Auditing Cyber Security:

Evaluating Risk and Auditing Controls

ABSTRACT

Cyber security has become a prevalent issue today facing most organizations, one that is recognized by companies to be an enterprisewide issue requiring thoughtful attention. Investments in controls are necessary to protect organizations from increasingly sophisticated and widely available attack methods. Intentional attacks, breaches and incidents can have damaging consequences. This white paper highlights the need for these controls implemented as part of an overall framework and strategy, and focuses on the subsequent assurance that is needed through management review, risk assessments and audits of the cyber security controls.

ISACA®

Trust in, and value from, information systems

INTRODUCTION

Cyber security is receiving increased attention from the boards of many organizations today in large part due to the bad publicity generated from recent large data breaches. Senior members of management and corporate boards have lost their positions, and organizations have had to spend valuable resources in post-breach cleanup and to make their clients and customers "whole." Infrastructure spending has increased as organizations attempt to prevent the breaches from occurring, and security technology investments in incident detection and response mechanisms are climbing to limit the damage and liability should the event occur.

These activities to enhance the infrastructure and defense mechanisms are welcomed investments to those charged with protecting from and responding to the attacks, but they represent only one necessary component of any cyber security program. The fundamental questions that need to be asked are those such as:

- Where is the best place to invest the next security dollar?
- Is the right amount being invested?
- Are there areas of risk that are not being addressed?
- Is the current infrastructure sufficient?
- Are the dollars invested that we have today being used wisely?
- How are competitors approaching this and what are they spending on information asset protection?

The answers to these questions are best answered by: 1) evaluating the current and emerging risk to the organization, and 2) auditing the security controls that are current or planned to be in place to protect the information assets. Without executing formal processes to determine the risk, identify controls to mitigate the risk and subsequently audit the controls, company assurance that information assets are being adequately protected would be subject to chance. Without formal processes, there is the risk that inappropriate tools would be purchased without understanding where the tool fits into the architecture. Did this tool replace another tool? Will this tool improve the cyber security capabilities sufficiently beyond the current tool set to warrant the additional cost? Based upon the risk that the organization currently has, could the money have been spent better somewhere else? Are the current tools implemented and being attended to, or were they purchased and are now shelfware?

This white paper will provide some guidance on evaluating the risk and auditing the cyber security controls for an organization. These concepts apply to organizations large and small, even though the investment dollars and approaches will be focused differently and of a different scale.

CYBER SECURITY CONTROL SPECIFICATION

Each organization should design controls specific to the risk posture of the organization and ensure that processes and people are in place to continuously manage the controls. Control issues typically are not due to the failure of the technology, but more often are the result of individuals not executing the process or using a process that is poorly defined. Administrative, technical and operational controls can be sourced from many places, such as COBIT® 5 for Information Security[1] as a baseline.

One of the primary goals of any cyber security program should be to limit the attractiveness for the attacker. Hacking has moved well beyond the script kiddie threat stage, and the more time it takes an attacker to penetrate a system, the less desirable that target becomes. If an attacker wants to break into a car at a shopping mall during the holidays, it would be easier to jiggle all the car door handles to find the one whose owner did not lock it vs. breaking into the first car the attacker sees with a crowbar, potentially setting off the alarms. Control investments are made across the organization through technical, administrative and operational investments in people, process, technology and growing a security-oriented culture. These investments may include:

- Awareness investment
- Policy investment
- Intrusion detection systems
- Event logging
- Incident response
- Vulnerability scanning
- Information asset classification
- Forward intelligence
- Architecture and technology hardening
- Systems hardening

