Compliance & Ethics Professional®

November 2017

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org

Meet Jimmy Chatsuthiphan

Senior Director of Ethics & Compliance for Asia Pacific Diebold Nixdorf Singapore

See page **16**

by Mark Lanterman

The components of strong cybersecurity plans, Part 1: Maturity assessment

» Maturity assessments lay the groundwork for cybersecurity programs and allow management to establish desired improvement in comparison to current capabilities.

» A security assessment helps establish security governance by providing an independent check on information technology staff, increased awareness of security risks and threats, and prioritization of IT spending for the purposes of risk mitigation.

» A security audit focuses on the completeness, design, implementation, and efficacy of internal security controls.

» Vulnerability scanning is an ongoing process in an organization that is both offensive and defensive depending on its use.

» Ultimately, a penetration test is only a fraction of developing a strong cybersecurity plan. However, these tests are frequently needed for compliance with regulations that set the minimum requirements for cybersecurity programs.

As organizations, companies, and individuals adapt to new technologies, awareness about the potential risks and dangers associated with these devices has grown. Headlines within the past few years have focused on a growing number of companies becoming victims of hacking, spear phishing, and other acts of cybercrime. Unfortunately, it would seem that within this digital landscape, it's not a matter of if, but when. With these odds, many people are wanting more assurance when it comes to keeping their assets safe.

Lanterman

In response to a growing awareness of cybersecurity trends and organizational responsibility that extends far beyond the IT department, many people request penetration testing of their organization's security infrastructure. Penetration testing and security assessments have almost become synonymous terms. Conflating penetration testing, vulnerability scanning, and social engineering among other security assessment components is common. However, all are separate components of complete security assessments.

In a series of five articles, I will condense the components of digital security programs to maturity assessment, security assessment, security auditing, technical vulnerability scanning, and penetration testing. Though last in this series, it would seem that in spite of recent attention being paid to strong security postures, penetration testing is given the most weight in organizations' attempts to

establish strong policies and procedures. However, comprehensive security plans require attention to all five of the aforementioned components, conducted on a regular basis. The maturity assessment is the first step in this ongoing process.

A maturity assessment defines management desires and expectations regarding the operation of its security program. During this critical phase, the personnel, processes, and technology capabilities in several key security areas are assessed. In this manner, a contextual understanding of the organization's security culture is developed.

Methodologies involved in this stage include a review of critical security controls in relation to the NIST Cybersecurity Framework. Comparison between established baselines and current regulatory requirements will provide information for subsequent gap assessments.

Security professionals will present management with an established risk context, measure the capability in adopting new procedures, and propose appropriate strategies depending on the outcomes of the initial review and baseline assessment. The purpose of this is to obtain management support in improving existing policies and developing new policies.

In terms of deliverables, the maturity assessment is indispensable in that it provides management and relevant stakeholders with a quantitative statement, or score between 0–5, of an organization's current security status. In its simplest form, a maturity assessment is conducted by reviewing the practices in each key security area and then assigning a maturity level to each area. Each level is associated with a numeric score. An overall score is calculated by averaging all the scores from the key areas.

A score of 0 equates to a certain key area having no maturity. A 1 is at an initial level of maturity and demonstrates that certain practices within a key area are just beginning to be realized. A 2 is an ad hoc maturity level score, meaning that some practices exist within a key area, but they are applied inconsistently. A score of 3 indicates a defined degree of maturity, meaning that an organization is aware of the key security area and has a plan for instituting policies. A score of 4 is associated with a managed maturity level, meaning that an organization is equipped with metrics on what has been defined for desired policies within a certain key area. A score of 5 indicates an optimized maturity level, meaning that continuous improvement within a key area is accounted for by an organization in addition to knowledge and implementation of existing policies. More sophisticated techniques, such as assigned various weights to key areas or practices, may be applied to achieve more variation in scoring. The key aspects of a security model tend to include several maturity levels that define a continuum, from least capable of consistent outcomes to an optimized and self-sufficient process of continuous improvement. Various models have differing numbers of levels, but typically, there are three to five levels.

Maturity levels are simplified stages representing a composite continuum of many factors. The following examples illustrate possible levels:

1. Processes: Undocumented to documented, manual to automated, siloes to integrated, external requirements to optimized internal requirements

2. Technology: Single purpose to orchestrated, simple to complex, open source to commercial
3. People: Generalized to specialist workforce, security awareness ranked from low to high

Due to the variety of factors to be considered, maturity assessments are subjective. Other security program components to be discussed in future articles are progressively more objective.

The Department of Energy's Cybersecurity Capability Maturity Model (C2M2), the National Institute of Standards and Technology's Cybersecurity Framework (CSF), International Standards Organizations 27001, and the Center of Internet Security's Critical Security Controls are some of the most popular frameworks leveraged to identify the key areas and practices to be evaluated in a maturity assessment.

The primary purpose of the maturity assessment is to engage an organization's management in developing a cybersecurity strategy. Management's awareness of good cybersecurity practices rises when key areas are assessed in relation to creating a durable security program. Reviewing baseline results may be eye-opening, especially when considered in relation to an organization's score on a continuum. Once the baseline maturity assessment is complete, management should identify areas needing improvement and establish a potential revision timeline. Usually, priorities are identified by observing the largest gaps between current capability and management's desired capability.

