Realtime
publishers

The Shortcut Guide™ *To*

Business Security Measures Using SSL

Dan Sullivan

Copyright Statement

This sponsored eBook is valid until July 12, 2012.

Realtime
publishers

Chapter 2: Common Vulnerabilities in Business IT Systems

Businesses, governments, and other organizations face a wide array of information security risks. Some threaten the confidentiality of private information, some threaten the integrity of data and operations, and still others threaten to disrupt availability of critical systems. Chapter 1 examined the role of organized cybercrime, the prevalence of malicious software and the underground marketplaces that facilitate the exchange of stolen information, and tools of the cybercrime trade. In this chapter we turn our attention inside the organization. Although the external threats are considerable, they are not the only component in the risk equation. Another important set of factors are the vulnerabilities that lie within an organization.

For our purposes, we will broadly organize these vulnerabilities into two categories: technical weaknesses and organizational weaknesses. This specification is to draw attention to the fact that information security is not just about technology, although that is an obvious component. How we perform business operations, how we attend to information systems management, and how we train and help others understand the nature of security risks can make a critical difference in the overall effectiveness of an information security strategy. Perhaps more importantly, it is crucial to understand that technical controls will not compensate for poor organizational practices, and the best trained staff and most well intentioned IT professionals will not be able to protect information assets without proper technical controls. An overall security posture is a combination of technical and organizational controls.
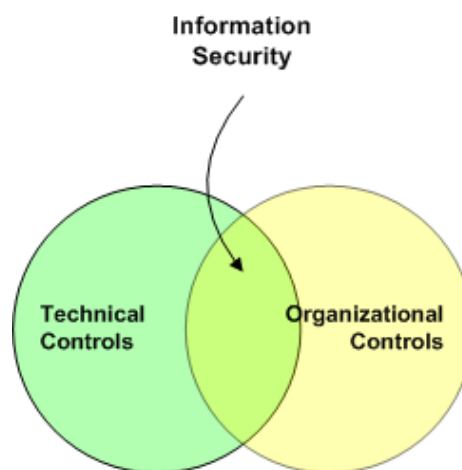
Figure 2.1: Technical and organizational controls overlap and are both essential to information security.

This chapter will examine common weaknesses in technical and organizational controls and then discuss options for addressing those weaknesses.

Technical Weaknesses

Technical weaknesses are vulnerabilities that can be mitigated using technical controls, such as the implementation of new firewall rules or an update of antivirus signatures on a client device. There are many different types of such vulnerabilities; we will concentrate on several that are all too common:

- Unencrypted communications

- Insufficiently patched operating systems (OSs) and applications

- Insufficient use of antivirus and personal firewalls

- Weak boundary security

- Poor application security

For each of these, let's consider types of attacks enabled by these vulnerabilities and their cost to business.

Unencrypted Communications

Rapid, reliable, and trustworthy communications are essential in today's business world. Although postal mail and telephones are still used widely, some of the most cost-effective communications take place online. We routinely email colleagues, customers, clients, and other professional and personal contacts. Instant messaging is especially useful for geographically distributed teams who need an electronic equivalent of talking across the room or over the top of a cubicle partition. Many have taken to social networking services, from LinkedIn and Facebook to Twitter, to keep up to date with large groups of individuals. All these communication mechanisms have their advantages and few would want to ban them from the office, but with their convenience and efficiency comes security risks.

When communications are transmitted in unencrypted forms—such as plain text—there is the potential for someone to intercept the message to learn the contents or tamper with the contents before they arrive at the intended recipient's inbox. We will consider two examples of such attacks: the man-in-the-middle (MITM) attack and the replay attack.

Man-in-the-Middle Attack

An MITM attack injects a malicious third party into a communication between two presumably unsuspecting victims. The purpose of the attack is to control the communications between the two victims and alter messages between them. Several conditions must be in place for an MITM attack to succeed:

- The attacker must have access to the communication channel between the two parties

- The attacker must be able to impersonate each of the victims sufficiently to overcome technical controls and potential suspicions on the part of either victim.

- The attacker must be able to alter, inject, or remove messages sent on the communication channel without detection

Accessing communication channels used to require access to wired network equipment, such as routers or hubs, but the prevalence of wireless networks allows attackers to gain access to a communication channel from a distance.