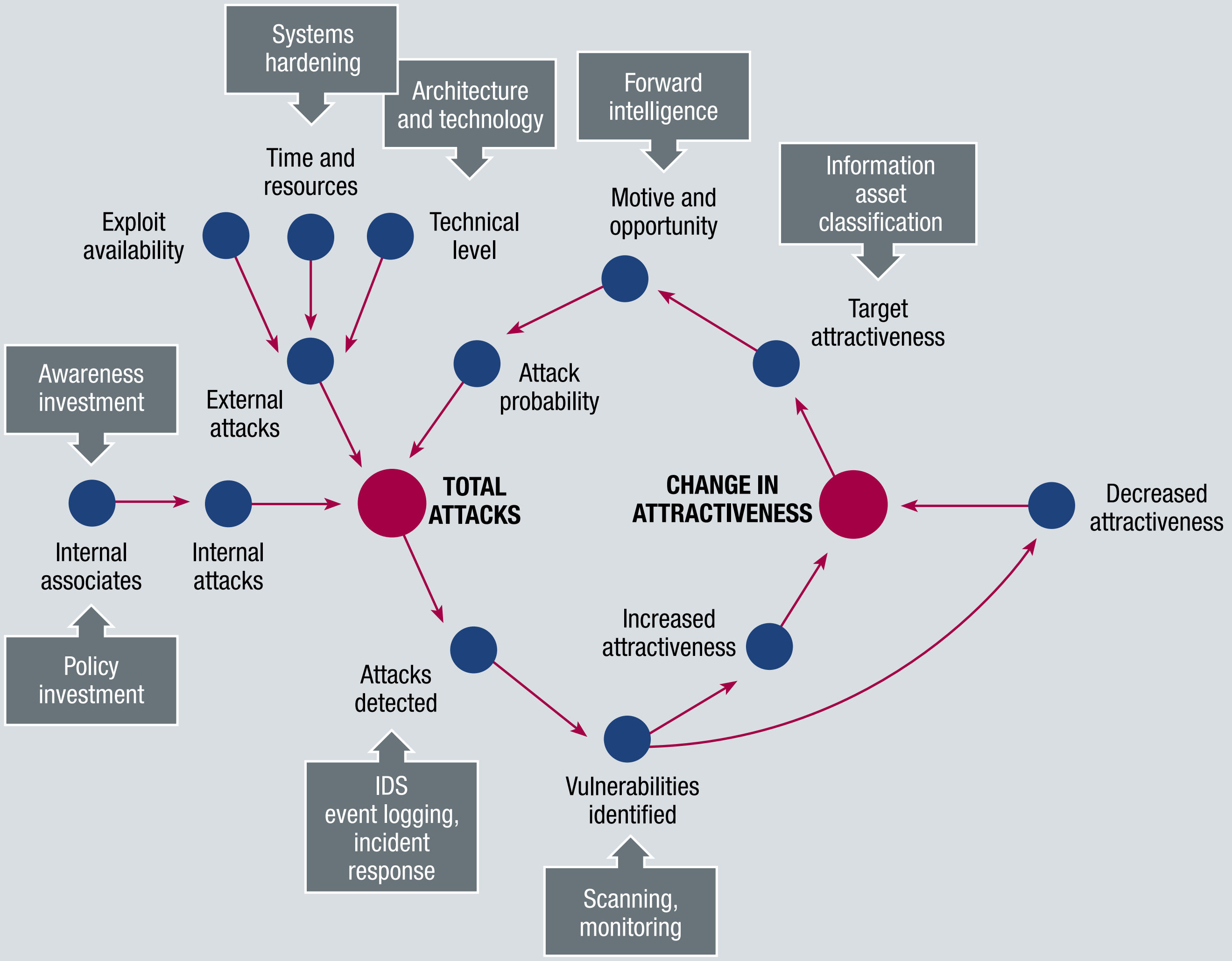
[1] ISACA, *COBIT 5 for Information Security*, USA, 2012, *www.isaca.org/COBIT/Pages/info-sec.aspx*

The attractiveness decreases as investments are made in cyber security controls in the preceding list (see **figure 1**).

Leveraging Different Cyber Security Control Frameworks

There are many approaches available for specifying cyber security control environments, such as National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations.*[2] The purpose of SP 800-53 is to provide guidelines for selecting and specifying security controls for information systems supporting executive agencies of the federal government. The NIST model, in contrast to the COBIT® 5 model, is very prescriptive in nature and may be overwhelming to many organizations. SP 800-53 contains very detailed definitions and may be best used to complement and help develop the organization-specific detailed activities to perform the COBIT 5 practices, which, in turn, as indicated in the previous section, support the overarching cyber security process.

FIGURE 1—TARGETED CYBER SECURITY INVESTMENTS



SOURCE: ISACA, *Transforming Cybersecurity*, USA, 2013, figure 58

[2] National Institute of Standards and Technology (NIST), NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, USA, 2015, *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*

The Center for Internet Security (CIS) promotes critical controls to provide a prioritized set of cyber security practices to reduce the risk of cyberattacks.[3] These are technical-based controls—such as ensuring that accurate inventories of authorized and unauthorized devices are available, secure configurations are created, vulnerabilities are assessed and remediated, and administrative privileges are controlled—prioritized with increased level of control importance. The idea is that by mitigating these cyber security gaps, the bar is raised for the external hacker to gain access. The controls are important, and this process differs from the COBIT 5 approach as there is less focus on development of processes to support the business objectives, and the primary focus is on the technical controls that need to be implemented. These controls, as with the NIST SP 800-53 controls, are useful in building the detailed activities to support the processes and practices needed, but the COBIT 5 process enablers are necessary to ensure the right cyber security activities are performed efficiently and effectively. These constructs are not readily apparent by using solely the CIS Critical Controls.

International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001, Information technology—Security techniques—Information security management systems—Requirements[4] and the Information Security Forum Standard of Good Practice for Information Security[5] can be used to supplement the processes of the five domains of the *COBIT 5 for Information Security* framework. The relevant guidance in these standards, along with the NIST SP 800-53 controls, has been mapped to the COBIT 5 framework in the *COBIT 5 for Information Security* appendices. Using the COBIT 5 framework and the associated processes provides the overarching governance and management assurance that adequate cyber security coverage exists, from the governance and planning of cyber security activities to the ongoing operation and measurement of the program.

Implementing Controls

Even organizations that are low on the maturity scale have often implemented controls that are necessary as a first line of defense, but may not have planned the implementation by thoughtful identification and implementation of the aforementioned frameworks. For example, they may have implemented a firewall, antivirus software, limited user education about password construction and backups. Each of these controls serves a purpose to protect information assets. However, the same low-maturity organization may not have placed adequate attention in ensuring that the firewall rules are updated regularly, antivirus software may not be installed on all workstations or contain the latest signatures, or end users who are on leave may miss the security awareness training. Therefore, even though controls may appear to be in place, the organization must regularly engage in independent audits to ensure these processes are well designed and executed properly.

