feature

Planning for Information Security Testing—A Practical Approach

Once approval to perform an information security audit and, most likely, a penetration test (pen-test) of an organization's networks and systems has been obtained, then what? Where to start? Planning it requires a great deal of thought and consideration and, for first timers, this task can be quite daunting. Poor planning can have serious consequences for the network, causing unwanted business disruption and, in the worst-case scenario, permanent harm. Depending on the risk appetite of the organization, the scope of the pen-test could be drastically different.

The first thing one needs to understand is that information security auditing is not a one-size-fits-all type of engagement. It is reasonable to start small and slowly progress to more complex engagements. It is also important to note that different networks and applications can progress in different stages.

For example, if an organization has a supervisory control and data acquisition (SCADA) system that has never been tested, nor even scanned for vulnerabilities, one might want to consider not starting the information security testing by deploying a full-blown pen-test. It would be prudent to start with a vulnerability assessment to test the waters and use the results to harden the system for a future pen-test.

The model in **figure 1** proposes a guideline for maturing testing activities by correlating different combinations of the "rules of engagement," which will be covered in detail in this article, with risk tolerance. These preset combinations can be used as a starting point.

Before considering the rules of engagement, it is important to know the types of information security testing:

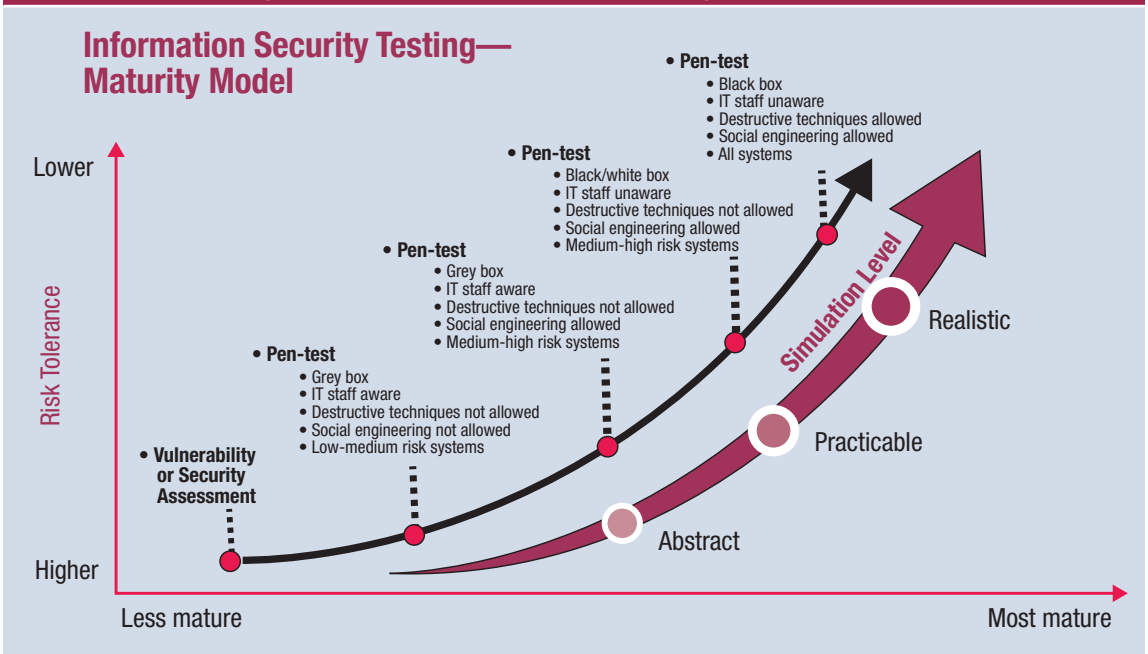
- **Vulnerability scan**—This scan examines the security of individual computers, network devices or applications for known vulnerabilities. Vulnerabilities are identified by running a scanner, sniffers, reviewing configurations, etc. Vulnerabilities identified are never exploited. This test tends to be less disruptive and also inexpensive when outsourced.
- **Security assessment**—This builds upon the vulnerability assessment by adding manual verification of controls to confirm exposure by reviewing settings, policies and procedures. It has a broader coverage. Assessment of physical security safeguards would be covered here.
- **Penetration test**—This happens one step ahead of a vulnerability assessment. It takes advantage of the known and unknown (e.g., zero-day attacks) vulnerabilities. It also makes use of social engineering techniques to exploit the human component of cybersecurity. Note that vulnerability assessment is included in pen-testing. Vulnerability assessment is the starting activity that would be scheduled to look for vulnerabilities. It is called the discovery phase (or reconnaissance) of the test cycle. Penetration testers must run a vulnerability scan to identify weak points to be exploited.
- **Social engineering**—Although social engineering is actually a pen-test technique, many companies not yet ready for a pen-test might opt to only deploy a phishing email campaign, for example, to verify how many of their users are vulnerable to this technique and require further training. Results

