CHAPTER 5

# Who Is Responsible for Security?

**Bill Gardner**
*Marshall University, Huntington, WV, USA*

## INFORMATION TECHNOLOGY (IT) STAFF

If asked, most people would say the information technology staff is responsible for securing the data of the organization. This is true because the IT staff is responsible for setting up the servers, network, client computers, firewalls, and other security products located at the edge of the organization's network. They are also likely in charge of installing antivirus software and critical security patches to software and operating systems.

In reality, most IT folks are more concerned with keeping systems up and running than keeping an eye on data security issues. It's the nature of what they do. That's why most organizations rely on security solution hardware and software to keep an eye on data security.

As a result, many IT departments are too overburdened to deal with security in a holistic, proactive approach. As a result, it often ends up at the bottom of the priority list.

The other issue is that keeping systems up and running take a lot of training and technical skill. As a result, the IT team might not be completely up-to-date on what they need to do to secure the organization's data.

It is important not to forget IT when planning and implementing a security awareness program. Help desks are regularly targeted by social engineers in password reset attacks. Unless you give your IT folks the same information and training in regard to security awareness, there might be gaps in their knowledge because assumptions are being made about their level of knowledge of nontechnical attacks such as social engineering, dumpster diving, and phishing.

## THE SECURITY TEAM

Some organizations are not large enough to have security teams. If you are lucky enough to have the budget for a security team, they can only guard against known threats. They cannot keep your users from opening attachments and opening links, but they can be an important part of delivering the security awareness message and reminding users of their responsibility to help protect the organizations data.

## THE RECEPTIONIST

The receptionist is usually the first line of defense in most organizations. It is the receptionist's job to greet visitors and to direct the visitor or the caller to the correct person to help the customer or visitor in a polite manner. Since the receptionist is likely the first person a visitor sees or the first person they talk to on the phone, the receptionist is the public face of the organization. The duty of the receptionist it to answer questions and to generally provide a good customer service experience. Anything else would reflect poorly on the organization. Social engineers will take advantage of this situation.

Why would a determined attacker spend time and money to steal data by attacking through the firewall when they can just walk in to a company wearing a delivery man's or a telephone repairman's uniform and place data taps on the network or walk out the back door with the company's backup tapes, a computer, or even the organization's server.

Receptionists were never meant to be security guards, yet because of this threat, we have put them in that position. It is very important receptionists receive security awareness training so they understand the unique position they are in, know how to identify social engineering threats, and put in place physical security policies that help them keep your organization safe. These policies include items such as guest/visitor sign-in sheets, guest/visitor badge policies, and guest/visitor escort policies.

## THE CEO

The CEO has access to everything on the organization's network. The CEO is also a busy person whose top priority is to make sure the organization is running efficiently and with an eye on the bottom line. The CEO has a huge target on their back. Attackers would love to gain access or steal the CEO or other key manager's computer or laptop.

Management is often the hardest to get to security awareness training events. As a result, it is important to remember to find alternative forms of delivery for security awareness training and reminders for the CEO and other management types.

## ACCOUNTING

If an attacker is interested in money, they are going to launch a spear phishing attack against the organization's accounting department. On security assessments and penetration tests, it is shocking how little thought goes into securing the part of the organization whose mission is to handle money. It is not uncommon to find passwords, bank account log-in information, and wire transfer information kept in text documents, unencrypted and without password protection on the desktops of accounting employees. One successful spear phishing attempt would put the attacker in a position to empty the organization's bank accounts.

## THE MAILROOM/COPY CENTER

The mailroom/copy center needs to use computers just as much as anyone else. In fact, a large amount of information, which can include financial data and medical records, are stored on their computer for copying and mailing jobs. As a result, these roles need to be included in security awareness training as well.

## THE RUNNER/COURIER

These are the people who have charge of the organization's backup data while it's being taken to off-site storage. Do they know how to keep the tapes or other media in sight at all times? What if they leave it on a desk during a delivery to another location? What if they leave them in the delivery vehicle and they are stolen? These are huge risks to an organization's data that need to be addressed. As a result, these folks need to be included in the security awareness training.

## EVERYONE IS RESPONSIBLE FOR SECURITY

Users by the nature of their job duties inherit certain risks. Treating everyone the same, regardless of education level or user role, is a huge mistake. Highly educated professionals such as doctors, lawyers, accountants, and college professors can be the hardest groups to target for security awareness training because they feel their years of education have made them immune to social engineering tricks. Yet many of these professionals, especially lawyers, are being

targeted because security programs and security awareness programs have been overlooked as a priority.

In recent years, Chinese hackers have targeted Toronto's Bay Street law firm to derail a $40 billion acquisition of the world's largest potash producer [1]. In November 2013, a Pittsburgh man was sentenced for "recklessly damaging a computer and password trafficking" in a case that involved a law firm's computer system [2]. As late as 2012, the FBI has warned lawyers that their firms need to increase their security because they were being targeted [3].

It's not just lawyers, accountants are being targeted as well [4]. Many professional organizations are repositories of confidential information, thus becoming targets. In May 2014, the Justice Department issued a 31-count indictment of five Chinese military officers for breaking into the networks of six American corporations to steal intellectual property. The data were worth billions of dollars accounting to the indictments.

