



STRATEGIC CYBER INTELLIGENCE

INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

CYBER INTELLIGENCE TASK FORCE

MARCH 2014



ACKNOWLEDGEMENTS

INSA CHAIRMAN

Ambassador John Negroponte

INSA SENIOR INTELLIGENCE ADVISOR

The Honorable Charlie Allen

INSA SENIOR NATIONAL SECURITY ADVISOR

Ambassador Bob Joseph

INSA STAFF

Ambassador Joe DeTrani, *INSA President*

Chuck Alsup, *INSA Vice President for Policy*

Maureen McGovern, *INSA Senior Fellow*

English Edwards, *Marketing & Communications Coordinator*

Rick Dembinski, *INSA Intern*

Adam Goldwater, *INSA Intern*

Garrett Johnson, *INSA Intern*


CYBER COUNCIL LEADERSHIP

Terry Roberts, *INSA Cyber Council Co-Chair* 

Ned Deets, *Software Engineering Institute, INSA Cyber Council Co-Chair* 

CYBER INTELLIGENCE TASK FORCE WRITING TEAM

Kristen Dennesen, *Senior Threat Intelligence Analyst, Client-Directed Research* 


John Felker, *Director, Cyber and Intelligence Strategy U.S. Public Sector, Enterprise Services* 

Tonya Feyes, *CEO, TF Solutions*

Sean Kern, *Lt Col, USAF, Assistant Professor* 


CYBER INTELLIGENCE TASK FORCE EDITING TEAM

Randy Borum, *Professor and Coordinator for Strategy & Intelligence Studies, School of Information* 

Andrea Little Limbago, *Chief Social Scientist* 

Charlie Shaw, *President, Charles E. Shaw Technology Consulting, Inc.*

EDITORIAL REVIEW

Joe Mazzafrò 

COPY EDITORS

Beth Finan

Amanda Patino

*** Participation on the Task Force/Council or Subcommittee does not imply personal or official endorsement of the views in the paper by any members or their respective parent organization(s).*



Join the discussion for this white paper online using #INSAWhitePaper

INSA SUPPORTS A HEALTHY PLANET

INSA White Papers are printed on recycled paper that is 50% recycled content including 25% post consumer waste.



“The construct of strategic, operational, and tactical levels of intelligence aids...in visualizing the flow of intelligence from one level to the next. This construct facilitates the allocation of required collection, analytical, and dissemination resources and permits the assignment of appropriate intelligence tasks.”

JOINT PUBLICATION 2-0, JOINT INTELLIGENCE

EXECUTIVE SUMMARY

In a September 2013 white paper, *The Operational Levels of Cyber Intelligence*, the Intelligence and National Security Alliance (INSA) proposed definitions for the strategic, operational, and tactical levels of cyber activity. While there has been much emphasis on tactical cyber intelligence to help understand the “on-the-network” cyber-attacks so frequently in the news, there has been little discussion about the strategic and operational levels in order to better understand the overall goals, objectives, and inter-relationships associated with these tactical attacks. As a result, key consumers such as C-suite executives, executive managers, and other senior leaders are not getting the right type of cyber intelligence to efficiently and effectively inform their organizations’ risk management programs. This traditionally tactical focus also hampers the capability of the cyber intelligence function to communicate cyber risks in a way that leaders can fully interpret and understand.

The fundamental purpose of this white paper is to promote thought and dialogue on the importance of cyber intelligence, specifically strategic cyber intelligence, to senior leaders' risk-informed decision making in public, private and academic sectors, ultimately leading to improved strategy, policy, architecture, and investment. The paper discusses the:

- Nexus between strategic cyber intelligence and risk management in relation to strategic cyber intelligence consumer and producer roles and responsibilities.
- Role of strategic cyber intelligence analysis based upon the National Institute of Standards and Technology (NIST) risk assessment methods: vulnerability-based, threat-based, and impact-based.
- Inextricable linkage between intelligence production and information sharing.

Strategic cyber intelligence offers senior leaders an accurate assessment of how to direct cyber-related expenses in line with an organization's risk heuristic. Leveraging strategic cyber intelligence to address strategic information requirements allows an organization to:

- Effectively assess, explain, and quantify risk to senior management and other key stakeholders.

