



# DATA SECURITY AND ETHICAL HACKING

## Points to Consider for Eliminating Avoidable Exposure

By Ronald I. Raether Jr.

**E**thical hacking may not be a familiar term to most people, but to data and corporate security personnel, the concept is well known and the practice is essential. Government regulators, industry groups, and pundits all agree that challenging one's own data security construct by critical assessment and testing is a fundamental component of any effective data security regime. Likewise, protection of intellectual assets from corporate espionage and the mischievous hobbyist hacker requires monitoring and making controlled attempts to break the defenses described in written policy and procedures.

Security assessments can take many forms. Many companies are familiar with perimeter scans that test a system's ability to withstand attempts to break through the perimeter firewalls—the wall between outside hackers and inside users. Companies employ tools developed over time to prod and punch the network architecture to locate potential vulnerabilities. Using the same techniques and methods of a criminal hacker, these individuals became known as ethical or white hat hackers. The important difference is that unlike the criminal hacker who turns his or her tools to malicious and destructive purposes, companies employ ethical hackers to learn from the experience and further improve

security if the lessons learned are properly analyzed, changes implemented, and information is disseminated to all interested parties.

But as security threats have evolved, so too have the types of assessments being conducted. Companies have learned that data security threats and vulnerabilities do not end at the wall built around their data infrastructure. Today, a company may assess its applications to identify any vulnerability in the code or architecture. The areas of review vary based on the company's needs but can include security of e-mail, Web and wireless access, instant messaging, application development, and database management. Many companies also are looking at their susceptibility to social engineering and pretexting.

While performing ethical hacking is the right thing from a security standpoint, such conduct may unintentionally create avoidable legal and contractual exposure when advanced precautions are not taken. To illustrate this point, consider an application vulnerability that permits the ethical hacker to access data regulated by the Fair Credit Reporting Act (FCRA). Like any good tester, the ethical hacker gets as far as the vulnerability permits. In our hypothetical, the ethical hacker takes several screen shots of FCRA data and executes a robotic script to capture 1,000 records—not the whole database, but just enough to demonstrate the vulnerability. The problem is that the FCRA limits the disclosure of data to specific enumerated permissible purposes,

which do not include internal use for security testing.

With some thought and planning, however, exposure can be limited or avoided entirely. Many issues will be unique to each business and possibly each testing situation. While the specific solution may vary, common questions exist. This article discusses many of these questions that aid in structuring a security assessment program that does not unintentionally create exposure and noncompliance. Such common questions include (1) what application or process will be tested; (2) what type of data may be exposed, and what is the source of that data (questions important in identifying applicable laws); (3) who will conduct the testing, and have they been properly screened and educated as to the limits imposed by law or contract; (4) what techniques will be used, and do these techniques raise contractual or other compliance issues; and (5) who will receive copies of any reports, and what controls are in place to prevent dissemination to improper persons or for forbidden purposes. Exploring these questions and addressing issues unique to your client or the specific testing situation will help considerably in limiting possible exposure that today may be overlooked by many companies.

### Data at Issue

Whether designing a security process or engaging in testing required by an existing process, it is essential to have a thorough understanding of the

*Raether is a partner at Faruki Ireland & Cox P.L.L., in Dayton, Ohio. His e-mail is rraether@ficlaw.com.*

process or application being tested. In most scenarios, the tester is looking to see what and how much information is accessible (and the relative sensitivity of the information) with techniques commonly used by criminals. The tester (ethical hacker) intrudes the system and data, and otherwise acts in a manner not intended by the business model. Such testing may violate the laws and contractual obligations governing the system. Appreciating the legal and contractual risks, many managers are beginning to prohibit the use of live data for development testing and to avoid making this live data available to application development testers. This same prohibition—prohibiting the use of live data during ethical

obtained the information directly or through a reseller from a state motor vehicle record department, then the information will be governed by the Driver's Privacy Protection Act (DPPA). Like the FCRA example discussed above, there is no permissible use for security testing in the DPPA. In contrast, the Gramm-Leach-Bliley Act, 15 U.S.C. § 6821(d)(1), specifically provides that "[n]o provision of this section shall be construed so as to prevent any financial institution . . . from obtaining customer information of such financial institution in the course of—(1) testing the security procedures or systems of such institution for maintaining the confidentiality of customer information." Until Congress clarifies

not employed by the company should execute a written agreement to act within those requirements and agree to indemnify the company for any breach of these promises.

Likewise, the company may be a party to a contract that places limits on the data and its use. Such is the case where a financial institution contracts with a third party to manage, store, or transfer customer data. Under this circumstance, the financial institution is required by the Gramm-Leach-Bliley Act to contractually impose compliance with this law on the third-party service provider. A similar requirement is created by the Health Insurance Portability and Accountability Act (HIPAA). Under these circumstances, access by an ethical hacker without necessary precautions may violate these contractual requirements, creating liability for yourself and possibly your client. Confidentiality provisions also might be violated by ethical hacking. Knowledge and analysis are required to avoid such potential pitfalls.

