Available online at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/CLSR

Computer Law & Security Review

An approach to minimizing legal and reputational risk in Red Team hacking exercises

*Joseph V. DeMarco**

DeVore & DeMarco, LLP, New York, NY, USA

ARTICLE INFO

Article history:

Keywords:
Data protection
Data security
Cybercrime
Cybersecurity
Cyber-resilience
Computer intrusions
Ethical hacking
Network and information security
Penetration Testing
Red Team

ABSTRACT

Robust cyber-resilience depends on sound technical controls and testing of those controls in combination with rigorous cyber-security policies and practices. Increasingly, corporations and other organizations are seeking to test all of these, using methods more sophisticated than mere network penetration testing or other technical audit operations. More sophisticated organizations are also conducting so-called "Red Team" exercises, in which the organization tasks a small team of highly skilled and trained individuals to try to gain unauthorized access to physical and logical company assets and information. While such operations can have real value, they must be planned and conducted with great care in order to avoid violating the law or creating undue risk and reputational harm to the organization. This article explores these sometimes tricky issues, and offers practical risk-based guidance for organizations contemplating these types of exercises.

1. Introduction

As the amount and variety of data being stored has increased exponentially over the years, so have the challenges in keeping it safe. As a result, information security professionals have needed constantly to re-invent how to proactively test and assess the physical and technical vulnerabilities of company systems, so much so that the defenses themselves raise legal and reputational risks. "Red Team" operations conduct internal physical and logical testing to determine whether unknown vulnerabilities exist at a corporation,[1] which would permit unauthorized access to company data and systems, often without any warning to internal security personnel. This article discusses the risks of trying to break into your own network and to hack your own data.

2. The Red Team operation

Red Teaming is a form of "ethical hacking" which involves the use of techniques and methods similar to those of a criminal hacker or state-sponsored organizations to simulate a real cyber-attack (often paired with a physical intrusion) so that the corporation can learn about weaknesses in their defenses. The theory is that by simulating an attack, the Corporation

* Corresponding author: Partner, DeVore & DeMarco, LLP, New York, NY, USA.
E-mail address: jvd@devoredemarco.com

[1] Although governmental entities and NGOs can also benefit from Red Team testing, this article focuses on the issues implicated when a private corporation or similar private-sector entity conducts such operations.

https://doi.org/10.1016/j.clsr.2018.05.033

can prompt appropriate changes and security improvements based on observed cyber-weaknesses. As readers of this publication are likely aware, one common example of ethical hacking is the penetration test, whereby a Company enlists a technology consultant to test certain points of vulnerability in the company's system at a certain period in time in coordination with the Company's IT personnel. In contrast, Red Teaming involves a more comprehensive cyber-security assessment of a company, often over a longer period of time and usually with little or no warning to employees within the company. Indeed, knowledge of the exercise is sometimes limited only to a handful of senior management – and in some cases, to increase the realism of the test, the CISO and head of physical security (or their functional equivalents) are deliberately *excluded* from the "circle of trust" and have no knowledge of the exercise until it is concluded.

Typically, the operation aims to identify both the cyber and physical vulnerabilities in a Company's network and systems. The Red Team (which is carefully selected and operates under strict supervision) often begins by gathering as much information as possible from publicly available sources about the "target" whether it is the corporation as a whole or a division or even single facility of the Company. This "reconnaissance phase" can also include the collection of information on Corporate personnel who will be targeted. Often, those employees' social media profiles are a rich source of data that can be used to learn who to target in order to gain access to company facilities, systems, or confidential information. The Red Team generally does not leverage knowledge of internal operations, sources of information, Corporate network access; rather, they seek to emulate access and availability of an external attacker. Once potential weaknesses are identified, the Team then employs many of the same tools that a black hat hacker would use to compromise company servers and networks, including "social engineering"[2] techniques that solicit critical information from employees under false pretenses. In addition, physical intrusion testers may be tasked with surreptitiously gaining access to areas in Company facilities to identify weaknesses in physical security or, place a device on the Company's system to aid the hacking. For example, a tester may pose as a package delivery person or use a cloned building access card to get access to a server room, or just to computers that are unattended. They may even scatter "infected" thumb drives in company offices in the hope that someone might plug them into a corporate computer.[3]

The Team may or may not provide some limited information to the company's IT department in advance for certain parts of the operation. Black Box testing is when the Company provides no information prior to the start of testing to the Team about the company's network and the Company's network defense organization has no prior knowledge of the test. Grey Box testing is when the Company provides partial details of the target systems and the network defense organization may have some notice of the test. White Box testing is when a Company provides the Team with full and complete details of the network, applications, and internal procedures and when the Company's network defense organization knows about the test in advance. The recommendations below are generally applicable to all of these scenarios.

3. Legal risks

3.1. *Access to sensitive information*

Even though the Company voluntarily authorizes[4] the hacking, it does not mean that the hacking is free of a variety of statutory and contractual legal risks. The Company's systems likely contain a variety of personal information that is subject to local and foreign national laws (and both federal and state laws in the United States). For example, in the U.S., under federal and state data breach statutes, Companies who hold personal information that is inadvertently exposed must undertake an extensive investigation and expensive remedial measures to inform affected individuals of the breach. Additionally, the exposure or deletion of data may give rise to causes of action in tort or could violate contractual provisions between the Company and third parties. A properly conceived Red Team operation should, through knowledgeable legal counsel, analyze these laws in advance, so as not to trigger a "false alarm" and needless data breach report by the Corporation.

