Realtime
publishers

The Shortcut Guide™ To

Business Security Measures Using SSL

Dan Sullivan

Introduction to Realtime Publishers

by Don Jones, Series Editor

For several years now, Realtime has produced dozens and dozens of high-quality books that just happen to be delivered in electronic format—at no cost to you, the reader. We've made this unique publishing model work through the generous support and cooperation of our sponsors, who agree to bear each book's production expenses for the benefit of our readers.

Although we've always offered our publications to you for free, don't think for a moment that quality is anything less than our top priority. My job is to make sure that our books are as good as—and in most cases better than—any printed book that would cost you $40 or more. Our electronic publishing model offers several advantages over printed books: You receive chapters literally as fast as our authors produce them (hence the "realtime" aspect of our model), and we can update chapters to reflect the latest changes in technology.

I want to point out that our books are by no means paid advertisements or white papers. We're an independent publishing company, and an important aspect of my job is to make sure that our authors are free to voice their expertise and opinions without reservation or restriction. We maintain complete editorial control of our publications, and I'm proud that we've produced so many quality books over the past years.

I want to extend an invitation to visit us at http://nexus.realtimepublishers.com, especially if you've received this publication from a friend or colleague. We have a wide variety of additional books on a range of topics, and you're sure to find something that's of interest to you—and it won't cost you a thing. We hope you'll continue to come to Realtime for your educational needs far into the future.

Until then, enjoy.

Don Jones

Copyright Statement

This sponsored eBook is valid until July 12, 2012.

Chapter 1: Security Threats to IT Operations in the Age of Cybercrime

Over the past decade, businesses have had to adapt to an array of technical changes, including an increasingly hostile cyber environment. We saw the early precursors of cybercrime decades ago when computer use was limited to a relatively small group of specialists and electronics enthusiasts. Innovative programmers, some still in high school, would find ways to display annoying messages on their friends' computers and from there spread to other devices via shared floppy disks. This kind of part practical joke-part vandalism form of malware has been overshadowed by the more serious, technically complex, and financially lucrative form of today's cybercrime.

In this guide, we will examine major types of threats to information security that businesses face today as well as techniques for mitigating those threats. One of the most important tools available to us is SSL technology.

> **Note**
>
> This is actually something of a misnomer. Secure Socket Layer (SSL) protocols have largely been replaced with Transport Layer Security (TLS) protocols but by convention, we continue to use the term "SSL."

With SSL technology, we enable secure communication, identity verification, and ultimately trust between businesses. SSL technology does not exist in a vacuum, though. Information security is a multifaceted challenge that requires coordination of a variety of security measures, so this guide will examine the business and technical practices that weaken security as well as best practices for improving information security. This guide is organized into four chapters:

- Chapter 1 describes the evolving nature of security threats, including the development of an underground economy for cybercrimes. It also covers the business resources targeted by criminals and the impact of poor security on business operations and innovation.
- Chapter 2 examines common vulnerabilities in IT systems and business practices that undermine information security.

- Chapter 3 focuses on developing and maintaining a high-impact security strategy. In this chapter, the emphasis is on reviewing business practices and workflows, assessing technical infrastructure, and refining security policies and procedures.

- Chapter 4 concludes this guide with a discussion of practices for implementing a business-centric security management strategy. Topics range from protecting infrastructure to securing desktops and other endpoint devices. Special attention is paid to end-user security-awareness training. A checklist of practices and technologies is included to help you begin implementing the measures important to your environment.

Taking the adage "know thy enemy" to heart, we start with a look at the nature of cybercrime.

Evolving Information Security Threats

Before delving into the details of today's cybercrime environment, let's dispel any last semblance of malware, hacking, and related activities as simply mischievous pranks or technical vandalism. Those days are gone.

Minimal Threats: Experimenters and Dabblers

Of course, there are curious, ingenious programmers experimenting with operating systems (OSs), browsers, and application software trying to break them or use them for unintended purposes. There are also less ingenious, less skilled dabblers, known as "script kiddies," who use tools provided by their more technically advanced colleagues. The former group is not a significant threat as long as their work is not let loose into the wild; the latter are not much of a threat because much of their computer-generated malware is easily detected and contained by today's antivirus systems. More significant threats come from attackers with a different set of motives.

