, followed closely by those who focused on its role as information on impending threats, and finally by a remaining contingent who saw it as a form of predictive analysis. To be fair, responses contained significant overlap, and follow-on interviews indicated confusion about I&W concepts across the board. When disaggregating survey data, it was clear that cyber I&W concepts were heavily driven by the respondent's industry. Asked fundamentally what cyber I&W is, respondents in industry interpreted I&W as an analytic methodology, those in academia emphasized its monitoring and information utility, and those in government viewed it as predictive analysis. These different approaches were manifested further when looking at common techniques used to identify impending attacks: Approximately 60% of respondents used the Lockheed Martin-developed intrusion kill chain, illustrating some consistency in techniques, but the survey otherwise revealed a diverse breadth in techniques and approaches. Moreover, the survey revealed a diverse breadth in techniques and approaches where almost half of the respondents reported using some sort of computation model while half integrated qualitative use cases and case studies.

Based on our analysis, and based on input from non-government experts in industry and academia, INSA defined cyber I&W as *an analytic process where an anticipated scenario in cyberspace is decomposed into indicators that can be continuously monitored to provide warning of the scenario coming to fruition.*

[1]*Department of Defense, Joint Intelligence, Joint Publication 2-0, October 22, 2013, p. GL-12. At http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp2_0.pdf.*

[2]*Department of Defense, Department of Defense Dictionary of Military and Associated Terms, Joint Publication 1-02, March 23, 1994 (as amended through September 1, 2000), p. 220. At https://www.fpa.org/usr_doc/38112.pdf.*

[3]*Department of Defense, Cyberspace Operations, Joint Publication 3-12(R), February 5, 2013, p. II-9. At https://www.hsdl.org/?view&did=758858.*

METHODOLOGY

To add clarity toward solidifying best practices, share lessons learned, and formulate a common cyber I&W framework, the INSA Cyber I&W Working Group pursued a multi-method approach to extract both quantitative and qualitative insights. The first step was to survey executives and senior practitioners across government, industry, and academia on cyber topics directly and tangentially related to the concept of cyber I&W. Questions focused on organizations' preparedness and maturity level for cyber I&W, as well as their perspective on the threat and their allocations of resources to address it. Second, we conducted a series of follow-on interviews with key government, industry, and academia experts to get a qualitative view of best practices and challenges around the development and implementation of the I&W concept. Third, we conducted quantitative data analytics on the survey to glean additional insight into hidden trends that would be relevant to this effort. Finally, we analyzed and synthesized all of the available information to construct the insights and recommendations in this paper.

Challenges to effective cyber I&W fell into three categories: a shortage of personnel with both cybersecurity and intelligence analysis skills, a dearth of financial resources, and a lack of a framework for approaching I&W in the cyber domain.

KEY CHALLENGES

Challenges to effective cyber I&W fell into three categories: a shortage of personnel with both cybersecurity and intelligence analysis skills, a dearth of financial resources, and a lack of a framework for approaching I&W in the cyber domain.

KNOWLEDGEABLE TALENT

Survey respondents from all sectors echoed well known concerns about the shortage of trained cybersecurity workers in general and amplified this fact with the lack of cyber intelligence expertise. The number of vacant cybersecurity positions increased 74% between 2011 and 2015, according to an analysis of data from the Bureau of Labor Statistics.[4] According to ESG, 44% of organizations are short on staff with strong cybersecurity and networking knowledge.[5] With such a massive limitation on cybersecurity talent writ large, it is no surprise that there are even fewer professionals within this pool who have the advanced analytic tradecraft skills needed to undertake I&W analysis.

[4]*Steve Morgan, "Cybersecurity labor crunch to hit 3.5 million unfilled jobs by 2021," CSO Online, June 6, 2017. At https://www.csoonline.com/article/3200024/security/cybersecurity-labor-crunch-to-hit-35-million-unfilled-jobs-by-2021.html.*

[5]*Jon Oltsik, Doug Cahill, and Bill Lundell, "Cybersecurity Skills Shortage: A State of Emergency, Enterprise Strategy Group," February 2016. At http://www.esg-global.com/hubfs/ESG-Brief-Cybersecurity-Skills-Shortage-Feb-2016.pdf.*

While many human resources experts have focused on the need to get additional skilled cyber workers in the pipeline, far fewer have focused on the benefits of retaining skilled workers who are already in the cyber workforce. In a recent study on retention, burnout, stress, and industry culture topped the list of factors for those leaving the industry. Moreover, the share of women in the industry has been dropping for years and is now stagnant at around 10%.[6] Given the workforce shortages and need for distinct viewpoints, the industry simply cannot afford to be losing skilled female personnel. In addition, the industry requires diversity and balance among key skills such as strategy, policy, technology and operations.

Similarly, many companies continue to treat cybersecurity as a component of information technology rather than as a distinct field of expertise in itself.[7] Concrete career development tracks are essential to grow capacity within the information security community, as well as to ensure institutional memory and expertise within organizations. Furthermore, organizationally subordinating cybersecurity to IT deprives cybersecurity of key enablers needed to elevate cybersecurity to a core corporate function, such as dedicated resources (including personnel), focused strategic plans, specialized training opportunities and career paths, and senior managers who can advocate effectively for cybersecurity equities within the organization. As those in the private sector reaffirmed in follow on questions, the lack of a defined career path for cybersecurity leaders limits growth and negatively impacts retention. As they noted, this should include developing leaders (not managers), offering mentorship, and ensuring the cybersecurity workers do not spend their entire day solely on some of the "busy work," but provide opportunities for cybersecurity professionals to learn and attain new skills. One respondent noted that this will also raise the bar within organizations, and stressed the need for multi-disciplinary teams to best support robust cyber threat intelligence efforts.