Before other elements of the comprehensive security plan can be devised, the baseline maturity assessment serves as the initial step, followed immediately by gap assessment. Simply put, a gap assessment is a technique used to communicate the differences between the desired and current states of an organization's security structure. It is a frequently applied technique when new regulatory requirements are anticipated. Regulatory compliance can be understood as the desired state, the current state is revealed through the maturity assessment, and gaps between the two are uncovered through the gap assessment. Applied more broadly, a gap assessment can compare management's ideal security capability in relation to the maturity assessment. These inputs are elemental in forming a realistic information security strategy that aligns with management's desired goals. When conducted annually, improvement and trends in maturity assessment scores can be tracked.

In the second article of this series, I will delve into the components of conducting a thorough security assessment based on the initial findings unearthed during maturity assessments and gap assessments. A security assessment identifies the risks to organizational assets based on recognized threats and vulnerabilities. These assessments comprise technical, administrative, and physical considerations. It should be noted that this part of the testing also pays attention to human vulnerabilities in addition to an organization's technical vulnerabilities. Security assessments are then followed by security auditing, technical vulnerability scanning, and penetration testing, the least critical aspect of establishing a strong security posture in your organization. ✳

Mark Lanterman *(mlanterman@compforensics.com) is Chief Technology Officer of Computer Forensic Services. A former member of the U.S. Secret Service Electronic Crimes Task Force, Mark has 28 years of security and forensic experience and has testified in more than 2,000 cases.*

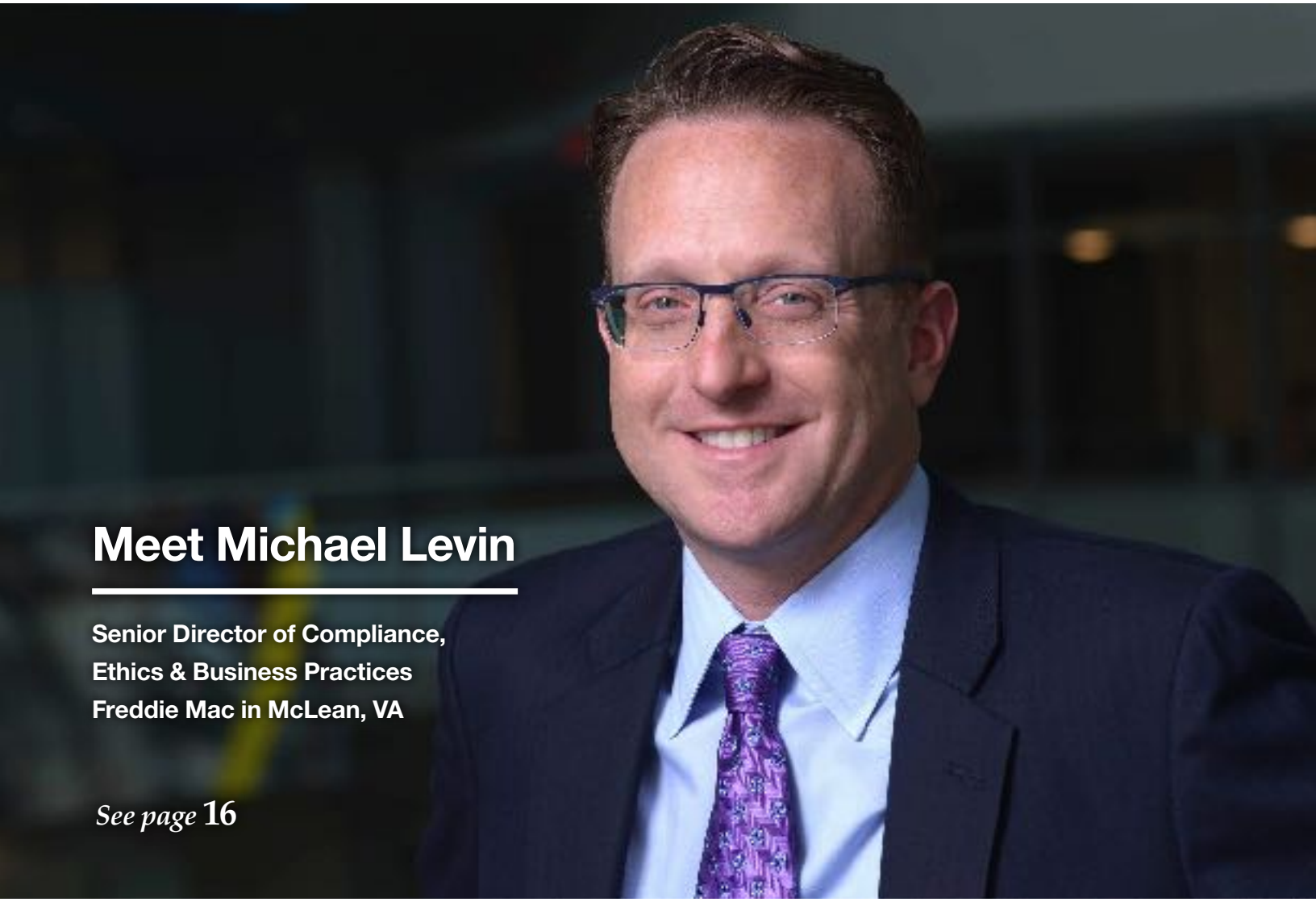
Compliance & Ethics Professional®

December 2017

SCCE

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org



Meet Michael Levin

Senior Director of Compliance, Ethics & Business Practices
Freddie Mac in McLean, VA

See page **16**

By Mark Lanterman

The components of strong cybersecurity plans, Part 2: Security assessment

» Maturity assessments lay the groundwork for cybersecurity programs and allow management to establish desired improvement in comparison to current capabilities.