> "For years the Chinese—especially, but not exclusively, a Shanghai-based department of the People's Liberation Army called Unit 61398 (where all of the indicted officers work)—have been hacking into the computer networks of U.S. corporations, defense firms, and financial institutions. President Obama and a few Cabinet secretaries have raised the issue in several diplomatic forums. Each time, Chinese officials have denied the charges and challenged the Americans to produce some evidence. The indictment is, in this sense, the reply: Here is the evidence—and in staggering detail" [5].

Threats such as Chinese hackers and industrial espionage do not ring true with all employees of an organization. The mailroom staff, secretaries, and receptionist, for example, have very little concept of what industrial espionage or intellectual property is, let alone how to protect it. As a result, attackers will use this knowledge gap in the form of phishing, infected attachments, and other social engineering to exploit these users and then pivot their attacks to steal the data they are after. We have already made receptionist security guards; now we make mailroom staff, secretaries, and other support staff network defenders through an effective security awareness program.

With the proliferation of social media sites and the proliferation of social engineering attacks and scams on social media, the risk is more than just clicking links in e-mail and opening the wrong attachment. There is also the risk that the confidential and privileged information that might aid an attacker might be posted to social media. Many users pick passwords based on information such as their pet's name, their spouse's name, their birth date, or other information that an attacker can find on social media. Users can also unintentionally reveal operational details of the organization such as the location of branch offices or the type of antivirus software installed on the organization's computers. While

most people think of the traditional sites for social networking such as Twitter and Facebook, there are literally hundreds of social networking sites that users might be using [6,7]. In the case of LinkedIn, the service actually caters to business networking. Beyond data leakage, these sites can house malware. Since anyone can typically upload any code they want to these sites, social media sites have been the points of infections for zero days in the past [8]. With the prevalent use of social media in originations at all levels, informing users of the threats that exist on social media platforms and how to detect and avoid them is especially important.

In the case of midlevel managers and at higher levels in the organization, it can be useful to point out the financial harm a data breach can cause an organization. The recent breach at Target shows how a company can suffer financially and how repercussions can extend to people losing their jobs [9]. No one wants to be involved in a resume-generating event. Target has experienced a large amount of financial pain that has been directly linked to the breach from low earnings to the cost of ongoing litigation related to the breach [10,11]. The Target breach is remarkable because it is the first clear-cut and well-publicized case of a retailer suffering large financial losses as a result of the credit card breach. During the TJX breach in 2007, the stock actually rose after initial losses, and the stock has continued to do well over time. TJX remains one of the largest breaches in history [12,13].

In the case of employees, it is important to emphasize the amount of personal information the organization collects about them in order to pay them and provide them and their dependents with medical and other insurances. When risk is made personal, more people will take notice of the importance of securing the organization's data because it has now been explained how a breach could also affect their personal data. People check their bank accounts from work, shop from work, and have pictures of their loved ones stored on their computer. How would they feel if the flight reservations of their college-aged daughter ended up in the wrong hands?

When risks and the consequences of a breach are personalized, compliance with policies that keeps information safe will increase. No matter what our position in our respective organizations, we are all network defenders.

## Notes

[1] China-Based Hackers Target Law Firms to Get Secret Deal Data. http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html [accessed on 22.05.2014].

[2] Pittsburgh Man Sentenced for Role in Law Firm Hack. http://www.fbi.gov/pittsburgh/press-releases/2013/pittsburgh-man-sentenced-for-role-in-law-firm-hack [accessed on 22.05.2014].

[3] China-Based Hackers Target Law Firms to Get Secret Deal Data. http://www.bloomberg.com/news/2012-01-31/china-based-hackers-target-law-firms.html [accessed on 23.05.2014].

[4] Security Issues for Accountants. http://www.lagfoa.org/Security-Issues-for-Accountants.pdf [accessed on 23.05.2014].

[5] Why Did the Justice Department Indict Five Chinese Military Officers? http://www.slate.com/articles/news_and_politics/war_stories/2014/05/justice_department_indicts_five_chinese_military_officers_can_the_obama.html [accessed on 23.05.2014].

[6] Beyond Facebook: 74 Popular Social Networks Worldwide http://www.practicalecommerce.com/articles/2701-Beyond-Facebook-74-Popular-Social-Networks-Worldwide [accessed on 26.05.2014].

[7] List of social networking websites http://en.wikipedia.org/wiki/List_of_social_networking_websites [accessed on 26.05.2014].

[8] Details Emerge On Latest Adobe Flash Zero-Day Exploit http://threatpost.com/details-emerge-on-latest-adobe-flash-zero-day-exploit/104068 [accessed on 26.05.2014].

[9] Target CIO resigns following breach. http://www.computerworld.com/s/article/9246773/Target_CIO_resigns_following_breach [accessed on 24.05.2014].

[10] Target Earnings Show Pain of Data Breach Is Far From Over http://www.businessweek.com/articles/2014-05-21/target-earnings-show-pain-of-data-breach-is-far-from-over [accessed on 26.05.2014].

[11] Target Faces Nearly 70 Lawsuits Over Breach http://blogs.wsj.com/riskandcompliance/2014/01/15/target-faces-nearly-70-lawsuits-over-breach/ [accessed on 24.05.2014].

[12] Giant Retailer Reveals Customer Data Breach http://online.wsj.com/news/articles/SB11690615328207923 [accessed on 24.05.2014].

[13] Yahoo Finance: TJX Stock Chart http://finance.yahoo.com/echarts?s=TJX+Interactive#symbol=TJX;range=my [accessed on 24.05.2014].