Auditing Cybersecurity

Martin Coe, DBA, CISA, CISM, CPA, is an accounting professor at Western Illinois University (USA). His research has been published in professional and academic journals and he is regarded as an expert in the fields of accounting, accounting information systems and information systems auditing. He is also the president of Vistabon, an IT auditing firm. Coe has managed information technology vulnerability assessments since 1998.

Information security risk has dramatically evolved; however, security strategies that are typically compliance-based and perimeter-oriented have not kept pace. Consequently, sophisticated intruders can bypass perimeter defenses to perpetrate attacks that are highly targeted and difficult to detect. This article discusses an approach to assess the adequacy of a firm's cybersecurity posture.

The results of the *Global State of Information Security Survey* published by PricewaterhouseCoopers (PwC) in September of 2013 show that while information security risk factors have dramatically evolved, security strategies that are typically compliance-based and perimeter-oriented have not kept pace.[1] Consequently, sophisticated intruders can bypass perimeter defenses to perpetrate dynamic attacks that are highly targeted and difficult to detect. The results of the PwC survey suggest that today's elevated risk landscape demands a new approach to security—one that is driven by knowledge of threats, assets and adversaries.

Given the need for a strong cybersecurity posture, there have been various efforts to create cybersecurity standards. One such standard is ISO 27001, *Information security management systems*,[2] which provides a set of specifications against which an organization can have its information security management system independently certified. ISO 27001 is tied to ISO 27002, *Information technology—Security techniques—Code of practice for information security controls*,[3] which contains 39 control objectives for protecting information assets from threats to their confidentiality, integrity and availability. Each of the 39 objectives is then broken down into many specific controls. The standard does not require any specific controls to be implemented, but rather leaves it to the user to select those controls appropriate for their specific requirements.

Another standard is the US National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.[4] NIST SP 800-53 identifies 198 security practices that are divided into 18 families and three classes. Each of these security practices has been mapped to ISO 27001. SP 800-53 defines three security baselines that provide a starting point for determining the security controls that should be implemented for low-impact, moderate-impact and high-impact IT systems. These baselines could serve as the basis for a risk-based security standard for various categories and subcategories of assets.

In February 2013, recognizing that the national and economic security of the US depends on the reliable functioning of critical infrastructure, US President Barack Obama issued Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*.[5] The order directed NIST to work with stakeholders to develop a voluntary framework (based on existing standards, guidelines and practices) for reducing cyberrisk to critical infrastructure. NIST released the first version of the *Framework for Improving Critical Infrastructure Cybersecurity* on 12 February 2014.[6] The framework, created through collaboration between industry and government, consists of standards, guidelines and practices to promote the protection of critical infrastructure. The prioritized, flexible, repeatable and cost-effective approach of the framework was designed to help owners and operators of critical infrastructure to manage cybersecurity-related risk.

While the certified public accountant's (CPA's) external audit responsibilities do include the responsibility to assess security as part of certain engagements, such as audits of controls at service organizations, the CPA's financial statement audits do not usually include the responsibility to assess cybersecurity. However, the internal IT audit function frequently does include the responsibility to assess cybersecurity. Indeed, assessing security is a key component of the Certified Information Systems Auditor® (CISA®) job practice analysis, which reflects the responsibilities of IT auditors.[7] Regarding cybersecurity assessment approaches, IT audit standards include a procedure related to cybersecurity assessment. ISACA's IS Auditing Procedure P8 Security Assessment—Penetration Testing and Vulnerability Analysis, (P8)[8] provides scope and procedure guidance related to cybersecurity assessments.

CYBERVULNERABILITY ASSESSMENT APPROACH

Managing many cybervulnerability projects has revealed valuable insights into approaches used to assess a firm's cybersecurity posture. Utilizing ISACA's IS Auditing P8 offers an approach that focuses on attack vectors and has assessment phases for the relevant attack vectors (i.e., the Internet and the internal network).

