THE SECURITY INTELLIGENCE CENTER

Next Steps: Beyond Response to Anticipation

A joint research report by
the Internal Audit Foundation
and Crowe Horwath

By Raj Chaudhary, CGEIT, CRISC, and Dave McKnight, CISSP

Crowe Horwath®

INTERNAL AUDIT FOUNDATION™

About The Internal Audit Foundation

The Internal Audit Foundation has provided groundbreaking research for the internal audit profession for the past four decades. Through initiatives that explore current issues, emerging trends, and future needs, the Internal Audit Foundation has been a driving force behind the evolution and advancement of the profession.

The Global Internal Audit Common Body of Knowledge (CBOK) is administered through the Internal Audit Foundation. CBOK is the world's largest ongoing study of the internal audit profession, including studies of internal audit practitioners and their stakeholders. One of the key components of CBOK is the global practitioner survey, which provides a comprehensive look at the activities and characteristics of internal auditors worldwide.

Visit the CBOK Resource Exchange at www.theiia.org/goto/CBOK to download the latest reports.

Table of Contents

Contributors

Raj Chaudhary
CGEIT, CRISC, Principal,
Crowe Horwath – *USA*

Dave McKnight
CISSP, Crowe Horwath – *USA*

Executive Summary

As cyberattacks grow in frequency, severity, and complexity, cybersecurity professionals are urging organizations to move beyond a defensive and reactive approach to a more proactive approach, allowing for the prediction and anticipation of cybersecurity threats. Recognizing this emerging trend, the Institute of Internal Auditors' Audit Executive Center (AEC), in collaboration with the Internal Audit Foundation, elected to supplement recent research by conducting a Quick Poll survey of chief audit executives (CAEs) to ask specific questions about their organizations' use of security operations centers (SOCs) as part of their cybersecurity strategies.

Responses were received from 130 CAEs, representing organizations of various size from many industries. In addition to providing insights into specific SOC policies and practices, the AEC Quick Poll survey results also suggest that some conclusions can be drawn about CAEs' general levels of involvement in monitoring and reviewing their SOC operations. In order to assure complete anonymity, the survey respondents were not asked to provide identifying or qualifying information about their organizations.

Using the survey findings as a starting point, researchers from Crowe Horwath conducted a series of follow-up interviews with information security executives in various organizational structures and geographic locations, and with various sensitivities to cybersecurity threats. The objective was to gather first-hand examples of current best practices.

To protect the companies' identities, the interview responses were normalized into three general types of organizations: 1) large companies with global operations, 2) large companies with national operations, and 3) medium-size companies with regional operations. The responses were summarized along those lines in this report. The research team also interviewed representatives of a number of leading vendors that offer cybersecurity intelligence solutions and services.

In addition to offering a summary of that research, this report is intended to help cybersecurity professionals, CAEs, and other stakeholders to explore broader issues and to answer two questions:

1) How can organizations move beyond merely reacting and responding to cybersecurity incidents and instead start to identify, anticipate, and actively defend against known and emerging threats?
2) What role can CAEs play in encouraging and facilitating this shift from a reactive to a proactive stance?

By addressing—and ultimately answering—these questions, organizations can take the critical first steps to advancing their cybersecurity initiatives regardless of whether they are first establishing a SOC, or advancing further and establishing a fully functioning security intelligence center (SIC).

1) The Emerging Cybersecurity Question: Detect and Respond, or Anticipate and Stop?

Cybersecurity consistently ranks among the top technology concerns with senior management, internal auditors, audit committees, and boards of directors. Recently, cybersecurity topped the list of risks discussed by authors Philip Flora and Sajay Rai in "Navigating Technology's Top 10 Risks: Internal Audit's Role," a Core Report published as part of the Global Internal Audit Common Body of Knowledge (CBOK) study conducted by the Internal Audit Foundation in 2015.

Based on survey responses from the 2015 Global Internal Audit CBOK Practitioner Survey, the report noted that 73 percent of survey respondents characterized the risk of a data breach as either "moderate" (39 percent) or "extensive" (34 percent). Internal audit practitioners who were IT specialists rated the risks even higher. More than 8 out of 10 (82 percent) respondents characterized the risk of a data breach as either "moderate" (36 percent) or "extensive" (46 percent).[1]

As cyberattacks become increasingly commonplace, much of the discussion among security professionals has moved from the desire to avoid and block all intrusions. Instead, there is growing recognition that despite everyone's best efforts to prevent it, there is always a probability that an intrusion will occur. This shift in outlook has extensive implications in terms of cybersecurity operations. Once it is recognized that 100 percent protection 100 percent of the time is not achievable, the cybersecurity emphasis can begin to shift from a defensive posture to a more offensive and proactive one that focuses on learning about how certain threats operate, how their effects can be limited or mitigated, and how the incident response time (from identification to remediation) can be accelerated.

As the cybersecurity posture of organizations begins to mature, they can shift to a more proactive approach that will reduce the impact of cyber incidents.

With each incident, organizations can begin to build a wealth of knowledge by documenting each attack and response. Similar attack vectors can be detected and addressed as organizations modify their security architectures, both to defend themselves and plan their responses.

