THINK LIKE A HACKER:
Strategies to defend against advanced social engineering and external penetration

INTRODUCTION

Imagine you’re working at your desk on any given day and an email pops up with the subject, “Urgent Matter: All Employees Please Update Your Contact Information,” from what appears to be a valid company email address. The message content appears to be legitimate, and even includes your president’s email signature and the company logo. In it, too, is a link you’re requested to click in order to update your private information. With no red flags waving, you do it.

Unfortunately, that was a spoofed email address, and you’re the victim of a phishing scam. By clicking that link, you’ve just self-injected malware onto your computer, possibly exposing your company’s network—and your customers’ information—to cyber criminals.

This white paper examines strategies to defend against dangerous cyber criminals: how to recognize both social engineering and external penetration attacks; ways to identify both types of threats; and strategies to protect your network, institution and customers from falling prey to today’s sophisticated hackers.
It’s the work of an unethical hacker who has used a particular type of cyber threat—advanced social engineering—to trick you into becoming an unwilling participant in their crime. Perhaps the single most dangerous enemy facing today’s financial institutions, hackers attempt to infiltrate your network in the name of one, or several, malicious goals:

- For their own personal or financial gain
- To perpetrate a broader fraud or theft
- To harm the reputation and success of your company

**THE DAMAGE HACKERS CAN DO**

Since it was established in 2000, the Internet Crime Complaint Center (IC3) has received almost 3.5 million consumer complaints of Internet-based crimes and scams. According to its *2015 Internet Crime Report*, the IC3 received 288,012 complaints last year, amounting to $1,070,711,522 in reported losses.

While the total number of complaints has not risen substantially over the years, the reported monetary losses have grown significantly. The reported loss in 2012 was $525,411,110. By 2015, this number had more than doubled (see chart below).

The fact that the stakes are rising so quickly tells us that cyber criminals are becoming more effective with each breach, hack or scam. And any one of your customers is a potential victim awaiting a substantial loss. Will this cybercrime trend slow down? Not a chance.

Threats come in many shapes and forms, but going online to pull off their goals uniquely identifies these hackers as cyber threats, and anyone with an Internet connection qualifies.

Potential cyber criminals include:

- Recreational/criminal hackers
- Competitors
- Vendors
- Employees

Neither avoiding the issue nor assuming a network is secure is a viable option, when considering today’s highly sophisticated attackers—as well as a financial institution’s requirement under the Gramm-Leach-Bliley Act (GLBA) to protect consumers’ personal financial information.

Failure to achieve (or at least strive for) a bulletproof security posture can lead to:

- Disruption of business operations
- Compromised, lost or stolen confidential information
- Temporary or permanent damage to reputation
- Significant punitive damages for non-compliance with government regulations (GLBA)
- Becoming the subject of lawsuits from customers or members who have been negatively affected
- Being used as an intermediary for illegal activities

Will this cybercrime trend slow down? Not a chance.
THE TWO MAJOR TYPES OF CYBERATTACKS:
Social Engineering and External Penetration

There are two main methods used to accomplish a hacker’s dirty work—social engineering, by which perpetrators exploit lapses in employee judgment to uncover system information, and external penetration, whereby unauthorized users gain access to your network via perimeter services or devices.

Social engineering applies psychological tactics to poach confidential information from unsuspecting staff. Cyber criminals ingratiate themselves to employees or manipulate them into giving up classified data via face-to-face encounters or such destructive tactics as spoofed emails. Warning behaviors include requests for confidential information, intimidation and name dropping. More advanced social engineering is emerging, including the phishing example mentioned earlier.

Likewise, external penetration comes in many forms, including password attacks, session hijacking, viruses and worms. Hackers patiently gather information about your network, then pick the best time to strike. Once inside, they steal or distort confidential data and often disable security features to enable larger future attacks and avoid detection.

To protect against external penetration, all employees—technical and non—should be trained to look for signs of an attack in progress, from suspicious emails and system modifications to unusual network glitches.