The assessment phases are typically conducted utilizing the Tenable Network Security Nessus vulnerability scanning tool (Nessus)[9] combined with other assessment procedures. Nessus utilizes the Common Vulnerability Scoring System (CVSS) to facilitate risk assessment. A risk assessment requires a qualitative analysis of vulnerabilities within a network. The Forum of Incident Response and Security Teams (FIRST)[10] created CVSS to normalize the methodology of analyzing risk. CVSS provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. CVSS consists of three metric groups: base, temporal and environmental.[11] The base metric represents the intrinsic qualities of a vulnerability. The temporal metric reflects the characteristics of a vulnerability that change over time. The environmental metric represents the characteristics of a vulnerability that are unique to any user's environment. When the base metrics are assigned values by an analyst, the base equation computes a score ranging from 0.0 to 10.0 as illustrated in **figure 1**.

The Nessus reports use the base metric group to aid in the performance of qualitative risk analysis.[12] Vulnerabilities with a CVSS base score in the 7.0-10.0 range are critical, those in the 4.0-6.9 range are major, and those in the 0.0-3.9 range are minor. The CVSS scores correspond to the Tenable severity levels, which are:

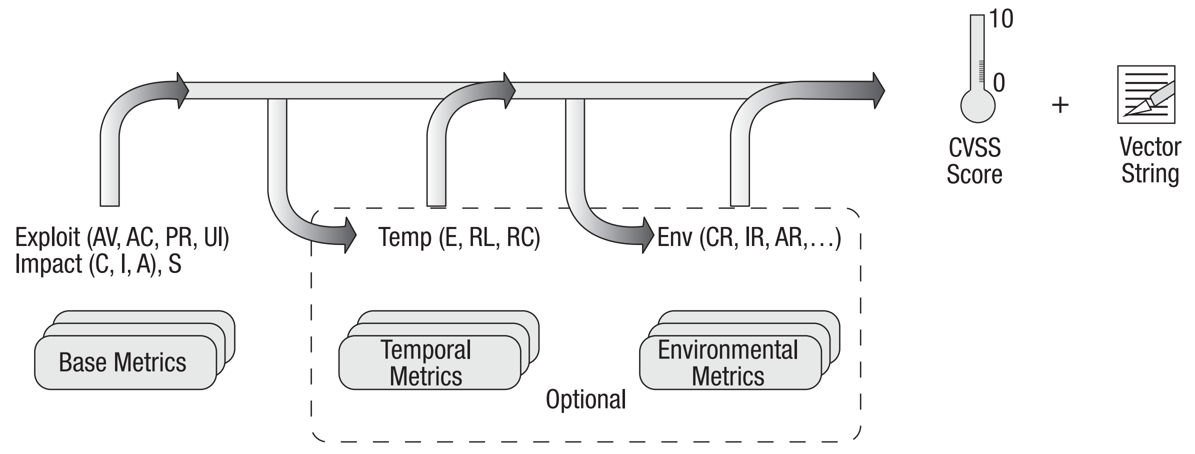
- 10.0 = Critical
- 7.0-9.9 = High
- 4.0-6.9 = Medium
- 0.0-3.9 = Low

At each severity level, the number of vulnerabilities is displayed along with the percentages of those vulnerabilities in each CVSS score grouping.

The assessment team uses the Nessus results to identify hosts that warrant interrogation. In general, the team focuses on hosts that have vulnerabilities rated as medium, high or critical. The team then performs procedures to confirm the validity of the findings and rule out false positives. The team uses a variety of tools to assist in the interrogation of vulnerabilities. Another term for this aspect of the assessment is exploitation.

Often the goal of exploitation is to gain control over a system. More specifically, an exploit is a way to leverage a

Figure 1—CVSS Metrics and Equations



Source: FIRST.Org, Inc., *https://www.first.org/cvss/specification-document#i1.1*. Reprinted with permission.

security flaw or circumvent security controls. The process can take many forms; however, the goal is usually to gain administrative access to a computer or device. The wide range of activities, tools and options related to exploitation make this step more of an art than a science. Indeed, exploitation is one of the most ambiguous phases of the cybersecurity assessment process. The reason for this is simple; each system is different and each target is unique. Depending on a multitude of factors, the attack vectors will vary from target to target, so skilled attackers have to understand the nuances of each system they are attempting to exploit.[13]

While the assessment approach discussed here is an effective way to assess cybersecurity, there are several propositions to improve the cybervulnerability assessment process.