As these shifts occur, the cybersecurity maturity level of an organization will begin to elevate as all who are concerned step back and take a smarter view of cyberthreats, resulting in the "anticipate and stop" approach. This transition is important because as proactive and routine processes become stronger, organizations will find that they are able to shorten the time needed to contain and resolve incidents, decrease the associated costs, and reduce the impact of incidents.

As indicated in the next two sections, the survey findings show that many organizations will not realize an immediately successful shift in outlook. Moreover, a very mature cybersecurity operation, or precise prediction of coming attacks, is not yet a practical or achievable goal.

Cybersecurity maturity is not a matter of an organization's financial spending or head count. Rather, the measurement is an indication of how effective an organization is at balancing investments in security solutions, capable employees, and efficient procedures with the organization's risk appetite and the calculated impact of qualified cyberthreats.

Organizations that rate higher on the cybersecurity maturity scale are not necessarily spending more dollars overall, but are taking a more predictive approach to cybersecurity intelligence by integrating well-rounded security solutions and avoiding bolt-on products. As they do this, they also help bring the issue of cybersecurity further into the mainstream and make the anticipation and mitigation of attacks a more manageable experience. By following this example, organizations that are less mature in cybersecurity can begin to focus their existing IT security resources and budgets more intelligently as they make the transition to a more mature approach to the overall cybersecurity challenge.

2) The Foundation: Common Terminology, Frameworks, Metrics, and Tools

In order to gain a better perspective on the current state of SOC adoption and implementation in organizations, the IIA's Audit Executive Center (AEC), in collaboration with the Internal Audit Foundation, conducted a Quick Poll survey of CAEs in June 2016. The AEC received responses from 130 CAEs who represented organizations of various sizes across North America.

In order to assure complete anonymity, respondents were not asked to provide identifying or qualifying information (e.g., location, size, or industry). Subsequent follow-up interviews were used to provide an additional understanding of how practices vary in organizations of different sizes and complexity.

Cybersecurity as a discipline is still evolving, and not all practitioners share the same understanding of certain terms. Therefore, before analyzing the survey responses, it is useful to establish some common terminology. It is also helpful to establish a standard method of evaluating and characterizing the relative maturity levels of organizations along with an overview of some widely used cybersecurity tools.

Common Terminology

A common set of organizational threat categories and responses is useful not only for the purposes of this report, but also in the broader scheme of things. One early step toward greater cybersecurity maturity is for an organization to begin developing common terminology so that IT, management, and board members speak the same language when discussing risks, threats, impacts, and proposed responses.

Several sources provide guidance in establishing cybersecurity terminology. The "Computer Security Incident Handling Guide (Special Publication 800-61),"[2] published by the National Institute of Standards and Technology (NIST), offers guidance on establishing response protocols to various types of attacks, and includes a brief glossary of terms. A more comprehensive NIST publication, "Security and Privacy Controls for Federal Information Systems and Organizations (Special Publication 800-53),"[3] contains a much more extensive glossary.

One of the most widely used sources of common definitions is the Vocabulary for Event Recording and Incident Sharing (VERIS),[4] which is a set of metrics designed to provide a common language for describing security incidents in a structured and repeatable manner. VERIS users collect and report incident data using consistent terminology to help support better decision-making. VERIS is also used by organizations such as Verizon and IBM to publish detailed breach reports.

Drawing on these various sources makes it possible to compile an abbreviated list of fundamental terms that can serve as a starting point for a more extensive glossary specifically tailored to an organization's security needs. Some of those terms are listed in Appendix A.

Frameworks and Metrics

In addition to a common understanding of terms, a successful cybersecurity initiative also requires a common understanding of the desired goals and outcomes. An essential early step in this effort is choosing an effective and appropriate cybersecurity framework, which will serve as the centerpiece of any cybersecurity risk management program.

A cybersecurity framework is a structured guide designed to establish and maintain the confidentiality, integrity, and availability of data and information networks. Because of the size, complexity, and evolving nature of cyberthreats, there is no one-size-fits-all framework applicable to all organizations.

Among the many frameworks now available, one of the most widely used is the NIST Framework for Improving Critical Infrastructure Cybersecurity, which was prepared with extensive private sector input and originally issued in February 2014. The NIST framework was designed to be comprehensive and widely applicable to various types of organizations and can serve as the basis for more specialized, industry-specific frameworks.[5]

Organizations can also create their own frameworks based on the International Organization for Standardization (ISO) standards, such as the international standard that describes best practices for an information security management system (ISO 27001),[6] and the international standard that provides a guide for cybersecurity though specific recommendations (ISO 27032).[7]

Another widely used IT framework is COBIT 5, a business framework for the governance and management of enterprise IT, published by ISACA (the organization formerly known as the Information Systems Audit and Control Association).[8] In terms of specific cybersecurity concerns, ISACA also published "Implementing the NIST Cybersecurity Framework," which maps NIST controls to COBIT 5 where applicable.[9] Other relevant guidance can be found in the Federal Communications Commission (FCC) Cybersecurity Planning Guide.[10]

Regardless of which framework an organization chooses for managing its cybersecurity program, it must be adapted to reflect the organization's size and the nature of the information assets being protected. Moreover, it is critically important that the organization also regularly and systematically evaluate its progress in improving its threat detection capabilities and the effectiveness of its responses.