SOCIAL ENGINEERING

Verizon’s 2016 Data Breach Investigations Report, comprising findings from law enforcement agencies, forensic services firms and other entities, indicates that more than 100,000 security incidents occurred in 2015. The report analyzed 64,199 of those security incidents and their corresponding 2,260 confirmed data breaches. Of the total security incidents analyzed, 14.9 percent were attributed to social engineering methods. When seeking to identify and prevent social engineering attacks, it’s helpful to remember that things are not always what they appear to be.

There are several types of social engineering tactics, including:

- **Phishing**—using legitimate-looking emails from a trustworthy company to glean confidential or financial information and perpetrate identity theft
- **Vishing**—phishing using Voice over IP (VoIP) systems
- **Smishing**—phishing using text messages
- **Baiting**—leaving a tempting piece of media, like a flash drive, out in plain sight in hopes a victim will take it and insert it in their computer, unleashing malware
- **Quid Pro Quo**—literally means something for something. For instance, an attacker will call random numbers at a company and offer a cheap gift in exchange for information.
In addition, face-to-face tactics include approaching an employee at their desk and requesting private information; dumpster diving, which is literally digging through trash bins to find confidential data; shoulder surfing, involving passing by work stations to surreptitiously glean information; and its partner, eavesdropping, whereby attackers listen to private calls or conversations.

Social engineering works because, simply put, it’s easy. It doesn’t require vast technical skills, but rather the simple ability to manipulate the natural human tendency to trust fellow human beings. It also can target any employee in the institution, most likely employees with little to no knowledge of hacking. Further, a financial institution’s security is only as good as the people who perform its day-to-day operations.

Social Engineering Testing
A social engineering exercise employs the same techniques that an unethical attacker uses to exploit the misplaced trust or misguided actions of a financial institution’s employees in order to gain confidential information. The testing is completed in two phases—conducting the exercise and post-test reporting.

Conducting the Exercise
A professional social engineering tester—often referred to as an ethical or white hat hacker—will work to uncover any inadvertent weaknesses in employees’ ability to keep key information confidential. This should not be viewed as a punitive or “gotcha” exercise against the employees, but rather as an acknowledgment of the sinister intentions and underhanded techniques of unethical attackers. With that intent in mind, the tester will conduct exercises to determine the effectiveness of institutional training efforts to educate employees regarding the components of the institution’s Information Security Program.

Mimicking an unethical attacker, the tester will attempt to glean confidential information by:
- Manipulating employees through the everyday tools they use to do their jobs: the Internet, email and telephone
- Checking for restricted information left unsecured on desks, in trash cans or shred bins and unattended computers

Post-Test Reporting
After the exercises have been conducted, the tester will compile an objective report that provides the financial institution with a realistic assessment of how its employees responded to the social engineering exercises, as well as comprehensive recommendations for safeguarding your network.

The end goal of a social engineering test is to identify opportunities for additional, updated or expanded training on the financial institution’s Information Security Program. A comprehensive tester will include recommendations for those training opportunities within their post-test report.

There are extensive benefits to proper social engineering testing:
- Introducing employees to social engineering tactics and testing their susceptibility
- Testing adherence to any established policies and procedures
- Creating threat awareness
- Keeping social engineering top of mind
- Ensuring test results can be leveraged during training
EXTERNAL PENETRATION

According to Verizon’s data breach report, external threat perpetrators have been responsible for the vast majority (at least 75 percent) of confirmed data breaches in each of the last six years. In all but 2012, that majority amounted to 80 percent or more.

To pull off a successful external penetration attack, a determined cyber criminal will take his time and be patient, slowly gathering information about an institution’s network, monitoring patterns and changes to discover weaknesses—and wait for the right time to strike.