Control Shelf Life

Controls are implemented to address the threat environment and the operating infrastructure known at the time. As threat environments change, such as the shift to cloud, mobile, Internet of Things (IoT), big data, security analytics and the need for new classes of controls to address the new location of the information, so must the controls change. The audits on these controls will also change, as new areas must now be audited (i.e., auditing the backup strategy for a cloud application or the password controls on a mobile device) to address controls that were not necessary in the past. Deficiencies once accepted in prior audits may no longer be accepted due to new laws and regulations or the growth in the amount of data and subsequent increased risk to the organization.

MULTIPLE LINES OF DEFENSE AND REVIEW PROCESSES

The audit and review universe is spread across three lines of defense, each of which contributes to the overall assurance of the cyber security program.

[3] Center for Internet Security (CIS), CIS Controls Library Resources, *www.cisecurity.org/critical-controls/Library.cfm*

[4] International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001, Information technology—Security techniques—Information security management systems—Requirements, 2013, *https://webstore.ansi.org/RecordDetail.aspx?sku=ISO%2fIEC+27001%3a2013&source=msn&adgroup=27001&keyword=iso%20iec%2027001&utm_source=bing&utm_medium=cpc&utm_campaign=Campaign%20%231&utm_term=iso%20iec%2027001&utm_content=27001*

[5] The Information Security Forum (ISF) Standard of Good Practice for Information Security, 2016, *www.securityforum.org/tool/the-isf-standardrmation-security/*

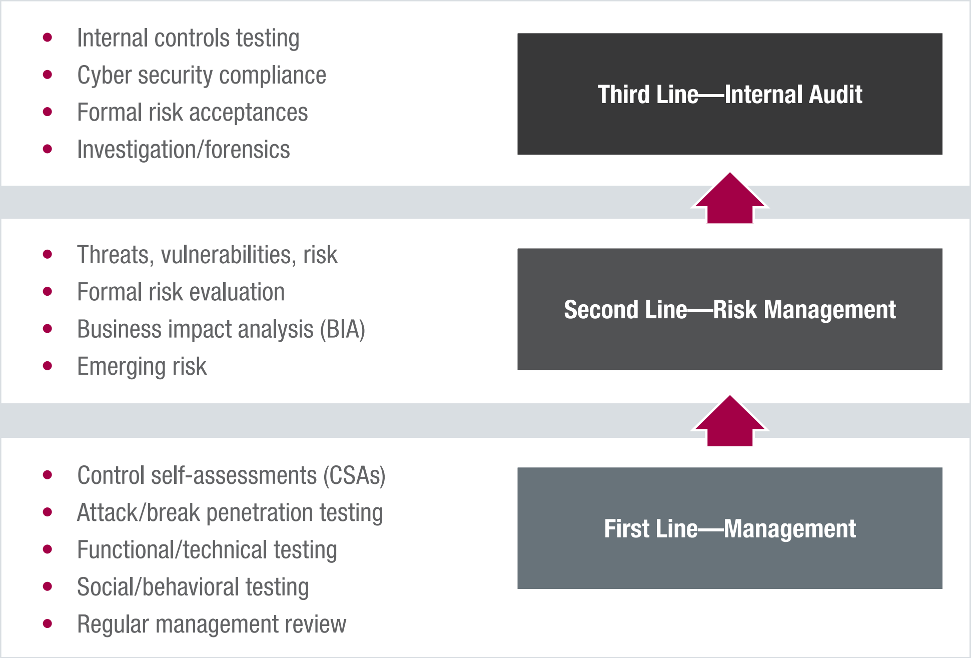
These lines of defense are management, risk management and internal audit (see **figure 2**). Reasonable independence is achieved, as the controls that were discussed in the preceding section, such as ensuring firewall rules are set, may be reviewed as part of a control assessment (first line—management), risk assessment of a high-value asset (second line—risk management) or through a third-line control by an internal audit. Having these audits and reviews performed by independent functions increases the likelihood of detecting control weaknesses and provides further checks and balances.

Management Review

As the first line of defense for the enterprise, management across the organization is assumed to have a vested interest in ensuring that cyber security controls are present and operating effectively. Responsibility and accountability are typically delegated from senior management to carry out various testing activities, such as control self-assessments (CSAs), attack and breach penetration testing, functional and technical testing, social/behavioral testing, and management reviews. Each of these processes is part of business processes designed to identify control weaknesses or deficiencies in either the design or the ongoing execution of the control.

With the prevalence of cloud services and increasing movement of data beyond company perimeters, many organizations are now issuing questionnaires to their third-party vendors to gain some comfort regarding the protection of their information assets. These questionnaires can become very voluminous and represent an additional burden on small firms not equipped to answer the questions. Request for proposal (RFP) processes for vendors are also requesting reports indicating their compliance to ISO/IEC 27001, Statements on Standards for Attestation Engagements (SSAE) 16 Service Organization Control (SOC) 2 type reports,[6] and third-party standardized vendor security scorecards. It behooves an organization to create a master database of questions and answers to enable accurate and timely response to these requests. Business opportunities may be lost without being able to demonstrate compliance with basic security controls.