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA web site *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

Karina Korpela, CISA, CISM, CRISC, CISSP, PMP
Is the IT audit manager at AltaLink, a Berkshire Hathaway Energy Company and Alberta, Canada's largest transmission provider. Korpela has more than 15 years of international experience with IT audits, cybersecurity assessments, performing data analytics and developing continuous controls monitoring applications for many different business processes. She began her career at Coopers & Lybrand as a system administrator and she was later invited to join its Computer Audit Assistance Group (CAAG) as an IT auditor. She can be reached at *karina.korpela@altalink.ca.*

Paul Weatherhead, CISSP
Is the vice president and chief technology officer at Digital Boundary Group, an information technology security assurance services firm serving clients throughout North America. He is frequently called upon to advise North American clients in the financial services, law enforcement, municipal and provincial government, utilities, and professional services sectors on corporate IT security and network intrusion investigations. Over the past 17 years, Weatherhead has focused on network security and threat management consulting, having performed more than 400 IT security assessments in Canada, the United States and the United Kingdom. He regularly conducts network security training courses and has instructed at the Canadian Police College.

Figure 1—Information Security Testing Maturity Model



Source: K. Korpela. Reprinted with permission.

are reported, but information gathered is never used to penetrate the network.

> **"Ideally, pen-tests can be run just once a year while vulnerability assessments should be performed more frequently."**

An assessment is not better than a pen-test or *vice versa*. They provide different outcomes and value. Their applicability will depend on the organization's risk tolerance, systems' sensitivity and the security infrastructure maturity. But, ideally, pen-tests can be run just once a year while vulnerability assessments should be performed more frequently. Both the vulnerability scan and pen-tests can be performed against the internal and external systems and network devices. They both can be general in scope or focused on specific areas. **Figure 2** shows areas of focus and their applicability.

Rules of Engagement

These rules should be thought of as the sound adjustment knobs in a home theater system. One combination might be better for a smaller room in which cable TV is being watched, while another combination might be better for a bigger room where a DVD is being played. Once these rules are understood, it gets easier to decide the objectives and scope for testing.

A different set of combinations can be applied to each system within the scope. In one highly sensitive network, one may only run a vulnerability scan and in other, more robust networks, one might run a more realistic pen-test. Or, the sound can be tuned as the

Figure 2—Focus Areas				
Focus Areas/Types	Vulnerability Scan	Security Assessment	Pen-test	Social Engineering
Routers and switches	I	I	I	-
Firewall	I	I	I	I
Intrusion detection system (IDS); intrusion prevention system (IPS)	I	I	I	I
Wireless network	I	I	I	-
Denial of service (DoS)	0	0	0	-
Password cracking	-	0	I	-
Social engineering	-	0	I	I
Stolen mobile devices	-	I	I	-
Application	I	I	I	-
Physical	I	I	I	I
Database	I	I	I	-
Voice Over Internet Protocol (VoIP)	0	I	I	-
Virtual private network (VPN)	I	I	I	-
Email security	I	I	I	I
Security patches	I	I	I	-
Data leakage	-	I	I	I
Telecommunication and broadband communication	I	I	I	-
I = Included | 0 = Optional | - = Generally not included				

Source: K. Korpela and P. Weatherhead. Reprinted with permission.

testing occurs. For example, when the tester does not succeed in penetrating the first line of defense, the test can be considered completed or additional information, or even access, can be provided to enable the tester to bypass it and restart testing from there. In this way, additional vulnerabilities can be identified should a future attacker manage to breach the first level of defense.