Actual Communications Channel

Actual Communications Channel

Apparent Communications Channel
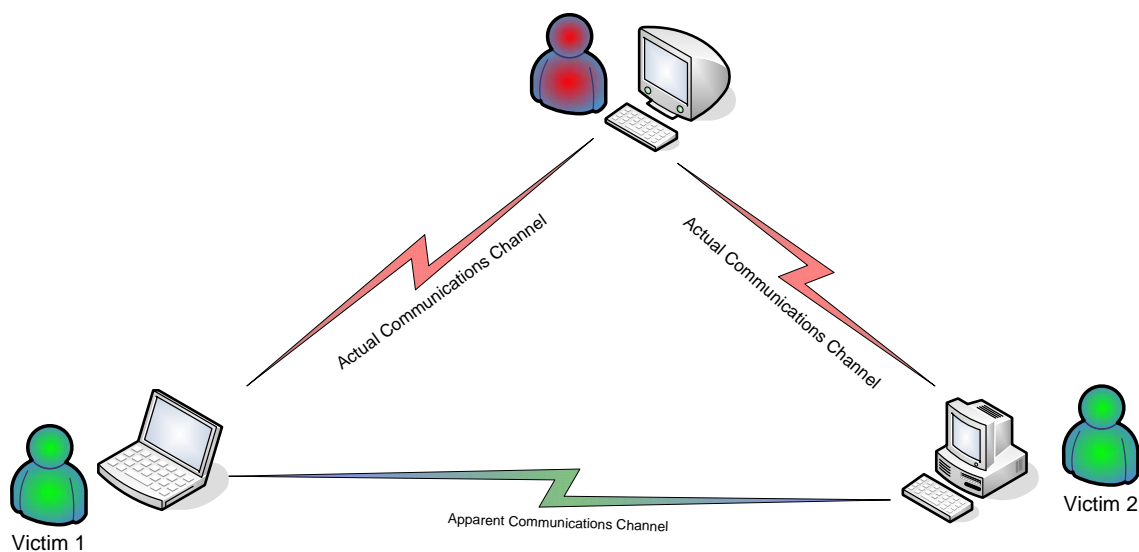
Victim 1

Victim 2

Figure 2.2: MITM attacks inject a malicious third party into a communications channel with the intent of reading and tampering with messages sent between victims.

To impersonate both victims, the attacker needs to overcome any technical controls in place. For example, unless authentication mechanisms are in place, such as those used in SSL-based communications, it is possible for an attacker to spoof, or impersonate, the victims. SSL communications can use a combination of public and private pieces of information known as keys to authenticate the parties in communication, so an attacker would need access to the private keys of both victims to carry out a successful MITM attack.

Note

SSL and Transport Layer Security (TLS) use both symmetric and asymmetric cryptography. Asymmetric encryption is used for authentication while symmetric encryption is used for large data transfers, as it is computationally more efficient. It is conceivable that an MITM attack could occur by breaking the symmetric key encryption after authentication has occurred. The use of strong symmetric encryption algorithms, such as the Advanced Encryption Standard (AES), makes that highly unlikely.

In addition to overcoming technical controls, the content of the messages injected by the attacker must be believable enough to convince the victim they are authentic. This is not difficult, especially in business communications where many exchanges are standardized. For example, it would not be difficult to change quantities on an order or replace a credit card number with another legitimate credit card number without raising suspicion.

Replay Attack

A replay attack is a type of MITM attack in which a message is captured by a malicious third party and resent or replayed for the target victim. For example, if Alice was to send a message to Bob saying "Send 100 widgets to Charles and charge to my account" and that message was captured by an attacker, the attacker could then resend the message to Bob. Bob in turn would then have orders to send a total of 200 widgets to Charles and charge them all to Alice. In a more realistic example, the message would be a structured transaction following a well-defined protocol, but the point is that unprotected messages can be captured and used again in unintended ways.

One way to protect against replay attacks is to use some type of session variable. For example, each message from Alice to Bob would include a message counter. The message counter is incremented after each transaction is sent. If this technique were used, Bob would recognize the second message sent by the attacker was a repeat of the first message and could safely ignore it. However, if the message transmission is in plain text (that is, unencrypted), the attacker could simply change the value of the message counter.