FIGURE 2—LINES OF DEFENSE AND TYPICAL REVIEW ACTIVITY


Internal controls testing
Cyber security compliance
Formal risk acceptances
Investigation/forensics
Third Line—Internal Audit
Threats, vulnerabilities, risk
Formal risk evaluation
Business impact analysis (BIA)
Emerging risk
Second Line—Risk Management
Control self-assessments (CSAs)
Attack/break penetration testing
Functional/technical testing
Social/behavioral testing
Regular management review
First Line—Management

SOURCE: ISACA, *Transforming Cybersecurity*, USA, 2013, figure 45

[6] American Institute of Certified Public Accountants, Statements on Standards for Attestation Engagements, 2016, *www.aicpa.org/Research/Standards/AuditAttest/Pages/SSAE.aspx*

Management review is not a check-the-box or hold-an-annual-meeting activity, as this is intended to identify where control gaps are so that they can be mitigated. **The attackers are leveraging some of the same tools, such as penetration testers and vulnerability scanning/exploit tools, to test the network.**

Cyber Security Risk Assessment

Management ultimately owns the risk decisions made for the organization—decisions that are based on guidance the security officer and enterprise management provide, through the risk management processes, on the appropriate direction to take. The risk is present in the operational areas of the company and controls implemented must support the protection of assets. The business manager needs to be guided as to how to determine the level of confidentiality, integrity and availability (CIA) controls necessary for the department to sustain its business operations.

Companies may leverage a qualitative risk assessment process that can provide an adequate measure of risk at a lower cost than a detailed, quantitative method. Quantitative methods can provide the appearance of providing precise measurements or dollar amounts related to the risk, but these calculations are often based on subjective probability measures that are not so precise. Management can more readily understand and interpret high/medium/low or red/yellow/green charts than detailed mathematical formulas. For this reason, many organizations use a qualitative approach. The objective in any risk assessment is to communicate the state of the risk such that the easier the risk assessment is to understand, the more valuable it is.

Risk assessment approaches typically involve examining the environment through the following constructs.

Scope the System

The system boundaries and requirements for CIA need to be known. The system and data included in the risk assessment should have a documented business purpose, technical specification and controls identified that are currently operating within the system. Understanding these requirements and whether this is a low, moderate or high system with respect to CIA requirements will help frame the system for the risk assessment. Failure to accurately scope the system can result in critical assets being excluded from the security protections.

Identify Threats

Threats are those dangers that have the potential to impact CIA if adequate controls are not in place to thwart the damage. These may span from human threats (e.g., carelessness, human error, espionage, sensitive data disclosure, social media exploits, sabotage, fraud), to environmental threats (e.g., power/heating, ventilating, air conditioning [HVAC] fluctuation, cable cuts, theft, sensitive media disposal, server rooms, broken water pipes, fire), to technical threats (e.g., lack of logging, malicious code, unauthorized access, session takeover, mobile media loss, hardware/software failure, remote access). Has the organization identified the threats that are specific to itself? For example, if the data center is near a train track over which hazardous materials are transported, has this been accounted for? Or is the organization involved in activities that might attract hacktivism interest? **Each organization needs to evaluate the threats based upon the industry in which it operates and the motives of the attacker.**

Vulnerability Identification

Vulnerabilities are extremely critical to the risk evaluation process. Specifically, vulnerabilities provide the opportunity for an exploit to occur; logically, therefore and by definition, without a vulnerability present there is no risk, while with a vulnerability the risk can be potentially tremendous. Many of these vulnerabilities in system software, procedures and internal controls are the result of a control not being applied. Someone may have desire to walk into an art museum and take a valuable painting off the wall; however, one would suspect that the ability to walk out the front door with a valuable art piece would face a series of alarms and security guards stopping the theft. These are vulnerabilities that have been mitigated by appropriate controls. So, the question is, has the organization reviewed where the vulnerabilities are to honestly evaluate the risk? Are these vulnerabilities carried over from year to year without review and just accepted?

Existing Control Identification

An attacker is less likely to succeed, even with motive (threat), and opportunity (vulnerability), if the vulnerability is mitigated through an existing primary or compensating control. When designing and implementing a control, the goal should be to ensure the CIA of the information resources. To ensure control effectiveness and sustainability it must be part of the overall governance process. Control design, monitoring and testing is key to this process including ownership. The ISACA white paper *Internal Control Using COBIT® 5* provides specific details on this process.[7] Also, the control frameworks such as *COBIT® 5 for Security*, ISO/IEC 27001, NIST Cybersecurity Framework (and NIST SP 800-53 controls mentioned previously) provide excellent controls to choose from at the governance and detailed control levels. These can be supplemented by more detailed vendor guidance.

Determine Impact Severity

This step assumes that the vulnerability has been exploited and now the organization can evaluate and respond to the harm that has been done. Finance can provide insight into the costs of a system outage, or experienced/external sources on data breaches can be leveraged to determine if the cost would be high to the organization or regarded as a write-off. Impacts may include unauthorized disclosure of information, destruction of data, loss of systems, loss of reputation, loss of market share and the value of the asset compromised. Sometimes the impact may not be readily known, such as in the case of a stolen product list, marketing plans or design specifications for a new product, until later when a competitor is increasing sales at the company's expense (leveraged customer lists or internal pricing lists) or building an identical product at a lower cost (research and design costs unnecessary).

While it is important to have corrective controls in place to respond to an exploited vulnerability, it is more important to ensure preventive controls are operating effectively and efficiently to mitigate the probability of an attack. An effective risk assessment will guide management in determining the appropriate level of controls. However, it is management who is responsible to implement preventive, detective and corrective safeguards depending on multiple variables.