» A security assessment helps establish security governance by providing an independent check on information technology staff, increased awareness of security risks and threats, and prioritization of IT spending for the purposes of risk mitigation.

» A security audit focuses on the completeness, design, implementation, and efficacy of internal security controls.

» Vulnerability scanning is an ongoing process in an organization that is both offensive and defensive depending on its use.

» Ultimately, a penetration test is only a fraction of developing a strong cybersecurity plan. However, these tests are frequently needed for compliance with regulations that set the minimum requirements for cybersecurity programs.

Part 1 of this article appeared in the November 2017 issue of Compliance & Ethics Professional.

In the first article of this series, I described the role of maturity assessment as a part of a robust security program. Following a maturity assessment, which defines how capably management desires a program to operate, a security assessment identifies the risks to organizational assets, based on particular threats and vulnerabilities. This test serves to determine the probability of a threat being realized, assesses current controls, and calculates the residual risk that still exists in spite of these controls. Security assessments are a subset of an organization's overall risk management practice.

Lanterman

Following a maturity assessment that defines management desires and expectations and a gap assessment that communicates the differences between an organization's current and desired security posture, a security assessment helps establish security governance by providing an independent check on information technology staff, increased awareness of security risks and threats, and prioritization of IT spending for the purposes of risk mitigation. It also provides the basis for a comparative annual analysis of an organization's security program.

At this point, it may be surprising to think that penetration testing is separate from the security assessment phase of developing a strong cybersecurity policy. The security assessment is a preliminary step that ideally occurs before a penetration test, as the likelihood

of threats and risks are developed at this stage. The impact and calculation of residual risk in addition to the identification of mitigation activities also occurs during the security assessment.

The first step in a security risk assessment is to identify prioritized assets. Cybersecurity resources should be devoted to the assets that would cause the most damage to an organization if they were to be compromised. Examples include intellectual property, customer lists, servers, applications, and physical location.

The second step is to identify potential threats to the assets. A threat is simply an undesirable event aimed at an asset or group of assets that could result in loss, improper disclosure, or damage. While a denial of service, malicious code, and disclosure/exfiltration of data are examples of cybersecurity threats, fraud errors and sabotage are additional threats to a company's IT assets that are physically based.

A threat to an organization is only successful if a vulnerability is exploited, either because of a flaw in an existing control or because no control was implemented. With this in mind, it should be noted that threats do not cease to exist when faced with strong cybersecurity protocols. While threats associated with our technological world do not necessarily diminish, an organization's ability to cope with them and reduce risk increases with levels of security strength.

A threat to an organization is only successful if a vulnerability is exploited, either because of a flaw in an existing control or because no control was implemented.

Vulnerabilities, like controls, can be administrative, physical, or technical in nature. Administrative vulnerabilities relate to design flaws in policies or procedures. Physical vulnerabilities are deficiencies in personnel, location, or utilities and include flaws in awareness training, background checks, or lack of electrical backup, among others. Technical vulnerabilities are weaknesses in the logical controls, such as flaws in application or operating system code or password misconfigurations.

Risk is the loss to assets that results if a threat is successful. This is the core concept of any security program, the crux upon which all security activities and goals rest. Controls, also known as safeguards, are the activities and techniques employed by organizations to reduce risk. (A discussion of the relationship between risk and controls will be further covered in the third article of this series.)

To complete a security assessment, an assessor will conduct interviews with relevant stakeholders. As threats, risks, and their impacts become more complex, it is important that an assessor collects information beyond the IT department. Everyone has a role to play in effective cybersecurity practices. Documentation regarding an organization's administrative, physical, and technical controls is imperative to develop an understanding of potential risks and threats and their impact on an organization. Remember identifying possible consequences is

especially difficult since the risks are multi-faceted and may include damage to an organization's finances, reputation, compliance, and operations.

Frameworks that are typically leveraged for a security risk assessment include the National Institute of Standards and Technology's Special Publication 800-30, *Guide for Conducting Risk Assessment*; International Standards Organization's 27001/2; and ASIS International's *General Security Risk Assessment Guideline*.

The above resources provide guidance for many parts of the security risk assessment process, including the calculation of risk. Calculating risk is usually a hybrid of quantitative and qualitative measures. While quantitative measures are more desirable due to their objectivity, in practice, risk is usually presented in quantifiable measure, such as dollars lost, as well as qualitative high, medium, and low assessments. Residual risk represents the risk between the general risk and the controls implemented. Residual risk is low when sufficient controls are implemented and high when there are insufficient controls.

An assessor will document all the threats, vulnerabilities, and risks identified during the review in a report. The report will also include the assessment of risk, its likelihood and impact, consideration of controls, and recommendations for improved security and risk mitigation.

A security risk assessment helps establish security governance, provides an independent check on IT staff, and increases awareness of security risk and threats. Combining the maturity assessment and security risk assessment allows an organization to prioritize IT spending by investing resources in implementing safeguards that improve the capability of key areas as well as reducing the greatest risks to the organization.

A security risk assessment helps establish security governance, provides an independent check on IT staff, and increases awareness of security risk and threats.

