Information Security for Small Businesses

Russell Morgan

Abstract—New technology allows small businesses to use many of the same information systems employed by large enterprises. In doing so small businesses open themselves up to many threats that were traditionally associated with large corporations. It is imperative to their continued success that they recognize these pitfalls and take steps to address this issue. This paper examines some of those threats and offers some solutions for the problems.

I. INTRODUCTION

Due to technological advances, the rapid growth of the Internet, and a significant decline in computer and network equipment prices in recent years, many technologies and systems that were once only available to large corporations are now employed by the small business community [1]. Thanks to the Internet and the world of e-commerce, small businesses can dramatically increase their customer base and reach new markets by selling their products and services online.

Employing more technology to reach these new markets opens up the small business to a myriad of problems. As noted by Paul Kurtz of the Cyber Security Industry Alliance (CSIA), “The potential for e-commerce is enormous. The next round of innovation and services on the Internet can only grow if home users and small businesses are confident in their information systems. Security is perhaps the greatest obstacle to the expansion of online commerce and services.” [4]

Some of the threats to security are attacks by hackers, viruses, worms, and spyware along with a host of other related dangers. When a company makes a decision to secure their information assets it is important they understand the concept of information security. This concept can be traced to the early days of mainframe computing. The Committee on National Security Systems (CNSS) defines “information security as the protection of information and its critical elements, including the systems and hardware that use, store, and transmit that information.” The CNSS is based on the CIA triangle which itself is founded on the principles of confidentiality, integrity and availability [12]. A breakdown of any aspect of the CIA triangle leads to compromised data and can shut down the company’s computer systems or expose valuable data to unauthorized parties.

While many companies focus on the more publicized threats of hackers, worms, and viruses by installing security devices such as firewalls, they often overlook other factors [2]. Some of the overlooked factors are disaster recovery from both hardware failures and natural disasters and the threat posed by employees or ex-employees. Data theft or sabotage can be just as devastating, if not more so, than a physical or natural disaster.

It is understood that small businesses are the backbone of the economy in the United States. They “represent 99 percent of all employers, employ 52 percent of all private workers, and provide 51 percent of the private sector output.”[10] Based on these facts, it is easy to see why small business should be more observant of their information technology security needs.

This paper will look at the security problems facing small businesses, potential impacts of security breaches and offer suggestions for solutions on how to address the issues.

II. IN DEPTH ANALYSIS OF THE PROBLEM

A. Internet related threats

A recent survey shows that a new broadband connection can expect up to three attempts at unauthorized access within the first 48 hours of its operation. Attaching this same computer to a local area network only increases this risk [3]. Due to the open nature of the Internet, there are virtually no built in security controls and Cyber theft is now a lucrative business. Some of the threats from the Internet are viruses, worms, spyware, spam, phishing scams, hackers and bot networks.

Viruses are the most well-known and destructive problems businesses face. Viruses generally travel via e-mail messages. There are many different kinds of viruses. Some merely reproduce themselves and are more nuisance than actual problem. Others, however, can actually destroy data or otherwise render the computer useless. Some of the highest profile viruses are Nimda, Melissa, and I Love You.

The next major threat is worms. While they are closely related to viruses, they do not usually require human interaction to spread. Worms travel on networks, taking advantage of flaws in programs to replicate themselves and spread from computer to computer without any human help and can cause so much traffic that they shut down networks.

Spyware has caused much debate among the IT community as to what programs are actually spyware. One traditional definition for spyware is software that installs itself on a computer without the knowledge of the user and accesses information from applications running on the computer. Newer forms of spyware include programs such as keystroke loggers. These programs are designed specifically to steal personal information such as logon information to Internet banking sites. It is hard to detect many key logging programs
so this is one of the more dangerous threats to information security.

Although not a security risk in the traditional sense Spam is a problem nonetheless. Spam is generally considered to be unwanted commercial e-mail [16]. Many organizations receive so much of this unwanted e-mail that it shuts down e-mail servers and causes delays in business. This is a compromise of the availability part of the CIA triangle.

Phishing scams are among the newer methods of attacking company or personal information. These scams are generally in the form of fake e-mails claiming to be from legitimate sources such as Citibank, Pay-Pal or other well-known financial organizations. The goal of these e-mails is to get the user to click a link, which takes them to a phony web site that most of the time, looks very similar to the legitimate site. These fake sites ask the user to enter personal, or possibly company, information relating to bank accounts. Once this information has been harvested it can be used to drain the company or user’s bank account.