- Collaborate in a more meaningful manner with members of law enforcement, defense organizations, the intelligence community, and the information security community on interests at large.
- Demonstrate an appropriate standard of diligence to auditors, regulators, and stakeholders.
- Reduce the exposure of the business to regulatory or legal sanctions.
- Demonstrate responsible security resource expenditures by defending not just what is important to the firm but what is relevant to the threat.

The ultimate goal of such a program is to reduce risk to an organization's critical mission and assets. It enables senior leadership to make informed decisions and proactively defend the enterprise. A successful strategic cyber intelligence model will play a crucial role in defending private companies and government sectors by providing, through 2014 and beyond, the necessary intelligence to prevent potential incidents that have the ability to cripple U.S. Security and economy.

INTRODUCTION

The “flow of intelligence” occurs across the strategic, operational, and tactical levels of an organization. As such, there is no simple demarcation from one level to the next and, as discussed in the previous INSA white paper, *“Operational Levels of Cyber Intelligence,”* these levels actually overlap in practice. Nonetheless, they provide a useful construct to aid organizations in directing the appropriate resources and effort toward intelligence activities that support strategic objectives. This paper will discuss the first, or strategic, level of intelligence.

There has been much emphasis on tactical cyber intelligence to support the “on-the-network” fight, but there has been little discussion about the strategic and operational levels. As a result, key consumers such as C-suite executives, executive managers, and other senior leaders may not be getting the right type of cyber intelligence to efficiently and effectively inform the organization’s risk management program. The tactical focus is apparent from the language used by the U.S. House of Representatives to define cyber threat intelligence as “information in the possession of an element of the intelligence community directly pertaining to a vulnerability of, or threat to, a system or network of a government or private entity, including information pertaining to the protection of a system or network... (H.R.3523).” Note the focus on “system” and “network” rather than an organization’s strategic assets such as intellectual property, trade secrets, sensitive business information, and other data that contribute to an organization’s competitive advantage, including brand protection. This traditionally tactical focus also hampers the capability of the cyber intelligence function to communicate cyber risks in a way that leaders at operational and strategic levels can fully interpret and understand.

This white paper seeks to demonstrate the centrality of cyber intelligence, specifically strategic cyber intelligence, to senior leaders’ risk-informed decision making, ultimately leading to improved strategy, policy, architecture, and investment.

RSA defines cyber intelligence more broadly as “knowledge about cyber adversaries and their methods combined with knowledge about an organization’s security posture against those adversaries and their methods”¹ from which situational awareness and/or actionable intelligence is produced. In RSA’s words, actionable intelligence is “knowledge that enables an organization to make decisions and take action.”² The Carnegie Mellon Software Engineering Institute uses “the acquisition and analysis of information to identify, track, and predict cyber capabilities, intentions and activities that offer courses of action to enhance decision making”³ as its definition of cyber intelligence.

In consideration of the definitions above, INSA believes that strategic cyber intelligence, as well as the other levels of cyber intelligence, will have a slightly different meaning for each organization because of size, complexity, mission and related attributes. As such, each organization would be best served by defining the levels of cyber intelligence for its own unique circumstances, using the following six key criteria:

1. The nature, role, and identity of the consumer;
2. The decisions the consumer will make;
3. The time frame in which the consumer tends to operate;
4. The scope of collection;
5. The characterization of potential adversaries;
6. The level of technical aptitude available for cyber intelligence collection.

Based on these criteria, strategic cyber intelligence is produced for senior leaders in both private and public sectors. It is used to inform the development of organizational or national strategy and policy that will direct the organization over the long term (3+ years). Collection is broad and will target cyber intelligence related to the sector to which the organization belongs and likely also includes complementary sectors (e.g., R&D and manufacturing, supply chain). Adversaries of interest may be a broad group of state and non-state actors with both intent and capability. Finally, strategic cyber intelligence is generally non-technical in nature. It focuses on inter/intra sector trend analysis, stated and unstated intent and objectives of potential adversaries, and other strategic indicators such as geopolitical events.

Strategic cyber intelligence is also a critical element of institutional risk management. It should consider threats, vulnerabilities, potential impact, and available countermeasures. It is important that the organization's intelligence function utilizes the existing organizational or enterprise risk frameworks to ensure cyber risks are understood in the context of all risks strategic leaders must assess. Strategic cyber intelligence should utilize existing enterprise

terminology, or through communication and awareness, adapt the culture to understand cyber terminology. It is helpful to think of this in terms of a "risk heuristic," which the Task Force defines, based upon the National Institute for Standards and Technology's (NIST) "Glossary of Key Information Security Terms," as:

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event.