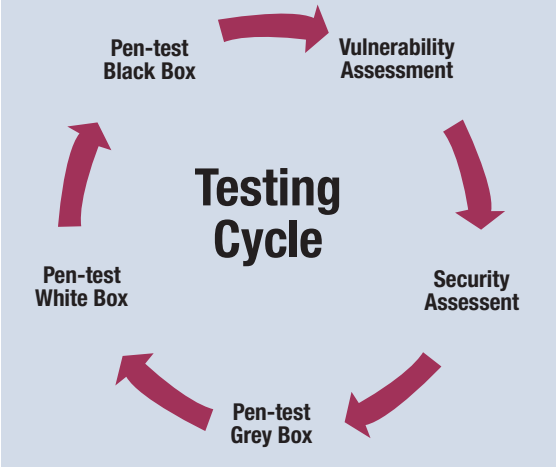
The combination chosen depends on the risk tolerance and the maturity of a company's cybersecurity processes. Nevertheless, these rules allow for flexibility in adjusting the test plan according to the systems and networks in scope.

It is important to keep in mind that in the always-evolving world of information security, reaching the highest maturity level and, as a consequence, becoming complacent can be dangerous.

Even though a higher maturity level is required to perform the most realistic testing, it comes with a price as it can give a false sense of security. A full-blown black box allows the tester to assess only the first line of defense at the time of testing. But what if a zero-day attack that exploits vulnerabilities behind that first line of defense occurs? How would the internal systems respond? Andy Grove's quote on complacency is very much applicable to information security: "Success breeds complacency. Complacency breeds failure. Only the paranoid survive."[1]

It is essential to apply a cyclical approach to information security testing as suggested in **figure 3**.

Figure 3—Testing Cycle



Source: K. Korpela. Reprinted with permission.

Strategy: Internal vs. External

The strategy determines whether testing should be performed from outside of the network such as from the Internet, or from inside the network or both.

> **"Not announcing pen-testing helps the organization to check the security threats that arise due to human errors and ignorance."**

- **External**—This is, perhaps, the most widely-used form of pen-testing. It addresses the ability of a remote attacker to get to the internal network. The goal of the pen-test is to access specific servers and the "crown jewels" within the internal network by exploiting externally exposed servers, clients and people.
- **Internal**—Contrary to what management usually thinks this is, it is not a strategy applicable to vulnerability assessment work only. Pen-tests can be run internally when the goal is to simulate what would happen if a company's own employee attempted to carry out an attack from within or if an attacker managed to gain access to a network. The target is typically the same as external pen-testing, but the major differentiator is the "attacker" either has some sort of authorized access or is starting from a point within the internal network. Internal testing can help businesses identify weaknesses in their second or third lines of defense, as an insider attack will bypass perimeter safeguards altogether. Internal testing can answer questions such as, "How well segregated is the network?" "Is the patching management effective?" If the attacker is in a network segment, internal testing can determine whether he/she can see any other segments, what he/she might see on those other segments, and what activities he/she can carry out.

Announcement: Covert vs. Not Covert

This section of the rules of engagement is used to document whether or not tests will be announced.

- **Not covert**—These pen-tests are those performed with the knowledge and consent of IT staff and, of course, upper management. The next decision is whether to defend the network against testers. This option, also known as the Blue Team vs. Red Team approach, can cut the test short as the defending team could just shut down the network once it has detected the testers. In order to maximize the pen-test, it is recommended that specific instructions be given that no action to stop the testers is to be taken in response to the pen-test at the time and duration arranged. This can be a great opportunity for the defending team to learn how to think like hackers by monitoring the attack and documenting which systems and sensors trigger alerts during the exercise.
- **Covert**—This option is also known as Red Team, and it involves performing a pen-test without the knowledge of IT staff, but with consent from upper management. Not announcing pen-testing helps the organization to check the security threats that

arise due to human errors and ignorance. It also examines the agility of the security infrastructure and the responsiveness of the IT staff.