Survey responses indicated that organizations in different sectors mitigated the impact of talent shortfalls in different ways. Government respondents tackled the personnel shortage through a range of workarounds, including relying more on technology and non-government employees (private contractors) to fill the gap. Several industry respondents attempted to compensate for the lack of labor with improved leadership, more effective management, and outsourced managed security services. Academics linked the personnel shortage to a dearth of resources, and so were generally unable to get work done when personnel were unavailable.

LACK OF EFFECTIVE CONTRACTS AND PROCUREMENT APPROACH

Despite projected enterprise spending in excess of $1 trillion from 2017-2021,[8] budgetary constraints remain a top concern of our respondents. In the survey of cyber executives and senior practitioners, the lack of sufficient budget ranked just beyond the talent gap, with 43% of respondents noting budgetary constraints as a key hurdle in implementing a cyber I&W framework. Interestingly, this was significantly skewed by industry respondents, the majority of whom listed budgetary constraints as the largest impediment for approaching a cyber I&W posture. Government respondents frequently cited a misallocation of resources to outdated technologies or approaches that are no longer sufficient for the sophistication of the range of attack vectors. This is consistent with the overarching finding on the lack of coherent and replicable cyber I&W approaches. Absent these frameworks, most organizations cannot efficiently target their spending, and thus, are left perpetually in a reactive mode. It is plausible that more innovative and broadly applicable processes could help organizations better allocate finite budgetary resources.

[6] *Andrea Little Limbago, "Increasing Retention Capacity: Research from the Field," white paper, Endgame, November 7, 2017. At https://www.endgame.com/resource/white-paper/increasing-retention-capacity-research-field.*

[7] *Dave Venable, "Information Security is Not Information Technology," CSO Online September 14, 2017. At https://www.csoonline.com/article/3225344/data-protection/information-security-is-not-information-technology.html.*

[8] *Randy Radic, "Outlook on Cybersecurity Stocks," Huffington Post, February 5, 2017. At http://www.huffingtonpost.com/entry/outlook-on-cybersecurity-stocks_us_589741c7e4b02bbb1816bb97.*

LACK OF AN I&W FRAMEWORK

Multiple survey questions asked about methods for acquiring information that can warn of an impending attack; organizations' ability to receive or disseminate this information; obstacles to sharing this information; and techniques to analyze information once obtained. Respondents indicated that no standard cyber I&W methodology exists across government, industry, and academia.

As shown in Figure 1, respondents provided a wide range of responses when asked what source of information they use that could warn of a malicious cyber event. Organizations overwhelmingly used cyber threat intelligence (CTI) to provide warning, with almost 87% of respondents indicating they use it in some form or another. All elements in Figure 1 could be considered information sources that collectively equate to CTI. We wanted to let the respondents come back with their perspective on CTI. Some responses included CTI as all-encompassing while others had CTI separate from other source of information.

There are different definitions of CTI across public and private sector entities, but at its essence the INSA Cyber Council defines CTI as *the collection, analysis and dissemination of tailored information specific to a customer requirement to inform decision-making, or action, in or through the cyber domain*. The information (e.g., indicators of compromise, DNS, ISAC information sharing, etc.) can come from anywhere, and ultimately it is not CTI until it is appropriately analyzed and disseminated specifically based on a customer requirement.

Other notable sources of information that the respondents used to warn of a malicious cyber event were Dark Web Data (42%) and Internal Network Data (38%). Roughly one-third (31%) drew on geopolitical data, indicating that many organizations assess the importance of tactical threat indicators in a strategic global context.

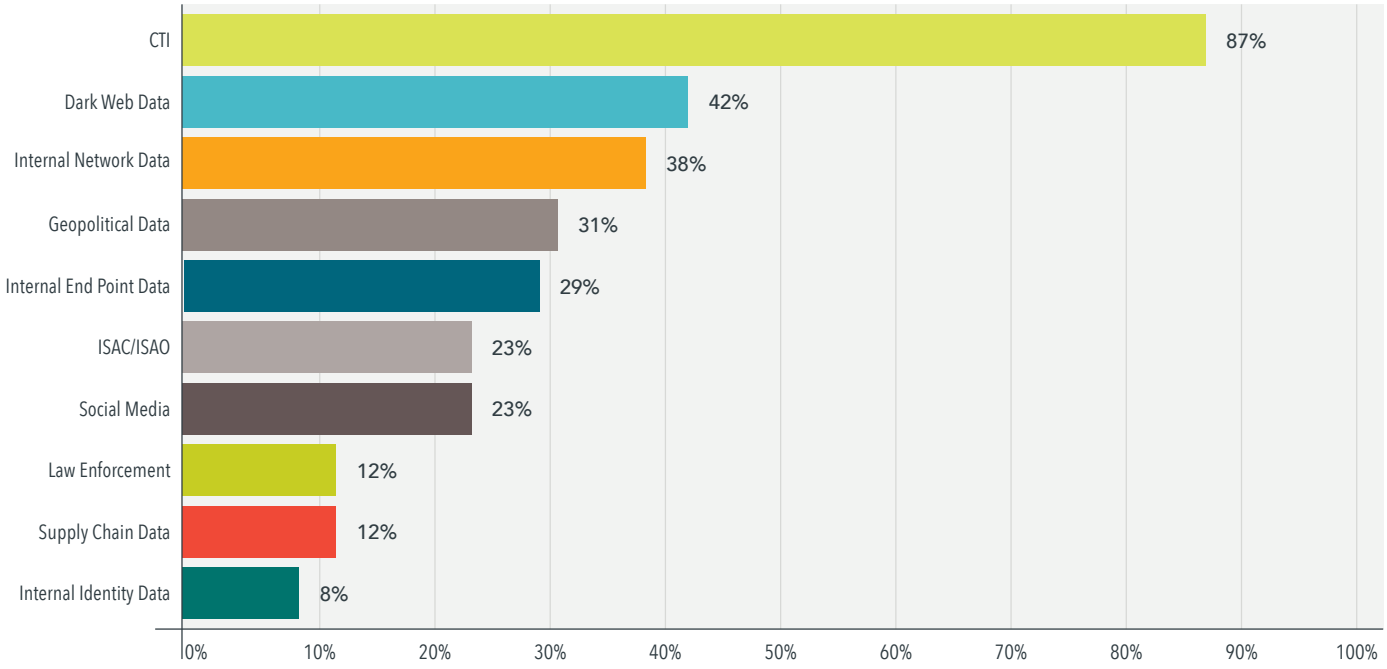


Figure 1: Information sources that can be used to warn of an impending cyber attack