Something Old, Something New: Cybercrime Puts a New Twist on Old Crimes

Cybercrime is blanket term that covers a broad range of crimes and malicious activities that can adversely impact a business' operations and even long-term viability. Forms of cybercrime include:

- Fraud, which can occur, for example, because of mistaken identity, poor access controls that allow unauthorized users to tamper with data, or misappropriating software tools to hide unauthorized transactions.

- Identity theft, which is facilitated by poor identity management, insufficient access controls, unencrypted communications, or other sloppy data protection measures.

- Embezzlement is a classic insider threat; computer technology can help enable as well as prevent this crime. Proper authentication, such as with digital signatures implemented with SSL technologies, can help mitigate this threat through non-repudiation. Extortion with a high-tech twist can come in the form of Denial of Service (DoS) attacks that effectively render network devices inaccessible because of an overload of malicious traffic. Many businesses in Estonia were affected by the widespread DoS attack on that country in 2007. In that case, the attack was prompted by political tensions between Estonia and Russia rather than immediate financial gain.

- Intellectual property theft is not a new problem, but like other forms of crime, it can take on new dimensions when business systems are interconnected. Take, for example, the case of a former Intel employee charged with stealing more than $1 billion in trade secrets from the company (Source: Press Release, U.S. Department of Justice. "Former Intel Employee Indicted for Stealing More than $1 Billion of Trade Secrets," available at http://www.cybercrime.gov/paniIndict.pdf). The man had received a job offer from competitor AMD and he spent the last several days at Intel downloading confidential and proprietary information, including 13 documents designated as "top secret" by the company's data classification standard.

Information technology (IT) has radically changed the way criminals can commit crimes and this exposes businesses to new types of threats. Of course, employees could steal trade secrets in the past by stuffing copies of documents in their brief cases. It is difficult to imagine one man stealing $1 billion worth of secrets using only a copier and a briefcase.

One thing to keep in mind about cybercrime is that the same IT that makes businesses more efficient and able to do more with less is the same technology that allows cybercriminals to do the same. IT professionals, fortunately, have the tools and practices to mitigate these risks. The purpose of this guide is to provide some guidance on which tools, such as SSL certificates, and practices, such as identity management, are appropriate for specific circumstances. Another thing to keep in mind about cybercrime is that the patterns of organization that have helped businesses, industries, and even global markets grow and succeed are now used to extend the reach and impact of cybercrime.

Cybercrime as a Global Industry

Several things that have made modern markets so successful—such as division of labor, specialization, brokers, and exchanges that bring buyers and sellers together—are emerging in the world of cybercrime as well. In 2006, Assistant Director Brian Nagel of the U.S. Secret Service's Office of Investigations observed:

Cyber crime has evolved significantly over the last two years, from dumpster diving and credit card skimming to full-fledged online bazaars full of stolen personal and financial information (Source: Press Release, U.S. Secret Service, "United States Secret Service's Operation Rolling Stone Nets Multiple Arrests," March 28, 2006, available at http://www.secretservice.gov/press/pub0906.pdf).

More recently, Kilian Strauss, of the Organisation for Security and Cooperation in Europe (OSCE) observed how difficult it is to keep up with the pace of innovation in cybercrime:

> These criminals, they outsmart us ten, or a hundred to one (Source: Sarah Marsh, "Cybercrime Could Be as Bad as the Credit Crisis," Reuters, November 29, 2008, available at http://www.itpro.co.uk/608466/cybercrime-could-be-as-bad-as-the-credit-crisis).

Cybercrime is now functioning like an industry. Like other industries, this one is profit driven, so patterns that work for businesses, such as outsourcing specialized services, forming markets to exchange goods and services, and countering competitive threats, will be found in cybercrime. As a first step to understanding this "industry," we need to understand the specialists that constitute the major actors, such as:

- Malware developers
- Bot herders
- Spammers and phishers
- Hackers and data thieves
- Brokers

Each of these actors plays a critical role in current-day cybercrime. Without any one of them, the nature of today's cybercrime would be significantly altered.