Red Team operatives should, to the extent possible, avoid viewing any electronic financial data, credit reports, employee or applicant data, or health data. Unless otherwise stated in writing, data exfiltration relating to employees—whether current, former, or prospective—of the Corporation should almost always be prohibited or only be conducted with prior approval and appropriate documentation. Similarly, exfiltration of data outside of the internal network should not be permitted. In addition, to maximize security, information compromised during a testing engagement should not traverse the internal network with risk of external exposure. Moreover, unless otherwise approved in advance, testers should not access or attempt to access customer data, sensitive employee information, or systems housing information not owned by the Company.

In terms of attack technique and tradecraft, malware should never be employed for any purpose during the exercise. In addition to implicating potential liability under local computer crime laws, the malware may damage data or spread to other systems in unpredictable ways that could give rise to a claim sounding in negligence, among other legal liabilities.

[2] Examples of "social engineering" include sending phishing emails to Company employees or "pre-texting," communicating with employees using a fabricated scenario to obtain information.

[3] Naturally, the drives will not contain any actual malware; they can, however, be configured to "beacon home" to the Red Team operations center with information about where the drive was connected and, potentially, who connected it. Targeted remedial measures can then be considered by management.

[4] As will be discussed elsewhere, see infra, it is crucial that internal or external legal counsel versed in the issues discussed herein be closely involved in the conceptualization and execution of the exercise. At the outset, counsel can guide the Corporation in the proper methods of exercise authorization so as to ensure that it is not "ultra vires" while at the same time maintaining the parameters of desired secrecy.

Instead, as a general matter, Red Team testing efforts should be conducted with technologies, tools, and platforms that are obtained from reputable sources and, in the event of Free and Open Source Software (FOSS), abide by all corporate use license agreements. Moreover, tools, technologies, and capabilities leveraged during testing should not be acquired from locations or sources considered un-reputable, or from sources that pose unintended risk to the system being tested. Crucially, the Red Team should never use stolen hacking tools (e.g., leaked National Security Agency tools) or tools that violate corporate use agreements. Testers should also never purposefully destabilize the confidentiality or availability of the Company's proprietary data and information. Finally, Red Team testing via social engineering methods with e-mail based phishing attacks should never include malicious software as part of the payload. In sum, the "Physician's Principle" – *primum non nocere* – should be scrupulously respected: Testing should be done in a manner in which the user or system is not put at any *additional* risk.

The Team should be especially careful to avoid actions that could adversely affect the Company's clients or other innocent third parties. The operation should avoid intercepting data flows coming to or from or entering the networks of entities other than the Company, including service providers. Failing to take proper precaution can result in serious damage, including the destruction of data, the exposure of personal information protected by statute, compromising of a power system or other essential service. If the Red Team has reason to believe that clients or other innocent third parties could be foreseeably adversely affected, they should first consult legal counsel prior to taking the action in question. If the Team inadvertently causes harm to a client or other innocent third parties, the Team should cease all activity and immediately contact the managers supervising the operation.

3.2. Law enforcement and physical safety

Because the Company's employees are unaware of the Red Team operation, there is always a risk that an attempted physical or cyber intrusion will be quickly escalated to law enforcement. The Company should carefully consider measures to minimize the risk of this occurring or, in some cases, whether prior notice to law enforcement about the operation is appropriate.

Prior to commencing a specific kinetic or cyber operation, the Team should select Company personnel who can – in the event that the Red Team's actions are detected by Company personnel or by clients – prevent the matter from being escalated to law enforcement. In the case of cyber operations, the team should consider providing a list to select personnel of all IP addresses that the operation will be directed from. In the case of physical penetration testing, the team should provide photographs and information about the tester's true identity and assumed identity to select personnel. The team should also inform select personnel once a specific kinetic or cyber operation has been completed. This deconfliction will ensure testing efforts are not interrupted and unnecessary investigation and analysis is not conducted.

In addition to law enforcement involvement, physical intrusion testing could potentially include the risk of a physical confrontation and bodily injury. Although the goal of the exercise is to breach the company's physical security, a tester should never resort to breaking and entering or other extraordinary measures that could result in property damage or a physical injury. During the testing lifecycle, if at any point a tester is "discovered," deception or social engineering is permitted within the bounds of these guidelines, but a tester should *never* impersonate a police officer, other first responders, clergy, public officials, lawyers, or doctors, and should be mindful about not breaking any local laws.

Testers should disclose testing activities and identities if the discoverer becomes hostile or asks for or seeks escalation. At no point during a physical testing engagement should testers leverage security weakness that put the tester or anyone else at risk of injury. Safety is the top priority when conducting physical intrusion testing. In the event the facility involved employs armed guards, it is imperative to discuss impacts and response process with supervisors prior to test execution.