Unlike a maturity assessment, the results of a security assessment are primarily qualitative. At this stage, a security assessor will deliver a comprehensive report documenting evidentiary records and will also provide an organization with recommendations for improved security, strengthened controls, mitigation activities, and resolving problems identified during the gap assessment.

In my next article, I will describe a third component of developing a strong cybersecurity protocol: security auditing. Security auditing moves beyond the results of a security assessment to improve upon existing mitigation controls and concludes on their effectiveness over a particular period of time. ✳

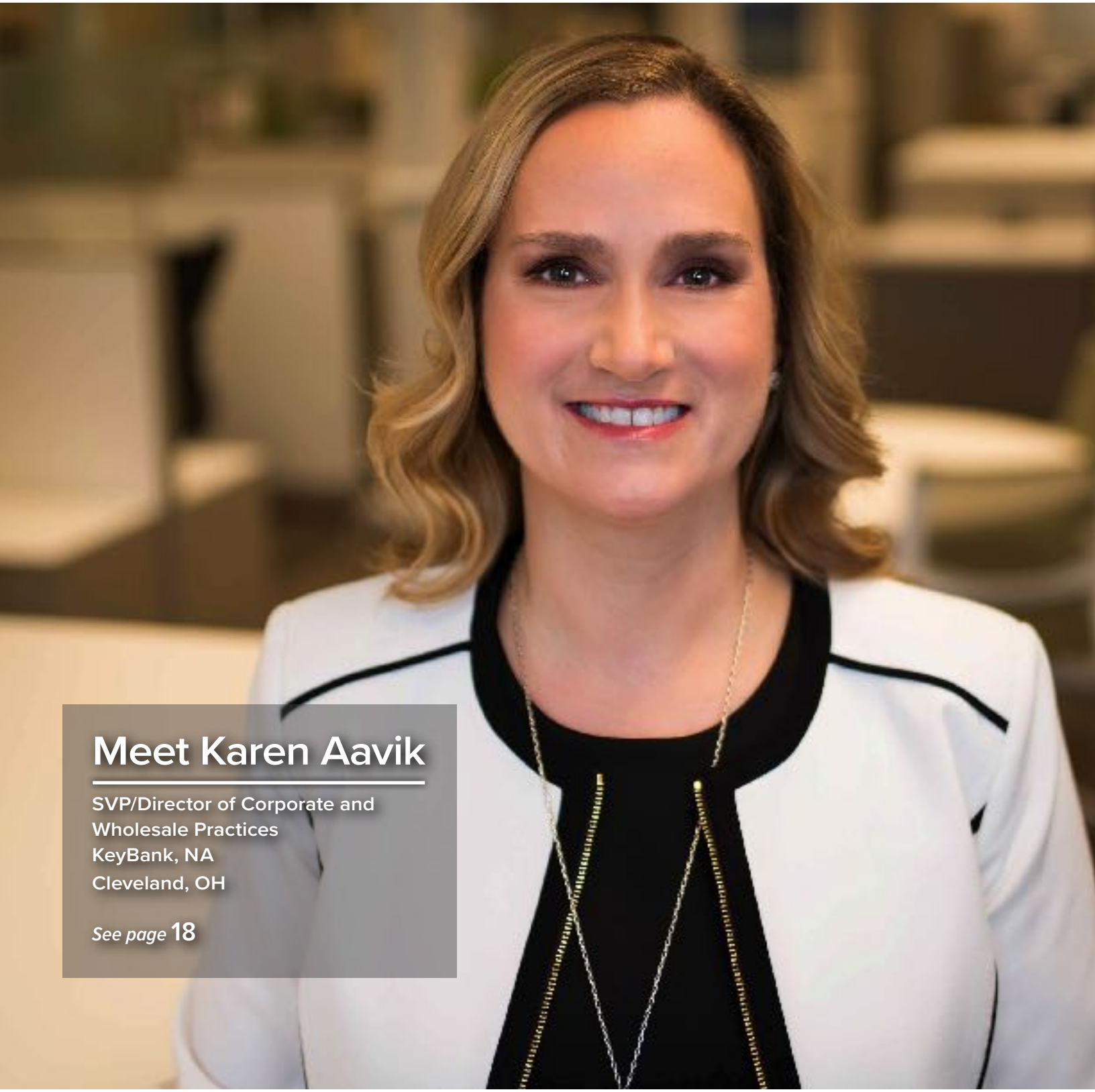
Mark Lanterman *(mlanterman@compforensics.com) is Chief Technology Officer at Computer Forensic Services, Inc. in Minnetonka, MN*

SCCE
corporatecompliance.org

Compliance & Ethics PROFESSIONAL

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

JANUARY 2018



Meet Karen Aavik

SVP/Director of Corporate and Wholesale Practices
KeyBank, NA
Cleveland, OH

See page 18

By Mark Lanterman

The components of strong cybersecurity plans, Part 3: Security auditing

» Maturity assessments lay the groundwork for cybersecurity programs and allow management to establish desired improvement in comparison to current capabilities.

» A security assessment helps establish security governance by providing an independent check on information technology staff, increased awareness of security risks and threats, and prioritization of IT spending for the purposes of risk mitigation.

» A security audit focuses on the completeness, design, implementation, and efficacy of internal security controls.

» Vulnerability scanning is an ongoing process in an organization that is both offensive and defensive depending on its use.