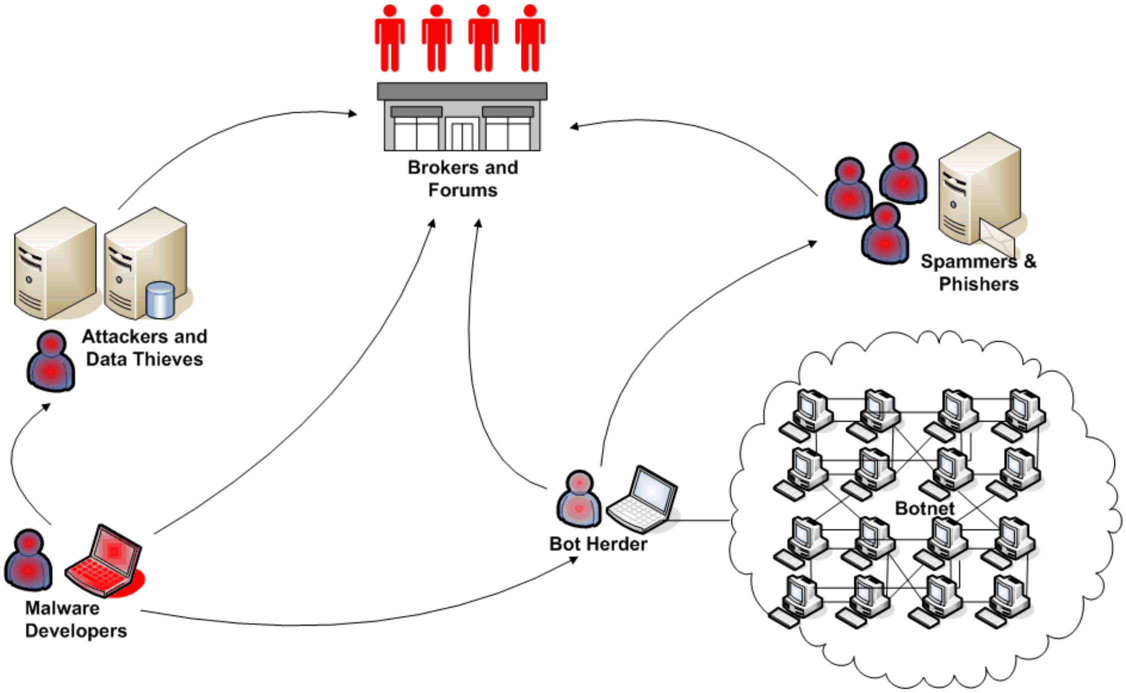

Figure 1.1: Cybercrime has evolved to support a complex mix of different skills and services much like legitimate businesses.

Malware Developers

Malware developers are the innovators that produce the new tools for the cybercrime industry. These software creators are the source of viruses, worms, Trojan horses, bots, rootkits, and other exploits. Given the financial motivation of cybercriminals, the malware that is in greatest demand is that which can lead to financial gain, including the ability to steal:

- Credit card data sufficient to successfully commit fraud
- Personal information that would allow someone to steal another person's identity
- Intellectual property, such as trade secrets, that can provide a competitive advantage to the ultimate recipient of the stolen goods
- Authentication credentials, such as usernames and passwords, that would allow an attacker to gain access to those kinds of data listed previously
- Computing and network resources that allow others to generate spam or launch DoS attacks at low or no cost

There is a specialization of labor in cybercrime, so it is not surprising that malware developers are not necessarily using their own software. That is left to others, such as bot herders and spammers.

Bot Herders

A *bot*, aka a *zombie*, is a computer under the control of someone other than its legitimate user. Put a group of bots together and you have a *botnet*.