Type: Grey vs. White vs. Black Box

Organizations must decide whether to share information about the system and networks with the assessing organization (tester). Those decisions are typed as:

- **Black box**—No information is shared with the testers. This simulates an external attack where testers will spend more time in the reconnaissance phase and, because of that, it tends to take more time and be more expensive.
- **Grey box**—Some information is provided to the testers—that which hackers would, perhaps, obtain when using reconnaissance tools or after obtaining access to local area networks (LANs). This decreases the time spent by the testers and, therefore, cost as well. Information given does not compromise the pen-test's validity. Examples of such information would be a list of out-of-scope hosts or a lighter version of network topology.
- **White box**—All information that testers need to exploit vulnerabilities is provided. This option is preferable when:
  - The scoping task is left to the testers to determine
  - A complete audit of its security is taking place
  - Organizations want to simulate an attack from an inside threat, such as a disgruntled IT employee who would already have access to such information

There is no right or wrong type, and all options can be done with or without the knowledge of IT staff. Black box offers a more realistic test from the outside hacker perspective, but white box has the potential to be more devastating because the testers will have the knowledge of what is important within a network and where it is located—something that external attackers do not usually know from the start. An internal attack approach will not always require a white-box type

Figure 4—NDT vs. DT Techniques

Nondestructive Techniques (NDT)	Potentially Destructive/Disruptive Techniques (DT)
• Passive research, including employees' social media accounts • URL spoofing and phishing • Physical/on-site social engineering • Remote/logical social engineering • Read corporate emails • Network mapping and operating system (OS) fingerprinting • Caller identification (ID) and email address spoofing • Network sniffing • **Vulnerability scanning*** • Network monitoring tools • Ping tools • Promiscuous mode detection tools • Cryptography tools • Domain Name System (DNS) tools • IP spoofing • **Port scanners*** • Firewall tools • Man-in-the-middle attacks • File manipulation • Poisoning of file-share networks • Investigation of personnel backgrounds • Scenario analysis	• ICMP flood (Smurf attack, Ping flood and Ping of death) • Teardrop • Application level floods • Distributed, reflected, degradation of service • Unintentional, DoS level II • Blind DoS • Tampering with system logs with the intent of deleting/ disguising trails • DoS attacks • Buffer overflow • Forced reinstall and restart • Brute-force attack • Structured Query Language (SQL) injection

*Vulnerability and port scanners are, by nature, nondestructive if configured appropriately.

Source: K. Korpela and P. Weatherhead. Reprinted with permission.

Enjoying this article?

- **Learn more about, discuss and collaborate on information security management and information security policies and procedures in the Knowledge Center.** *www.isaca.org/knowledgecenter*

of testing. For example, if the objective is to test what a hacker could do if he/she just walked into the company's office and plugged in a computer, then an internal testing strategy with a black-box testing type could be selected.

Technique: Nondestructive vs. Destructive

It is import to inform the testers which techniques will be allowed during the engagement. When nondestructive (NDT) methods are selected, testers will set up their tools to avoid causing a denial-of-service (DoS), for example, or any other attack that could disrupt normal business operations. NDT provides a proof of concept, but does not prove it. **Figure 4** lists commonly used techniques. These techniques should be discussed with the testers in advance when the organization notifies the testers which tests may be used during the engagement. Regardless of the technique selected, it is recommended to explicitly state which tools and techniques will be allowed and which will not. For example, there are attacks and tools that can be destructive by nature, but can be "tuned down" by the tester so that they will not cause a DoS, buffer overflow or any system to shut down.

> **"It is recommended to explicitly state which tools and techniques will be allowed and which will not."**

A very valid point to be addressed here is the use of open source and in-house developed tools by the tester for vulnerability assessments and pen-tests. Both types of software come with risk and benefits.

Open source means that the source code is available to all potential users, and they are free to use, modify and redistribute the source code. Considering that the source code is accessible, testers can often tweak the software, plug exploits and remove unnecessary features. This can improve efficiency, speed and security. The most commonly used open source software for information security testing is Linux Backtrack and Kali, which comes with a large community supporting it and, therefore, developing enhancements and versatile add-ons.

As for in-house developed tools, it is very likely that most experienced testers develop tools themselves to cover the gap between commercial and open source. An example would be the development of a tool to scan the network without locking Structured Query Language (SQL) accounts, which may happen when using a commercial scanner.