This assessment is often expressed in terms of a maturity model, which depicts an advancing state of maturity as an organization progresses from one level to the next. Maturity models are designed to provide a consistent and objective method for evaluating security program effectiveness and value. The concept is based on the process improvement training and appraisal processes that are commonly used in software development to assess the relative state of development. A more detailed discussion of how maturity models can be developed and implemented, along with additional reference information, can be found in Appendix B.

Tools Deployed

As organizations work to advance from "baseline" or "evolving" levels of cybersecurity maturity to "intermediate" or more "advanced" levels, some of the significant milestones will involve the development and implementation of specific software tools that are designed to address particular aspects of any cybersecurity initiative. Such tools can typically be grouped into three general categories:

1) Threat-intelligence gathering tools:
    a) Survey peer and industry data to identify new and emerging threats that are being discovered and reported by other security organizations.
    b) Alert the cybersecurity team about specific threats that could have an impact on the organization.
    c) Identify vulnerabilities and weaknesses that could be exploited or triggered by a threat source.
2) Event collection tools:
    a) Gather and correlate data on observable occurrences within the organization's network or IT systems or networks.
    b) Gather data on suspect events so that response and mitigation efforts can be launched quickly while collecting and correlating data for further analysis of potentially recurring threats.
3) Analytics tools:

a) Evaluate an event and determine if an actual incident or cyberattack has occurred, and if so, determine what type of incident or attack it was.

b) Identify the potential threat actors or sources, as well as the particular category or type of threat action that was involved.

The acquisition of such tools must follow the same procurement process used to acquire any other information system component.

3) The Current State: Security Operations Centers and the Use of Intelligence Tools

The June 2016 AEC Quick Poll survey of CAEs provides some useful insights into the current state of SOCs and the various cybersecurity tools that they use, as well as their cybersecurity policies and practices. The survey also raised some questions about CAEs' general levels of involvement in the broader domain of information security.

SOC Usage and Characteristics

The AEC Quick Poll survey responses indicate that while a number of organizations have established formal SOCs to help manage cybersecurity risk, there are still significant opportunities for audit executives to become more actively engaged in this area. More than one-third (34.6 percent) of the survey respondents said that their organizations had already established a formal SOC; another 10 percent were considering it (Exhibit 1).

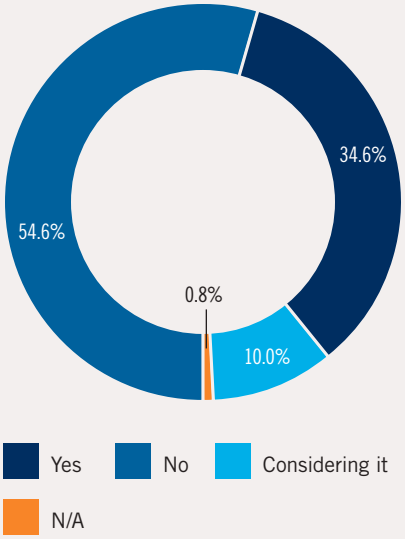
The results suggest that a sizable number of organizations have recognized the significance of cybersecurity threats and are taking active measures to address them. The results also suggest that more than half of the organizations polled have not considered taking such steps.

It's reasonable to assume that some portion of those responses came from smaller organizations, where establishing a formal SOC as an internal function might not be cost effective or necessary in order to advance to the next level of cybersecurity maturity.

CAEs who indicated that their organizations did have a SOC were asked a follow-up question about its size. It is important not to draw unwarranted conclusions from the responses since they were elicited from CAEs in organizations of all sizes. Speaking in general terms, the survey suggests that SOCs tend to be moderately sized departments within the larger information security functions. About 4 out of 10 (39.5 percent) organizations reported 5 or fewer full-time equivalent employees (FTEs) attached to their SOCs (Exhibit 2).

Exhibit 1: General Usage of Security Operations Centers

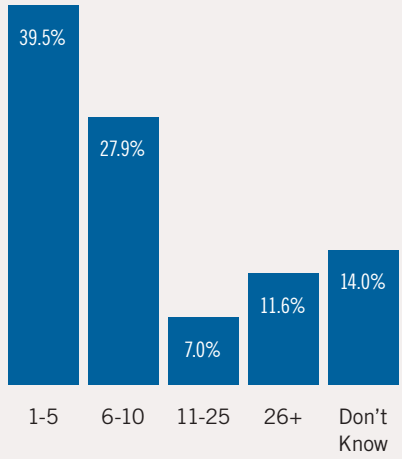
Does your company have a formal security operations center?