Determine Risk Level

Risk is typically determined by examining the likelihood of occurrence and the impact, resulting in a risk level by accepting the current state of threats, vulnerabilities and control environment. The organization has the opportunity to mitigate the risk through the application of additional controls. Once these controls are applied, the risk remaining is the residual risk. The organization should implement controls until the residual risk is at an acceptable level and management is willing to formally accept the risk. There is risk in everything and the "sweet spot" is finding a level of risk that enables a benefit commensurate with the cost. For example, implementing controls such as virtual private networks (VPNs) and two-factor authentication mitigates the risk of man-in-the-middle or eavesdropping attacks (threat) to an acceptable level for most organizations by removing the vulnerability that would exist without the implemented control. For a highly secret government entity, this control may not be enough, and restrictions to private networks and increased access authorization may be a required control based on the CIA requirements of the information system and assets.

Develop a Cyber Security Risk Response

When risk rises to the level where attention is needed (e.g., a high or medium risk, or a combination of multiple types of low risk), management must decide which approach to take. The most obvious approach is to invest in people, technology or processes to mitigate the risk. However, this requires resources and money the organization may not have. The organization also may have uncovered many risk areas through this process and needs to plan the mitigation on a prioritized basis over several years as funds permit (most likely case).

Alternatively, there are other options for resolving the risk. The risk could be assumed or accepted as is if it fits within the company's risk appetite. In other words, the company is willing to take the chance that the event will not occur, possibly because the impact is low or the probability of threat is insignificant. For example, an organization may not invest in a new malware endpoint protection product that targets ransomware because it perceives the cost to be low (restore from backup tapes, workstation is on a segmented network) or there are other threat prevention mechanisms in place, such as end-user phishing education awareness and email scanning

[7] ISACA, *Internal Control Using COBIT 5*, USA, 2016, *www.isaca.org/internal-control*

technology to rewrite and test for malicious links. In cases where the risk is accepted, an effective method is to have the risk accepted by someone at the senior management level, supported by a business justification, plans for future mitigation and a signature.

The organization may decide to avoid the risk by decommissioning the server with an unsupported operating system no longer receiving patches. It may decide to limit the risk by adding other detective or preventive controls to mitigate the risk. It may add into its processes alarms in the network logging products to alert when data exfiltration appears to be occurring on the device.

Cyberinsurance is another way to mitigate the risk through transference to another entity. While this will not mitigate the risk or transfer the ultimate accountability, it can reduce the financial impact of the event if it does occur.

To ensure adequate funding, cyber security remediation plans typically need to be executed over a period of time. Organizations should expect that certain types of reviews, such as critical vulnerabilities, must be addressed within seven, 30 or 90 days, depending upon the asset and the organization. These instances need to be reviewed by the auditors to ensure that the vulnerabilities are being addressed within the time frames; if not, changes to the processes or expectations to appropriately address the threat must be identified. Frameworks such as *COBIT 5 for Information Security*, ISO/IEC 27001 and the NIST Cybersecurity Framework are tools to promote governance of cyber security risk to ensure it is mitigated to an acceptable level.

Emerging Risk

Ten years ago, most organizations were not addressing mobile, cloud and social media. It has only been in the past ten years that an explosion in these platforms has been experienced, and now it seems almost everyone has at least one social media account and a phone in their pocket. The Internet of Things (IOT) is causing changes in the products we buy. Threat intelligence is being shared through organizations. **Ransomware, targeted attacks, spear phishing, and increased adversary capabilities cause us to reevaluate the threat environment and our defenses to it on a regular basis.** The risk assessment is not a once and done vehicle. Cyber security incidents should be reviewed for new scenarios of attack, and prevention, detection and response actions must be identified and brought into the risk assessment.

Internal Audit

The importance of having defined processes, trained and competent cyber security resources, and a governance framework to ensure that appropriate actions are carried out by the senior leadership and managed effectively on a daily basis to address current and emerging threats cannot be overstated. While those being audited may at times view it as a business disruption to gather evidence and participate fully in the audit, this external view is critical to ensure that the program is meeting the business objectives. The process builds additional accountability in the organization being audited and makes the control environment stronger.

The internal audit department usually has a dotted-line reporting relationship to the audit committee to ensure that an independent view is being communicated to the board level of the enterprise. Historically, these discussions have been on the financial, operational and information system audit areas; however, cyber security is increasingly receiving the attention of the board, and the internal audit department is playing a vital role. The internal audit function provides internal controls testing, cyber security compliance, formal risk acceptance, and support for investigations and forensics.