» Ultimately, a penetration test is only a fraction of developing a strong cybersecurity plan. However, these tests are frequently needed for compliance with regulations that set the minimum requirements for cybersecurity programs.

Part 2 of this article appeared in the December 2017 issue of Compliance & Ethics Professional.

In the last two articles of this series, I discussed the role of maturity assessment and security assessment as connected though distinct aspects of a strong security program. This article will delve into a third and comparatively more in-depth component. Security auditing builds upon the information collected as a result of the security assessment portion in order to come to conclusions about the efficiency of an organization's internal controls.

Lanterman

A security audit focuses on the completeness, design, implementation, and efficacy of internal security controls. Although controls are identified during the security assessment to mitigate identified risks, a security assessment provides only a rudimentary evaluation of the control design. Perhaps more importantly, a security assessment is conducted under the assumption that the controls are effective in mitigating risks. Conversely, a security audit will delve much deeper into how a particular control is designed and how it is implemented over a period of review. Periods of review are decided by management based on the amount of assurance desired that a control is operating as expected. This period typically lasts 12 months but can ultimately be any length of time depending upon the needs of the organization.

Security audits can vary widely in their scope and rigor. Although some controls are identified during the security risk assessment, security auditing is another method of independently reviewing the

completeness and accuracy of the risks and controls. Controls have many different potential categorizations to identify potential vulnerabilities in their design and implementation.

A typical categorization is preventive or detective. Preventive controls prevent a risk from occurring. For example, to prevent damage to a server, the organization may secure the data center with a key card lock and restrict access to appropriate personnel. A detective control detects that either a preventive control failed or that a risk materialized. In the previous example, a detective control may be a review of the access log to the data center to detect that access was improperly granted to an unauthorized individual. As identified in the second article of this series, controls can be categorized as administrative, physical, or technical. Administrative controls are typically process-oriented and relate to the establishment of policies and procedures. Physical controls can relate to people, locations, or utilities, whereas technical controls relate to logical controls.

Categorizing controls is important to support a common security principle: Defense in depth. This principle ensures that there are appropriate layers of controls so that if some fail, others will still be there to further reduce the risk. A risk should generally have a preventive and a detective control. Although preventing a risk from occurring at all is preferred, it is not always feasible. Combining a control to detect any failures of the upstream process is advisable. Having a mixture of administrative, physical, and technical controls over a key risk area is recommended. This security principle aptly illustrates that no security program is perfect. In consideration of evolving risks and vulnerabilities, organizations should account for possible deficiencies in even the strongest controls.

Categorizing controls is important to support a common security principle: Defense in depth.

Typical frameworks for generalized security audits include the Center for Internet Security's Critical Security Controls, the National Institute of Standards and Technology's (NIST) Special Publication 800-53, *Security and Privacy Controls for Federal Information Systems*, and ISACA's Control Objectives for Information Technology (COBIT) 5. When evaluating technical controls on a specific system, particularly for baselining the expected configurations, the Defense Information Systems' Security Technical Information Guide (STIG) and the Center for Internet Security's Secure Baselines provide significant guidance.

Controls are tested through observing the individuals responsible for performing a control, reviewing documentation to evidence that a control was performed, and interviewing key people responsible for the design, execution, and review of controls and independent testing. In independent testing, an auditor will obtain data and perform the control to determine if the same result was obtained by the control performer. For areas of risk that may have inadequate controls, an auditor may produce evidence that a risk materialized and its extent.

Security audits are the most objective of the security components that have been discussed in the first three articles of this

five-part series. By concluding on the adequacy and operational effectiveness of controls, it provides feedback to the maturity assessment and the risk assessments. Is the organization more or less mature based on the recommendations in the audit? Were any threats, vulnerabilities, or controls overlooked in the security risk assessment? Were controls operating as expected to prevent a risk, or does more residual risk exist than was previously identified?

Similar to maturity and security assessments, security auditing could be described as a defensive measure designed to test the strength of internal controls that prevent recognized threats in addition to minimizing residual risk. In the next part of this series, I will describe the role of yet another defensive measure. Technical vulnerability scanning is an essential, though often overlooked, technique used to develop a strong security plan. This technique is incorporated into the three previous overarching components and is utilized routinely for organizations to remain aware of potential problems in their security infrastructure. This defensive measure is a crucial aspect of the final offensive security measure: penetration testing.

Mark Lanterman *(mlanterman@compforensics.com) is Chief Technology Officer at Computer Forensic Services, Inc., in Minnetonka, MN.*

Don't forget to earn your CCB CEUs for this issue

Complete the *Compliance & Ethics Professional* CEU quiz for the articles below from this issue:

- **A three-year mapping effort: Focus on compliance** by Charlotte D. Young (page 31)
- **Defining, mitigating, and reducing harassment in the workplace** by Julia Méndez (page 43)
- **Key compliance concerns for 2018** by Mónica Ramírez Chimal (page 63)

To complete the quiz:

Visit **corporatecompliance.org/quiz**, log in with your username and password, select a quiz, and answer the questions. The online quiz is self-scoring and you will see your results immediately.