Next, we wanted to determine the means by which the respondents either receive or disseminate information that can forewarn of threatening actions or intentions. Although results varied, the majority of respondents receive or disseminate warning information via free flow text (80%) and email/instant messaging (70%). (See Figure 2.) Receiving information through email or similar listservs

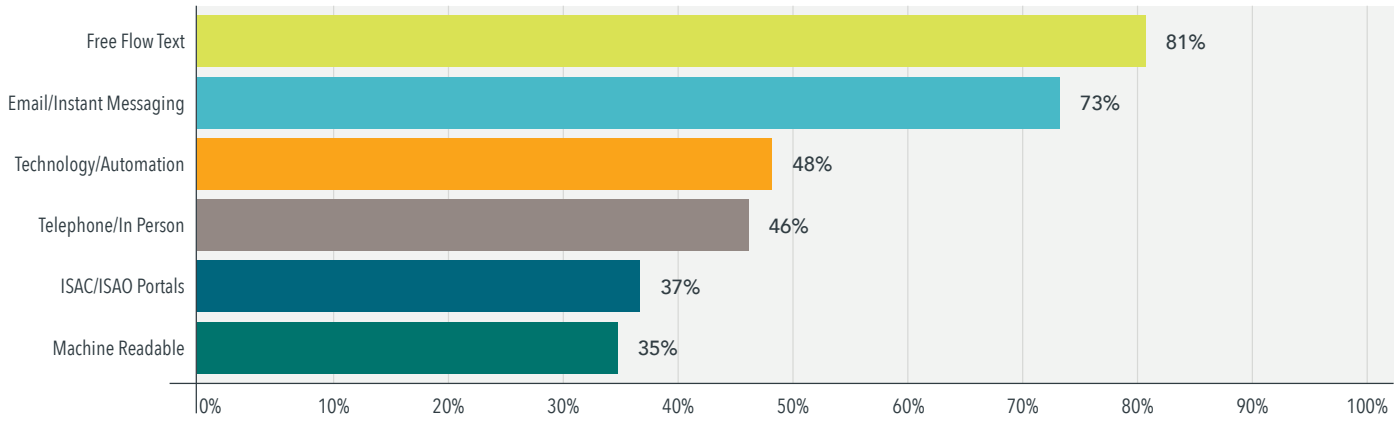


Figure 2: Means by which organizations disseminate or receive information related to warning

can slow available reaction time, particularly compared to, for example, orchestration technologies that automate workflow when threat information is received. The less time available to react to a warning, the less the usefulness of the warning itself. In this context, even with information in hand of an impending attack, without an expeditious means to deliver it for action, it's worthless. If the warning is not delivered until after the attack has occurred, the warning is not intelligence or I&W information, it is news.

Almost half of the respondents did in fact rely on automation, which means that some organizations use both slower means of communications and automated processing. Thus, many enterprises pursue multiple lines of communication to ensure all relevant parties are informed in as timely a manner as possible.

Third, we asked the respondents to identify constraints that limit sharing of information that warns of an impending cyber threat. (See Figure 3.) Not surprisingly – given that the primary means of sharing is through free flow text – 54% of the respondents indicated that the speed of sharing is one of the most limiting factors. Interestingly, a lack of awareness of where and with whom to share the information was also identified as a top factor by 54% of the respondents, and one third of respondents cited poor processes or a lack of processes for handling warning data. These responses point to the likely value of a predetermined framework for handling warning information and coordinating a response.