Threat Agent: The intent and method targeted at the intentional exploitation of vulnerability.

Impact: The magnitude of harm that can be expected to result from the consequences of a Threat Agent successfully exploiting vulnerability.

Countermeasure: Actions, devices, procedures, techniques, or other measures that reduce vulnerability.

The Task Force's description of a cyber intelligence definition and accompanying risk heuristic offer a useful way to frame this paper in defining strategic cyber intelligence. First, the paper discusses the nexus between strategic cyber intelligence and risk management in relation to strategic cyber intelligence consumer and producer roles and responsibilities. Second, this paper describes the role of strategic cyber intelligence analysis in the context of three NIST risk assessment methods: vulnerability-based, threat-based, and impact-based.⁴ Finally, a discussion will ensue regarding the inextricable linkage of the development of intelligence and information sharing.

STRATEGIC CYBER INTELLIGENCE AND RISK MANAGEMENT

The involvement of senior leadership is critical for a strategic cyber intelligence program to be an effective component of risk management. Senior leaders are the consumers and it is their role to define and clearly communicate the organization's critical intelligence requirements. NIST emphasizes this point:

*To be effective, organization-wide risk management programs require the strong commitment, direct involvement, and **ongoing support from senior leaders**. The objective is to establish strategic risk assessment and then institutionalize the appropriate risk management into the day-to-day operations of an organization as a priority and an integral part of how organizations conduct operations in cyberspace.⁵*

Further, Joint Publication 2-0 offers examples of senior leader intelligence requirements:

1. Commander's Critical Information Requirements (CCIR)
2. Priority Intelligence Requirements (PIR)
3. Friendly Force Information Requirements (FFIR)

Though associated with the Department of Defense (DoD), intelligence requirements apply equally to the private sector. It is the senior leader's responsibility to orient strategic cyber intelligence analysis resources against the enterprise's most critical mission and business needs and strategy, rather than leaving it to the analyst.⁶ An overall enterprise approach taking into account risk versus benefit needs to be applied. Identifying an organization's assets of value such as intellectual property, business operations, agency/company financial information, and personally identifiable information (PII) is an important aspect of an organization's overall risk assessment. Strategic cyber intelligence can assist in determining which assets are relatively more valuable and potentially more vulnerable. These are key leadership decisions. Methods such as: risk scoring of threats and vulnerabilities by potential impact, business impact analysis, and other approaches can help align the enterprise's analysis and security steps, and inform decision making with regard to mitigating identified threats and vulnerabilities.

Current practices may not adequately reflect cyber risk in a strategic context. Day-to-day, risk-based security management is often based on a compliance mindset and predicated on practices and policies intended to secure networks, data, applications, and operating systems. A recent survey of 1,300 IT professionals in the U.S. and UK illustrates this inclination toward a narrow network focus. The Ponemon

DEFINING STRATEGIC CYBER INTELLIGENCE REQUIREMENTS

In defining strategic cyber intelligence requirements, three important sets of information needs must be settled by senior leaders and integrated to form the basis for sound decision making.

1. What information the senior leadership team needs to make strategic decisions (Critical Information Requirements)
2. What information about the potential adversary (or external environment) is needed (Priority Intelligence Requirements)
3. What security posture is in place related to your organization's assets of value (Friendly Forces Information Requirements).

These three sets of intelligence form the basis for beginning the strategic planning process.

Institute asked how the respondents planned and conducted risk-based security management program governance.⁷ The responses included specific, tactical metrics such as: time taken to patch, number of policy violations, uninfected endpoints and data breaches, status of end user training, and amount of unscheduled downtime.

From a strategic perspective, these are not metrics that should be reported to support the decision making of an organization's senior leaders. The only cyber-related considerations that matter in a strategic sense are those that impact an organization's ability to achieve its strategic objectives. Examples include:

- Does the organization operate in a high, moderate, or low cybersecurity risk industry?
- What is the value of the organization's information and information flows to potential threat actors?
- What are the confidentiality, availability, and integrity risks to the organization's assets?
- What legal liabilities exist related to the type of information stored, such as PII or Health Insurance Portability and Accountability Act (HIPAA)-protected data?