Alice and Bob might try to outwit eavesdroppers by having a non-obvious pattern in the way they increment the counter. Instead of incrementing the message counter by one, they might increment by 2, 101, the number of the day of the month of the transaction, or any other pattern. Unless the attacker knows the proper increment, the expected message counter would be incorrect and the recipient would recognize the message as invalid. Attackers could solve this problem by monitoring traffic between Alice and Bob until they have enough sample transactions to determine the rule for incrementing the message counter.

This simple example illustrates how "homegrown" solutions to protecting confidentiality can break down. Cryptography, the study and development of encryption algorithms, is a science as is cryptanalysis, the study of code breaking. It is highly unlikely that someone other than a specialist in cryptography could develop a sufficiently difficult-to-crack algorithm to warrant attempts at such development. A better solution is to use public algorithms, such as AES. Confidentiality is assured by a combination of the strength of the algorithm, which is publicly known, and the keys, which are kept private, used to encrypt messages.

```
<Order>
  <Message-Counter>18763</Message-Counter>
  <Bill-To>
    <Company-Name>ABC Enterprises</Company-
Name>
    <Address>1010 Main St. Springfield, IL 62701</
Address>
    <Account>ABC123456</Account>
  <Bill-To>
  <Items>
      <Item>
    <Part-Number>XY7631</Part-Number>
    <Quantity>12</Quantity>
    </Item>
    <Item>
    <Part-Number>NN8123</Part-Number>
    <Quantity>12</Quantity>
    </Item>
  </Items>
  <Message-Counter>18763</Message-Counter>
  </Bill-To>
</Order>
```

Encryption Key (Private)

Plain Text Message (Private)

Encryption Algorithm (Public)

```
CB1D029FC2641D086C285110158AF585
A14745BE97068660AF08E6AAC9ABC27E
23DBDF4DF6353D0C3E7D391209F54F26
89B50B409A198F303BD7F6273D1A580E
70BA585857B026A8173B6D74F9F2502C
6038C7CBD1802BD5799495C13E44D5A9
41CFDB83DBA2ED159E135F266E60A288
51F3B61E7826B83DC6F135B44AE0B4E0
4E8BAD08B9DFF7C28BE5AE040F0930E1
593B7B4ECFB9FEDC902AD5A485EB46DC
B0C81BA5AD21B7E0882BFC14A47697EF
70BA585857B026A8E2721822D39E9772
C5AB90DB738C8C1E2E3E8A20FD9E94BA
7FA1488B5783B8885351B790AA0589CD
CD9531F3851114A81BEA99448E1FA075
B847423AAEBA525C4448C77BAF0CA434
414D5982C6F61B95B19BA54F514BDAB9
3D277181201457F64C22BFC26FA6C933
```
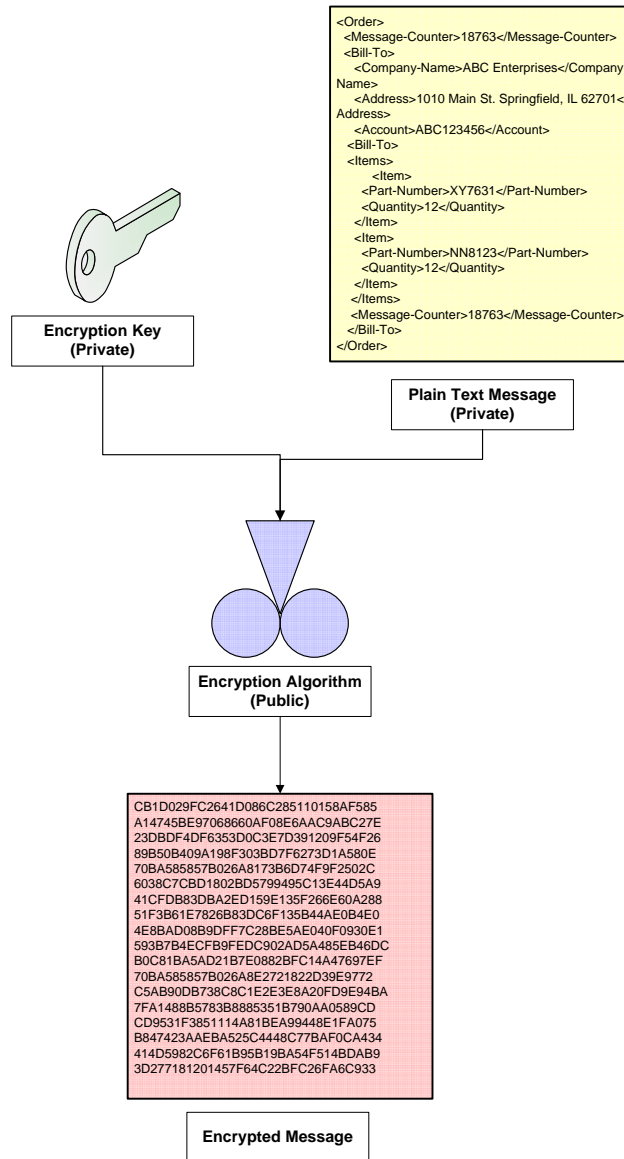
Encrypted Message