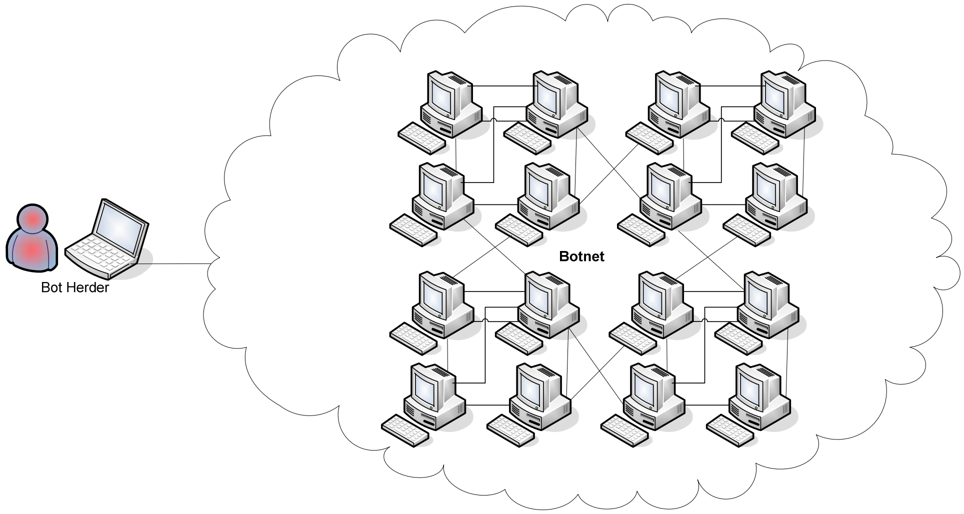

Figure 1.2: A botnet is a collection of compromised computers controlled by a bot herder. The most resilient botnets do not depend on a single server for command and control structure; rather, they use more distributed communications methods and employ recovery techniques to work with different bots should other bots they had been working with become unavailable.

From a purely disinterested point of view, botnets are highly useful distributed systems. They provide on-demand computing and networking services to the people that control them. They can generate phishing lures and send those lures to millions of email recipients or launch DoS attacks to disrupt business or government operations. The legitimate business world has an analog of botnets in the form of cloud computing.

Cloud services provide (legitimately) on-demand computing resources, storage, and networking for specialized projects or ongoing business operations. Amazon's S3 storage service and EC3 computing services are probably the best known examples of cloud services. The reason botnets are popular in cybercrime is the same reason cloud computing is of growing interest to business: little or no capital investment is required, the ongoing operational costs are minimized, and you can scale rapidly to meet peak demand without having to maintain peak capacity during less-demanding periods.

The resiliency of botnets became clear recently. In a well-publicized counterattack against spammers in November 2008, the Internet service provider (ISP) that had been hosting command and control servers for the 450,000-bot Srizbi botnet cut off service to the bot herder. For several days, there was guarded hope that this might put a dent into the amount of spam generated, but that hope was short lived. The botnet developers had planned for such a contingency and the bots were able to re-establish communication with new command and control servers.

Spam is not the only potential way to make money with botnets; launching DoS attacks is another revenue stream. In one case, a Michigan business man was sentenced to 30 months in prison for conspiring with a bot herder to disrupt competitors' business by launching DoS attacks against their Web sites and online sales servers (Source: U.S. Department of Justice Press Release, "Michigan Man Gets 30 Months for Conspiracy to Order Destructive Computer Attacks on Business Competitors," August 25, 2006, available at http://www.cybercrime.gov/araboSent.htm). Other businesses using the same ISP hosting the victim were also adversely affected. These included a major online retailer, banks, and a communications and data services company.

How big is the botnet problem? In 2007, 10% of online computers were infected by malware and by the end of 2008, that number is expected to have grown to 15%, according to researchers at the Georgia Tech Information Security Center (Source: David Stevenson "Profit from the Fight Against Cyber-Crime," Money Week, December 19, 2008,available at http://www.moneyweek.com/investment-advice/profit-from-the-fight-against-cyber-crime-14304.aspx).

Spammers and Phishers

Although most of us will not have much direct contact with malware developers and bot herders, we are all too familiar with the products of spammers and phishers. If we can say anything positive about these purveyors of unwanted and unsolicited email, it is that they are persistent, they are efficient, and they are effective.

The constant deluge of junk email we get in our email and content-filtering systems is a testament to spammer's persistence. The problem shows no signs of abating and, given the resiliency of botnets like Srizbi and the expected increase in the size of botnets, it is prudent to assume that spamming and phishing are with us for the long term.

We can deduce the efficiency and effectiveness of spammers by the fact that they choose to continue to operate. The low cost of spamming means that minutely small response rates can still yield a profitable business model. In the case of phishing, we can deduce that extra time and effort to create smaller targeted attacks, known as "spear phishing," pay off as well.