“Senior leaders will measure and invest in what they understand – strategic intelligence about their cyber posture helps them do just that.”

To illustrate how answers to these and other questions will influence the intelligence requirements of senior leaders, consider the case of a company that runs a high-volume e-commerce operation and considers availability of its website to be critical. Consequently, intelligence on threat

actor tactics, techniques, and procedures (TTPs) related to a distributed denial of service (DDoS) attack is likely of high strategic importance. Likewise, a company that is considering new operations in a foreign country would place a high value on cyber intelligence that helps them orient their security posture to indigenous threats.

As these examples illustrate, network metrics are not sufficient risk analyses on their own. Rather, senior leaders must define their organizations' strategic cyber intelligence requirements based on what assets and programs are of critical value to the business and the organization. Organizations may look to gather intelligence both inside and outside the organization.

In the public sector, the main producers of intelligence are the Department of Homeland Security (DHS), the Department of Justice (DoJ), and the DoD. In March 2013, DHS, DoJ, and DoD mutually defined specific roles that each will fulfill to support national cybersecurity. The “U.S. Federal Cyber Security Operations Team” agreement assigns DHS the responsibility to disseminate domestic cyber threats and vulnerability analysis through the National Communications and Cyber Information Center (NCCIC) and the private-sector Information Sharing and Analysis Center (ISAC) construct.⁸ DoJ's National Cyber Investigative Joint Task Force (NCIJTF) investigates, analyzes, and correlates ongoing cybercrime incidents since DoJ leads all domestic national security operations. Finally, DoD is responsible for gathering foreign cyber threat intelligence.

Private sector organizations with sufficient resources may develop organic cyber threat and/or business intelligence units for their strategic cyber intelligence requirements. Smaller organizations may opt to outsource theirs to private cyber security and cyber intelligence providers and others with global access to threat information.

Cyber intelligence assists decision makers and influences not only security but also the overall stability of the enterprise. The point to be made is that senior leaders will measure and invest in what they understand – strategic intelligence about their cyber posture helps them do just that.

STRATEGIC CYBER INTELLIGENCE AND THE THREE METHODS FOR ASSESSING RISK AS DEFINED BY NIST: *Threat Assessment, Vulnerability Assessment, Impact Assessment*

THREAT ASSESSMENT: STRATEGIC CYBER INTELLIGENCE'S PRIMARY ROLE

Many organizations do not consider themselves to be attractive targets for a cyber incident until after the event occurs. In order to prevent strategic surprise, organizations should perform a threat-based assessment that takes an outward-looking, intelligence-driven approach to understanding the threat landscape and identifying potential threats. Based on an inventory of the organization's critical assets, the strategic cyber intelligence function must evaluate which cyber threat actors are likely to target the organization in a cyber incident and why. Potential actors of interest include malicious insiders, cyber criminals, terrorists, hacktivists, nation-states, and the interactions and collaborations of these actors.⁹ Once the organization has identified which actors pose a threat, subsequent analysis must consider their motivation and intent, as well as their technical and analytical capabilities. This analysis is a continuous process.

With a strong understanding of the adversary, the enterprise can evaluate risk, which may include direct impacts to the organization or collateral damage that threat actors did not originally intend. The organization must then evaluate what strategic vulnerabilities the threats might exploit to compromise the organization's information assets such as intellectual property and IT infrastructure. The vulnerability assessment discussed in the next section, combined with the threat assessment, provides a basis for this evaluation and delineates the organization's potential attack surface. By assessing these factors, the threat intelligence team provides senior leaders and risk managers with an invaluable tool for understanding the firm's exposure to a potential incident.

The organization should also seek to understand the adversary's thought process through red teaming. Red team analysts are well-versed in adversary doctrine, strategies, and TTPs. This enables them to "step into the shoes" of the threat actor. The analytical process should ask, "Based on the adversary's strategic goals, which organizations would I target, and how?" and "What methods would I use to achieve my objectives?" A well-executed red teaming exercise asks these questions through the lens of the adversary's socio-cultural frame of reference, as well as its perspectives of the threat landscape, and perceptions of its constraints, source of authority, and its adversary. This "know your enemy" exercise mitigates the likelihood of "mirror imaging,"¹⁰ enabling the organization to explore the adversary's possible motivation and intent, as well as avenues of attack, including hypothetical scenarios not yet observed in the operating environment. In addition to understanding adversary motivation and intent through red teaming, the threat assessment must drive the organization's understanding of how shifts in the threat environment affect adversary behavior and outcomes.