Figure 2.3: Confidentiality is ensured if a message and the encryption key are kept secret; there is no need to use a secret or home grown algorithm. In fact, public algorithms are subject to a great deal of cryptanalysis scrutiny and are more likely to provide codes that cannot be broken in a reasonable amount of time with reasonable resources.

MITM and replay attacks could be quite costly to businesses for two reasons. First, individual transactions could be repeated or tampered with as a means to commit fraud. The potential cost of a single act of fraud may be great enough on its own to justify implementing stronger security measures, such as using SSL for all business-essential communications. Perhaps a greater reason for concern is that without SSL encryption, *any* electronic communications could be called into question. This position is extreme but the lack of trust in communications systems could undermine business operations and efficiencies. Will salespersons call customers on the phone to verify electronically submitted orders? The use of a second means of communication, known as *out-of-channel communications*, is one way to reduce potential fraud, but it is highly inefficient for both parties. Securing communications with SSL-based communications is more efficient and practical for business operations.

Encrypting message transmissions protects data in motion. Data at rest and the servers and other devices used to store and process that data require additional technical controls to provide sufficient security for typical business operations.

Insufficiently Patched OSs and Applications

One of the most memorable malware attacks to broadly impact the Internet hit in January 2003. The SQL Slammer worm spread across the globe and infected tens of thousands of machines in minutes. The worm's Denial of Service (DoS) attack slowed Internet traffic and effectively blocked traffic on some segments. The malware took advantage of a vulnerability in the SQL Server database and the Microsoft SQL Server Desktop Engine. Microsoft had released a patch 6 months before the attack; unfortunately, many users of the affected systems did not patch their systems.

Although the impact of SQL Slammer was quite dramatic, the existence of program vulnerabilities is far from rare. The National Vulnerability Database (http://nvd.nist.gov/home.cfm), which tracks known vulnerabilities, listed 35,142 software vulnerabilities as of early February 2009, publishing on an average of 15 vulnerabilities per day. Vulnerabilities are not limited to popular databases and OSs; consider some of the vulnerabilities discovered over the past few years in widely used applications:

- Internet Explorer—A vulnerability in IE could allow remote code execution (Microsoft Security Advisory 961051).

- Microsoft Access—A vulnerability in an ActiveX Control could allow remote code execution(Microsoft Security Advisory 955179)

- Microsoft Excel—A vulnerability in Excel could allow remote code execution (Microsoft Security Advisory 947563)

- Xterm (Linux)—The default configuration of xterm on Debian GNU/Linux, and possibly Ubuntu, could potentially allow arbitrary code execution (CVE-2006-7236)