Hackers and Data Thieves

Some attacks are launched at a broad pool of potential victims; the attackers are trolling with wide nets to catch as much as possible. Other attacks are more targeted and seek to victimize a single business. Some examples of this include:

- The largest breach to date occurred at TJX Companies which operates T.J. Maxx and Marshalls stores in the US as well as T.K. Maxx stores in the U.K. and Ireland. The cost was more than $100 million to the company itself with other costs to banks who had to re-issue credit cards.
- The supermarket chain Hannaford Bros. Co. suffered a data breach from December 2007 to March 2008 when attackers were able to capture data in transit.
- In 2008, extortionists tried to compel Express Scripts, a pharmacy benefits management company, to pay or else risk having personal information about millions of customers exposed. In a noteworthy twist, the company refused to pay and instead offered a $1 million reward for information leading to the arrest and conviction of the perpetrator(s).

Hackers and data thieves can use many different techniques to compromise corporate computers. Vulnerability scanners can probe networks and devices on networks looking for unpatched software that can be exploited to gain elevated privileges or access otherwise restricted data. Information sent over wireless networks that is not encrypted may be picked up by eavesdroppers. Poorly designed Web applications may expose databases to SQL injection attacks that can leak private and confidential data. Weak passwords and default passwords can leave servers and network devices vulnerable to dictionary attacks. With so much valuable data within business systems and so many ways to launch targeted attacks, it is not surprising that criminals have taken to this opportunity.

Brokers and Exchanges

Markets depend on buyers and sellers being able to efficiently find each other. Brokers facilitate this process in many markets and cybercrime is once again following tried and true patterns of business. Cybercriminals who have managed to steal valuable data can sell it through collaborative systems such as underground forums.

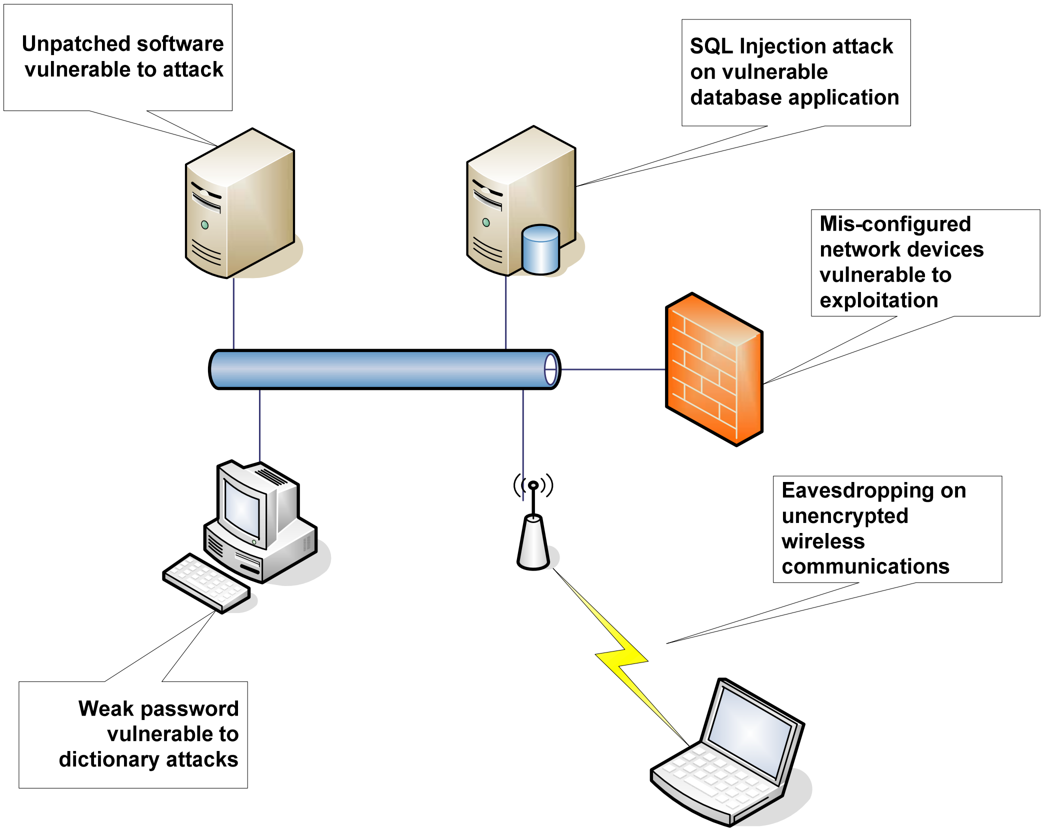
Unpatched software vulnerable to attack
SQL Injection attack on vulnerable database application
Mis-configured network devices vulnerable to exploitation
Eavesdropping on unencrypted wireless communications
Weak password vulnerable to dictionary attacks

Figure 1.3: Attackers can exploit multiple types of vulnerabilities on desktops, servers, databases, applications, and networks to steal private and confidential business data.