SKILLS AND TOOLS

The assessment team needs to include skilled attackers who understand the nuances of each system they are attempting to exploit. For example, assessors should have a current and thorough understanding of security related to operating systems, firewalls, routers and other network devices. The team should also utilize a mix of tools to perform the assessment. For example, assessors should utilize a variety of programs to discover potential vulnerabilities and determine if the vulnerability can be exploited.

> “Exploitation is one of the most ambiguous phases of the cybersecurity assessment process. The reason for this is simple; each system is different and each target is unique.”

- **Proposition 1a**—Cybersecurity assessments should require a step to ensure that assessors understand the nuances of each system they are attempting to exploit.
- **Proposition 1b**—Cybersecurity assessments should require a step to ensure that assessors have a variety of tools at their disposal.

RISK FOCUS

It is important to eliminate false positives. Given the large number of vulnerabilities identified by Nessus, the task to eliminate false positives can be significant. The assessment team should utilize a risk-based approach to focus audit energy on areas of greatest risk. Such an approach is consistent with the NIST framework.

- **Proposition 2a**—Cybersecurity assessments should be risk-based.
- **Proposition 2b**—Cybersecurity assessments should require a step to ensure that false positives are eliminated.

PATCH MANAGEMENT

IT change and patch management can be defined as the set of processes executed within the organization’s IT department designed to manage the enhancements, updates, incremental fixes and patches to production systems, which include application code revisions, system upgrades and infrastructure changes.[14] Patch management tasks include:

- Maintaining current knowledge of available patches
- Deciding what patches are appropriate for particular systems
- Ensuring that patches are installed properly
- Testing systems after installation
- Documenting all associated procedures, such as specific configurations required

Patches often are designed to fix security vulnerabilities. Indeed, many of the recommendations to address vulnerabilities identified in a cybersecurity assessment include the installation of a specific patch. Accordingly, implementing patch management practices such as a tactical, integrated and automated approach to handling vulnerabilities can boost a company’s cybersecurity posture. Likewise, successful patch management policies can also help with security audits and compliance audits. For example, continuous auditing routines could be developed to ensure that patches are applied on a timely basis.

In response to increased cyberattacks, there is a need for models to focus limited administrator attention and build cases for additional resources. One proposed method is based on Markov-decision processes for the generation and graphical evaluation of relevant maintenance policies for cases with limited data availability.[15] Since cybersecurity assessments provide security information by host, steps should be taken to categorize hosts (i.e., ordinary host with no sensitive data, critical host with sensitive data) to ensure that maintenance policies are directed toward the most critical hosts.

- **Proposition 3a**—Cybersecurity assessments should include an assessment of patch management policies.

- **Proposition 3b**—Cybersecurity assessments should leverage continuous auditing procedures to ensure that patches are applied on a timely basis.
- **Proposition 3c**—Cybersecurity assessments should categorize hosts to ensure that maintenance recommendations can be directed toward the most critical hosts.

ATTACK VECTORS AND DEFENSE-IN-DEPTH

Given that adversaries can attack a target from multiple points using either insiders or outsiders, an organization needs to deploy protection mechanisms at multiple locations to resist all classes of attacks. Defense-in-depth is a practical strategy for achieving information assurance in today's highly networked environments.[16] Accordingly, some information security postures utilize a defense-in-depth model. Such a model refers to the way hardware and software is configured to provide different levels of security. A defense-in-depth model recognizes that not all resources require the same level of security. In addition, this model can mitigate exposures that might otherwise exist. For example, if a server is vulnerable to an exploit because it is not able to be updated, a defense-in-depth layer can be added to mitigate the exposure. Accordingly, cybersecurity assessments should include a review of defense-in-depth security layers. Likewise, since a company may accept a risk related to one attack vector by relying on defense-in-depth, the assessment should include various exploitation paths to test defense-in-depth.