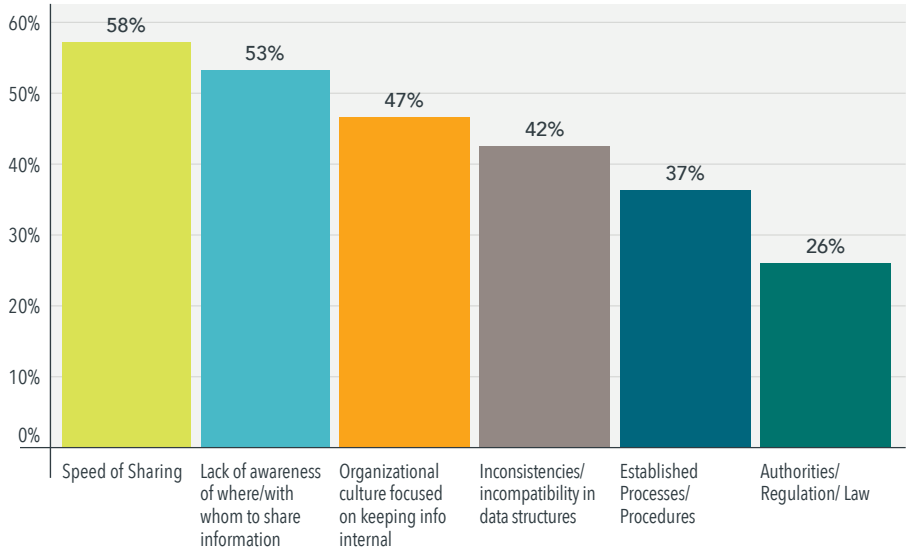


Figure 3: Constraints that limit information sharing

Finally, we asked respondents what analytic techniques and/or methodologies they believe are most useful in developing indicators of an impending cyber attack. This question was designed to glean best practices on what organizations do once they have received relevant information around a future event – under the assumption that they have time to react to it. The kill chain was chosen by almost two-thirds of respondents, likely reflecting the high percentage of respondents who work in government or in the defense industrial base, where it is prominent. However, most respondents indicated that their organizations pursue multiple analytic techniques. Interestingly, both qualitative case studies and computational models are implemented by over 40% of respondents, demonstrating the necessity to blend subject matter expertise with automated tools. As Figure 4 shows, respondents use a wide range of additional approaches, making clear that neither government nor industry has yet to coalesce around a specific approach or set of applicable structured analytic techniques inherent to cyber I&W.

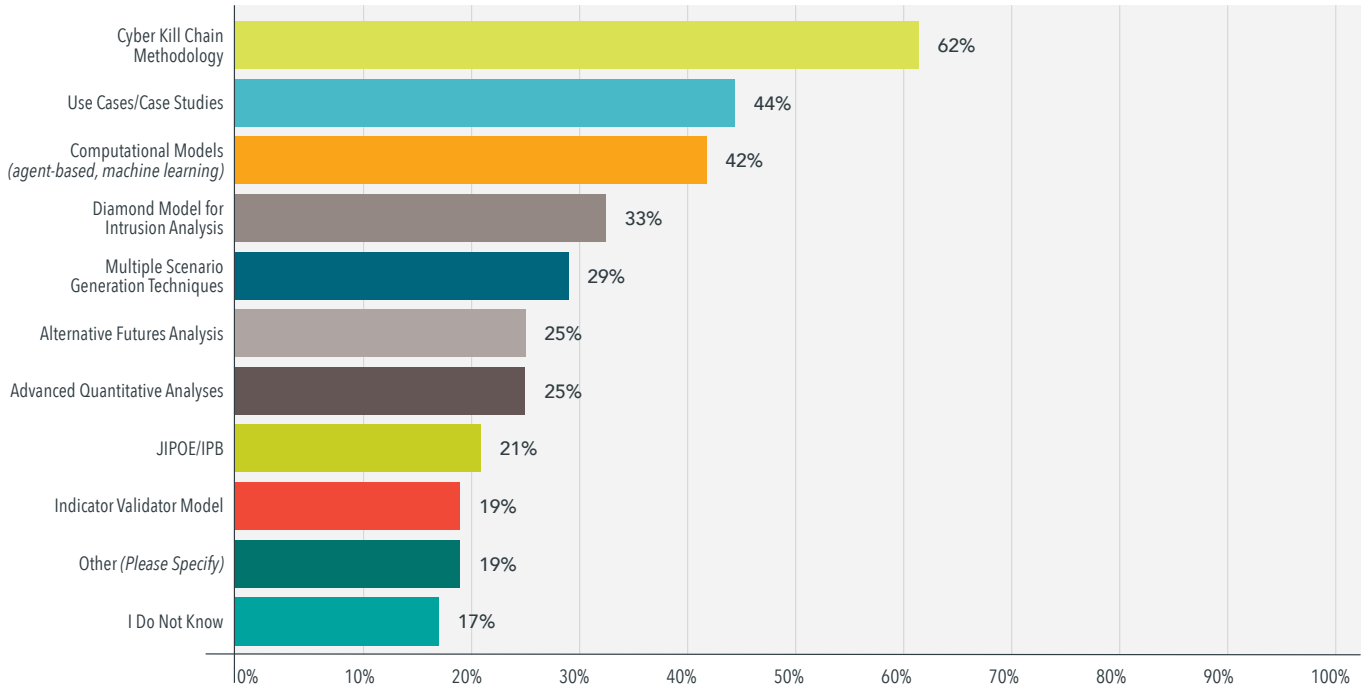


Figure 4: Most useful analytic techniques for developing indicators

Throughout the course of our research it became clear that a practical approach to I&W within the context of malicious cyber activity was needed.

OVERESTIMATION OF MATURITY LEVELS AND CAPABILITIES

Organizations' overestimation of the maturity level of their enterprise defenses potentially creates a false sense of security that may lead to complacency. Overly confident network security officials may feel little need to continually investigate the dynamic nature of threat actors' capabilities and intent as applied to their own vulnerabilities. When an organization is overly confident of its ability to blunt an attack, it tends to de-prioritize warning of a threat. Perhaps this thinking is part of an overall cyber risk management strategy: if an organization feels it can mitigate vulnerabilities quickly while minimizing any impact to their network if one were to be exploited, then it might believe the warning of a threat isn't as critical. INSA believes all elements are critical to an effective cyber risk strategy: identifying and prioritizing mitigation

> Respondents focused on what they perceived as the greatest threat…Such myopia makes it likely that organizations would miss efforts by an unexpected adversary or a known adversary employing innovative techniques.

of vulnerabilities; monitoring and warning of cyber actor capability and intent; and when the inevitable breach occurs, minimizing impact by leveraging redundant capabilities, back-up processes, and business operations outside the cyber environment.

Regardless, it is clear that many organizations often do overestimate their capabilities and underestimate their vulnerabilities. Our results provide some data to support this claim. Across all respondents, no one ranked their cyber maturity level as a zero or one, the lowest potential scores. During follow-on interviews, two out three government respondents stated that organizations are likely overstating their capabilities, at the very least, to provide some type of warning. An interviewee from the private sector, for example, noted e-business lacks the maturity of the military sector and financial sector in prioritizing and fixing vulnerabilities. In this regard, there was consensus that understanding the attack surface, and in turn protecting the breadth of the attack surface, is very much in its infancy.