Increasing Numbers and Sophistication of Attacks

Some security researchers monitor communication channels as well as other indicators of overall cybercrime activity, and have observed patterns that indicate an upturn in cybercrime activity. For example:

- In one study spanning a one-year period, 69,130 advertisers sought to sell stolen information in underground forums; the top-10 sellers offered $16.3 million in credit card data and $2 million in bank account data (Source: Symantec Press Release, "New Symantec Report Reveals Booming Underground Economy," November 24, 2008, available at http://www.symantec.com/about/news/release/article.jsp?prid=20081123_01).
- One security service provider observed a 30% increase in network and Web-based security events over a 4-month period among their clients; the number of events rose from 1.8 billion to 2.5 billion events per day (Source: IBM Press Release, "Citing a Surge in Online Cybercrime, IBM Bolsters Security Service," December 4, 2008, available at http://www-03.ibm.com/press/us/en/pressrelease/26232.wss).
- The price of stolen information is dropping. Credit card numbers now sell for $2 to $3 and full victim profiles, with credit card number, mother's maiden name, Social Security number, and so on are selling for $10 (Source: Taylor Buley, "Crime Still Pays for Identity Thieves—Just a Little Less than It Once Did," Forbes, October 27, 2008, available at http://www.forbes.com/security/2008/10/25/credit-card-theft-tech-security-cz_tb1024theft.html).

Clearly, cybercriminals are adapting to new opportunities presented by the changing economic landscape. There are likely multiple reasons for the increase, on both the supply and the demand side. The global downturn leaves fewer legitimate opportunities for computer professionals, some of whom may be turning to cybercrime. Victims looking to make up for lost income can be easy prey for phishers and other scammers. Along with the increase in volume of attacks, there is an increase in sophistication of attacks.

Case Study in Credit Card Theft

From late 2007 to early 2008, a major supermarket chain was subject to a sophisticated data breach that netted more than 4 million credit and debit card numbers for the attackers. 300 stores in the Hannaford Bros. chain had servers infected with malware that intercepted credit card data and sent it to servers outside the country. Unlike other well-publicized data breaches, Hannaford Bros. was not storing more data than allowed under industry rules and the company was in compliance with Payment Card Industry (PCI) standards.

The problem was that data was captured as it was transmitted from the point-of-sale device to transaction processing service. This example shows that even when in compliance with industry standards, data breaches can still occur. Even when data is transmitted on trusted networks, encrypting data in transit using SSL technologies can mitigate the risk of this type of attack.

Doing Business in the Age of Cybercrime

Cybercrime is evolving and becoming more dangerous. It is useful to think of cybercrime as an industry with similar division of labor, service provider models, and drives to efficiency and revenue growth seen in legitimate businesses. We also need to keep in mind that compliance with regulations is a minimal set of requirements for securing business information. Malware developers, bot herders, spammers, phishers, and other attackers have demonstrated that they can and will develop new techniques to bypass security countermeasures.

Now that we have highlighted some of the structural characteristics of the cybercrime industry, let's turn our attention to business targets of their attacks.

Business Resources Targeted by Cybercrime

Businesses have primarily two assets of value to cybercriminals: information and computing resources. Both are actively sought after in the cybercrime underground economy.

Targeted Information Assets

Information is in many ways an ideal target for criminals. It is intangible, so you do not need to be in physical proximity of the information to steal it. There are many ways to hide your identity and eliminate traces of malicious activity. Perhaps best of all, large amounts of valuable information tend to be stored in centralized repositories, such as databases, or are transmitted across common paths, such as from a point-of-sales system to a transaction processing server. In such cases, it takes only marginally more effort to steal thousands or even millions of credit cards than it does to steal one or two.