There are two interrelated concepts for tracking strategic level changes within the threat environment. First, understanding and evaluating the threat as a baseline of adversarial behavior is foundational for more proactive indicators. But, at a strategic level, understanding of the potential threat is not enough. It is essential to be aware of patterns of behavior (especially as

they pertain to the kinds of targets and frequency of attacks), evaluate threat strengths and weaknesses over time, and explore key events and personas that drive the behavior of a cyber threat. This is where a comprehensive understanding of aspects outside of the technical domain is essential to complement the tactical and operational levels of cyber intelligence. Second, geopolitical context, human networks, and world events can all greatly influence the development of cyber indicators. Together, these two concepts provide a strategic level, common cyber intelligence picture, and empower organizations with a more holistic understanding of the threat landscape. Ideally, these are not explored in analytic silos, but rather as key components of the larger cyber intelligence picture.

At a strategic level, an enterprise may pose the following questions as part of a cyber Indications and Warning (I&W) framework:

- How does the enterprise define the threat environment, in terms of mission and business operations?
- What is the political and economic landscape in each region of concern? What is the precedent for threat activity in the region? What future outcomes could shift the operating environment?
- Can the enterprise mitigate, eliminate, accept, transfer, or avoid the risk?
- Which threat actors operate in this environment or pose a threat to specific operations?
 - How do these threat actors pose a threat to the enterprise?
 - Do the threat actors pose an indirect risk, such as attacks on the enterprise supply chain?
 - What factors drive the threat's decision making? What potential changes in the threat environment might impact the adversary's decision tree?
 - How do the firm's business operations intersect with the adversary's goals? What changes to the operating environment might increase/decrease the probability of threat activity? What resource

decisions will be required to enact those changes?

- What are the threat's capabilities, common TTPs, and the likely impacts to the enterprise?

These questions enable the development of an I&W framework that allows the organization to track current and potential future threats as they relate to business operations. It is important that the I&W framework be integrated into the enterprise risk and decision frameworks at the operational and strategic levels. For example, an energy company may determine that because of its involvement in environmental policy issues, the company is likely to be targeted in any hacktivist campaign focused on global warming. Therefore, the company integrates collection and analysis of environmental protest activity into its strategic I&W framework.

Regardless of the business context, an effective I&W implementation continually scans the threat environment for anomalies and assesses how the adversary will adapt to changes. Therefore, organizations should supplement strategic I&W collection with an operational I&W program that tracks day-to-day changes in the operating environment.

An organization's threat assessment function can evaluate potential cyber threats using open source intelligence collection and analytical exercises. However, even a robust collection and analysis program will not cover the complete range of possible and actual threat activity. For this reason, the organization must supplement ongoing collection and analysis efforts with information sharing efforts.

The threat assessment enables an evaluation of the cyber threat landscape and how an organization's critical information assets fit into that landscape. Through an understanding of the strategic context of business operations, the organization can prioritize which threat actor classes should be the subject of intelligence collection efforts. Moreover, strategic threat assessment enables organizations to implement defenses and educate stakeholders through a better understanding of its adversary's collection requirements and long term strategic goals.

To realize the benefits of a strategic threat assessment program, organizations must continually assess the threat

landscape and evaluate the impetus behind threat actor activity. By understanding the threat actor's intent and long-term strategic goals, organizations place themselves in an enhanced position to protect assets of value and minimize the threat's impact.

VULNERABILITY ASSESSMENT: A KEY CYBER INTELLIGENCE AND CYBER DEFENSE PARTNERSHIP

Following NIST's recommendations, organizations should adopt a vulnerability-oriented risk analysis approach as part of a risk management program. An organization starts "with a set of predisposing conditions or exploitable weaknesses/deficiencies in organizational information systems or the environment in which the systems operate, and identifies threat events that could exercise those vulnerabilities together with possible consequences of vulnerabilities being exercised."¹¹

Strategic cyber intelligence analysis supports a vulnerability-oriented risk analysis by engaging the organization's cybersecurity experts to gain understanding of the organization's existing cyber-enabled critical mission and business function and process vulnerabilities. Vulnerabilities related to the sector or complementary sectors in which the organization operates, as well as key trust relationships with other organizations and agencies are key concerns at the strategic level. One method for addressing these issues is to assess an organization's "attack surface."

