TechTarget | SearchFinancial Security

E-guide

PRO+ Content

# A Step-by-Step Guide to Security Risk Assessments

6 key components of effective information security assessments

## In this e-guide



## In this e-guide:

**Information security assessments can be effective for identifying and fixing issues in your enterprise's policies before someone exploits them.**

**Take the time necessary to properly plan out your information security assessment, ensure the work is completed and see to it that the proper staff members in IT, development, management and elsewhere are made aware of the findings so that the issues can be addressed.**

**In this guide, information security consultant Kevin Beaver reveals 6 key components of effective information security assessments.**

**Make sure all of these areas are being considered and are getting the attention they deserve.**

In this e-guide



# Best practices for an information security assessment

**Kevin Beaver**, Information Security Consultant - Principle Logic, LLC

What is the best way to measure information security risk? The best way is to jump right in and look for specific vulnerabilities in your systems and applications; this is not unlike measuring the health of human beings through magnetic resonance imaging, blood analysis and the like. Some people call these exercises IT security audits. Some call them penetration tests. However, performing an in-depth analysis of an environment is not just comparing policy against how things actually work -- IT security audits -- or only trying to break in and prove a point -- penetration testing -- so I prefer to call these exercises *information security assessments*. They're broader and more meaningful and they help demonstrate where security policies and procedures are failing.

The semantics of security testing can be debated ad nauseam but the ultimate goal is to find and fix the weaknesses before someone exploits them. It's up to security professionals to ensure that the proper steps are taken to see things through, so that the risks identified can be understood, resolved or otherwise accepted as part of the information risk management lifecycle. The following are key components of effective information security assessments. Put politics and ego aside and make sure all of these areas are being considered and are getting the attention they deserve:

## In this e-guide




- **Support**

No good information security assessment program ever got off the ground or succeeded long term without the support of management. It's as simple as that. If leadership is not willing to invest the resources required to take an honest look at their enterprise information systems environment, then everything else will be an uphill battle. Focus on getting -- and keeping -- the right people on board. The onus is not on management, but rather on IT and security staff members and leadership.

## In this e-guide



- **Scope**

This is arguably the most important phase of a solid information security assessment. I've seen countless examples where systems, applications and even entire network environments are excluded from security testing. The reasons are almost always the same: "There's not enough time or money," and "We're not required to test such and such systems." It's okay to fine-tune your scope but you have to make sure all of your critical systems are looked at -- sooner as opposed to later. Eventually, you need to look at your entire environment because all it takes is one seemingly benign system, network segment or security process to put everything in jeopardy. Be sure to consider external systems, internal systems and systems hosted by third parties in the cloud -- including your marketing website. Also, authenticated security testing of both operating systems and web applications is an absolute necessity. Make sure that everything is fair game for testing -- including your people, processes and physical security systems.

- **Testing**

Start with vulnerability scans, sift through the scanner findings, perform manual analysis and see what's vulnerable to attack in the context of your environment and business. At a high level, it's really that simple. This phase should include password cracking, wireless network analysis and especially email phishing. Entire works, such as my book Hacking For Dummies, have been written about this phase of security assessments. The important thing is to look at the enterprise environment from the perspective of a malicious user, see what can be exploited and then demonstrate what can happen so that the issue can be analyzed and, if necessary, resolved.

## In this e-guide



- **Reporting**

A 500-page PDF report from a vulnerability scanner won't cut it. A clear and concise security assessment report that outlines prioritized, common sense findings and recommendations is what's needed. The final report doesn't have to be long. It just needs to cut to the chase and outline specific areas of weakness that need attention from the perspective of a security professional -- again, taking the context of the systems and the business into account. It can incorporate elements of penetration testing and IT security auditing. I'm not fond of the common approach of organizations blindly following vendor prioritizations for vulnerabilities. An example of this is the vulnerability scanners, often following the Common Vulnerability Scoring System or similar ratings, providing a *severe* rating for Simple Network Management Protocol being enabled with default community strings on an otherwise noncritical network printer. If those findings are considered severe, then what would a weak firewall password, SQL injection on a core web application, or a missing patch that's remotely-exploitable on a critical server be considered? It's all about context and common sense. The worst kind of information security assessment that you can perform is one that does not have a formal report and, therefore, the issues go unseen and unaddressed.

- **Resolution**

If you find problems, fix them. I often see security assessment reports and the specific findings they contain go unacknowledged indefinitely -- or at least until the finding is reported on the following security assessment. This is an easy fix: assign responsibility and ensure that everyone is held

In this e-guide



accountable. The next go-around of your information security assessment, perhaps in six months or a year, will determine whether or not the issues have been resolved. Alternatively, you might consider performing a remediation validation of critical and high-priority findings as a follow-up to your security assessment, 30 to 45 days after the report has been delivered and the findings have been assigned.

- **Oversight**

Ensuring ongoing security between your security assessments will require something as simple as the tweaking of existing systems and software, possible implementation of new technical controls and an outright overhaul of your policies and processes. Rather than trying to attain perfect security, the goal moving forward should be reasonable security with shorter and shorter time windows for catching flaws and resolving them. Furthermore, management must be kept engaged. Many executives are on board with what's required, in terms of compliance and contractual obligations. It doesn't matter if they're interested or not. Keep the right people in the loop with your security assessments. This will not only demonstrate return on their investment, it's essential for ongoing buy-in. Otherwise, security is out of sight and out of mind and, therefore, not a priority.

The bottom line is that every enterprise has information and computing assets that criminal hackers or malicious insiders want for ill-gotten gains, or careless users may lose or otherwise damage. It's foolish to believe that you can secure or be immune to the information risks that you don't acknowledge. And enterprises cannot simply rely on IT security auditing or pen testing alone. Neglecting security assessments is not a defensible option for due care. Furthermore, it's security -- and potentially career --

## In this e-guide



suicide to uncover information risks that end up being ignored. Take the time necessary to properly plan out your information security assessment, ensure the work is completed and see to it that the proper staff members in IT, development, management and elsewhere are made aware of the findings so that the issues can be addressed.

As much as some security professionals and vendors would like for you to believe, information security assessments are not a difficult exercise and do not have to be expensive given the virtually-guaranteed return on investment. Warren Buffett once said, "You only have to do a very few things right in your life so long as you don't do too many things wrong." Your information security program will be a reflection of what you sow -- or fail to sow -- including having a program for ongoing security assessments. Make sure this is a priority. Even when performed periodically and consistently over time, these assessments are not the perfect solution to all of your security woes. However, you can rest assured that if you choose to ignore this essential exercise, history will undoubtedly repeat itself.

Next article

## In this e-guide



# About SearchFinancialSecurity

IT security pros turn to SearchFinancialSecurity.com for the information they require to keep their corporate data, systems and assets secure.

Get in-depth technical advice and learning materials related to the strategies, technologies and business processes associated with ensuring security in high-risk financial environments.

Nowhere else will you find such a highly targeted combination of resources specifically dedicated to the success of today's IT-security professionals.

**For further reading, visit us at http://SearchFinancialSecurity.com/**

Images; Fotalia