One of the biggest traditional fears of doing business online was the threat from hackers. While this is a very real fear, traditionally hackers were motivated by a sense of accomplishment rather than financial gain. That being the case, data theft was a much smaller problem for many companies. In recent years hackers have evolved and are now selling their services to criminals. One of the major services being sold is access to bot networks. These bot networks are collections of computers that have been compromised by the hacker so they can be controlled remotely. Once a significant number of machines are being controlled the hacker can sell access to these networks to criminals. The bot networks can be used in launching denial of service attacks, to send spam e-mail or to simply spread their control mechanisms to other computers.

Because the potential for expanded markets and increased revenue is so great, many companies are willing to accept the risks involved with these threats [15].

B. Other threats

Data loss is devastating, regardless of the cause. While most people are more familiar with threats from the Internet, other threats can be just as damaging, if not more so. Some of these threats include data loss due to hardware failure or natural disaster, as well as sabotage, whether intentional or unintentional by employees or ex-employees.

Highlighted by the recent devastation in the Gulf Coast area of the United States, natural disasters pose a serious threat to information security. Many companies lost not only their networking hardware, they lost entire buildings as well. If proper off-site backup procedures were not in place, the business may never recover from this event.

Fires have decimated many businesses over the years and if there is no adequate off-site backup available, all company date may be lost. This is another example where an offsite backup might be the only thing saving the company.

Even with perfect security mechanisms in place, there is still a large potential for data loss due to hardware failures. The biggest area for concern here is with hard drive failure. While hard drives have become much more reliable over the years they still fail from time to time. Even with this knowledge many companies don’t have proper backup procedures in place. Some, unbelievably, fail to back up at all.

One issue that can never be completely controlled is the human factor. Once again, even perfect technological security cannot account for intentional or unintentional human actions. An unscrupulous employee could steal data to use for profit elsewhere. They could also simply delete or change data to cause difficulty for the employer. Even if there are no employees trying to cause problems or steal data thoughtlessly or accidental actions by dedicated employees can cause irreparable damage to a company’s information assets.

One of the more recent technological advancements that can provide big benefits for small businesses is wireless networking. Using wireless LANs a small company can save on wiring costs while at the same time taking advantage of all the traditional network services. Another benefit is the ability to use laptops and hand held devices anywhere in the office. While these devices offer a lot of benefits and freedom they are not without risks. One of the main risks with wireless LANs is that many are not secured. Some that are secured are using minimum security that can be easily bypassed. Even if the local company network is secured the company’s data can still be vulnerable if a wireless user connects at a WiFi hotspot. While these hotspots are great in that you can check your e-mail from the local coffee house or airport, there is very little security on these connections. Allowing connections from these unsecured wireless networks can compromise properly configured security mechanisms on the internal corporate network [3].

A lack of staff and small IT budgets can cause security problems for the small business. While most medium and large organizations have Information Technology departments many small businesses don’t even have one person dedicated to IT tasks. In these situations there are often vulnerabilities related to un-patched systems or improperly configured equipment. Since these companies don’t have IT staff it is highly probably they don’t have anyone thinking about information security. These companies probably do not have defined policies relating to system use or configuration. Not having information security policies can lead to uneducated users, which can lead to compromised systems.

Along with the technological threats there are also non-technical threats that can cause the same amount of damage. One of these which is largely overlooked is ‘dumpster diving’. This refers to obtaining information from discarded paper copies, or possibly, discarded disks and tapes. Many businesses will focus on the technological aspects of security and overlook something as simple as proper disposal of sensitive data [5]. Another threat in this area is improperly
secured servers or networking equipment. If a server console is not properly locked up it is an easy target for an attacker. The servers could be physically sabotaged or possibly even stolen.

III. EFFECTS ON SMALL BUSINESSES

Many small business owners think they are not at risk because of the size of their business and information assets. Most think that the large corporations with more assets are the only ones at risk. This is not true. Small businesses do not have the resources or personnel to address security as well as the large corporations and are therefore more at risk. In fact, 56 per cent of small businesses have experienced at least one security incident during the past year [8]. A small system without adequate protection can be attacked by random broadcasts, which can destroy their computer and/or their network [6].

As recently as July 2005, it was reported that nearly half of all small and mid-size businesses were not even using the most basic security procedures such as installing anti-virus and anti-spyware programs [7].

Due to increased federal regulations, such as the Sarbanes-Oxley Act, many large corporations have significantly increased their network security. Cyber criminals are now turning toward the small business community looking for easier targets [7]. This should alarm small business owners because studies have found that small and medium businesses engage in fewer deterrent efforts than do larger enterprises [19].