Types of external penetration techniques include:

- **Session hijacking**: an attacker hijacks a network session shared by two systems by masquerading as one of them
- **Password cracking**: identifying the password of a user or administrator to gain access to a system
- **Denial of Service (DoS) attacks**: an attack that bombards a system, causing it to crash or deny access to legitimate users
- **Web-application attacks**: allow hackers to manipulate data, and can even lead to the compromise of the host device or internal network
- **Malicious software**: includes viruses planted in a file or program that replicate and cause significant damage; worms engineered to propagate throughout networks; and Trojan horses, disguised as legitimate programs, but causing major system damage

Vulnerability Assessments and External Penetration Testing

Two main types of security testing can protect financial institutions against most threats: vulnerability assessments and external penetration testing. Both can benefit institutions by showing the impact of an attack rather than theorizing about it, ensuring controls work as expected, identifying ways to improve security, finding the flaws before the attackers and making examiners happy.

A vulnerability assessment is designed to yield a prioritized list of the environment’s vulnerabilities and is generally for institutions that already understand they are not where they want to be in terms of security. The scope, in industry terms, is breadth over depth.

This type of assessment, which ensures GLBA guideline compliance, can easily be performed using a remote scanning device—configured by a certified provider—that is plugged into the organization’s network. The device will scan the entire network, including hardware and software, and perform internal vulnerability, patch management and port scanning functions.

The assessment provider will then analyze the data and prepare a detailed report with recommendations for securing your network.
By contrast, a penetration test’s ethical hackers seek to achieve a specific, attacker-simulated goal. A typical goal could be to access the internal network and gain privileged account usage, obtain contents of the prized customer database on the internal network, or modify a record in a human resources system. The test determines whether a mature security posture can withstand an intrusion attempt from an external hacker. Here, the scope is depth over breadth.

A thorough penetration test consists of these essential elements:

- **Reconnaissance**—entails learning about the target using little or no interaction. This compares to a burglar watching a neighborhood to determine the patterns of its residents as well as their types of possessions and whether they have security systems. Reconnaissance includes Internet searches, website reviews, IP block information and Domain Name System (DNS) interrogation.

- **Scanning**—is the first major contact with the target’s systems, involving looking for potential openings. This is likened to a burglar rattling doorknobs and checking for unlocked windows. Scanning includes network mapping, port scanning, operating system (OS) fingerprinting, service detection and vulnerability scanning.

- **Gaining Access**—is where the hacker comes in, with an attempt to compromise the system. The step is similar to the burglar breaking into the home using the most vulnerable door or window. Gaining access features password and web application attacks and exploiting vulnerable software and configuration flaws.

- **Maintaining Access and Covering Your Tracks**—are the final two steps that are performed only upon successful penetration into the institution’s network. It should be noted that many organizations forego these steps because they are highly intrusive and involve manipulating systems, applications and files.

The test determines whether a mature security posture can withstand an intrusion attempt.
CHOOSING A PROVIDER THROUGH DUE DILIGENCE
Many information security vendors offer external penetration and social engineering tests as well as vulnerability assessments. The scope and intensity of the services provided vary by vendor, as do qualifications. Therefore, a financial institution should conduct thorough due diligence on any potential vendors.

The following questions provide a good starting point toward making your choice:
- What exactly is included in the test?
- Will the vendor use both manual techniques and powerful automation to conduct tests? Can they explain the techniques?
- Will business disruption be minimal?
- What measures will the vendor take to ensure tests will be performed without harming my network?
- What will the vendor include in post-test deliverables?
- What credentials do the vendor’s consultants carry?
- Can the consultants think like a hacker? Are they knowledgeable on the techniques?

Given the widespread threat of cyber criminals, as well as strict regulations regarding consumer information privacy, it is of utmost importance for a financial institution to maintain bulletproof networks and systems through security testing. Is there a cost associated with these tests? Of course, but the cost of disrupted business, reduced customer confidence, fines and lower profitability resulting from an attack are far greater.

CSI takes risk management and regulatory compliance seriously.

ABOUT CSI REGULATORY COMPLIANCE
CSI takes risk management and regulatory compliance seriously; we know you do, too. Since regulations constantly change, we’ve developed comprehensive solutions that address today’s requirements and adjust to meet tomorrow’s demands. Our industry-leading solutions include consulting, social media compliance, testing and watch list screening. Financial institutions and businesses alike trust CSI’s expertise to enhance their compliance programs and reduce operational costs.

Learn more at csiweb.com.

2http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/