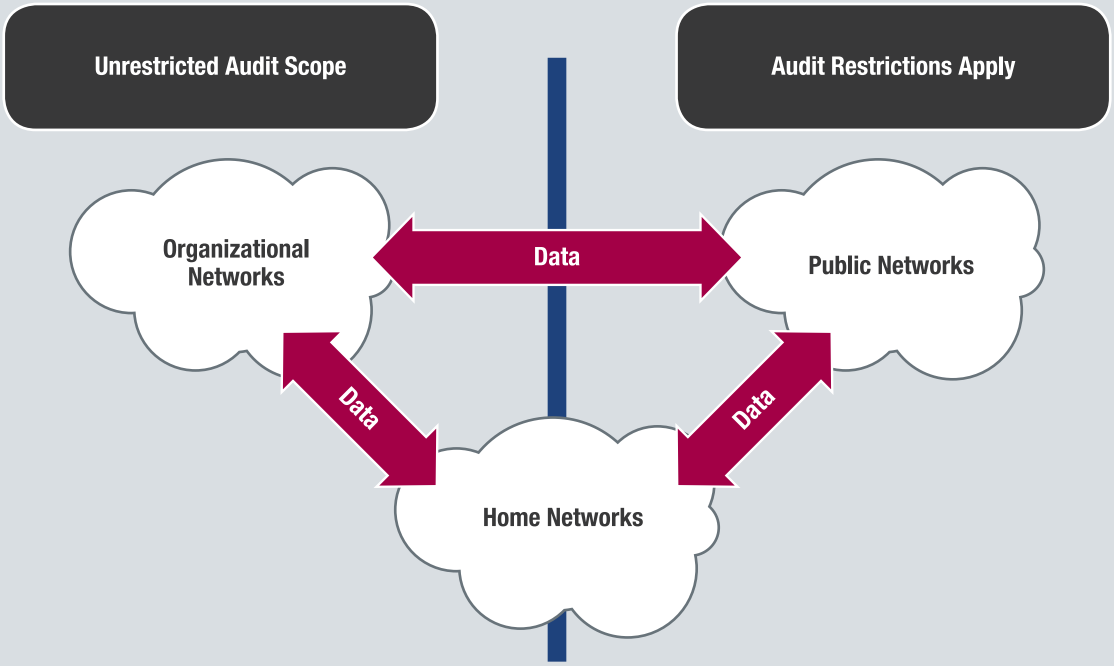
Cyber security audits should be planned on an annual cycle, taking into account consideration of the business cycles, to cause minimal disruption to business activities and increase the chances of full participation of the information technology (IT), legal, human resources (HR) and business areas necessary for the audit. With appropriate planning and time for the departments to gather the evidence (at least three or four weeks should be provided ahead of the audit), the audit can be focused on discovering the problem areas and evaluating the risk vs. waiting for and repeatedly requesting the information multiple times. Audits should be planned activities with entrance, daily update and exit meetings, and exact expectations for each stage clearly communicated. Testing activities frequently require account setup and access to carry out activities, and failure to provide these in a timely manner can elongate the audit.

Audit Scope

Organizations are rarely monolithic entities with all the information processing occurring within the company or fully accessible to the auditors. Users may be using their home networks while working from home, applications may be executing in the cloud, or there may be private confidential systems (e.g., HR information, legal documentation) that may need further access or authorization to enable an audit (see **figure 3**). As data may flow across these systems and present risk, these restrictions should be recognized and addressed so that the audit coverage is clear in scope. Users may need to sign work-at-home agreements permitting the audit of their environment, or the use of mobile devices may need to be supported by a document signed by the user that information about and configuration of the device are subject to audit.

Vendors handling information—particularly information that has high sensitivity or where personal data are involved—should be required to demonstrate how they are protecting the information. This could be accomplished through a right-to-audit clause included in the contract, a security standard certification (e.g., ISO/IEC 27001, SSAE 16 SOC2 report, Cloud Security Alliance (CSA) Control Matrix report[8]), and contractual liability for information entrusted to their care. Vendors will attempt to limit their liability; however, they should be willing to provide one of these assurances as they are being depended upon to protect the information and represent an extension to the enterprise. When a breach occurs, the reputation damage is most likely to be targeted at the organization entrusted with the data by the client or customer, not the downstream vendor processing the data.

FIGURE 3—AUDIT BOUNDARIES



SOURCE: ISACA, *Transforming Cybersecurity*, USA, 2013, figure 46

[8] ISACA, *COBIT 5 for Information Security*, USA, 2012, *www.isaca.org/COBIT/Pages/info-sec.aspx*

Because cyber security audits are usually more technical and complex than general audits, different approaches may be taken to facilitate the audit, depending upon the governance, risk, management or assurance area of review (see **figure 4**).

Cyber Security Goals and Related Audit Objectives

Audits can take many shapes and have different focuses with respect to cyber security overall governance or technical testing. Different aspects of the program should be tested over time. For programs that may be in the initial states of maturity, the focus may be centered on ensuring that the policies, procedures, standards and guidelines are relevant, approved by management, and frequently updated and reviewed in response to business changes. For more mature programs that have the basics in place, the audit may shift to examine how current and emerging risk is being identified and addressed. With the attention shifting today to detection and response, the organization may wish to audit to determine how well prepared it is in the event of a breach.

Because it would be impossible to audit all areas of the business, it is essential to look at the high-value areas to audit. For example, what would happen if the telecommunications link between a call center and the necessary systems were to fail? Are appropriate controls in place to handle a denial-of-service attack for an e-commerce-oriented website? Does the organization have the appropriate monitoring controls in place to ensure that data exfiltration activities would be noticed in time, or have the data environments been segregated to protect these data from a targeted attack?