The cost of unpatched systems to businesses can be significant. As the example vulnerabilities highlighted in the previously list show, commonly deployed applications can be used to execute arbitrary code. When malicious code can be executed with administrator or root privileges, it is difficult if not impossible to prevent an attacker from gaining control of a device. Unpatched applications can provide attackers with a stepping stone to committing data breaches, tampering with databases, or denying access to mission-critical applications.
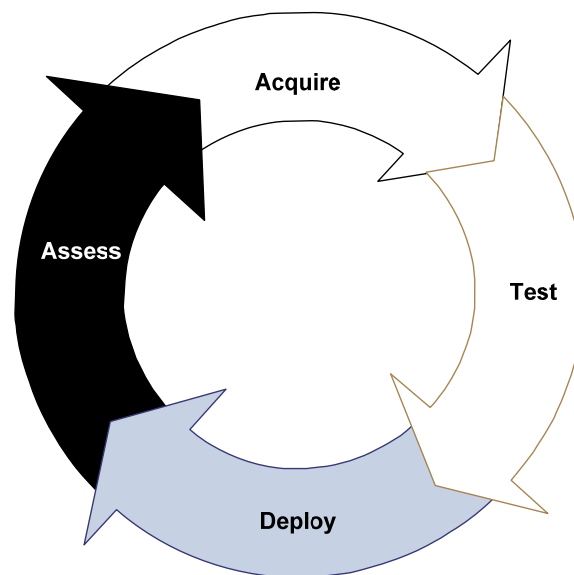
Figure 2.4: The patch management cycle starts with acquiring patches from vendors and other sources, testing them to ensure critical functions are maintained, deployed to devices, and assessed in operations.

Keeping track of applications, versions, configurations, and patch levels is challenging but a set of practices known as the patch management cycle (see Figure 2.4) is designed to address these challenges. The key steps in the patch management cycle are (1) acquiring the patch, (2) testing the patch in a controlled environment, (3) deploying the patch to production systems, and (4) assessing any problems with a patch deployment. Asset management systems can improve the efficiency of patching by automatically pushing patches to devices and providing reports on the status of patch operations. Hardware vendors are improving remote device manageability through offerings such as Intel's vPro and AMD's support for the desktop and mobile architecture for system hardware (DASH); asset management and patch management tools may take advantage of these for additional efficiency improvements.

The same tools that help with patch management can also help with another typical technical weakness.

Insufficient Use of Antivirus and Personal Firewalls

Using antivirus software is like driving with seat belts—we all know we should use the precautionary measure. The analogy quickly breaks down though. Although we rarely need seat belts because most of us have few if any accidents, most users are likely to encounter malicious software. Part of the problem is the prevalence of malware.

Malware can infect devices from multiple points of entry into a system:

- Malware attached to emails

- Malware-infected media files, such as video and music files

- Malware downloaded when visiting a compromised Web site, a technique known as a "drive-by download"

- Malware transmitted from another infected machine on the network using weaknesses in firewall configurations or network vulnerabilities to infect other devices

Anti-malware vendors are constantly updating signature-detection database and behavior-analysis systems used to detect malware. Like application and OS patching, anti-malware software has to be routinely updated to counter new and emerging threats. Malware developers know this, and some malware includes code to block updates. Sometimes the blocking techniques are simple, such as editing a local file used to map domain names to IP addresses, so antivirus software is directed not to the vendor's update site but to another non-functional site (thus, updates are never downloaded).

Personal firewalls can help stem the spread of malware by blocking traffic on ports that are not needed for legitimate purposes. This can, for example, prevent worms from accessing a device via a blocked port; it can also block outbound traffic, such as spam generated by a bot that has already infected the machine. Low-cost and free personal firewalls are readily available for Windows; Mac OS X and most Linux distributions include firewalls. Proper firewall configuration can provide an additional layer of security on devices.

The cost of insufficient use of antivirus and personal firewalls is manifested in poor performance in devices, unnecessary consumption of bandwidth in the case of devices infected with botnet software, increased demand for Help desk service to diagnose performance problems, and the cost of removing malware once it is detected.

Keyloggers and video frame grabbers are particularly dangerous types of malware. These not only compromise the systems they infect but also are designed to steal information, such as login credentials or confidential information, and transmit it to a point where the attacker can retrieve it. One of the reasons passwords and other authentication mechanisms should be updated frequently is because they may be leaked or stolen. Credit cards, drivers' licenses, and digital certificates all use expiration dates because something can go wrong and those artifacts, for whatever reason, cannot be trusted. Credit card and drivers' license issuers cannot go into the field and retrieve the cards (at least in any practical sense). Similarly, we cannot recover stolen passwords. Malware is just one of the reasons to frequently change authentication information.

