COMPLIANCE WEEK
THE LEADING INFORMATION SERVICE ON CORPORATE GOVERNANCE, RISK, AND COMPLIANCE



# What Makes a Good 'Pen Tester'

John Reed Stark | December 8, 2015

John Reed Stark
Columnist

Just as maintaining good health requires an annual physical checkup, maintaining robust cyber-security requires an annual cyber-security checkup—but the world of cyber-security checkups is confusing.

First, even the consultant jargon is unclear. Firms sell penetration testing, risk and security assessments, data security audits, application security evaluations, code reviews, and other similarly described services. For purposes of this column, I will put all of them under the label of penetration (or "pen") testing, which is standard parlance and also considered the lowest common denominator for evaluating cyber-security.

Pen tests can range from using a few commercial tools to analyze network security and harden network architecture; to using intricate operations of customized software and social engineering to try to hack into a client's network; to initiate a full-scale, all-inclusive risk appraisal of a company's overall safety and cyber-security.

The only certainty for compliance professionals is that the selection of a pen tester is one of the most important, yet most difficult, decisions in their job description.

So what exactly makes a good pen tester?

**The Basics**

Pen testers must have substantial technological abilities, including expertise in testing web applications, mobile applications and devices, software products, third-party service providers, cloud solutions, and IT infrastructure. One mark of a good pen tester is to be a thought leader in the infosec community–authoring theoretical publications, giving peer conference presentations, contributing to open source projects, writing blogs, or publishing vulnerabilities. It also helps if a pen tester has so-called "blue team" experience, (that is, he or she has managed networks or systems or developed applications).

Good pen testers mimic the methods used by sophisticated attackers to identify vulnerabilities before they can be exploited. That is best achieved by using specialized, manual testing; not by running automated tools. No two pen testing engagements are ever the same; even the same vulnerability can vary wildly in different environments, and having a proprietary set of tools evidences a pen tester's ability to venture off-script and improvise when necessary. Proprietary tools also typically allow for a more detailed explanation of the so-called "kill chain" or path of an attack.

Testing cyber-security fortification also requires a comprehensive plan to determine defense capabilities and weaknesses and ensure the wise application of resources. What works best is a disciplined yet flexible methodology that incorporates a company's organizational culture, operational requirements, and tolerance for risk, and then balances that against current technological threats and hazards. Since data breaches are inevitable, risk is the appropriate paradigm for analysis; in the end, a proper pen tester quantifies risk, develops meaningful risk metrics, and conveys the effectiveness of risk mitigation options in clear and concise terms.

Good pen testers mimic the methods used by sophisticated attackers to identify vulnerabilities before they can be exploited. That is best achieved by using specialized, manual testing; not by running automated tools.

**Constituency Briefings**

Good pen testers bring more than just technological expertise to the table. They also become a key facet of their client's external relations and business development.

For instance, pen testers who understand the current regulatory framework of a client's enterprise—including the SEC, FINRA, HIPAA, FERC, CIP, PCI, and whatever other regulatory scaffold applies—can make significant contributions to compliance and regulatory response. Similarly, when a company's customers, partners, insurance company, or other interested parties asks cyber-security-related questions or require completion of a cyber-security compliance questionnaire, good pen testers help by providing confidence and assurances to these third parties and by interacting as part of the team responding to their requirements or demands.

Along those lines, constructively conveying the results of pen testing to technical and management audiences is often more important than the testing itself. Good pen testers are comfortable in the server room, the C-suite and the boardroom, giving briefings, fielding questions, and making recommendations.

## Related articles

Transforming the Cyber-Security Paradigm (http://www.complianceweek.com/blogs/john-reed-stark/transforming-the-cyber-security-paradigm)

**Incident Response Expertise**

It's always optimal when the contractor who installed your home plumbing, electrical, or HVAC system, is also around to trouble-shoot that system when problems arise. The same goes for pen testers.

A good pen tester's goal during an engagement is not only to fortify cyber-security; it's also to be on call when an attack happens. Since few companies employ the kind of engineers, programmers, and digital forensic specialists who can tackle today's increasingly sophisticated cyber-attacks, good pen testers also serve a data breach response role. Having a pen tester on speed dial who has data breach response capabilities, and who also already understands (and helped fortify) a company's defenses, can be critical.

**Physical Security**

Remember that cyber-attacks can sometimes begin with a physical breach. For instance, an outsider may break into a company's headquarters and surreptitiously gather fodder for a social engineering scheme (such as a *spearfishing* campaign), or an employee may gain access to a company's network and wreak havoc.

Hence, good pen testers understand how to review the physical security of facilities, including management's plans for reception and entry checkpoints; ID scanner and other access records; video or still footage; physical logs; and even elevator and garage records.