One possible solution is to obtain the consumer's consent when the data is obtained. Many of the United States' data laws (and the laws of other countries) permit any use if the consumer's consent is first obtained. (E.g., 18 U.S.C. § 2721(b)(13) provides that "[p]ersonal information . . . may be disclosed . . . [f]or use by any requester, if the requester demonstrates it has obtained the written consent of the individual to whom the information pertains.") Where there is a direct relationship with the consumer, such a solution may be possible with proper planning. In many instances, there may not be a direct relationship with the consumer or the data may already be in the company's possession and going back to the consumer to obtain consent is not possible. A section in the company's privacy policy to obtain indirect consent may not be sufficient depending on the applicable law.

Where actual or implied consent cannot be obtained, the company may be forced to place limits or controls on how far the ethical hacker exploits a system or network, such as telling the

## The palette of potentially applicable laws is broad and sweeping.

hacking—arguably applies to security testing or ethical hacking. While the legal and contractual issues remain the same when engaging in ethical hacking, the same solution (prohibited use of live data) cannot apply since the ethical hacker must test the live environment, which includes live data.

As a result, there must be an understanding of the types, source, and use of data at issue, and of the facts that determine the specific laws and the contracts that may apply to the business unit or application being tested. The palette of potentially applicable laws is broad and sweeping. Financial institution data could be regulated by numerous laws and regulations, including the Gramm-Leach-Bliley Act, the red flag rules promulgated by the Federal Trade Commission, or if trading in securities, Regulation S-P issued by the Securities and Exchange Commission. When you start considering the complete data compliance landscape, you recognize that hundreds of laws and regulations might apply.

For example, whether an ethical hacker's access to an individual's date of birth is prohibited may depend on the source of the data. If the company

that security is a proper component of all data privacy laws, uncertainty exists.

If the data you are securing was at any time located in another country, then the law of that country also might limit what can be done by the ethical hacker. For example, the European Union has in place Article 25(1), which provides that personal data cannot be exported from the European Economic Area (EEA) unless the importing country provides "adequate" protections. The United States is not considered to be a nation with laws that provide "adequate" protections. As a consequence, if the tester or the subject is located in the EEA, then restrictions may apply that in the course of the challenge testing could be violated.

An analysis must be done to identify these requirements and to develop solutions. A set of controls and instructions should be drafted to capture these requirements and provide clear instructions to the ethical hacker. Everyone involved in the process should be informed about all requirements, and continuous monitoring should be put into place to ensure compliance. Ethical hackers

hacker to stop once he or she gets to defined points in the system, and for the purpose of remediation assume that the vulnerability gets all the way to the protected data, or to completely avoid specific systems or data repositories. Contracts with customers to process or handle third-party data should include provisions establishing the right to access the data for security testing, providing limits to liability and indemnification provisions. With some creative thinking a solution can be developed; you simply want to be aware of the risks and develop a solution that navigates those risks.

### Techniques Create Unique Obligations

Understanding what data is at issue provides only a partial picture. The assessment techniques to be used also must be understood. Defining at the inception what work will be done by the ethical hacker, and thus what laws and contractual obligations may come into play, will allow you to be proactive in setting terms and conditions that permit compliance with the law and avoid inconsistencies with contractual obligations. At the point of engaging the ethical hacker, understanding these limits will permit you to put in place controls and other contractual provisions to reduce exposure.

Two examples are illustrative of what is at issue. Not all security concerns are technical in nature but may concern exploitation of human errors and process deficiencies. Data thieves are now using old-fashioned deception tactics to infiltrate a business and subvert security controls, both physical and technical. One type of testing to address these issues involves attempts by the ethical hacker to trick employees into disclosing information, also known as social engineering or pretexting. For security, information is king. A criminal (or ethical hacker) may need to accumulate information from numerous sources to identify and exploit a vulnerability.

For example, the ethical hacker may get surreptitious access to someone's personnel file to obtain information to mislead the source of the

desired information (e.g., a secretary with access to company trade secrets) or to conduct an electronic hack (e.g., security questions based on personal history). Many companies permit use of the employee identifier in some component of authentication, such as a password. Access to the personnel file might violate HIPAA (if medical records are included) or even the employment contract or employment laws. If, in the above example, the human resources function is outsourced to a separate company, electronic interceptions could violate the Electronic Communications Privacy Act, the Computer Fraud and Abuse Act, the Stored Communications Act, or the agreement with the service provider. Proactively addressing any issues in the contracts with your employees or outside service providers might resolve many of these issues. Otherwise, steps must be taken to avoid violations of the law during the ethical hack.

Another example demonstrates the importance of understanding how perimeter scans or application assessments are conducted. Many companies rely on other companies for part of or their entire information technology infrastructure. Each of these relationships is likely governed by software and use licenses. These licenses may limit access to employees, limit the

number of licensed users, or prohibit reverse engineering or similar uses that might be employed by an ethical hacker. A comparison must be made to understand where the techniques used by the ethical hacker might conflict with restrictions in the license agreements. Of course, going forward, access for security testing should be included in all software licenses and related agreements.