The risk of these tools disrupting business or causing a propagation of malware could be controlled by:

- Not allowing installation on the target systems
- Running the tool(s) against nonproduction systems or test systems first
- Ascertaining that the tester acquired open source tools from trusted sites and performed a Secure Hash Algorithm 2 (SHA2) checksum to verify integrity
- Ascertaining that the tester has used a valid software development framework, which could include peer review, for in-house software
- Ascertaining that the tester has appropriately patched and upgraded software

And for social engineering techniques such as Caller ID and email address spoofing, one may choose to allow it to be deployed passively, that is, only for the purpose of gathering information during the reconnaissance phase. Other considerations include whether testers will be allowed to break into the company's premises, break into employees' homes and/or hack employees' social media accounts.

These tools and techniques can be flagged as allowed only with prior consent and can be handled on a case-by-case basis.

Statement of Work

Aside from assigning well-skilled and experienced professionals to perform the test and knowing the rules of engagement, it is also essential that a test plan be developed to establish the parameters such as objective, scope, assumptions and risk.

Using a template as shown in **figure 5** provides the tester with clear expectations for the testing and transparency and outlines the plan in a nontechnical way in order for upper management to approve it.

Background

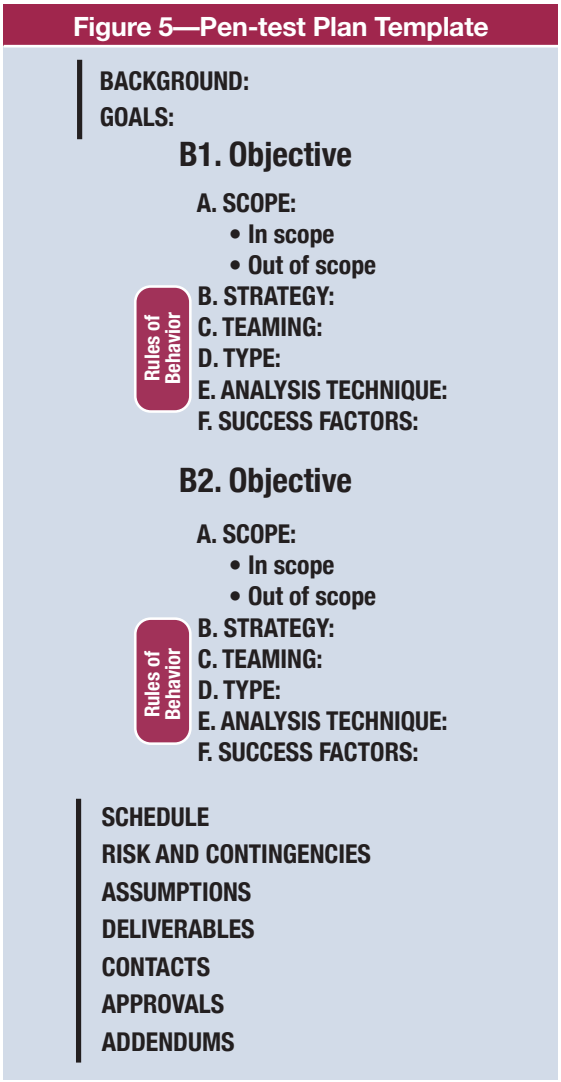
When developing the test, it is critical to keep in mind that it will require approval from upper management (senior executive level is preferable) and, therefore, the background should provide them with context by detailing the need for performing this type of work, a summary of previous tests, the rationale for the objective and scope selected, changes made to the IT environment, new threats, and so on. Here is where the justification for using a third-party assessing organization could be provided.

Goals

What will be the area of focus (refer to **figure 2**) for the test? Or, will it be general? Is there a particular threat against which the company needs to test its controls? For example, an organization may choose to test against one particular vulnerability such as the Heartbleed bug, or it may choose to test if it is possible for hackers or a disgruntled employee to obtain unauthorized access to the enterprise resource planning (ERP) systems and wire money to an off-shore bank account. But for most companies, good starting goals could simply be: Is the organization secure? Is the organization compliant?