Source: AEC Quick Poll, June 2016

Exhibit 2: Size of Security Operations Centers

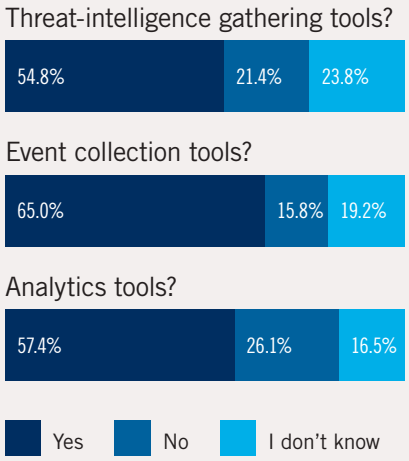
What is the number of FTEs attached to the SOC?



Source: AEC Quick Poll, June 2016

Exhibit 3: Use of Cybersecurity Intelligence Tools

Does your company use...



Source: AEC Quick Poll, June 2016

Cybersecurity Tool Use

CAEs were also asked about their use of the three general types of cybersecurity tools: threat-intelligence gathering tools, event collection tools, and analytics tools. Slightly more than half of the respondents reported that their organizations use threat intelligence and analytics tools, while nearly two-thirds (65 percent) said that they use event collection tools (Exhibit 3). While these results cannot tell us whether these tools are being used correctly and efficiently, the responses do suggest that organizations have begun to implement the functions associated with a SOC even if they have not yet taken the steps to establish a formal center.

A closer look at the results reveals some additional points worth considering. For example, when asked about their organizations' use of threat-intelligence gathering tools, nearly one-quarter of the respondents (23.8 percent) did not know if such a tool was used. That relatively high number suggests that in many cases, internal audit departments may not be fully engaged with the IT function in the area of security operations.

Similar trends appeared when respondents were asked about their company's use of event collection and analytics tools. In these areas, a significant number of CAEs did not know if such tools were in use.

Participants who responded that their organizations did use at least one of the three categories of cybersecurity tools were asked to identify which tools their organizations used. Among those CAEs willing and able to name other cybersecurity tools used, there was a surprisingly diverse list of choices, with no single family of tools dominating the list (Exhibit 4).

Exhibit 4: Other Cybersecurity Tools Used

Threat-Intelligence Gathering Tools	Event Collection Tools	Analytics Tools
• FireEye (Mandiant) (2) • IBM • LogRhythm • McAfee • Perspective • Soltra • Vectra Networks	• LogRhythm (2) • Splunk (2) • ArcSight • Cylance • FireEye • Perspective • SIEM Appliance • Snort	• ACL Analytics (4) • ArcSight • McAfee • Microsoft BI • Perspective • Qlik • SQL BI • Tableau

Source: AEC Quick Poll, June 2016

4) Looking Forward: Evolving From SOC to SIC

Crowe researchers conducted an additional study of emerging trends in terms of both cybersecurity intelligence tools and evolving best practices among organizations to explore further the findings suggested by the AEC Quick Poll survey. This research included both literature reviews and in-person interviews with users of intelligence information and several selected tool vendors.

A review of current literature in the cybersecurity arena reinforces the impression that industry leaders expect their roles to evolve from being primarily reactive and responsive to being proactive and anticipatory, identifying threats and potential areas of vulnerability, and sharing these observations with other users.

A Gartner analysis published at the end of 2015 recommended that security operations teams use security operations, analytics, and reporting (SOAR) technology solutions to enhance their existing risk and compliance, vulnerability assessment, and security information and event management (SIEM) platforms. Gartner estimated that by 2019, 30 percent of midsize and large enterprises will be using SOAR technology to make security operations more intelligence driven.[11]

In 2014, the MITRE Corporation, a not-for-profit research organization based in the United States, published a report describing a similar conclusion. The authors observed that "[c]ommon security elements, such as firewalls and anti-malware technology are important defensive components, but a threat-oriented defense will call for additional measures and information-collection capabilities to counter the range of sophisticated threats."[12]

Put another way, security intelligence tools will continue to advance, both in terms of their adoption by organizations and the tools' additional capabilities. Examples include the growing use of machine learning to expedite processing, and the use of automation to take action when a qualified employee is unavailable to respond.

Along with the implementation of advanced tools, the AEC Quick Poll survey also confirmed that those organizations that excel in both processing and taking action against adverse security attempts generally share another trait. They have cultures that allow open discussion about information security-relevant topics, observations, and improvement opportunities. Moreover, this information is shared not only among their internal business and operations departments, but also with peers and partners outside the organization. As organizations become more accustomed to sharing such information internally, they appear to become more comfortable with external sharing.

While organizations await the development and implementation of new solutions, they should consider focusing on integration and communication opportunities to embed information security-related standards throughout the organization. Such efforts may also include an evaluation of leadership reporting in order to validate that key roles and responsibilities are appropriately supporting the evolution of the organization's cybersecurity maturity. This effort will be a critical component in enabling the organization to expand the SOC into a fully functioning and proactive security intelligence center (SIC).