Many small business owners, having never experienced the impact of a security breach, are complacent and exhibit a passive response to the technological threat to their computer infrastructure [9]. They display the “if it’s not broke, don’t fix it” attitude and are not stirred to action until it is too late. They do not plan or budget for solutions to the possibility of trouble and, therefore have nowhere to turn when it happens.

A good example of the type of problem that could arise, was the MyDoom worm. This was a worm that spread rapidly via e-mail, reaching its peak in February 2004. It was delivered as a well-disguised attachment, which, when opened installed a backdoor that allowed unauthorized access to an affected computer. This would allow for a variety of harmful ways this computer could be accessed in the future [6].

Another example showing the passive response flaw is a New Jersey utility consultant operating as a sole practitioner who bought a new computer so he could manage his business better. Having been told that anti-virus software was already installed, he thought he was safe. He did not realize that he had to update on a regular basis. As a result, his system became infected with an e-mail virus, which spread to his customers through bogus e-mails. This resulted in several of his clients discontinuing their business relationship with him [6].

Spam, while not a direct security threat, can still have devastating effects on businesses. GroundStrike Collections, a small business in Texas that sells over the Internet, was hit by a spammer and the result was potentially devastating. The spammer found a back door into the company’s website and used the feedback form to send thousands of pornographic e-mails. The e-mails appeared to come from the company. After hours of trying to stop the e-mail GroundStrike’s owner, Sam Juliano, pulled the Ethernet plug on his server in a last ditch effort to stop the Spam. “For a little company like ours, if you lose a few customers like that, it’s devastating,” Mr. Juliano says” [17].

On the disaster recovery front the US Department of Labor estimates that over 40% of businesses never reopen following a disaster [18]. A survey of 237 small businesses found that 73% have no written plan for disaster response [16]. Given these two facts it is easy to see why a disaster recovery plan should be drafted by all businesses.

IV. SOLUTIONS

The first step in securing a company’s information is to create a security policy. This policy defines acceptable use of the company’s network and data. It also contains specifics on data retention, data destruction, physical security and Internet access.

After the policy is in place the first step is to tighten the physical security and lock down all the technological assets. This involves physically securing the server or servers and securing other networking and telecommunications equipment. Once the physical security has been established the company can move on to the technological aspects of the security plan.

Implementing a firewall on the Internet connection is one of the first steps that should be taken to secure the network. A firewall can limit incoming and outgoing traffic. A properly configured firewall is one of the best tools available in regards to securing the network. Firewalls will keep out a lot of unwanted traffic, but it can’t stop viruses and spyware. These programs are designed to travel over common protocols that are allowed through the firewall. To help stop these threats all network computers need anti-virus software as well as anti-spyware software.

If the budget allows, an intrusion detection system is also a good idea. While the IDS system does not necessarily stop a problem, it at least alerts you to the presence of an attack.

There are several steps that can be taken to secure wireless LANs. Some of these are very simple and can be implemented for relatively low cost. Others are fairly high end and would only be employed by the largest corporations with very large budgets. One simple step that can be taken is to change the SSID from the default. Limiting the range of addresses available and restricting access to trusted devices are two more steps that can be taken to secure the wireless LAN. Finally using WEP or preferably WPA to encrypt data traffic is a very
important step in securing your wireless data.

One consideration to be aware of with wireless networks is that the security standards are still evolving. One recommended course of action is to treat wireless devices as unknown users. Require authentication for any wireless users and encrypt the connections [14].

Protecting physical and technical assets alone does not provide adequate protection. All users of company information should be educated about proper access methods and handling of data [11]. This is where the written security policy and user education comes into play.

Another option for small businesses is to outsource their security. Many small companies lack full time IT staff or the budget to employ them, so they outsource their IT needs. Those companies could outsource their information security as well. [13] One recommendation is to use the same company. However, it may be a good idea to choose a separate vendor that would check the work of the IT support company.

Backup systems are an important part of any information security implementation. A successful backup system includes redundant hardware such as RAID hard drives or dual power supplies. Uninterruptible power supplies and battery backups are also an essential part of the backup plan. These systems protect against unwanted shutdowns and power surges. The most important part of the backup plan is the data backup itself. A successful plan provides for nightly backups as well as storage of these backups at an offsite location.

V. Conclusion

As small businesses employ more and more technology security vendors are expanding their offerings by creating products specifically for the small business market. Therefore the small business owner can rest a little easier knowing that help is on the way. Information security is not a one-time project, however. It is an ongoing process that requires continual monitoring and updating [4]. Preventative measures considered good today may not be satisfactory tomorrow as threats are continually evolving.

References