Weak Boundary Security

As systems become more distributed and we adapt more service-oriented architectures, we find the need to move data further and sometimes across organizational boundaries. This practice is undermining the traditional notion of the network perimeter.

In the past, a company may have had all traffic moving over a firewall between the internal network and the Internet. Traffic across this boundary was restricted to those protocols needed for Web browsing, email, and instant messaging. Today, companies may have

- A database hosted by a third-party site with database protocols used to exchange data between client and server

- Internal applications invoking Web services provided by business partners; confidential data is moved back and forth between these two systems (in which case, digital certificates should be used to authenticate the partner's Web service and SSL should be used for communications)

- Remote users connecting to the corporate network using virtual private networks (VPNs)

Network perimeters today are more porous than they have been in the past. Now rather than depending too heavily on boundary security, we must have multiple layers of overlapping security (known as defense in depth) to protect data and systems. This security includes implementing technical controls to avoid the common weaknesses described in this section as well as securing data at rest and in motion with the use of encryption. Organizations that do not address the boundary security requirements risk well-known problems, including data breaches, compromised devices, and the potential loss of computing and network services.

We must be careful not to confuse information security with just network security; applications are another broad area of concern in information security.

Poor Application Security

It is somewhat ironic that improvements in our ability to protect OSs and network devices have led to a heightened awareness of application vulnerabilities. Like water seeking the lowest level, attackers look for the easiest way to reach their target. Today, the target is often information. Application vulnerabilities include:

- Injection flaws, such as SQL injection attacks in which SQL commands are sent as part of input data

- Cross-site scripting attacks, which allow attackers to execute scripts within the context of a user's browser

- Poorly managed authentication in distributed applications that allow, for example, a victim's username and passwords to be stolen

- Insecure communications, in which private and confidential information is sent in unencrypted or easily decrypted form

All of these and other common application vulnerabilities can be avoided with sound coding and software engineering practices.

> **Note**
> For more information about application security, especially Web applications, see the Open Web Application Security Project (OWASP) at http://www.owasp.org.

Automated application vulnerability scanning can help identify vulnerabilities in deployed applications and pre-deployment code. Some scanners work with source code using static analysis to identify weaknesses apparent from the structure of code, such as potential out-of-bounds references; other scanners perform dynamic analysis and probe applications for vulnerabilities while they run. The latter is especially useful when source code is not available.

As noted earlier, even widely used applications can contain vulnerabilities. Businesses, government agencies, and others can mitigate the risk and potentially avoid the cost of having application vulnerabilities exploited if they are detected before the system is moved into production. It is also less disruptive and more cost effective to correct problems as early as possible in the software development life cycle.

It should also be noted that incorrect configurations can lead to application vulnerabilities. Using default configuration and default passwords, for example, provide an easy way for attackers to get started compromising an application. As a general rule, configurations should implement only functions needed by business requirements. The more subsystems enabled in an application, the greater the surface area for an attack. Each unnecessary subsystem may bring with it vulnerabilities that can be leveraged by attackers.

This section has highlighted some of the technical weaknesses that can undermine information security. Not surprisingly, these weaknesses span the breadth of IT infrastructure from network architecture to endpoint devices to the ways we transmit sensitive and confidential information. Weaknesses, however, are not limited to technical issues.

Organizational Weaknesses

In many respects, the challenges of implementing and managing effective technical controls pale in comparison with the difficulties in addressing organizational weaknesses, such as insufficient or ineffective security awareness training. This section will consider how end user security training, security policies governing mobile devices, and the inappropriate use of business computers and networks can result in security vulnerabilities.

End User Training and Security Awareness

Technical controls alone will never constitute a comprehensive security strategy. Humans can override, alter, disconnect, turn off, and ignore technical controls. Technology is a supporting part of security controls; it is not the full picture; thus, it is imperative that employees, contractors, consultants, and business partners understand their role in the information security mosaic that protects business assets and data.

