Originally published in

New York Law Journal

March 02, 2018

Pen Testing: The Good, the Bad and the Agreement


By Ian G. DiBernardo and Jeffrey Mann

Although conducting pen testing is prudent and becoming common, it is also fraught with potential pitfalls. When embarking on such a project, a company should fully understand its scope and include certain contractual protections with the pen tester.

Cyberattacks have become commonplace over the last few years. No industry is immune to attacks, which have only increased in frequency and intensity as hackers and bad actors have become more sophisticated. One way a company can protect against cyberattacks is to have testing (which can mimic a hacker intrusion) performed on its computer systems and networks to uncover vulnerabilities. This is known as penetration or "pen" testing.

Although conducting pen testing is prudent and becoming common, it is also fraught with potential pitfalls. When embarking on such a project, a company should fully understand its scope and include certain contractual protections with the pen tester. This article discusses best practices related to pen testing, including relevant contractual provisions and precautions to take before, during and after embarking on this potentially risky endeavor.

Increased Need for Pen Testing

In recent years, requests for pen testing have increased dramatically. This is in part due to new privacy and security laws and frameworks that have been adopted in various jurisdictions and industries that either mandate or recommend pen testing as part of a company's data security program. For example, the National Institute of Standards and Technology (NIST), in its "Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology" (Special Publication 800-115), provided an overview of useful vulnerability validation techniques that can be utilized as part of a cybersecurity policy, which include pen testing.

Recently, New York enacted the State Department of Financial Services Cybersecurity Regulations for Financial Institutions (NYS-DFS 23 NYCRR 500), which became effective on March 1, 2017. Under the regulations, all "Covered Entities" are required to enact a cybersecurity program that "includes monitoring and testing … designed to assess the effectiveness of the Covered Entity's cybersecurity program." This monitoring and testing requires "continuous monitoring or periodic Penetration Testing and vulnerability assessments" (23 NYCRR 500.05). As the regulations state:

Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities *shall* conduct:

(a) annual Penetration Testing of the Covered Entity's Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and

(b) bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity's Information Systems based on the Risk Assessment.

Id. (emphasis added). Compliance with these penetration testing requirements for Covered Entities is mandated as of March 1, 2018.

Based on these, and other, recommendations and requirements, companies are investing in pen testing, some for the first time and others with renewed focus.

Pre-Contract Diligence

Pen testers come in various forms, that range from large, well-established consulting companies to emerging niche tech providers, and not all pen testers are created equal. Because of the sensitive nature of the work that is being performed, a company should investigate each

potential pen tester before allowing it potential access to the company's systems and data. While each project is unique, a company should investigate a variety of factors before choosing the right provider, including, for example, by focusing on both the pen testing entity and its systems. For example, diligence should include considering whether the pen tester uses consultants or employees, as well as the tenure and experience of its team. Similarly, at the diligence phase, a company should understand the extent to which a pen tester utilizes any third-party systems or tools and, in any event, confirm such systems themselves have been tested and certified.

Moreover, by having the diligence memorialized as a standard "checklist," pen testers can be rigorously compared, and performing robust diligence early in the process will help avoid costly surprises and delays down the road.

Scope of Testing

In general, pen testing is implemented by a software vendor that undertakes certain actions (that may mimic actions that a hacker may take) to uncover vulnerabilities of a particular computer network. Because your computer network is only as safe as your least-protected link, it is important that tests cover a wide variety of software and hardware, while not losing sight of the forest for the trees. Therefore, prior to undertaking the testing, a company should among other items, consider: Which applications and systems will be tested? What access points will be tested? Are there touch points with third-party providers (e.g., a cloud provider) that will need to be tested?

Preparing for the pen testing can include the pen tester detecting information about network architecture, systems and applications, as well as profiling the company through publicly available information in a manner similar to which a hacker might find such information. Alternatively, the company can provide this information to the tester. Vulnerabilities that the tester may uncover can range from minor issues, like misconfigured servers or outdated program code, to major issues like compromised credentials or inadvertently exposed gateways that can leave proprietary or personal information open to attack. Regardless of the magnitude of the problem uncovered, the goal of these tests is to isolate any issues in a controlled way so that they can be rectified before a data breach or other security contravention occurs.

Confidentiality and Third-Party Concerns

It is also imperative when entering into an arrangement for penetration testing to negotiate an agreement that proactively protects the company in several key respects. This includes having robust confidentiality provisions. Beyond protecting information provided to the pen tester, confidentiality obligations should extend to information collected, even from public sources, by

the pen tester during an initial investigatory phase of the testing, information obtained during the testing, results of the testing, including any reports, as well as any other information that a company would not want to become public.

Additionally, a company must also consider if any third-party information or systems are implicated in the pen testing. For example, a company undertaking pen testing should consider whether it has licensed any third-party software that is governed by an agreement prohibiting pen testing, either explicitly or implicitly. For some pen testing, the company may provide technical information pertaining to its systems and applications, and care must be taken to ensure such information does not include third-party confidential information and does not otherwise violate an obligation owed to the third party.

While confidentiality is important in many relationships, due to the unique role of a pen tester, the intricacies of the confidentiality provisions take on added significance.

Limits on Testing

In addition to choosing a pen testing company, it is important to stipulate what resources will be used and the specific parameters regarding where and by whom the testing will be performed. Preferably, a company should try to limit the testers to highly qualified individuals who are either employed by or consulting for the pen testing company, and who are bound by legal and contractual obligations to maintain the confidentiality of the company's information and the specifics of the pen testing program. It is also crucial to know if the testing will originate from the United States or a foreign country. If there are concerns about storage or access in certain foreign countries, the agreement should expressly exclude pen testing from those countries. A company should also understand whose resources will be utilized to perform the testing. For example, if hardware belonging to a third party is to be used, additional safeguards may need to be put in place.

Allocation of Risk/Liability

It would be fantastic if no vulnerabilities were found by the pen testing. However, the agreement must identify what happens if the pen testing identifies vulnerabilities or the testers are able to improperly access data or information on or about your system. Because the question of who bears the risk in the event something goes awry can be of great consequence to your company, it is wise to include robust warranties, covenants and indemnification provisions that can protect your company in the event of a future dispute. These can include service provider warranties, as well as warranties related to data accessed during the testing and afterwards. An additional covenant should require the tester to ensure the system is restored to its original level of operability (other than correction of vulnerabilities) once the

testing is completed. In other words, the tester should guarantee that the testing will not harm the network or its operability following the testing. If the test damages the company's systems or makes them less secure, this could negate any benefits that pen testing is intended to generate.

For financial companies that are subject to additional regulations and regulatory oversight, there are added concerns. As part of any agreement, a financial company should seek to obtain the tester's agreement to be bound by the same data security and data privacy regulations that the financial company is bound by. The more robust this protection is in the agreement, the more helpful it will be in satisfying questions that regulators may raise regarding compliance. For example, the agreement can include indemnification for any third-party or regulatory claims that arise from the testing. Like other relationships, it is important to make sure that both sides are vested in the success and safety of the project. It can be better in an agreement to account for as many eventualities as possible, rather than trying to sort things out after an incident occurs.

Conclusion

Penetration testing is an important tool in a company's cybersecurity arsenal, and in some cases it is even required by regulators. However, to ensure the full benefit of pen testing, while avoiding additional risk, companies need to manage the project, including through diligence and thoughtful and robust contractual protections.

Ian G. DiBernardo is the co-practice group leader of the intellectual property and technology group of Stroock & Stroock & Lavan LLP. Jeffrey Mann is a special counsel in that group and a Certified Information Privacy Professional (CIPP/US)