Stephen Northcutt of the SANS Technology Institute describes an organization's attack surface as its "reachable and exploitable vulnerabilities." In the context of defense-in-depth, Northcutt lists three attack surfaces worth considering: network, software, and human.¹² An alternative to this attack surface model is to use the concept of cyberspace "geography" to model an organization's attack surface. In this model, the domain can be viewed as a number of layers. This is currently embraced by a number of departments and agencies, including U.S. Cyber Command.¹³ In one version of this model, cyberspace is comprised of a geographic layer, a physical network layer, a logical network layer, a device layer, a persona layer, and the actual individual user layer.

Whether using the SANS or six-layer cyberspace model, it is important to consider trust relationships between the target organization and other organizations since a risk taken by one is a risk assumed by all. NIST defines trust as "a belief that an entity will behave in a predictable manner in specified circumstances."¹⁴ NIST further states three characteristics associated with trust. Trust is (1) usually relative to a specific

circumstance or situation, (2) generally not transitive, and (3) generally earned, based on experience or measurement.

Strategic cyber intelligence analysis should understand and account for these domestic, international, public, and private sector linkages and interdependencies as they develop the model. For example, trust relationships with a particular industry or company size may put an organization at risk, as illustrated in the 2013 Verizon Data Breach Investigations Report which categorized data breaches based on industry and company size.¹⁵ Verizon noted that the manufacturing industry and companies with fewer than 1,000 employees were hardest hit by likely cyber espionage-related incidents. Strategic cyber intelligence analysis must consider these relationships in the overall threat assessment for their organization.

An accepted standard in the cybersecurity realm is to categorize vulnerabilities as people, process, and technology weaknesses (often denoted as "PPT"). PPT vulnerabilities should be assessed for each attack surface and/or each cyberspace layer. Further, cybersecurity usually centers around three common goals: confidentiality, integrity, and availability (often denoted as "CIA"). Factoring in PPT and CIA provides a rich, diverse vulnerability space assessment.

IMPACT ASSESSMENT: THE MISSION AND BUSINESS COST OF A SUCCESSFUL EXPLOIT

The third and final approach to Risk Assessment according to NIST is impact-oriented. This approach "starts with the identification of impacts or consequences of concern and critical assets, possibly using the results of a mission or business impact analyses and identifying the threat events that could lead to and/or threat sources that could seek those impacts or consequences".¹⁶

Whereas the strategic cyber intelligence function was the lead for the threat-oriented analysis and a supporting partner to the organization's cybersecurity experts in the vulnerability-oriented analysis, in impact-oriented analysis the strategic cyber intelligence function directly supports senior leaders.

Senior leaders are responsible for establishing strategy, governing, determining risk tolerance, and developing and executing the resourcing strategy to manage risk for the organization. Strategic cyber intelligence analysis should inform these functions to reduce uncertainty and improve decision quality. A firm understanding of the impacts the senior leaders view as critical to the organization's mission and business processes is a prerequisite for success.

One area in which strategic cyber intelligence analysis can serve senior leaders is with respect to quantitative risk analysis, which attempts to assign numerical values to risk components which in turn improve the building of business cases and return on investment discussions. Quantitative risk analysis can be difficult for the enterprise in the cyber area; good quality intelligence will increase the confidence of decision makers in the risk data.

A common methodology involves determining the exposure factor (EF) and annual rate of occurrence (ARO) for a given risk. An exposure factor is the subjective, potential

percentage loss to a specific asset if a specific threat is realized.¹⁷ But how often can one expect a given risk to be realized? Estimating the annualized rate of occurrence attempts to answer that question. The ARO is the estimated likelihood of that risk materializing within a 12-month time frame. Strategic cyber intelligence analysis performs estimative analysis to assess the probability or likelihood that a threat has the intent and capability to exploit the given vulnerability. Once the ARO is determined, the organization can then calculate the annualized loss expectancy (ALE) which is used for strategic resource decisions.¹⁸

CYBER IS A TEAM SPORT: A RISK ASSUMED BY ONE IS A RISK SHARED BY ALL

The private sector can and should tie in to public-sector strategic cyber intelligence producers through mechanisms such as the ISAC. This is one leverage point for private-public information sharing which is an essential element of strategic cyber intelligence. In the words of General Keith Alexander, Commander, U.S. Cyber Command and Director National Security Agency, "Securing our nation's network is a team sport" that requires close collaboration between government and the private sector.