Organization Profiles – Evolving Best Practices

While the establishment of a SOC—or ultimately the transition from a SOC to a SIC—is widely anticipated among cybersecurity leaders, the AEC survey results indicate that there is still considerable ground to be covered before SIC operations become commonplace. As noted in the preceding section, slightly more than one-third (34.6 percent) of the survey respondents currently have a SOC in place; another 10 percent are just considering it. This impression was reinforced by interviews with a number of representative organizations.

The follow-up interviews were conducted in order to add further depth and detail to the initial survey responses, drilling down to understand SOC practices in organizations of various sizes and industries. To protect the identities of the companies that were interviewed, responses were organized into three types of organizations: 1) large companies with global operations, 2) large companies with national operations, and 3) medium-size companies with regional operations. Following are some generalized observations about SOC operations based on the interviews:

1) LARGE COMPANIES WITH GLOBAL OPERATIONS

- This category includes both private and publicly traded organizations that have a global footprint. Their security focus typically involves a large customer base, owned intellectual property, or both.
- These organizations were generally found to have a formalized cybersecurity operations center that works in collaboration with other IT resources. Typical SOC operations include threat detection, malware analysis, support of incident investigations, companywide awareness, and relationships with several vendors for the purposes of intelligence and trend analysis.
- Common tools and support providers that were encountered included Carbon Black (formerly Bit9) for endpoint security, Mandiant Incident Response for forensic investigation, and both FireEye and Palo Alto Network's WildFire cloud-based security platforms for aggregating, analyzing, and sharing threat data.
- In many instances, staffing levels in these centralized operations were relatively lean—sometimes consisting of 12 or more highly efficient professionals. However, because of their global diversification, the companies rely heavily upon regional information security professionals in numerous countries with mini-SOCs. The overall size of the team, including both the centralized SOC staff and those in regional SOCs, can be relatively large.
- This dispersion of duties is made necessary because of both the wide array of data protection rules that apply in various countries and their constant evolution. For example, the European Union (EU) is expected to launch new data protection regulations in 2017 that will replace the current EU data protection directive (DPD). The existing 1995-vintage EU DPD incorporates a patchwork of slightly

different laws that vary among the 28 EU countries, while the new regulation will be implemented by all EU members. Such ongoing changes make it more practical to disperse response planning and execution among local facilities while maintaining a centralized analysis and coordination function.

In addition to cyber intelligence collection and analysis, these regional SOCs typically also engage in the creation and distribution of new intelligence reports that are shared internally and externally with other information sources, including state and national law enforcement agencies and sponsored information sharing and analysis centers (ISACs).

2) LARGE COMPANIES WITH NATIONAL OPERATIONS

- Some of the largest U.S. organizations have only recently established SOCs with organization-wide responsibilities for maintaining cybersecurity. Until relatively recently, information security was often the responsibility of various IT teams in subsidiary companies and local offices.
- Those companies that now operate SOCs typically engage a staff of several dozen FTEs. In the most mature organizations, the majority of these staff members are analysts who do not have IT management or maintenance responsibilities. This is a significant shift from earlier structures in which cybersecurity analyses were performed by nonspecialized employees who also juggled other IT duties. This is also somewhat different from the pattern that was frequently seen in the first group of companies interviewed, where lean central staffs relied more heavily on regional offices.
- The analysis teams typically operate in shifts, offering full coverage for nights and weekends. Among the observed best practices were weekly staff development calls to help maintain team integrity and vision. The most mature SOCs also maintain liaisons with their chief information officer (CIO), chief information security officer (CISO), and specialized litigation and privacy teams. In companies where cybersecurity is a particularly critical client concern, the SOC leader might also participate in business acquisition and client retention activities.
- Much of the SOCs' work is focused on event analysis, real-time monitoring, and intrusion triage. In large companies, oftentimes SOCs log several billion system or network events annually, with several hundred found to be actual incidents requiring further investigation.
- In mature organizations, management is usually committed to the importance of communicating threat intelligence to other internal IT resources. This effort typically includes breach reports and flash advisories, as well as regular information feeds, all of which could be characterized as threat intelligence communication.

3) MEDIUM-SIZE COMPANIES WITH REGIONAL OPERATIONS

- Unlike the global and U.S.-based organizations in the first two groups, the third category of organizations usually has a much smaller involvement in cybersecurity as a practice, and often has only minimal involvement in the threat intelligence aspects of cybersecurity.
- Even in industries that might be considered prime targets for threat actors, cybersecurity is often one of the many functions performed by a general corporate IT office. In many instances, specific cybersecurity responsibilities are focused on by one or two individuals who also manage a wide range of other technology operations.
- Obviously, this leaves little to no time for active threat intelligence gathering or analysis. Instead, these organizations often rely on third-party vendors to provide relevant services, leveraging their capabilities and using automated updates.
- The solutions commonly encountered by such organizations include event and alert monitoring by an outsourced vendor, firewall protection from primary telecommunications providers, and patch management programs. Some of the more mature organizations are also looking into a next generation endpoint security product to protect their employees' individual workstations.
- Information on threats is often communicated via the company intranet, and while some individual training is provided to employees to improve security awareness, there often are no specific metrics for measuring the effectiveness of these efforts.