To ensure that the testing adds value to the organization, it is crucial to identify and understand the areas of risk and/or the potential weakest link in fending off cyberattacks. Risk assessment frameworks can be helpful in identifying the goals for testing. Organizations that have performed a business impact analysis could use this as input into identifying specific areas of business risk and adjusting the testing accordingly. For example, an organization that identifies research and development data as its most important assets could develop a test plan that includes attempts to gain unauthorized access to the data. Organizations may wish to involve the third-party testers in this phase, as they may be able to suggest current industry trends.

Figure 5—Pen-test Plan Template



Source: K. Korpela and P. Weatherhead. Reprinted with permission.

Objective

It is advisable to provide testers with specific objectives. What should testers do once they obtain access to the network? Should they leave crumbs? Should testers find a specific application and create user accounts? Those objectives will become clear and easy to define as the organization gets familiar with its systems and cyberrisk. A good place to start is to define objectives related to the first and/or second lines of defense such as firewalls.

Scope/Out of Scope

The testing criteria can be either a full-scale test for the entire network and systems or a more narrowly defined test for target devices such as web servers, routers, SCADA, firewalls, DNS servers, mail servers and file transfer protocol (FTP) servers as listed in **figure 2**. To determine the extent to which the testing should be done, these questions should be asked:

- What will be tested?
- In the case of social engineering only, which employees are in scope?
- From where it will be tested?
- When should the test not be performed?
- Are production systems out of scope?
- Which hosts are out of scope/restricted?
- By whom will it be tested?

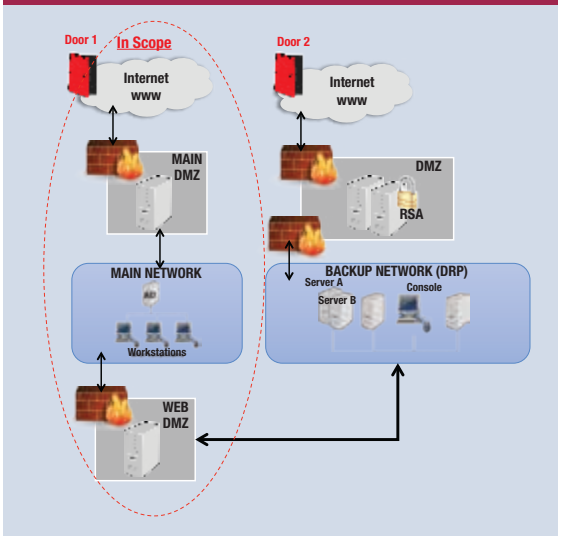
Most assessing organizations will use the number of hosts, users, external IPs and locations in scope to calculate the engagement's cost.

It is helpful to have a nontechnical diagram that shows the networks in scope and testing starting points (doors) (**figure 6**). It will provide upper management with additional context and visual understanding of the scope.

Success Factors

When will the test be considered a success? Is it when the tester breaks into the network or when a breach is not possible? Is penetrating the network enough proof of the need for stiffening controls?

Figure 6—Example of Nontechnical Network Diagram



Source: K. Korpela and P. Weatherhead. Reprinted with permission.

The measurements defined in the Goals section of this article could be repeated here to determine, in detail, which activities must be performed by the assessing organization or even by the IT staff to consider the test successful.

Schedule

If the issue of timing is not resolved properly, it can be catastrophic to an organization. It is easy to imagine the uproar if a DoS test was performed on a university on the day its students are scheduled to take their online examinations. This is an example of poor timing as well as lack of communication between the penetration testers and the university. Good planning and preparation will help avoid such bad practices.

A pen-test does not last forever and, therefore, it is important to be explicit in the plan of a finite period for testing. The plan should also request that testers notify organization stakeholders when testing has begun on the day it was agreed to commence.

Contacts

A contacts list should be developed to identify all the key people (including their names, roles, email addresses and telephone numbers) participating in the planning, coordination and execution of tests. Those who should be contacted first in case of concerns, changes and emergencies should be clearly identified. The list should not include staff that is not meant to know about the testing; their inclusion might confuse the assessing organization.

Risk and Contingencies

All the possible risk factors and their likelihood of occurring during the test period must be specified. An example of a risk might be that the testing activities may inadvertently shut down the network causing interruption of daily business functionalities. Once risk factors have been listed, a table can be prepared with the preventive controls and mitigation strategies in case the risk materializes (**figure 7**).