You may also fax or mail the completed quiz to CCB:

FAX: +1 952 988 0146

MAIL: Compliance Certification Board
6500 Barrie Road, Suite 250
Minneapolis, MN 55435, United States

Questions? Call CCB at +1 952 933 4977 or 888 277 4977

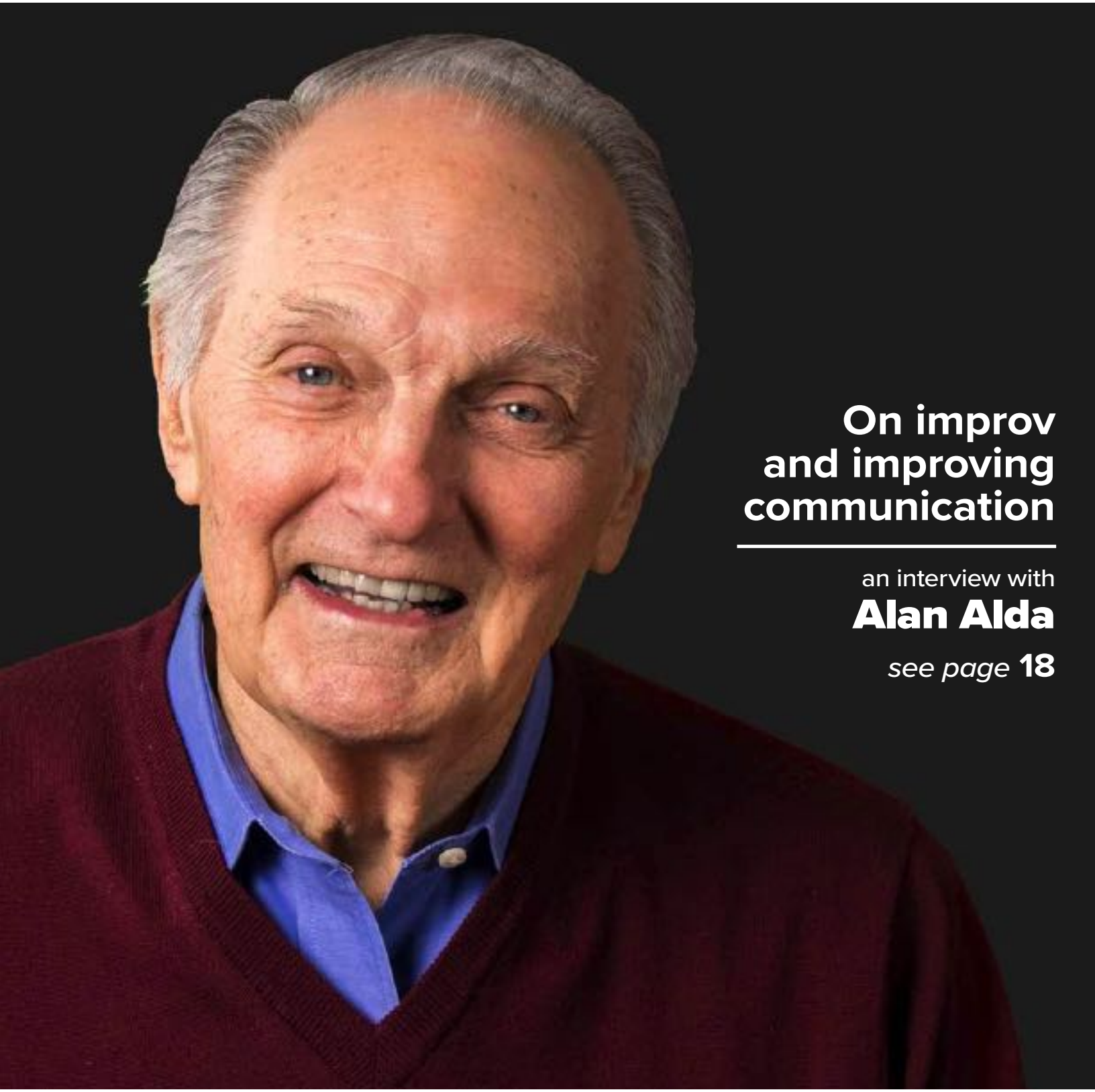
To receive 1.0 non-live Compliance Certification Board (CCB) CEU for the quiz, at least three questions must be answered correctly. Only the first attempt at each quiz will be accepted. *Compliance & Ethics Professional* quizzes are valid for 12 months, beginning on the first day of the month of issue. Quizzes received after the expiration date indicated on the quiz will not be accepted.

SCCE
corporatecompliance.org

Compliance & Ethics PROFESSIONAL®

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

MARCH 2018



On improv and improving communication

an interview with
Alan Alda

see page **18**

by Mark Lanterman

The components of strong cybersecurity plans, Part 4: Technical vulnerability scanning

» Maturity assessments lay the groundwork for cybersecurity programs and allow management to establish desired improvement in comparison to current capabilities.

» A security assessment helps establish security governance by providing an independent check on information technology staff, increased awareness of security risks and threats, prioritization of IT spending for the purposes of risk mitigation.

» A security audit focuses on the completeness, design, implementation, and efficacy of internal security controls.

» Vulnerability scanning is an ongoing process in an organization that is both offensive and defensive depending on its use.

» Ultimately, a penetration test is only a fraction of developing a strong cybersecurity plan. However, these tests are frequently needed for compliance with regulations that set the minimum requirements for cybersecurity programs.

Mark Lanterman *(mlanterman@compforensics.com) is Chief Technology Officer at Computer Forensic Services Inc. in Minnetonka, MN.*

Part 3 of this article appeared in the January 2018 issue of **Compliance & Ethics Professional.**

Lanterman

As discussed in my previous three articles, strong security programs comprise both defensive and offensive measures. Maturity assessments, security assessments, security auditing, and technical vulnerability scanning are all defensive measures. However, since vulnerability scanners are often used by cybercriminals in an effort to find and exploit vulnerabilities, technical vulnerability scanning is both offensive and defensive.