To get a sense of just how difficult it is to mitigate vulnerabilities related to the human factor in IT security, consider some of the findings of a 2008 survey by Cisco and Insight Express on data leaks (Source:http://cisco.com/en/US/solutions/collateral/ns170/ns896/ns895/Cisco_STL_Data_Leakage_2008.pdf). Some of the more telling findings include:

- 10% of surveyed employees have stolen or know of other employees who have stolen data or devices

- 10% of employees have lost or were the victims of theft of a company-issued computer, mobile device, or portable storage device containing corporate data in the past 12 months

- 11% of US IT decision makers indicate their company has suffered a data breach that included the theft of company data

- The top three concerns for data leaks are, in order: portable USB drives, email, and stolen laptops

Realtime
publishers

These statistics demonstrate the widespread ignorance of sound security practices with regards to computer use or a disregard for those practices. Such breadth of weakness is not necessary to create a significant risk. For example, that same survey found that 14% of global respondents had changed security settings on their computers; 2% of US respondents had done so. Of those that did make changes, half of them admitted they did so to visit sites regardless of their company's policy, and more than one-third felt it was not the concern of their company if they did change security settings on company-issued devices! Like a chain that is only as strong as its weakest link, a small number of employees with cavalier attitudes are enough to compromise security.

Statistics such as these and anecdotal evidence about lost laptops, simplistic phishing lures, and irresponsible behaviors have led to a couple of myths about end user security awareness training that need to be dispelled.

End User Training Myths
Unfounded myths about users and their willingness or need to learn undermine an appreciation for what is necessary to improve the human factor components of information security.

Myth #1: "If security training worked, it would have worked by now."

This fatalistic view only rings true if we assume that our training methods are sufficient and we do not need to try other approaches. Widespread public health campaigns, such as anti-smoking efforts, and public safety campaigns, such as promoting the use of seat belts, have largely succeeded and can offer guidance on how to proceed. These successful campaigns are continuous and long running. Anti-smoking efforts that started in the late 1960s and early 1970s continue to some degree today. It is difficult to drive across state lines in the US without seeing signs to buckle up. Successful campaigns use a combination of techniques to get their point across, including humor. Talking crash test dummies taught us about car collisions. The point is that we should not give up on training employees about security because past methods have not worked; we can learn from others' successes.

Myth #2: "Younger workers are more tech savvy and therefore more skeptical of scams and do not need security training."

The idea that one generation will not repeat the mistakes of previous generations is appealing but lacks sufficient evidence to be believed. More importantly, social engineering attacks, malware, hacking techniques, and anti-forensic techniques are constantly changing. Some of us will not be tempted by a phishing scam promising extraordinary returns if we just send money to a foreign national in a temporary bind; that is no reason to assume we are immune to other scams or that we know all the ways attackers can infect a device with malware. Drive-by downloads from compromised Web sites were not known 10 years ago; why should we think that 10 years from now new techniques won't stump today's tech-savvy generation?

The impact on business, including the cost, of insufficient and ineffective end user training could be measured in computers infected with malware from sites users should not have visited, leaked information given in response to phishing lures that should have been ignored, and inaccurate data left after a disgruntled employee gained access to data using someone else's account left open after hours.

Lax Security with Mobile Devices

Mobile devices require both technical and organizational controls. Antivirus, personal firewalls, and vulnerability scanning (at least with tools such as the Microsoft Baseline Security Analyzer available at http://technet.microsoft.com/en-us/security/cc184923.aspx) fall on the technical side of the equation. Once again, the more difficult challenges come on the organizational side of things.

Part of the challenge with lax security with mobile devices is that employees are not aware of risks to mobile devices. The Privacy Clearinghouse Chronology of Data Breaches (http://www.privacyrights.org/ar/ChronDataBreaches.htm) has plenty of examples of stolen laptops containing tens of thousands of database records containing personal information. As more smartphones are used to access and store data, there will be more opportunity for confidential information to be lost or stolen. Employees should be trained in reasonable procedures for protecting mobile devices when they are in cars (a popular target) and in the use of encryption to prevent data from falling into the hands of thieves if a device is stolen.