Deliverables

It is critical to provide context and background to the results. For example, if the number of vulnerabilities reported has doubled from last year, it is important to add the total number of end points scanned to the results.

Reporting to management must be part of the pen-test engagement. Testers will often put together a detailed and very technical presentation summarizing the test results. Best practice is to have one technical, detailed presentation for the IT team (chief information officer [CIO] and key managers) and a separate, shorter presentation for the executives that summarizes the tests and focuses on business risk impact and mitigation plans. Best practice is to have the executive summary created by internal audit.

> **“Risk assessment frameworks can be helpful in identifying the goals for testing.”**

Examples of deliverables to be considered include:

- A detailed technical report on the vulnerabilities of the system explained in a way that is understandable by senior management. This report should also include, but is not limited to:
  - Outcome of the test in technical risk terms
  - Indication of the skills necessary to exploit the vulnerabilities (script kiddies, worm/virus writers, security researchers, professional hackers or hacktivists)

Figure 7—Example of a Risk and Contingency Plan

Risk	Risk Tolerance	Preventive Controls	Probability (%)	Mitigation Strategy	Residual Risk
Testing activities may inadvertently shut down the network causing interruption of daily business functions.	Medium	Attacks that could cause the network to shut down and hosts that could be sensitive to logical tempering are disclaimed as out of scope.	10%	Invoke the business resumption plan.	Low

Source: K. Korpela and P. Weatherhead. Reprinted with permission.

  - Explanation of false positives
  - Short-term (tactical) recommendations
  - Root-cause, long-term (strategic) recommendations
  - Security improvement action plan
- A report listing the cybersecurity controls (processes and/or technologies) currently in place that are working effectively and their categorization against industry best practices (weak, moderate, strong)
- A report showing the social-engineering methods used and the success rates at the company being assessed

Approvals

Obtaining consent from upper management before conducting a pen-test is vital. Depending upon organizational legal requirements, a separate release and authorization form may be required (in addition to the rules of engagement) that states that the assessing organization will be held harmless and not criminally liable for unintentional interruptions and loss or damage to equipment.

> **"It is critical to provide context and background to the results."**

Other Considerations

It is also recommended that plans explicitly state details regarding the following issues:

- **Scope**—Employees/locations out of scope for social-engineering activities
- **Report sanitization**—There is risk involved in the potential circulation of an unsanitized version of the report that includes the company's IP addresses and other important information. Organizations may want to consider having two versions of the report for different audiences and distribution methods.
- **Distribution method**—Organizations may want to consider using only secure methods to communicate unsanitized plans and other information being provided about the systems and networks.
- **Confidentiality**—The assessing organization must be made to understand that any information or data obtained during the pen-tests will be treated as confidential and will be returned or destroyed accordingly after the tests.

References

EC-Council ECSA, *LPT Courseware Manual*, v4, vol. 2

Scarfone, K.; M. Souppaya; A. Cody; A. Orebaugh; *Technical Guide to Information Security Testing and Assessment*, National Institute of Standards and Technology, NIST Special Publication 800-115, USA, September 2008, *http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf*

Tipton, H. F.; M., Krause; *Information Security Management Handbook, 6th Edition*, CRC Press, USA, 2007

Chan Tuck Wai, "Conducting a Penetration Test on an Organization," SANS Institute InfoSec Reading Room, 2002, *https://www.sans.org/reading-room/whitepapers/auditing/conducting-penetration-test-organization-67*

SANS Institute, "Guidelines for Developing Penetration Rules of Behavior," InfoSec Reading Room, 2001, *https://www.sans.org/reading-room/whitepapers/testing/guidelines-developing-penetration-rules-behavior-259*

SANS Institute, "Security Concerns in Using Open Source Software for Enterprise Requirements," InfoSec Reading Room, 2009, *https://www.sans.org/reading-room/whitepapers/awareness/security-concerns-open-source-software-enterprise-requirements-1305*

Endnotes

1 Grove, A. S.; *Only the Paranoid Survive: How to Exploit the Crisis Points That Challenge Every Company*, Crown Business, USA, 1999