Three types of information of value to cybercriminals are:

- Identity information
- Credit card and financial account data
- Proprietary information and intellectual property

Identity Information

Identity information is the key to successfully committing identity theft. The object of identity theft is to commit fraud using the credit profile of the victim. Identity theft victims may find fraudulent bank withdrawals, new accounts opened in their names, and even bankruptcy filed in their names. Specialized forms of identity theft can wreak even more havoc on victims. Medical identity theft, for example, occurs when someone uses another person's identity to receive payment for medical treatment or provide medical goods. In addition to the usual credit problems that follow for identity theft, these victims may have to correct inaccurate medical records. The ripple effects of identity theft can include complications with taxpayer records that need to be resolved with the Internal Revenue Service (IRS).

Credit Card and Bank Account Data

Credit card and bank account fraud is big business. One study found that almost one third of all advertisements in a cybercrime forum were for credit card data. In 2008, the FBI and other international law enforcement agencies shut down one forum, known as Dark Market, that had at its peak 2500 registered members (Source: FBI Press Release, "FBI Coordinates Global Effort to Nab 'Dark Market' Cyber Criminals," October 16, 2008, available at http://www.fbi.gov/pressrel/pressrel08/darkmarket101608.htm). The forum was notorious as a market for credit card data, login credentials, and even some equipment used in financial crimes. Breaking up that one forum resulted in 56 arrests and prevented $70 million in losses due to fraud.

Identity theft and credit card fraud are well-publicized aspects of cybercrime, so much so, that one might think cybercrime is primarily a problem for banks, retailers, and others with high volumes of consumer financial transactions. That is certainly not the case.

Proprietary Information and Intellectual Property

Trade secrets and other intellectual property are not the commodity products of cybercrime the way credit card and bank account data are, but it can still be a highly valued target. Consider some examples of cybercrime involving proprietary information:

- A former Netgear engineer was indicted for theft, misappropriation, and unauthorized downloading of trade secrets. It is alleged that the engineer used access to a semiconductor supplier's technical documentation to download trade secret information about the supplier's switches and transceiver products. He then took those documents with him when he went to work for one of the supplier's competitors (Source: U.S. Department of Justice Press Release, "Silicon Valley Engineer Indicted for Stealing Trade Secrets and Computer Fraud," December 22, 2005, available at http://www.cybercrime.gov/zhangIndict.htm).
- Two former employees of NetLogics Microsystems stole chip design trade secrets from their then employer as well as other companies and then started their own company in the hopes of obtaining venture capital funding for their efforts (Source: U.S. Department of Justice Press Release, "Two Bay Area Men Indicted on Charges of Economic Espionage, "Sept. 26, 2007).
- Three chemical company executives were indicted for conspiring with an employee of another chemical company to steal trade secrets. The indictment alleges one of the conspirators would download trade secret data to an external storage device prior to meetings. The conspiracy appears to have continued for more than 6 years (Source: U.S. Department of Justice Press Release, "Trade Secret Charges Filed Against Company Executives and South Korean Nationals," November 12, 2008, available at http://www.cybercrime.gov/shinIndict.pdf).

Cybercrime provides the means to avoid the high cost of research and development in intellectual-capital intense industries. It is not surprising that even within legitimate businesses, there are those that will turn to cybercrime or use IT systems in the course of their intellectual property theft.

Targeted Computing Assets

When you consider the cost businesses incur to purchase and maintain IT infrastructure, it becomes clear why cybercriminals would have an interest in stealing computing assets. Just as in legitimate businesses, cybercrime operators need to be able to ensure:

- They have adequate computing, storage, and network resources to meet demands
- Failover and disaster recovery procedures are in place
- Costs are minimized without adversely affecting performance
- Ironically, malware and attackers do not gain control of their infrastructure

Botnet malware and bot herders are integral parts of acquiring and maintaining a cybercrime infrastructure. As noted earlier, botnets are designed to avoid single points of failure and to gracefully degrade and ultimately recover in response to isolated failures. The more sophisticated botnets also use blended threats to detect bots in competitors' botnets, disable the alternate bot software, and add the bot to their own botnet. The benefit of well-designed bot software is a virtually free IT infrastructure; there are none of the typical support costs including power, hardware maintenance, service support, rent, software licensing, and so on.

As a baseline for the value of botnets, we can look to a legitimate provider of on-demand computing and storage: Amazon. The Amazon Simple Storage Service (S3) and Elastic Compute Cloud (EC2) provide customers with long-term storage and computing services for costs often below the charges small organizations, such as business IT departments, can offer. Nonetheless, there are costs.