Another problem, one that gets less attention, is the growing use of personal mobile devices in the workplace. Employees may purchase Blackberry and iPhone smartphones on their own and use them to access corporate data. These devices are not owned by the company, so there are limits to what the company can dictate while still allowing these devices to access corporate repositories. Consider how policies may need to be re-worked to accommodate these devices:

- If these devices were company owned, they could be standardized; however, the company may not want to limit access to only those with a particular device type or OS.

- As these are personal devices, companies may not be able to dictate how they are used when not accessing corporate systems. Sites that may be blocked from corporate networks may be readily accessible from a smartphone also used to access confidential data.

- Companies may have a policy dictating minimum security measures for an employee-owned device used on the corporate network but may not have the means to enforce that policy. For example, a policy may dictate up-to-date antivirus signatures but not be able to verify a configuration before allowing a user to download data to their device.

Here again, we have an example where technical controls are not enough. We need educated and cooperative employees who understand and follow policies. The cost to business, and presumably an employee's career, can be significant if a data breach is traced to a poorly-secured, personally-owned smartphone.

Inappropriate Use of Business Computers and Network Services

A final example or an organizational vulnerability is the improper use of computers and network services. Some might try to look at this from a lost productivity standpoint—if an employee is checking personal email or ordering personal items online, they are not productive from the company's perspective. However, it is equally plausible to argue that use of company systems allows an employee to attend to personal errands more efficiently and therefore leaves them more time to focus on their work. There is no universal formula for finding the proper balance, but we can reasonably conjecture that one exists. A more pressing problem than unproductive time is the potential to introduce malicious software on the network.

If an employee checks a personal email account, there may not be the same filters that are applied to the corporate email system, thus allowing malicious software to enter the network via email. Similarly, employees browsing to non-work-related sites can result in drive by downloading of malware. These sites are not just those considered inappropriate for the workplace; legitimate popular sites, such as news sites, could be compromised because of vulnerabilities in their systems which in turn result in an adverse impact on your network. The service support staff probably has enough to do without having to clean up a botnet infection on the corporate network because an employee surfed somewhere she did not belong.

Organizational weaknesses generally stem from human behavior. Changing human behavior is an art that may never be mastered. Nonetheless, helping employees understand the nature of security threats and their role in protecting the company's assets as well as themselves is the starting point to mitigating organizational weaknesses.

Options for Addressing These Threats

Broadly speaking, there are three approaches to dealing with technical and organizational weaknesses. There is always the option of doing nothing, or more properly, the option of continuing to function as is. At best, one can reasonably presume that the organization would continue with the same levels of risks. If there have been no major breaches, confidential communications have not been intercepted, and malware outbreaks are infrequent, this might seem like a prudent course of action. The problem with this scenario is that it assumes the overall security and business environment will stay the same. We know that is not true. Malware has become more difficult to detect, it spreads by more methods, the size of major data breaches is increasing, and cybercriminals appear to be getting better at covering their tracks during an attack.

At the other end of the spectrum is the spare-no-expense approach. Even in the best of economic conditions, this is not reasonable. We cannot simply buy security systems and deploy end point security applications like buck shot in the hopes of hitting all the weaknesses in our network.

A balanced approach is, not surprisingly, the one that is called for. We cannot let fear of security threats keep us from aligning security strategy with business strategy. One of the hallmarks of this alignment is identifying risks to the business strategy and then implementing a combination of technical and organizational controls.

The amount we spend on security should not exceed the value of the assets we are trying to protect and the costs incurred by the organization in the event of a breach. Losing a patient record may not directly cost a hospital, but it may have significant cost to a patient whose identity is stolen and could have detrimental impact on the trustworthiness of the hospital and its brand reputation. Regulations internalize some of those costs which were previously borne by those outside the organization. A risk assessment can help illuminate the assets we need to protect, the threats to those assets, and various combinations of technical and organizational controls that can help mitigate threats to those assets.

Summary

Sometimes we can be our own worst enemy. How we address technical and organizational weaknesses inside the organization can help or hinder our overall goals. Security is a function of technical controls, such as SSL for secure communications and disk encryption for reducing the risk of data compromise, and organizational controls, such as sufficient and effective training and realistic policies that account for changing ways employees access and use data. A balanced approach is based on risk management practices and incorporates both technical and organizational controls; this method can help mitigate risks while accounting for limited resources.

Realtime
publishers