Physical testing engagements should be pre-coordinated with supervisors, and include approval prior to test execution. This may include representation form Corporate security, local physical security, or a direct liaison at the actual facility being tested. Physical Intrusion testers should have a lanyard around their neck (hidden from plain sight) that includes a "safe passage" letter signed from physical security or responsible site location representatives noting that this is an authorized test. This letter should be accompanied with a direct contact number and the physical security tester's actual employee badge for de-confliction. The Team should always ensure that there will always be a Company representative—ideally the senior legal officer—who can be contacted during operations and who can be given as a name to law enforcement or security personnel.

4. Important best practices

4.1. Directing and defining the scope of work

As a threshold matter, it is crucial that legal counsel be closely involved in planning and supervising the Red Team exercise. As noted above, an array of disparate civil and criminal laws can be implicated in an exercise and a thorough knowledge of the applicable legal framework governing the Company and the exercise is crucial. In addition to core legal compliance, the use of outside counsel can, depending on the circumstances, bring the operation within the bound of counsel privilege. The benefits of this are outside the scope of this article, but they can be substantial.

In addition to the careful planning around the legal risks above, there are some more general principles that should govern the service agreement between the company and the Red Team vendor. The Company should clearly delineate in written Red Team Guidelines (RTGs) what information or systems are off-limits to testing, what testing devices are permited and the acceptable methods of physical intrusion testing. Any limits on social engineering methods should also be spelled out. Any changes in scope of testing or devices tested must be approved and included within a written Statement of

Work (SOW) prior to test execution. Red Team testers should always remain within the scope of testing defined in the RTGs and SOW.

Red Team testers should also abide by all Company policies that are affected by the operation and a Code of Conduct (COC) and Memorandum of Agreement (MOA) signed by all of the individual Team testers who are not full-time Company employees.

4.2. Information flows during testing

Documentation and reporting are essential to a well-managed operation. Red Team testers should document all their testing analysis and results including steps taken to achieve actions on objectives. These methods will enable re-testing or validation testing to occur with emulation of tester attack methods. During Red Team activities, testers should provide periodic – and in no event less than weekly – progress updates that describe in detail what has been discovered and what methods were used.

Results of Red Team testing activities should be consolidated in periodic reports and provide an overview of discovered vulnerabilities, weaknesses, exploitation success and remediation guidance on how to address the risk. Any final report should assess overall risk level of the system and the risk level of each vulnerability. As noted above, the Red Team should operate at the direction of counsel and all Red Team documentation should be labelled *“Privileged and Confidential: Prepared at Counsel Direction.”*

During Red Team Testing activities, if a tester discovers, exploits, or otherwise takes advantage of a weakness, risk, or vulnerability considered to be critical in nature, it is the obligation of the tester to disclose immediately this information to trusted supervisors, regardless of impacts to the testing process. These include the following as examples:

- Discovered breaches.
- Evidence of attacker remanence (tools, directories, files, malware, etc.).
- Vulnerabilities with high exploitation probability.
- Vulnerabilities that are exploitable for full, untraceable access.
- Vulnerabilities that could place lives, physical safety or public welfare at risk.

4.3. Insurance

Given the potential for damage to Company and third parties, it is important for appropriate officials to assess the risks against the terms of Company insurance policies, including general commercial liability policies, director and officer liability, errors and omissions coverage, and cyber insurance policies. Errors and omissions coverage, for example, will generally cover many claims arising from negligence, but it will not cover disclosure of personal information or personal injuries. Cyber insurance may cover disclosure of personal information, but may not insulate Directors and Officers from claims of malfeasance. It is possible that certain aspects of the scope of work are not insurable, in which case the Company may need to revisit the scope of work.

4.4. Protecting company relationships

Any of the dangers above can damage relationships with clients, other third parties, employees, and the Company’s perception in the media. Prior to signing the vendor contract, the Company should identify any potential sources of employee or third party data and build the exercise around that data as much as possible.

With respect to its own employees, the Company should request that the Red Team avoid engaging in “pretexting” of real persons or any misappropriation of the likenesses of other people. This prohibition includes using names or likenesses of persons that the Team knows are known to the target or who are connected to the Company or making representations to the target that could uniquely identify the online personality as a particular person, especially from the target’s personal history. Similarly, unless otherwise approved in advance, Red Team testers should not be authorized to log into the Company’s systems utilizing an employee’s access credentials. If the team acquires an employee’s credentials, the team should note that the credentials were successfully obtained and proceed no further. If the Red Team includes leveraging of employee credentials to determine extent of threat and impact, this must be done in a secure manner. Red Team testers must acknowledge and abide by these Guidelines; credentials should only be associated to business owned accounts; compromised credentials should only be used for the purposes of testing; and users should be alerted by the trusted agent at the completion of the test to change their password(s).

5. Conclusion

As the challenges to keeping data secure multiply, it is important for companies to subject their data systems to more rigorous scrutiny. Red Team operations should be considered alongside other penetration testing techniques with a realistic assessment of the legal and reputational risks associated with those operations. If properly guided by management and legal counsel, they can significantly increase the cyber-resilience of an organization.