A vulnerability scan is a security activity in which tools scan a particular device in order to identify flaws in operating systems and applications, misconfigured settings, and insecure ports and services. Vulnerability scanning is unique, because it is not an overall component of security programs, such as maturity assessments, security risk assessment, or security auditing. Rather, it is a technique that is leveraged by the other components. Security risk assessments use vulnerability scans to identify technical vulnerabilities in organizational assets. Automated scans identify the risk impact of the vulnerability on the asset as critical, high, medium, and low so that critical vulnerabilities can be mitigated on critical assets first.

Security audits look at vulnerability scanning from two perspectives: One as a control and one as a method of testing. Vulnerability scanning should be routine, because any one scan is only indicative of security strength for that moment in time. Security auditors also use vulnerability scans to independently test for the existence of certain vulnerabilities, to confirm certain

configuration settings, or to remediate testing. Finally, vulnerability scanning is a key technique for penetration testers to identify the weaknesses that they wish to exploit.

Routine vulnerability is an easy, cost-efficient, and important control to manage vulnerabilities. Instead of a cyber criminal finding the vulnerabilities, organizations should implement the necessary tools to find these vulnerabilities first and remedy them. The Center for Internet Security (CIS) Critical Security Controls rank vulnerability scans as the fourth most critical control.

Vulnerability scanning is an ongoing process that is both offensive and defensive depending on its use. In the context of strong security protocols, it should be used offensively to establish strong penetration test results, and defensively to identify and manage technical vulnerabilities before an outside perpetrator exploits them. By establishing baselines, identifying risks and threats, determining the strength of internal controls, and testing for vulnerabilities in technical infrastructure, an organization is well-equipped to develop sound plans for avoiding vulnerabilities and defensively acting against threats.

The fifth and final article of this series will describe the process and use of penetration testing as a component of a strong cybersecurity plan. The most requested security activity, penetration testing offers the most valuable results when conducted in relation to the other components and techniques. ✳

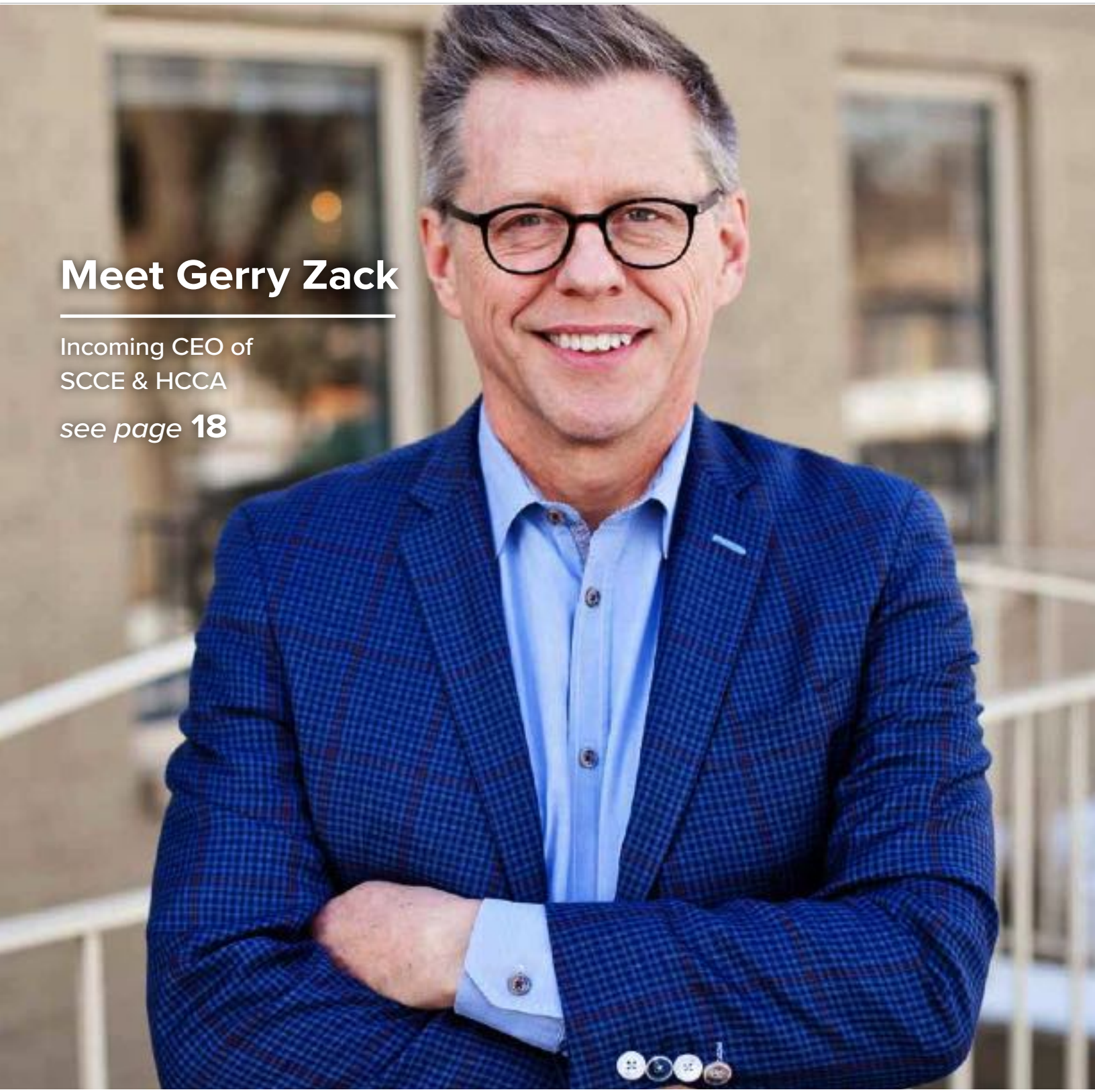
1. CIS Controls: Download the First Five CIS Controls Guide. Available at http://bit.ly/2DplvDK