The immaturity of organizational I&W capabilities is further highlighted by a lack of clarity regarding how warning processes work. More than twenty percent of respondents did not know the duration of gaps between the receipt of a warning of an attack and the actual response, a shortcoming that significantly impacts remediation and the impact of an attack. A cyber I&W process is ineffective if officials do not know the deficiencies of their organizations' responses, as such blind faith makes it harder to contain, mitigate, and respond to threat alerts.

In short, these interviews illuminated the extent to which security postures of organizations across government, industry, and academia are both nascent – where officials have incomplete understandings of their organizations' capabilities – and not well understood (or even over-confident with regard to maturity levels.

NARROW FOCUS ON KNOWN EXTERNAL THREATS

A malicious cyber actor is a threat to an enterprise when it has both *capability* and *intent* to exploit a *vulnerability* to gain unauthorized access to information or information systems. Any change in a capability, an intent, or a vulnerability can significantly modify the risk landscape for an organization. From this perspective, it is critical to have situational awareness of both external factors related to malicious actor capability and intent, and internal factors regarding an organization's own vulnerabilities.

In our follow-on interviews, respondents consistently noted a lack of visibility into external threats, and many respondents asserted that their situational awareness was narrowly focused on what they perceived as the greatest threat to their information systems. Such myopia makes it likely that organizations would miss efforts to penetrate a network by an unexpected adversary or even a known adversary employing innovative techniques. We believe this is a key challenge given the speed at which a capability, intent, and/or vulnerability can change in the cyber domain.

With the fast pace of technological and tradecraft change, and the creative use and reuse and existing capabilities, it is difficult to stay apace of threat actors' latest capabilities. Many of the most impactful ransomware in 2017, such as WannaCry (linked to North Korea), NotPetya (linked to Russia), and BadRabbit (linked to Russia) all leveraged exploits from the Shadow Brokers dump. Due to a proliferation of open source capabilities, threat actors increasingly have access to a treasure trove of sophisticated capabilities which they can deploy in novel ways that are difficult to anticipate.

Advanced capabilities are only a threat in the hands of an actor who intends to use it nefariously. Even though cyber threat analysts know a great deal about existing and potential threat actors, these actors' intentions can change quickly, whether due to state pressure, pursuit of profit, or just opportunistic chances to create havoc. The intent largely falls into two categories – opportunistic and targeted – and actors can move dynamically between these categories. For example, at the end of 2014, North Korea compromised Sony, causing massive destructive as well as reputational damages. In this case, the intent was to retaliate in response to a movie release. Two years later, North Korea was linked to an attack on the Bangladesh Central Bank with the SWIFT messaging systems acting as a conveyance of the eventual illicit transaction. The theft resulted in an $81 million loss.[9] The intent – and the capabilities deployed – varied significantly in each attack. A troubling development, however, is that the operational sophistication (or "tradecraft") demonstrated by malicious actors has advanced as swiftly as has their technological capabilities.

LIMITED INSIGHTS INTO INFORMATION TECHNOLOGY INFRASTRUCTURE

The follow-on interviews also revealed that respondents have little visibility into their own networks, such that they were unable to adequately assess their systems' vulnerabilities. This is a key challenge, as the depth and breadth of vulnerabilities greatly impacts exposure. For example, in 2014 a bug in OpenSSL, called Heartbleed, allowed attackers to pull a batch of working memory to servers, and made a range of high profile sites vulnerable, including Yahoo email accounts to video games and social networks. OpenSSL demonstrated that even widely used, legitimate software can be an attack vector. Threat actors increasingly hide malware within third-party software, which unknowingly propagates and diffuses the malware unbeknownst to the software vendor or user. Furthermore, the attack surface is also greatly expanding, as the exponential growth of the internet of things (IoT) and cloud-related services provides a wider range of entry points to a network that can lead to compromise. For the most part, these two trends portend an environment that is only becoming more vulnerable, expansive, and dynamic. It also is a key impediment in I&W. As an attack surface grows and understanding of vulnerabilities shrinks, it becomes difficult to know what to warn against.

> Organizations must more effectively integrate computational and automated methods into user-driven analytic frameworks.

To assess respondents' concerns regarding network vulnerabilities in this context, respondents were asked what kind of attacks or threats are most concerning to their organizations. Respondents from academia and government both noted data exfiltration as a higher concern than more specific types of malware or threat actors. This reflects a focus on preventing the theft of sensitive information – intellectual property for academic researchers and personal identifying information (PII) for government agencies that store such data on millions of citizens (clearance holders, taxpayers, recipients of agency services, etc.).

Responses from those in the private sector varied significantly. However, there was commonality with the outcome of the threats – any attack that impacts trust in a business, principally by undermining the target's ability to maintain operations and provide services – takes priority. Thus, corporations were concerned about ransomware and DDoS attacks, which could freeze up networks, and about SCADA attacks, which could prevent the delivery of services. At the very least, understanding what an organization cares about most can help facilitate an effective cyber I&W process under the guise of recognizing warning signs.

[9] *Joshua Hammer, "The Billion-Dollar Bank Job," New York Times, May 3, 2018. At https://www.nytimes.com/interactive/2018/05/03/magazine/money-issue-bangladesh-billion-dollar-bank-heist.html.*

A PROPOSED I&W FRAMEWORK

The lack of consensus surrounding cyber I&W illustrates a larger challenge across government and industry. On the policy side, to encourage more informed and proactive intelligence-driven defenses, the information security community would benefit from greater clarity on the fundamental building blocks of a cyber I&W framework. Organizations lack, for example, even a basic consensus on what is (or is not) a cyber attack more than 20 years after the first major breach of government systems – the penetration of computer systems at NASA, the Defense and Energy Departments, and universities doing government research, referred to as "Moonlight Maze".[10] No statutes exist to define what is or is not a cyber attack, which creates further confusion over what defensive measures (including active defense) may be permissible. Congress is considering legislation to define a cyber act of war, for example, demonstrating that the fundamental legal building blocks of a cyber I&W framework are still absent.