### Identity of the Ethical Hacker

The legal obligations based on what data and processes are at issue and what techniques may be employed will be influenced by who will conduct the testing. If the testing is done by a third party, then additional analysis and different contract provisions may be at issue. For example, a third-party ethical hacker may not be an agent or otherwise be empowered with the same rights of the company. As a result, what might be permitted by a company employee could be prohibited when the exact conduct is done by a third party. Likewise, laws or contracts may prohibit or create additional requirements for third-party disclosures, requiring additional steps or measures to reduce exposure. There should be an express written understanding between the company and the ethical hacker as to the scope and any limits of the engagement.

## Business Law Program Library

**A** valuable member benefit! It's quick, easy, and right at your fingertips. Search our program library for past and current meeting materials. You can search by title keyword, committee, topic, or meeting and year.

- Program materials and audio database
- Searching is easy
- Materials from 1999 to present
- Exclusive access to Section members



Go to [www.ababusinesslaw.org](http://www.ababusinesslaw.org) and click on Meetings Portal.

A standard contract likely does not resolve this requirement.

Regardless of whether the testing is done by an employee or third-party contractor, care must be taken in selecting the right person and making sure that what is learned is not later used to commit a crime. (See, e.g., "Bowie IT employee resigns amid city network security breach," [http://www.gazette.net/stories/062608/bowin-ew173015\\_32357.shtml](http://www.gazette.net/stories/062608/bowin-ew173015_32357.shtml).) Testing often permits the ethical hacker access to proprietary information, sometimes as part of the testing itself, such as when a grey or white box review occurs. Almost always, sensitive information is exchanged during the remediation process when the company discusses with the ethical hacker what was discovered and what should be done to prevent future attacks. At a minimum, the ethical hacker has gained knowledge about the system and its vulnerabilities. While these issues can be addressed in the engagement contract, more may be required by sound practice.

Trust is essential and should be earned. For the employee, that means background screening, a history of loyalty and exemplified proper use of protected information, and the absence of risky traits such as gambling and other addictions. The same level of review is needed for an outside vendor retained to challenge the data security environment. Understand who will be on the team, who will manage the team, where information will be stored, the security policy and procedures for the vendor, and the auditing and testing of those procedures. You should check references and confirm the legitimacy of all representations.

Both the internal and external ethical hacker should be closely supervised by a person who is accountable for

any failures. I remember visiting Berlin before the Wall came down and riding the subway through East Germany. The stops in East Berlin, which were not serviceable, had two guards—one German and the other Russian. I was told that this arrangement was in place to avoid a conspiracy to jump the train and defect. The same philosophy should be employed here. The supervising employee should know that a failure likely will result in being discharged or other disciplinary action.

### Controlling Dissemination

Finally, there must be a clear understanding as to who gets access to any reports from the ethical hacker, as well as the underlying data. It is the purpose of the report that will dictate not only the list of recipients, but also the process for creating the report and the form and substance of the report. Care and attention need to be given to these issues. The consequence could range from a wasted effort to the creation of a document that might be used later to assert the inadequacies of the company's security by government agencies or private litigants.

If the testing is intended only for internal use, then the ethical hackers should be engaged by the general counsel's office and other work done at the direction of the legal team representative. By doing so, the company can take advantage of any applicable privileges. Dissemination must be controlled to preserve these privileges. Of course, the purpose of the testing could eliminate the possibility of arguing the application of the attorney-client or self-evaluative privileges or the desire to do so. Like pulling the loose string on a shirt (you never know if doing so will cause your sleeve to fall off), waiving the attorney-client privilege to share test results could have broad and unintended consequences.

Dissemination also must be structured to comply with data regulations and contractual requirements. For example, releasing the report to an outside auditor or a customer to establish good security practices could violate laws that limit the disclosure

of protected data to third parties. The company does not want to reach the conclusion of a review only to determine that the report cannot be used for the intended purpose, forced to abandon the work to date, or spend more money and resources to create a compliant process or document. Likewise, the company does not want to support a process that, when subject to review and investigation, creates unintended exposure. For example, the company and the third-party hacker should come to an agreement on the treatment of theoretically possible, but not demonstrated, vulnerabilities and false positives. At a minimum, these reports provide information of tremendous value to criminal hackers. Lack of control over these reports exposes the company to unnecessary security risks and defeats the overall purpose of an information security program. Care must be taken at the beginning of any project, and throughout the project, to address and then vigilantly protect against these issues.

### Conclusion

Testing is an essential part of any data security program. If corrective action is taken and there is proper distribution of the lesson learned, then an ethical hack can reduce the potential exposure of the company to criminal hackers. The effort, however, must be done in a manner that does not expose the company to unnecessary liability. It is important to understand factors such as what data is exposed, what techniques will be employed, identifying the applicable legal obligations, and the implications of who will conduct the test and what will be done with the results. With a sufficient amount of analysis and preparation, risks can be addressed without compromising the efficacy of the testing, while preserving the mission of the information security program. Information security and legal functions can work together to create a process that is the most effective for the organization. In this case, an ounce of prevention may not only be worth a pound of cure, but also millions of dollars of avoidable liability risk. **BT**

### For more information

See M. Lamb & R. Raether, *Defining Data Security Measures That Protect Your Company and Customers*, ACC Docket (Dec. 2007).