FIGURE 4—PLANNING AND SCOPING

Area/Type of Review	Approach	Remarks
Governance: cyber security policy and related technical key operating procedures	Point in time, postimplementation after 2013 due date for updated policy	The policy update supports transformation. The audit will address the business function/local design and implementation of key operating procedures supporting the policy. A follow-up audit on deficiencies will be held in 2014.
Risk: risk register update, treatment and risk reporting in cyber security	Point in time for 2013 year-end, including 2012 risk audit results	The audit will address risk register accuracy, completeness and proper updating. Risk reporting (timeliness, completeness, accuracy) is included.
Management: cyber security incident reviews	Continuous, based on actual attacks, breaches and incidents	This is a semiformal review of any attack or breach (including near misses) as part of standard third-line-of-defense involvement.
Assurance: cyber security risk management process	Point in time and transformational, comparing 2012 against 2013 year-end	Audit will independently review the efficiency and effectiveness of the cyber security risk management process, i.e., the third line auditing the second line of defense.

SOURCE: ISACA, *Transforming Cybersecurity*, USA, 2013, figure 48

The audit objectives should be aligned with the cyber security goals to achieve the best business outcomes (see **figure 5**). Matching the cyber security program goals with the audit objectives will increase support for the audit within the cyber security management and *vice versa*.

External Audit

Organizations contract for the services of external auditors to provide independent assurance of the financial and operational controls primarily to ensure the controls design is effective and the implementation of the controls is operating as it should. Outside auditors are also used by external entities to ensure

FIGURE 5—CYBER SECURITY GOALS AND RELATED AUDIT OBJECTIVES

Cyber Security Goal	Audit Objective(s)	Remarks
Cyber security policies, standards and procedures are adequate and effective.	• Verify that documentation is complete and up to date • Confirm that formal approval, release and enforcement are in place. • Verify that documentation covers all cyber security requirements. • Verify that subsidiary controls cover all provisions made in policies, standards and procedures.	This audit addresses the universe of documents (governance side) and controls stipulated by these documents. "Effective" in this sense cannot audit more than the proper approval/release/enforcement cycle, whereas "adequate" can relate only to completeness, adequacy and integrity of the policies, standards and procedures.
Emerging risk is reliably identified, appropriately evaluated and adequately treated.	• Confirm the reliability of the risk identification process. • Assess the risk evaluation process, including tools, methods and techniques used. • Confirm that all risk is treated in line with the evaluation of the results. • Verify that the treatment is adequate or formal risk acceptances exist for untreated risk	This audit will usually span several years, focusing on processes, tools and methods in the first year. In subsequent years, auditors will most likely take samples of risk areas and drill down into the process. The audit may include external data to qualify the full coverage of "emerging" risk.
Cyber security transformation processes are defined, deployed and measured.	• Verify the existence and completeness of the transformation process and related guidance. • Verify that the transformation process is implemented and followed by all parts of the enterprise. • Confirm controls, metrics and measurements relating to transformation goals, risk and performance.	This audit, which will transpire over several years, is designed to cover the processes for transforming cyber security.
Attacks and breaches are identified and treated in a timely and appropriate manner.	• Confirm monitoring and specific technical attack recognition solutions. • Assess interfaces to security incident management and crisis management processes and plans. • Evaluate (on the basis of past attacks) the timeliness and adequacy of attack response.	This is an in-depth technical audit that looks at the technology for early recognition and identification of attack, then at the subsequent steps for escalating and managing incidents. "Timely" and "appropriate" are defined as specified in relevant policies, standards and procedures (no subjective audit judgment).

SOURCE: ISACA, *Transforming Cybersecurity*, USA, 2013, figure 47 that the services of the organization are meeting needs. These audits are typically on behalf of a governmental agency or regulator. Auditing cyber security controls can leverage the expertise of an external auditor and retain access to skill sets that may not be present within the organization. The technical skills required for specialized analysis, such as penetration testing, examining the server or firewall configurations, or reviewing the security information event management (SIEM) rule sets, may not currently exist in the internal audit department and could leverage external skill capabilities.

Cyber Security Maturity Models

A cyber security program maturity model could also be implemented to analyze the current state, with a view toward the desired state as other cyber security controls are assessed and new technology, people or process controls are implemented. Different organizations and frameworks have various names for the increasing levels of maturity; however, most adhere to some form of the following to demonstrate maturity: nonexistent (level 0), *ad hoc* (level 1), repeatable (level 2), defined (level 3), managed (level 4) and optimized (level 5).

At the nonexistent and *ad hoc* ends of the scale, cyber security is not a planned activity and may not have the executive awareness needed to move the program forward. Policies may be nonexistent or controls may be in place and not driven by policy or consistently applied. Tools may not exist or, when they do exist, are poorly executed. Obviously, this is not a state where organizations need to stay, but it is a state where many programs start out prior to the assignment of someone specifically responsible for cyber security and the broader information security program (e.g., chief information security officer [CISO], vice president of information security, director of information security).

At the top end of the maturity scale, cyber security is an important part of the culture, executive scorecards report the metrics tied to the financial and operational company performance, and industry frameworks are adopted to drive continuous improvement in the cyber security program. Reporting is also at a high enough level in the organization to obtain the necessary attention and funding.

Cyber security maturity tools are typically used by those responsible for managing the cyber security program to demonstrate year-over-year enhancement of the program. Multiyear road maps can then be generated, suggesting new tools and approaches to increase the maturity level. These can drive RFP processes to engage vendors to attain the best pricing and product fit in a systematic manner vs. responding to the latest threat. This also permits implementation of controls through planned mechanisms at a lower cost, as the project can be spread out over a longer period without needing to hire an expensive resource because the project needs to be completed immediately. This also permits relationships to be built among the business area, vendor, project manager and allocated technical resource to help guide the effort.