**Dark Web Surveillance**

After a burglary, a good cop checks the local pawnshops, hoping to track down any swag from the robbery. Good pen testers do the same—they surveil the so-called "Dark Web" or "Deep Web." That is the portion of the Internet accessed only by using special browsing software, and where criminal activity often occurs, such as the sale of stolen data. Good pen testers monitor the Internet, including the Dark Web, searching for signs that their clients have experienced any unauthorized exfiltration of data (such as someone selling their company's secrets or their customers' personal data).

**Avoiding a Culture Clash**

Nobody enjoys being second-guessed, yet that is exactly what an IT department experiences when a pen tester arrives.

Sometimes pen testers encounter a defensive IT department, especially when a company has recently experienced a breach and IT personnel are suddenly worried about losing their jobs. Other times IT departments welcome pen testers with open arms, hoping to gain their support for additional funding, expertise, or personnel.

Under either scenario, to avoid a possible culture clash, pen testing not only requires tact, thoughtfulness, and sensitivity, but also peacekeeping and even diplomacy skills.

**Beware the Laundry List or Heat Map**

Companies should avoid engaging pen testers who present deliverables in the form of a written list of problems or a so-called "heat map," which identifies the most serious potential weaknesses. Why? Because the reality is that most companies will not be able to cure all weaknesses (due to cost concerns, logistical impossibilities, practical barriers, and so forth).

Thus, though intended for a company's benefit, heat maps and laundry lists can also provide regulators, law enforcement, class-action lawyers, and other disgruntled parties with a roadmap for liability. Always remember that the first question from any regulator during any sort of examination or from any adverse party pertaining to a cyber-security issue, will be to review any pen testing results. Consider letting counsel quarterback the pen testing engagement, to insure communication lines are properly organized, thoughtfully orchestrated, and if appropriate, even veiled by attorney-client protections.

**A Final Lesson From Neil Carbone**

When I was three years old, my family moved into a new house. To manage our home's HVAC, electrical, security, and other systems, my late father hired a small company run by a superstar engineer named Neil Carbone. But Neil was not just a repair ace; he also became a part of our family. For the next 40 years, Neil's phone number was posted on our refrigerator door and we called him when anything went wrong. Neil became our most dependable and trusted adviser; he cared for our home (and our family) like it was his own.

When Neil stopped by annually to develop new ideas to make our house better, safer, more fuel efficient, and so forth, he never brought a checklist. Instead, Neil took a holistic approach toward servicing our home, observing not just how our family lived, but also incorporating how our house's environment was changing.

These two lessons from Neil are probably the most important for selecting a pen tester. First, good pen testers not only possess bona fide technological chops, an ethos of dedication, and a philosophy of service. Just like Neil, they also strive to become a compliance professional's trusted adviser.

Second, threat landscapes, activists, random hackers, and state-sponsored actors constantly evolve, refining their techniques, altering their motivations, and shifting their resources. Just like Neil, good pen testers take a holistic approach to their works, carefully considering changing threat actors, advance network telemetrics, and emerging attack vectors.

So when checking the references of pen testers (a must, by the way), in addition to considering the specific recommendations and caveats set forth in this column, consider most of all, my late father and Neil Carbone. Together they kept my home and family safe and prosperous for more than 40 years.

***John Reed Stark*** is President of ***John Reed Stark Consulting*** (www.johnreedstark.com), a firm that advises companies and corporate boards on data breach response, cyber-security and digital compliance. Stark's experience with data breaches touches upon all aspects of cyber-incident response, especially during early phases of crisis management, forensic analysis, malware reverse engineering, and law enforcement/regulatory liaison and containment, as well as the later phases of data-review, remediation, and disclosure and reporting. Stark also handles expert engagements pertaining to technological aspects of investigations, prosecutions, and enforcement matters conducted by the SEC, U.S. Department of Justice, and FINRA, and he also provides expert testimony on securities regulation on behalf of individuals, entities, and government agencies, including in opposition to, and on behalf of, the SEC and other government agencies. Stark's lengthy career includes: almost 20 years with the SEC's Division of Enforcement, the last 11 of which as founder and chief of the SEC's Office of Internet Enforcement; over five years as managing director (three of which heading the Washington, D.C. office) of an international cyber-security and data breach response firm; and an early stint as special assistant U.S. attorney in Washington, D.C., where he prosecuted federal cases relating to guns, drugs, and domestic violence. In addition to authoring several dozen articles about law and technology, Stark served as adjunct professor at Georgetown University Law School where he taught a course on cyber-crime for 15 years and has given numerous lectures on cyber-crime at the FBI Academy in Quantico, Virginia.