Across government, industry, and academia, greater insights on frameworks and approaches that work, and those that don't, would also be useful. This goes well beyond information sharing, requiring greater transparency and research into those analytic techniques that help enterprises better defend themselves with the resources they have available. Given the continually evolving threat landscape and the open source availability of sophisticated attack capabilities, organizations must more effectively integrate computational and automated methods into user-driven analytic frameworks as well. Too often these analytic frameworks focus solely on expert-developed methodologies or, conversely, take the human completely out of the loop with automation. Both are myopic approaches that not only ignore the potential of human-computer interaction, but also fail to consider the talent pipeline challenge.

[10]*See Kim Zetter, "New Evidence Links a 20-Year-Old Hack on the US Government to a Modern Attack Group," Vice, April 3, 2017. At https://motherboard.vice.com/en_us/article/vvk83b/moonlight-maze-turla-link.*

We propose a concept for a high-level framework for implementing a Cyber I&W program that will enable organizations to leverage structured analytic techniques and best practices to provide warning of an imminent malicious cyber scenario and proactively execute countermeasures against it. In this section, we offer a step-by-step overview on how to develop and implement a Cyber I&W program that addresses the shortfalls gleaned from our survey and interview results. The intent of this framework is to give government, academic, and industry professionals a practical analytic process in which an anticipated cyber attack is decomposed into indicators that can be continuously monitored to warn of an actual attack.

STEP 1: IDENTIFY & PRIORITIZE ASSETS

Identify what assets—to include data, personnel, devices, systems, and facilities—are most critical for the organization to fulfill its primary objective. This covers a wide range of areas, from increasing stock holder value and moving artillery across Eastern Europe to protecting customer data and reliably providing critical services. The first step falls under the category of asset management in the NIST Cybersecurity Framework and is focused on determining relative importance of an asset to prioritize its level of protection. Simply put, an organization cannot defend against everything and, based on our survey results, resources are likely to be an even more restricting factor. In cyber I&W, identifying and prioritizing what assets are most critical is the foundation necessary to be able to provide proactive warning.

STEP 2: REFINE THE THREAT

Threats to an enterprise in the cyber era can come in all shapes and sizes, from malicious nation states and non-state actors, to hacktivists, natural disasters and even colonies of "crazy ants" *(nylanderia fulva)* that, for unknown reasons, swarm electronics.[11] To provide effective warning, threats must be narrowed to those that could have the most consequential impact to the assets identified in step 1. From a threat actor perspective, this means determining who has the intent to target these assets and the capability to act on it. Although intent and capability can change, research should start with the top 10 to 15 threats as identified by the CTI team or equivalent via the following means.

STEP 3: ASSESS THREAT COURSES OF ACTION

Once the top 10 to 15 threats have been identified, a combined network defender and CTI team should decompose multiple scenarios by which each threat could or would take to achieve their objectives. The threat objective (e.g., deny system functionality or exfiltrate data) should be based on the assessed intent in step 2. In this case, the more discriminating scenario the better, as each adversary course of action (COA) should be distinct from each other so there is minimal overlap. The Lockheed Martin Intrusion Kill Chain and the MITRE ATT&CK methodology are both well-known models that can be used to develop various adversary COAs in this stage. The combined team leverages structured analytic techniques that can forecast the actions of an adversary, such as Role Playing or Red Hat Analysis[12]—taking the perspective of

[11] *Ben Guarino, "Swarming crazy ants with a penchant for destroying electronics are on the move in Texas," Washington Post, December 6, 2016. At https://www.washingtonpost.com/news/morning-mix/wp/2016/12/06/swarming-crazy-ants-with-a-penchant-for-destroying-electronics-are-on-the-move-in-texas/?noredirect=on&utm_term=.250541a9d84a.*

[12] *Step-by-step details on how to leverage this can be found in Richards Heuer, Jr., and Randolph Pherson, Structured Analytic Techniques for Intelligence Analysis, pp. 197-200.*

the attacker—to ascertain what steps the adversary would take in a given COA. This starts with how they prioritize their initial collection, to reconnaissance on specific areas through adversary-specific tactics, techniques, and procedures executed once in the network. There should be at least two COAs developed for each threat, a most likely and a most dangerous scenario. Caution should be given to only addressing known capabilities; elements such as insider threat techniques or supply chain interference should be included if the adversary may have a future capability to execute it. The key to this step is leveraging analytic techniques such as the previously mentioned Red Hat Analysis in order to minimize mirror imaging and think like the adversary based on their perceived worldview and objectives.