To this end, the U.S. government has followed recommendations of the 2009 White House Cyber Policy Review and the Center for Strategic and International Studies (CSIS) report "Security Cyberspace for the 44th Presidency" and implemented several information sharing regimes. Through these programs, private sector organizations can exchange cyber threat information with peer institutions from their industry sector, as well as receive critical threat updates from the U.S. Intelligence Community. While some challenges remain to establishing efficient information sharing, the U.S. government has achieved notable early successes such as the DHS ISAC program.

However, organizations must work with internal stakeholders, as well as counterparts at peer organizations and in the government, to actively participate in information sharing partnerships and ensure that information exchange is a two-way street. In this way, organizations can better anticipate and respond to threats because they have advance warning of threats through peers and government partners. Information-sharing partnerships enable strategic cyber intelligence producers to collect, analyze and disseminate products that are understandable and relevant to senior leaders and enable long term resourcing decisions that impact the organization's strategic objectives.


CONCLUSION

The ultimate goal of an organization's strategic cyber intelligence capability is to reduce risk to the organization's critical mission and assets of value. To achieve this, organizations must develop and maintain, with the participation of C-suite leaders, information requirements that orient the intelligence resources to the enterprise's critical mission and business needs. With these in place, the cyber intelligence function is positioned to conduct a strategic assessment of the enterprise's threats and vulnerabilities, and to assess potential impacts in the event of an incident. These processes enhance the enterprise's understanding of its attack surface, and enable it to correlate the attack surface with potential threat actors who have the intent and capability to exploit the organization's vulnerabilities. In turn, the analysis from this process enables senior leaders to make informed decisions to proactively defend the enterprise's mission and operations. In addition, for security practitioners, strategic cyber intelligence provides organizations with the following benefits:

- The ability to more effectively assess, quantify the risk to the business, and explain it to senior management and other key stakeholders
- Collaboration and information sharing in a more meaningful manner with members of law enforcement, defense organizations, the Intelligence Community, and the information security community of interest at large
- Demonstrates an appropriate standard of diligence to auditors, regulators, Boards, and other stakeholders which should reduce the exposure of the business to regulatory or legal sanctions
- Demonstrates responsible expenditure of security resources by focusing on defending both what is important to the firm and relevant to the threat.

To succeed in the cyber domain in 2014 and beyond, strategic cyber intelligence will play a crucial role in defending private companies and government sectors by providing the necessary intelligence to prevent potential incidents that could cripple our security as well as our economy.

In the world today, strategic cyber intelligence should no longer be solely the government's responsibility. To prevent future cyber incidents, the commercial sector, which owns the vast majority of the cyber infrastructure and the data, must work together with the government to strengthen cyber intelligence capabilities just as it has historically with other types of intelligence.



Strategic cyber intelligence should no longer be solely the government's responsibility.

Interested in continuing the conversation?

Send your feedback to comments@insaonline.org, and cite the name of this INSA White Paper in the subject line.