Prior management reviews, risk assessments and audit findings can be leveraged to build the maturity model to provide a holistic picture of the cyber security program maturity state and identify areas that will fill gaps in the risk assessment and decrease the likelihood of a subsequent internal or external audit findings.

CORRECTIVE ACTION PLANS

Reviews created through management, risk management processes or internal audit will identify gap or issue items needing resolution. Once these cyber security gaps are known and agreed to via the draft reports, actions need to be formulated within a reasonable time frame (10 to 30 days, depending on the organization) and corrective action plans agreed to by the business owners. The organization needs to monitor these agreed-upon activities, milestones and deliverable dates to ensure that the security posture is not weakened through inattention to the gap areas. Process (or business) owners should agree on the time frame for ongoing processes, such as 90 days for remediation of new vulnerabilities identified or reporting of all incidents within 24 to 72 hours.

SUMMARY

Failure to protect the information assets of an organization can have a devastating impact on business operations, financial condition and reputation in the marketplace. Appropriate investment in cyber security controls is necessary to reduce the attractiveness of the target for the attacker and increase the expense of the attack. Multiple frameworks such as *COBIT 5 for Information Security*, ISO/IEC 27001 and the NIST Cybersecurity Framework, along with the NIST SP 800-53 controls, provide processes that may combine to enable management of cyber security controls.

Equally important are the multilayered review defenses of management, risk management and internal audit to ensure that cyber security controls are well designed to protect the information assets and are operating effectively. Without these review processes, the organization sacrifices governance of the cyber security controls, as reliance of the control operating effectively depends on one area of failure—the department operating the control. The management reviews, risk management processes, internal audits and the business operations responsible for executing the cyber security controls are complementary to each other. Auditing the cyber security controls provides insight for improvement opportunities and should be embraced by the organization to enhance the maturity of the cyber security program.

Trust in, and value from, information systems

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA

Phone: +1.847.253.1545

Fax: +1.847.253.1443

Email: info@isaca.org

Web site: *www.isaca.org*

Provide feedback:
www.isaca.org/auditing-cyber-security

Participate in the ISACA Knowledge Center:
www.isaca.org/knowledge-center

Follow ISACA on Twitter:
https://twitter.com/ISACANews

Join ISACA on LinkedIn:
ISACA (Official),
http://linkd.in/ISACAOfficial

Like ISACA on Facebook:
www.facebook.com/ISACAHQ

ISACA®

ISACA (*isaca.org*) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity Nexus™ (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

Disclaimer

This is an educational resource and is not inclusive of all information that may be needed to assure a successful outcome. Readers should apply their own professional judgment to their specific circumstances.

Reservation of Rights

ACKNOWLEDGMENTS

ISACA wishes to recognize:

Author

Todd J. Fitzgerald
CISA, CISM, CRISC, CGEIT, Grant Thornton International, Ltd, USA

Expert Reviewers

Ian Cooke
CISA, CRISC, CGEIT, CFE, CPTS, DipFM, ITIL Foundation, Six Sigma Green Belt, An Post, Ireland

Khaja Khan
Ace Hardware Corporation, USA

John McGill
CISA, R&M Consulting, USA

Board of Directors

Christos K. Dimitriadis
Ph.D., CISA, CISM, CRISC, INTRALOT S.A., Greece, Chair

Theresa Grafenstine
CISA, CGEIT, CRISC, CIA, CGAP, CGMA, CPA, U.S. House of Representatives, USA, Vice-chair

Robert Clyde
CISM, Clyde Consulting LLC, USA, Director

Leonard Ong
CISA, CISM, CGEIT, CRISC, CPP, CFE, PMP, CIPM, CIPT, CISSP ISSMP-ISSAP, CSSLP, CITBCM, GCIA, GCIH, GSNA, GCFA, Merck, Singapore, Director

Andre Pitkowski
CGEIT, CRISC, OCTAVE, CRMA, ISO27kLA, ISO31kLA, APIT Consultoria de Informatica Ltd., Brazil, Director

Eddie Schwartz
CISA, CISM, CISSP-ISSEP, PMP, USA, Director

Jo Stewart-Rattray
CISA, CISM, CGEIT, CRISC, FACS CP, BRM Holdich, Australia, Director

Tichaona Zororo
CISA, CISM, CGEIT, CRISC, CIA, CRMA, EGIT | Enterprise Governance (Pty) Ltd., South Africa, Director

Zubin Chagpar
CISA, CISM, PMP, Amazon Web Services, UK, Director

Rajaramiyer Venketaramani Raghu
CISA, CRISC, Versatilist Consulting India Pvt. Ltd., India, Director

Jeff Spivey
CRISC, CPP, Security Risk Management, Inc., USA, Director

Robert E Stroud
CGEIT, CRISC, Forrester Research, USA, Past Chair

Tony Hayes
CGEIT, AFCHSE, CHE, FACS, FCPA, FIIA, Queensland Government, Australia, Past Chair

Greg Grocholski
CISA, SABIC, Saudi Arabia, Past Chair

Matt Loeb
CGEIT, FASAE, CAE, ISACA, USA, Director