Intelligence Tools – the Envisioned Future

A recurring theme in the technology vendor interviews that were conducted as part of this research was the need to help SOCs operate more efficiently and effectively by accurately screening out false positives. This is necessary in order to help focus analyst resources, which are often limited, onto those events that present the greatest likelihood of being an actual incident rather than a benign occurrence.

In a sense, this is the overarching purpose of all threat intelligence—to anticipate likely or potential threats so that security resources can be effectively deployed to the areas of greatest risk.

The vendors interviewed emphasized various methodologies for achieving this objective. Among the beneficial techniques were the following suggestions:

- Trusted circles or customer communities, which allow software users to communicate with each other and share intelligence regarding threats and vulnerabilities
- Enterprise integration, enabling threat intelligence solutions to work together with leading SIEM platforms and other cybersecurity systems

- Simple plug-in capabilities that enable rapid updates in response to changes in the threat knowledge base, either locally or from external intelligence sources
- The use of cloud technology to help minimize local storage requirements and reduce volume-based license fees for threat intelligence information

In addition, leading vendors are incorporating some elements of machine learning capabilities in combination with human interaction to fine-tune or adjust performance. Broadly speaking, most threat intelligence vendors recognize the need to move beyond simply gathering and storing data to focusing their development efforts on the next level of intelligence-predictive modeling. It should be noted that the term "predictive" could be misinterpreted as an implication that all cybersecurity threats can be identified and blocked with great precision, which obviously is not a realistic goal.

Even if it were achievable, the likely cost would present an obstacle, as many organizations must make technology trade-offs and prioritize their cybersecurity needs against other critical business technology needs. Nevertheless, the general concept is valid. The objective is to apply intelligence in such a way that it enables the SOC to anticipate the likely nature and source of future threat actions so that vulnerabilities can be identified and addressed proactively.

By using their own data repositories along with trusted external intelligence services as information sources, organizations can begin to implement defenses and responses before an attack occurs.

5) The Role of Internal Audit in the SOC and SIC

As part of its overall assurance responsibilities, internal audit has an important role to play in determining if cybersecurity risks are being addressed effectively. The responses to the AEC Quick Poll suggest a number of areas in which internal audit professionals have opportunities to improve and increase their contribution in this area, particularly in helping to pave the way for the establishment of a SOC or in elevating a SOC to a SIC.

As part of this effort, it can be helpful to consider internal audit's role in cybersecurity within the context of the broad data security functions that are outlined in the organization's cybersecurity framework. These functions are not necessarily within the direct scope of duties of internal audit. Nevertheless, as the third line of defense, internal audit is responsible for providing senior management and the board with independent assurance that needed activities are being performed by the first two lines of defense: 1) the lines of business and 2) the risk management team.

CAEs can also provide added value by pursuing a number of other specific steps that relate to their entities' SOC and general security operations. Many of these are closely related to the actions recommended in the Internal Audit Foundation Core Report, "Navigating Technology's Top 10 Risks: Internal Audit's Role," mentioned in Section 1 of this document. The authors of the report recommended seven key questions for internal audit to ask about cybersecurity preparedness. The questions are:

"1) Is the organization able to monitor suspicious network intrusion?

"2) Is the organization able to identify whether an attack is occurring?

"3) Can the organization isolate the attack and restrict potential damage?

"4) Is the organization able to know whether confidential data is leaving the organization?

"5) If an incident does occur, is a written crisis-management plan in place that has been tested and is in line with organizational risk?

"6) If an incident does occur, does the organization have access to forensic skills to assist with the incident?

"7) Is the incident team in place, and do they know their roles and responsibilities?[13]"

In addition to verifying general cybersecurity preparedness, internal audit can play an important role in helping the organization advance toward the establishment of a mature security intelligence operation. Internal audit's focus in this regard would include verifying that cybersecurity intelligence tools are up-to-date, with current patches and upgrades installed. Again, internal audit's role as the third line of defense is to verify that these actions have been performed, not to perform them directly. Internal audit also can review the training and credentials of SOC analysts to confirm up-to-date qualifications.

Finally, internal audit can also play a valuable role in reviewing the overall level of information security awareness and preparedness, and elevating that awareness organization-wide. One of the most effective ways to do this is by advocating for effective cybersecurity awareness training. Having effective tools is only one component of a successful information security strategy. People and their level of training and daily practice represent another area of risk for internal audit to assess.

These various activities are, in a sense, only the beginning. The IIA's September 2016 publication, "Global Technology Audit Guide (GTAG) 17: Auditing IT Governance," offers extensive additional information.[14] The guide is designed to provide internal auditors, in both the public and private sectors, with the knowledge they need to fulfill their responsibilities in providing assurance and consulting services for IT governance. In addition to describing elements of effective governance and performance frameworks, such as balanced scorecards, maturity models, and quality systems, it also discusses red flags to look for and describes example controls and guidelines to facilitate audits of IT governance.

By pursuing activities such as those listed here and in GTAG 17, internal audit executives can help improve their organizations' critical cybersecurity operations activities and help accelerate the transition to a fully functioning cybersecurity intelligence center.