SCCE
corporatecompliance.org

Compliance & Ethics PROFESSIONAL®

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

APRIL 2018



Meet Gerry Zack

Incoming CEO of SCCE & HCCA

see page **18**

by Mark Lanterman

The components of strong cybersecurity plans, Part 5: Penetration testing

» Maturity assessments lay the groundwork for cybersecurity programs and allow management to establish desired improvement in comparison to current capabilities.

» A security assessment helps establish security governance by providing an independent check on information technology staff, increased awareness of security risks and threats, and prioritization of IT spending for the purposes of risk mitigation.

» A security audit focuses on the completeness, design, implementation, and efficacy of internal security controls.

» Vulnerability scanning is an ongoing process in an organization that is both offensive and defensive, depending on its use.

» Ultimately, a penetration test is only a fraction of developing a strong cybersecurity plan. However, these tests are frequently needed for compliance with regulations that set the minimum requirements for cybersecurity programs.

Mark Lanterman *(mlanterman@compforensics.com) is Chief Technology Officer at Computer Forensic Services Inc. in Minnetonka, MN.*

Part 4 of this article appeared in the March 2018 issue of **Compliance & Ethics Professional.**

In the fifth and final installment of this cybersecurity series, I will discuss the role of penetration testing in developing a strong security program. As described in my previous four articles, a growing awareness of cybersecurity regulations, trends, and threats has led many organizations to request a penetration test of their technical infrastructure—without really knowing what that means, what its purpose is, and what degree of assurance it really offers.

Lanterman

Asking the right questions

When I ask a customer if they have already conducted a security assessment, know their controls, have implemented regular vulnerability scanning, and have security auditing procedures in place, they usually respond with, "That's what we're asking for. We want a penetration test." In this way, penetration testing and all the other components of cybersecurity plans have become synonymous terms. This conflation is especially prevalent in small to medium-sized firms. However, each component is separate and distinct within a mature security program, all components serve different purposes—leveraging different methodologies, providing different levels of assurance and benefits, requiring different skills from the assessor, providing different deliverables—and each component performs at different stages of a security program's development. In order to reap the most benefit from a penetration test, the organization should be able to answer the following five questions based on the previous maturity assessment, security risk assessment, and security audits:

1. Do we know what is connected to our systems and networks at all times?

2. Do we know what software is running, or trying to run, on our systems and networks?
3. Are we continuously managing our systems using "known good" configurations?
4. Are we continuously looking for, and managing, "known bad" software?
5. Do we limit and track the people who have the administrative privileges to change, bypass, or override our security settings?

A penetration test is an attempt to defeat boundary defenses and gain access to an organization's internal network by exploiting vulnerabilities. This test is used to determine whether an unmitigated risk exists. In this sense, it tests whether an outside attacker could bypass perimeter controls, gain access to the internal network, and establish command and control capabilities. Many techniques can be employed during a penetration test, including vulnerability scanning and social engineering attacks.

Social engineering attacks are targeted at exploiting the human vulnerabilities in an organization. Spear phishing emails, unauthorized issuing of credentials, and taking advantage of physical vulnerabilities can all be examples of ways in which an assessor will use social engineering during a penetration test.

Assessing vulnerability

If a security assessor is unable to stage a successful penetration test, this confirms that, taken as a whole, internal controls are operating effectively to externally protect the organization from threats. With these results, management may mistakenly assume that the organization is secure. However, unlike broader security audits, a penetration test provides limited assurance to a specific point in time. Depending on the timeline, results could vary substantially. A penetration test conducted one day could fail to reveal serious vulnerabilities that appear the next day. Risk levels are always changing, which is part of why a complete understanding achieved through maturity assessments, security assessments, security auditing, and regular vulnerability scanning is so critical. Penetration testing provides only a glimpse of an organization's overall security posture.

Ultimately, a penetration test is only a fraction of a strong cybersecurity plan. However, the fact remains that it is very important, and these tests are frequently required for compliance with regulations. A penetration test's objective is essentially to circumvent security controls, providing a different perspective than other security audit measures. Therefore, penetration testing may uncover issues that a traditional security audit or assessment may not.

A penetration test conducted one day could fail to reveal serious vulnerabilities that appear the next day.

Conclusion

Complete security plans incorporate a number of factors, all of which are important in establishing a strong cybersecurity posture. Each stage and technique of the process ought to be regularly conducted in order to provide baselines and comparisons for improvement. But it should be noted that, in spite of an organization's best efforts, no security policy is perfect. Given the constantly changing nature of technology and its inherent risks, security policies have to evolve to meet the demands of our digital landscape. ✳