STEP 4: BREAK DOWN SCENARIOS INTO INDICATORS

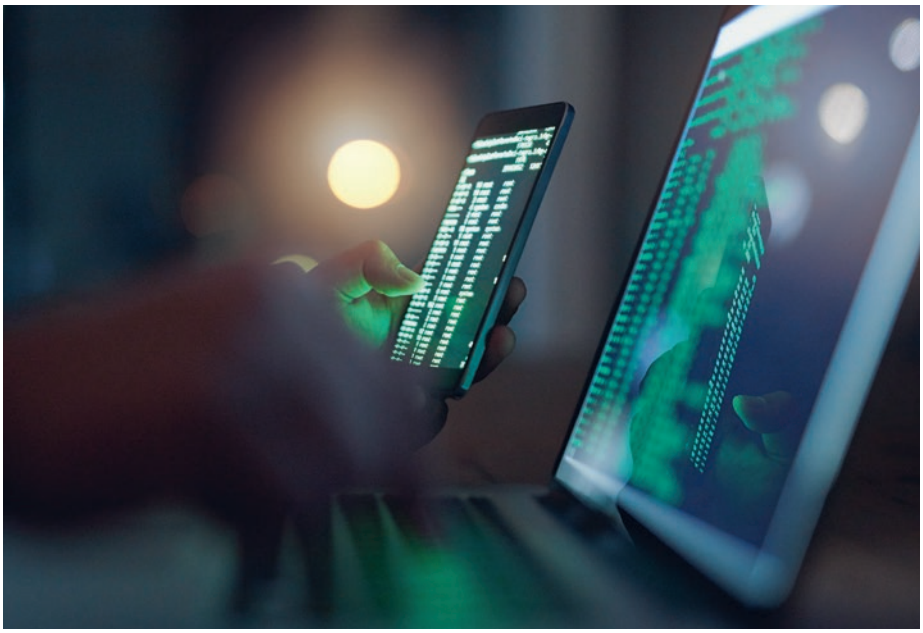
After the adversary COAs are developed, they must be "decomposed," or broken down, into indicators (a.k.a., road signs or trip wires) that can be used to highlight when a given COA is coming to fruition. This step is key to the indicators that make up the "indications" in "indications and warning." Indicators by themselves are not necessarily a cause for alarm, but they can show that an anticipated scenario is beginning to emerge. In this step, a series of indicators are generated for each assessed adversary COA. The number of indicators are relative and can be as few or as many as the team needs to adequately identify a given situation. Once they are developed, each indicator is brought through the Indicators Validator Model[13] to develop the most discriminating indicators for each scenario. This will eliminate indicators that would be highly likely to emerge in multiple scenarios as well as those that are most likely to only emerge in a single scenario.

STEP 5: PLAN AND EXERCISE COUNTERMEASURES

Once the series of COAs and subsequent indicators are developed for each threat, the CTI analysts and network defenders must determine what friendly actions will need to occur when warning of a specific scenario is beginning to emerge. Elements of this step may already be part of a risk management program or even an incident response plan, but – as identified in the survey results – people, process, and technology must all be in place and exercised ahead of time to effectively respond to warning of an imminent attack. Thus, in this step, network defenders must determine what countermeasures need to be put in place as an adversary COA is coming to fruition. That is, once warning is received: who is responsible for providing the information, via what mechanism, at what precedence; who does what with the warning, at what threshold; who is informed; what technology is leveraged; and what changes need to be made to the organizational posture. Often this would start as more detailed monitoring or prioritized collection and becoming progressively more impactful as the scenario plays out. The objective is to plan countermeasures for each indicator identified in step 4, in a given COA and exercise them regularly. Although an organization cannot plan for every possible scenario, assessing and planning against the most likely and most dangerous scenarios from primary threats can significantly decrease risk.

[13]*Step-by-step details on how to leverage this can be found in Richards Heuer, Jr., and Randolph Pherson, Structured Analytic Techniques for Intelligence Analysis, pp.140-142.*

STEP 6: ALIGN TO THE INTELLIGENCE CYCLE



At this point, information must be collected against each indicator via any viable collection method available to the CTI team. Depending on maturity level, this may be internal collectors (organic collection capability), external collectors (vendors or other organizations), or a combination of both. The CTI team must develop a collection requirement matrix to align each indicator, its relative priority, what is currently tasked to collect (internal/external) on it, and what its status is. Each indicator must have at least one collection resource assigned to it as well as a stated reporting requirement based on the priority. Although some indicators, if tripped, would warrant a notification within 24 hours, some may be considered "wake up" criteria and require immediate notification. These are often part of an organizations "priority intelligence requirement" process. The job of the CTI team is to ensure each indicator is being collected on, notification processes are set up when they are triggered, and analysis and production is in place to synthesize indicators within the context of the previously established adversary COAs. Each situation is different. In some cases, a single indicator may rise to a wakeup call; other times it may take multiple triggers to reach the same threshold. This process would have been solidified in step 5 during countermeasure planning based on what the network defenders require.

STEP 7: EXECUTE PROACTIVE COUNTERMEASURES

Finally, now that the cyber I&W program is in place, leverage the tailored collection posture to continuously monitor indicators being "triggered or tripped" for a previously assessed adversary scenario against critical assets. The CTI team (or equivalent) should disseminate this information to decision makers and network defenders on a routine cadence and on an ad hoc basis as key indicators are triggered or multiple indicators are apparent that implies imminent warning of an adversary COA. Adversary scenarios should be consistently re-evaluated as the threat landscape changes and indicators should be updated as capabilities change and vulnerabilities are altered. The end state is a robust I&W program that can provide warning of an impending cyber threat adversary action and proactively implement countermeasures to mitigate or minimize impact.

RECOMMENDATIONS

Survey responses indicated that cyber I&W has been hindered in government, industry, and academia by several trends, including a shortage of personnel with both cybersecurity and intelligence analysis skills, a dearth of financial resources, and a lack of a general framework for approaching I&W in the cyber domain. Organizations' ability to perform anticipatory analysis of malicious cyber activity is further hindered by overestimation of defensive capabilities, a narrow focus on known threat capability and intent, and limited insights into network vulnerabilities – all of which which make it less likely that an organization will be able to identify and mitigate unexpected attack techniques or aggression from unknown threat actors. Such inadequate reactive measures make it particularly critical that organizations take increasingly proactive approaches to understanding external threats and internal vulnerabilities and acting promptly on threat information once it is received.

The following are some recommendations that could help government agencies, private companies, and academic institutions prioritize resources and move organizations toward more proactive defense postures.