- **Proposition 4**—Cybersecurity assessments should include a review of defense-in-depth security layers.
- **Proposition 4b**—Cybersecurity assessments should include various exploitation paths to test defense-in-depth.

STANDARDS

Given the fact that a cybersecurity assessment should test an actual state against a desired state, it is necessary to have a standard against which to audit. At this point in time, NIST SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*,[17] which has been mapped to ISO 27001, is a logical standard to utilize. In addition, specific regulatory security standards that must be met for categories of assets or specific assets (e.g., ports/services and default account requirements related to critical infrastructure protection assets) should be utilized.

- **Proposition 5a**—Cybersecurity assessments should utilize standards such as NIST SP 800-53.
- **Proposition 5b**—Cybersecurity assessments should utilize specific regulatory security standards that must be met for applicable categories of assets or specific assets.

CONCLUSION

Cybersecurity assessments should be conducted in phases and focus on attack vectors, as indicated in IS Auditing P8. In addition, cybersecurity assessments should include steps to ensure that the assessment team has adequate skills and tools to perform the assessment. The assessment should focus on the greatest risk and include steps to reduce false positives. Given the importance of patch management, assessments should include steps to assess the adequacy of patch management. Since attacks can come from multiple points, assessments should include a review of defense-in-depth security layers. Since cybersecurity assessments should test an actual state against a desired state, assessments should utilize standards.

ENDNOTES

[1] PricewaterhouseCoopers, *The Global State of Information Security Survey 2013*, USA, *www.pwc.ru/en/riskassurance/publications/information-security-survey.html*

[2] International Organization for Standardization, ISO/IEC 27001, *Information security management, www.iso.org/iso/home/standards/management-standards/iso27001.htm*

[3] International Organization for Standardization, ISO 27002, *Information technology—Security techniques—Code of practice for information security controls, www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54533*

[4] National Institute of Standards and Technology, *Security and Privacy Controls for Federal Information Systems and Organizations*, SP 800-53, Revision 4, USA, 30 April 2013, *http://csrc.nist.gov/publications/PubsSPs.html#800-53*

[5] National Archives and Records Administration, Executive Order 13636, *Improving Critical Infrastructure Cybersecurity*, USA, 19 February 2013, *www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf*

[6] National Institute for Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity*, USA, 2014, *www.nist.gov/cyberframework/*

[7] ISACA®, Certified Information Systems Auditor Job Practice, USA, June 2011, *www.isaca.org/Certification/CISA-Certified-Information-Systems-Auditor/Job-Practice-Areas/Pages/CISA-Job-Practice-Areas.aspx*

[8] ISACA, IS Auditing Procedure P8, Security Assessment-Penetration Testing and Vulnerability Analysis, *IS Standards, Guidelines and Procedures for Auditing and Control Professionals*, USA,15 March 2008

[9] Tenable Network Security, Nessus, *www.tenable.com/products/nessus-vulnerability-scanner*

[10] Forum of Incident Response and Security Teams, *www.first.org/*

[11] Mell, P.; K. Scarfone; "A Complete Guide to the Common Vulnerability Scoring System Version 2.0," First.org, June 2007, *www.first.org/cvss/cvss-v2-guide.pdf*

[12] Dumont, Cody; "Understanding Risk," Tenable Network Security, 14 October 2014, *www.tenable.com/sc-dashboards/understanding-risk*

[13] Engebretson, Patrick; *The Basics of Hacking and Penetration Testing: Ethical Hacking and Penetration Testing Made Easy*, Elsevier, USA, 2013

[14] Institute of Internal Auditors, *Global Technology Audit Guide Change and Patch Management Controls: Critical for Organizational Success*, 2012

[15] Afful-Dadzie, A.; T. Allen; "Data-driven Cyber-vulnerability Maintenance Policies," *Journal of Quality Technology*, vol. 46, no. 3, 2014, p. 234-250

[16] National Security Agency, "Defense in Depth," USA, *www.nsa.gov/ia/_files/support/defenseindepth.pdf*

[17] *Op cit*, National Institute for Standards and Technology 2013