Appendix A – Common Cybersecurity Terminology

General Terms

CYBERATTACK

An attack targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment or infrastructure; destroying the integrity of data; or stealing controlled information

EVENT

Any observable occurrence in a network or system

EXFILTRATION

The unauthorized transfer of information from an information system

INCIDENT

A violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices

INFORMATION LEAKAGE

The intentional or unintentional release of information to an untrusted environment

INFORMATION SYSTEM RESILIENCE

The ability of an information system to continue to operate under adverse conditions or stress while maintaining essential capabilities, and to recover to an effective operational posture in a time frame consistent with mission needs

SECURITY INTELLIGENCE CENTER (SIC)

A proactive cybersecurity operation, in which the emphasis is on learning about and anticipating threats, rather than triage and incident response

SECURITY OPERATIONS CENTER (SOC)

A responsive cybersecurity operation, in which analysts focus on working through a list of alerts and incidents and launching appropriate responses

THREAT

Any circumstance or event with the potential to adversely affect organizational operations, functions, image or reputation, assets, individuals, or other organizations due to unauthorized access, destruction, disclosure, modification of information, or denial of service

VULNERABILITY

Weakness in an information system, security procedures, internal controls, or implementation that could be exploited or triggered by a threat source

Threat Actions and Categories

ENVIRONMENTAL THREATS

Natural events, such as earthquakes, floods, and atmospheric conditions, as well as hazards associated with the immediate environment or infrastructure in which assets are located, such as power failures and electrical interference

ERROR

Anything done (or left undone) incorrectly, inadvertently, or unintentionally, including omissions, misconfigurations, programming errors, trips and spills, and other malfunctions

HACKING

Attempts to intentionally access or harm information assets by circumventing or thwarting security mechanisms, including by brute force, SQL injection, cryptanalysis, and denial of service attacks

MALWARE

Any malicious software, script, or code run on a device that alters its state or function without the owner's informed consent, including viruses, worms, spyware, keyloggers, and backdoors

MISUSE

The use—either malicious or nonmalicious—of entrusted organizational resources or privileges for any purpose or manner contrary to that which was intended, including administrative abuse, policy violations, and use of nonapproved assets, etc.

PHYSICAL ACTIONS

Deliberate threats that involve proximity, possession, or force, including theft, tampering, snooping, sabotage, local device access, and assault

SOCIAL TACTICS

Using deception, manipulation, or intimidation to exploit the human element of information assets, including pretexting, phishing, blackmail, threats, and various scams

Threat Actors or Sources

EXTERNAL ACTORS

Sources outside of the organization and its network of partners, including criminal groups, lone hackers, former employees, and government entities, as well as acts of God and random chance

INTERNAL ACTORS

Threats originating from within the organization, including from full-time employees, independent contractors, interns, and other staff, who are trusted and privileged to varying degrees

PARTNERS

Various third parties that share a business relationship with the organization, including suppliers, vendors, hosting providers, and outsourced IT support, which have an implied level of trust and privilege

UNKNOWN ACTORS

Instances in which analysts are unable to identify the source of the threat

Sources: Adapted and abbreviated from the Computer Security Incident Handling Guide (NIST), Security and Privacy Controls for Federal Information Systems and Organizations (NIST), the Vocabulary for Event Recording and Incident Sharing (VERIS), and Crowe analysis

Appendix B – Cybersecurity Maturity Models

Most maturity models begin with a definition of the maturity levels themselves. This is followed by the development of specific questions or tests that validate process performance and assess the organization's maturity level. The next broad phase involves identifying and implementing appropriate remediation steps to improve low maturity. After this, the validation questions are applied again in order to reassess the maturity level and prepare for the next round of remediation steps.

The maturity model must be developed in a way that is consistent with the particular framework that is being employed and must be appropriate to the particular industry and operational characteristics of the organization. For example, the U.S. Department of Energy's Cybersecurity Capability Maturity Model (C2M2)[15] is focused on cybersecurity issues from the perspective of organizations that operate critical infrastructure. The C2M2 model and self-assessment are designed to correlate with the NIST framework.

Other examples of maturity models are Capability Maturity Model Integration (CMMI), a process-level improvement training and appraisal program, originally developed at Carnegie Mellon University and now administered by the CMMI Institute, a subsidiary of ISACA, and the COBIT Process Assessment Model.

Another example, which is also consistent with the NIST framework, was developed by the Federal Financial Institutions Examination Council (FFIEC) to help banks and other financial institutions identify risks and assess their cybersecurity maturity. Although the FFIEC model is targeted to the financial services industry, its general structure and the maturity levels it assesses serve as good examples of how the maturity model concept can be applied and adapted to many other types of organizations.

The process begins with the definition of the relevant cybersecurity domains. In the particular case of the FFIEC model, there are five such domains:

"1) Cyberrisk management and oversight

"2) Threat intelligence and collaboration

"3) Cybersecurity controls

"4) External dependency management

"5) Cyber incident management and resilience[16]"

Management then evaluates the organization's cybersecurity maturity level in each of the domains, taking into account unique characteristics, such as technologies and connection types, online and mobile exposure, organizational characteristics, and specific external and internal threats. The FFIEC model defines five maturity levels, as shown in Exhibit 5.