ENDNOTES

- ¹ *Getting Ahead of Advanced Threats*. Rep. RSA, The Security Division of EMC, Jan. 2012. Web. <<http://www.emc.com/collateral/industry-overview/cisoprpt2.pdf>>.
- ² *Ibid.*
- ³ "SEI Emerging Technology Center: Cyber Intelligence Tradecraft Project - Summary of Key Findings." Re.p.Carnegie Mellon University. 2013. Web. <<http://www.sei.cmu.edu/library/assets/whitepapers/citp-summary-key-findings.pdf>>.
- ⁴ United States. Department of Commerce. Computer Security Division. Special Publication 800-30 Guide to Conducting Risk Assessments. National Institute of Standards and Technology, Sept. 2012. Web. <http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf>.
- ⁵ United States. Department of Commerce. Computer Security Division. Special Publication 800-39 Managing Information Security Risk Organization, Mission, and Information System View. National Institute of Standards and Technology, March 2011. Web. <<http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>>.
- ⁶ Enterprise in this context includes suppliers, partners, and other members of the sector, and of complementary sectors in which the enterprise operates.
- ⁷ *The State of Risk-Based Security Management*. Rep. U.S. and UK Ponemon Institute, 2013. Web. <<http://www.tripwire.com/ponemon/2013/#metrics%20http://www.tripwire.com/ponemon/2013/#metrics>>.
- ⁸ "U.S. Federal Cybersecurity Operations Team." National Roles and Responsibilities. N.p., n.d. Web. <http://www.americanbar.org/content/dam/aba/marketing/Cybersecurity/2013march21_cyberroleschart.authcheckdam.pdf>.
- ⁹ United States. Government Accountability Office. A Better Defined and Implemented National Strategy Is Needed to Address Persistent Challenges. N.p., 7 Mar. 2013. Web. <<http://www.gao.gov/assets/660/652817.pdf>>.
- ¹⁰ Heuer, Richards J. *Psychology of Intelligence Analysis*. N.p.: Center for the Study of Intelligence, Central Intelligence Agency, 1999. 70. *Psychology of Intelligence Analysis*. Center for the Study of Intelligence, Central Intelligence Agency, Mar. 2007. Web. <<https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/PsychofIntelNew.pdf>>.
- ¹¹ 4 NIST SP 800-30, *Guide for Conducting Risk Assessments*, op. cit.
- ¹² Northcutt, Stephen. "The Attack Surface Problem." *Security Laboratory Defense in Depth Series*. SANS Technology Institute, n.d. Web. <<http://www.sans.edu/research/security-laboratory/article/did-attack-surface>>.
- ¹³ United States. Department of the Army. Military Operations. TRADOC Pamphlet 525-7-8. N.p.: n.p., n.d. *Cyberspace Operations Concept Capability Plan 2016-2028*. TRADOC, 22 Feb. 2010. Web. <<http://www.fas.org/irp/doddir/army/pam525-7-8.pdf>>.
- ¹⁴ United States. Department of Commerce. Computer Security Division. Special Publication 800-39 Managing Information Security Risk Organization, Mission, and Information Systems View. National Institute for Standards and Technology, Mar. 2011. Web. <<http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>>.
- ¹⁵ 2013 Data Breach Investigations Report. Rep. Verizon Enterprise Solutions, 2013. Web. <<http://www.verizonenterprise.com/DBIR/2013/>>.
- ¹⁶ 4 NIST SP 800-30, *Guide for Conducting Risk Assessments*, op. cit.
- ¹⁷ If an organization's intellectual property is valued at \$1,000,000 and it is estimated that in the event of a breach, 25 percent of the data could be exfiltrated before detection, and then 25 percent is the exposure factor. Multiplying the value of the asset with the exposure factor yields a single loss expectancy (SLE), which in this case would be \$250,000.
- ¹⁸ Assume that it is determined that the organization's intellectual property will likely be successfully exfiltrated once every six months. This equates to an ARO of 2 (i.e., two events in one year). Therefore, the ALE for this example would be \$500,000 (\$250,000 x 2 = \$500,000). With this value in hand, senior leaders know they can spend up to \$500,000 per year to mitigate the risk of a data breach.



**INTELLIGENCE AND
NATIONAL SECURITY
ALLIANCE**

ABOUT INSA

INSA is the premier intelligence and national security organization that brings together the public, private and academic sectors to collaborate on the most challenging policy issues and solutions.

As a non-profit, non-partisan, public-private organization, INSA's ultimate goal is to promote and recognize the highest standards within the national security and intelligence communities.

INSA has over 150 corporate members and several hundred individual members who are leaders and senior executives throughout government, the private sector and academia.

To learn more about INSA visit www.insaonline.org.

ABOUT THE INSA CYBER COUNCIL

The INSA Cyber Council is a group of current and former executives from the public, private and academic sectors with expertise in cyber security. The Council engages government and industry communities in pursuit of innovative solutions and thought leadership that will improve existing cyber security policies, practices and organization for both sectors.

ABOUT THE INSA CYBER INTELLIGENCE TASK FORCE

The INSA Cyber Intelligence Task Force was created to set the landscape for cyber intelligence by discussing why cyber intelligence is necessary and providing thoughts on how to develop this function in the cyber domain.



INTELLIGENCE AND NATIONAL SECURITY ALLIANCE

BUILDING A STRONGER INTELLIGENCE COMMUNITY

901 North Stuart Street, Suite 205, Arlington, VA 22203
(703) 224-4672 | www.insaonline.org