1. **Implement the Proposed I&W Framework.** In order to implement the cyber I&W framework above, a small dedicated group of CTI analysts should be trained on the structured analytic tradecraft techniques identified. For Red Hat Analysis, the team should also have access to cultural experts or outside entities that can effectively think like the adversary without mirror imaging. Given the framework will require input and analysis from the entire information security team, the cyber I&W lead should ensure a collaborative approach to working through the scenarios, indicators, and countermeasures. Given the results of the survey on lack of resources and funding, we attempted to provide a concept that would be low cost and high impact with little to no significant cybersecurity program changes needed. In essence, the cyber I&W framework was meant to be set up, implemented, and monitored with as little effort as possible given the reality of current fiscal and talent constraints. Executed properly, the above I&W framework would enable warning of an impending malicious cyber action against critical assets of an organization in order to proactively implement countermeasures.

2. **Foster a Talent Pipeline and Improve Personnel Retention Programs.** As discussed earlier, organizations have long focused on the talent shortage in cybersecurity. While recruiting and training merit continued emphasis, organizations in both government and industry would be wise to increase their focus on retention of skilled personnel. Broadening the talent pool helps both recruitment and retention by fostering greater diversity and a more inclusive environment. Cybersecurity is a multi-disciplinary field that increasingly benefits from a wide range of backgrounds and experiences. Organizations should think creatively about where and how they attract talent, structure job descriptions to be inclusive and appealing, and offer transparent career growth and professional development.

3. **Improve Understanding of Cyber Threats and Internal Cyber Defense Capabilities.** As our survey and follow-on discussions illustrated, organizations face large gaps in understanding the threat, their organizational capacity, and the attack surface. First, the range of attack vectors, from DDoS attacks to phishing campaigns to insider threats, are broad and far-reaching. Organizations must develop a broader understanding of industry attack trends, as well as local, regional and global attack trends, to better understand how and for what purpose an adversary may attack. Second, as this project confirmed, executives and those who work in firms' Security Operations Centers have widely different perceptions of an organization's defensive capacity. This gap impacts resource allocation and can even lead to a false sense of security if executives underestimate the threats they face or overestimate their organizations defensive capabilities (to include I&W). Every organization can be a target, and the sooner organizations acknowledge they are at risk and identify their most essential resources for protecting, the sooner they can begin to better comprehend the threat environment. Finally, our research revealed just how common it is for organizations to lack the proper understanding of the breadth and depth of their networks. It is extremely difficult to craft a cyber I&W strategy devoid of a comprehensive understanding of the various applications and nuances of an organization's network. Organizations should prioritize the creation of a comprehensive analysis of their vast networks, identifying those that contain the 'crown jewels' and focusing defensive efforts on protecting them.

4. **Convene a Best Practices Information-Sharing Group.** Given the wide range of cyber defense initiatives and the absence of formal I&W programs in nearly half of all respondents' organizations, government, industry, and academia could all benefit from a coordinated effort to share information and best practices. The Office of the Director of National Intelligence (ODNI) could charter an I&W working group with representatives from across the Intelligence Community to develop training in I&W tradecraft and analytic methods for cyber analysts from all sectors. An industry association could gather cyber defense experts from all sectors to share insights on ways to maximize cyber defense effectiveness through organizational reform, information-sharing, the implementation of a warning-driven cyber defense analytics capability, and human capital development.

5. **Conduct Exercises to Test Capabilities and Integrate Lessons Learned.** Once an organization has developed a durable I&W capability, they should periodically conduct simulated real-time exercises – driven by the priority threats to the specific organization – that involve all relevant stakeholders throughout the organization, to include the senior-most executives and decision makers, Board members (if applicable), cyber threat analysts, legal experts, and public affairs/media officials. Routinely testing I&W capabilities can expose gaps in preparation and response functions, surface hidden cyber vulnerabilities, and identify best practices and lessons learned that can be incorporated to strengthen an organization's I&W capabilities and resiliency planning.

> A Cyber I&W framework is essential to becoming more proactive, getting ahead of the threat, and managing risk.

CONCLUSION

Cyber I&W is relevant for virtually all organizations across sectors, as both targeted and opportunistic attacks render anyone susceptible to an attack. A Cyber I&W framework is essential to becoming more proactive, getting ahead of the threat, and managing risk. Our survey demonstrated that common shortcomings across the private sector, government and academia hinder organizations' implementation of a more proactive, well-informed, defensive posture.

There are many key factors that continue to limit progress toward implementation of cyber I&W frameworks across all sectors. The concept itself remains somewhat nebulous, which hinders both theoretical and operational advances in cyber I&W and limits the sharing of best practices and successful methodologies. A lack of both financial and human resources also appears to prevent robust cyber defense programs. Greater transparency on methodologies could help organizations develop more optimal approaches and resource allocations, particularly given the lack of consensus on best practices. Finally, given that almost half of those polled lack any kind of program warning of an impending cyber attack, there are significant opportunities to develop and implement even basic I&W initiatives by drawing on the experience of those organizations that do have such programs.

ABOUT INSA

The Intelligence and National Security Alliance (INSA) is a nonpartisan, nonprofit forum for advancing intelligence and national security priorities through public-private partnerships. INSA's government and private sector members collaborate to make government more effective and efficient through the application of industry expertise and commercial best practices. INSA's 160+ member organizations are leaders in intelligence collection and analysis, data analytics, management consulting, technology development, cybersecurity, homeland security, and national security law, and its 4,000 individual and associate members include leaders, senior executives, and intelligence experts in government, industry, and academia.

ABOUT INSA'S CYBER COUNCIL

INSA's Cyber Council seeks to fuse knowledge from industry, government, and academic experts in order to provide authoritative and influential insights regarding the national security challenges present in the cyber domain. The Council works to promote a greater understanding of cyber threats, challenges, and opportunities that can be addressed effectively through public-private collaboration.

INSA

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

Building a Stronger Intelligence Community

(703) 224-4672 | www.INSAonline.org