Exhibit 5: FFIEC Cybersecurity Maturity Levels

BASELINE

Baseline maturity is characterized by minimum expectations required by law and regulations or recommended in supervisory guidance. This level includes compliance-driven objectives. Management has reviewed and evaluated guidance.

EVOLVING

Evolving maturity is characterized by additional formality of documented procedures and policies that are not already required. Risk-driven objectives are in place. Accountability for cybersecurity is formally assigned and broadened beyond protection of customer information to incorporate information assets and systems.

INTERMEDIATE

Intermediate maturity is characterized by detailed, formal processes. Controls are validated and consistent. Risk management practices and analyses are integrated into business strategies.

ADVANCED

Advanced maturity is characterized by cybersecurity practices and analytics that are integrated across lines of business. The majority of risk management processes are automated and include continuous process improvement. Accountability for risk decisions by frontline businesses is formally assigned.

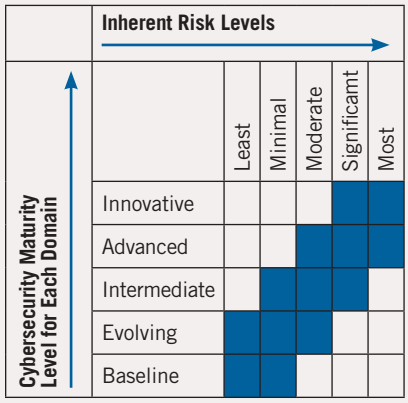
INNOVATIVE

Innovative maturity is characterized by driving innovation in people, processes, and technology for the institution and the industry to manage cyberrisks. This may entail developing new controls, new tools, or creating new information-sharing groups. Real-time, predictive analytics are tied to automated responses.

Note: Although designed for financial services organizations, this general structure and approach could be adapted to many other industries and types of businesses.

Source: FFIEC Cybersecurity Assessment Tool[17]

Exhibit 6: FFIEC Risk/ Maturity Relationship



Source: FFIEC Cybersecurity Assessment Tool[18]

Organizations in other industries would define a different group of domains specific to their business, and would develop comparable measures of maturity. Independent reviewers can provide useful guidance to help management determine whether the organization's maturity level is appropriate in relation to its risk. If it is not, management can then take steps to either reduce the level of risk or improve the cybersecurity framework maturity level. The objective is to achieve a level of maturity that is appropriate to the defined level of risk in each domain, as illustrated in Exhibit 6.

When adapting such an approach to their own entities, management and board members must take into account several variables, such as the size and breadth of the organization, its general industry or sector, the geographic areas in which it operates or has partners, its various technology platforms and services (including cloud exposure), its exposure to defined types or categories of threat actions, and its exposure to potential internal, external, and partner threat actors.

Regardless of the specific structure and terminology, the use of such a model provides management with an objective and consistent methodology for assessing the organization's inherent risk profile and maturity levels across the various domains.

Endnotes

1 Philip E. Flora and Sajay Rai, "Navigating Technology's Top 10 Risks: Internal Audit's Role," Institute of Internal Auditors Research Foundation (IIARF), 2015, p. 5, http://www.aiiaweb.it/sites/default/files/imce/pdf/navigating_technologys_top_10_risks_final_0.pdf

2 http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

3 https://www.nist.gov/node/557866

4 http://veriscommunity.net/index.html

5 "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0," National Institute of Standards and Technology, Feb. 12, 2014, https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

6 http://www.iso.org/iso/home/standards/management-standards/iso27001.htm

7 http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=44375

8 https://cobitonline.isaca.org/about

9 http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Implementing-the-NIST-Cybersecurity-Framework.aspx

10 https://transition.fcc.gov/cyber/cyberplanner.pdf

11 Oliver Rochford, Paul E. Proctor, "Innovation Tech Insight for Security Operations, Analytics, and Reporting," Gartner Inc. online report, Nov. 11, 2015, p. 2, https://www.gartner.com/doc/3166239/innovation-tech-insight-security-operations

12 Clem Skorupka and Lindsley Boiney, "Cyber Operations Rapid Assessment (CORA): A Guide to Best Practices for Threat-Informed Cyber Security Operations," The MITRE Corp., 2015, p. 5, https://www.mitre.org/sites/default/files/publications/pr_15-2971-cyber-operations-rapid-assessment-best-practices_0.pdf

13 "Navigating Technology's Top 10 Risks: Internal Audit's Role," p. 6.

14 https://na.theiia.org/standards-guidance/recommended-guidance/practice-guides/Pages/GTAG17.aspx

15 https://energy.gov/oe/services/cybersecurity/cybersecurity-capability-maturity-model-c2m2-program

16 https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_User_Guide_June_2015_PDF2_a.pdf

17 Ibid.

18 FFIEC Cybersecurity Assessment Tool, June 2015, page 9, available at: https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_User_Guide_June_2015_PDF2_a.pdf

RISK-17010-007A