Businesses are attractive targets for cybercriminals. They have valuable commodity data, such as credit card and bank account information, identity information sufficient to enable identity theft, as well as proprietary information that may be of value to less scrupulous competitors. Businesses also have well-managed computing infrastructures with the computing, storage, and networking services needed in the cybercrime economy. The business consequences of cybercrime include the immediate effects of data breaches and related attacks as well as subtler and sometimes underappreciated impact on business.

Poor Security's Impact on Business

Headlines about security breaches and data losses at major retailers, banks, and government agencies certainly do get attention, especially when costs are mentioned. The full cost of poor security is not captured even in these attention-grabbing incidents. They are more like the proverbial tip of the iceberg than a reflection of the full impact of weak security measures. To understand the full extent of cybercrime's adverse impact on business, we should consider the obvious as well as the less obvious consequences.

Damage in Plain Sight

The cost of poor security is apparent after a security breach. Consider a fictional but representative example. Suppose a disgruntled employee has decided that he has been underpaid and mistreated by his employer. To compensate himself, he decides to capture customer credit card data as it moves across the network. This employee has access to internal systems, so this task is not a problem, especially because this type of data is only encrypted when it is sent outside the trusted network. After the employee collects a sufficient amount of credit card data, he copies the data to his iPod, heads home, and posts an advertisement on a cybercrime forum. If he is successful, he will earn a couple of dollars for each account.

Now it is time to tally up the costs to the business:

- The cost of violating any of the many state and federal privacy regulations protecting consumer data
- The cost of possible industry regulation violations, such as PCI data protection standards
- The cost of litigation associated with lawsuits
- The cost of notifying customers of the breach and possibly paying for credit monitoring services for victims
- The soft cost of brand damage and loss of customer loyalty

These costs could have been avoided with the use of SSL technologies to encrypt communication between servers and endpoint devices.

Hidden Costs of Poor Security

Not all costs are as obvious as those related to data breaches and associated regulation violations. The less obvious costs come in the form of reduced effectiveness of business operations, and in particular:

- Reduced innovation
- Costly ad hoc responses to incidents
- Opportunity costs to other IT initiatives

Imagine a strategy session with executives and business managers planning to overhaul a business process with partners. Someone suggests working with suppliers to offer drop shipping from their facilities rather than maintain high levels of inventory within the company's warehouses. The company could work with the suppliers to leverage their shipping and order processing systems and rebrand the supplier's Web site to look like the company's when its customers are checking shipping information. A software development manager makes some suggestions about using Web services, passing customer data to the supplier, and receiving shipping details in return. So far, so good. Then one of the more security-conscious members of the meeting chimes in with questions such as:

- How do we ensure order information is not tampered with during transmission?
- How do we know protected customer information is not leaked?
- How will the company's application verify it is working with the supplier's Web service and not a fake Web service set up to capture customer information?

Without proper security measures, such as SSL technologies for encrypting data and verifying digital identities, innovative business processes such as these might be left on the drawing board. Ultimately, if we do not protect information assets, we can expose our businesses, partners, and customers to compromise.

Day-to-day operations can be adversely affected by poor security practices. Ad hoc responses to incidents such as malware infections and the need to patch applications can ultimately cost more than a more methodical approach. With proper asset management applications, patch management tools, and an incident response plan, businesses can more effectively and efficiently respond to adverse events.

Overall, the true cost of poor security is reflected in a combination of costs from data breaches and other security incidents and the opportunity cost of not implementing innovative procedures and processes because of fear of potential security problems. It is worth emphasizing that such fear is not unfounded; there may be significant risks to changing workflows and opening systems to work with business partners' applications when proper security measures are not in place. One of the goals of this guide is to provide you with information about techniques such as using SSL for encryption and digital identity verification to help control some of these risks.

Summary

Viruses and hacking are no longer just electronic forms of vandalism carried out by programmers demonstrating their technical prowess. Cybercrime has evolved into an industry-like phenomenon complete with markets, specialization of services, and multiple business models for turning stolen information and computing resources into cash. For businesses to succeed and thrive in such an environment, they must manage security processes and leverage technologies such as SSL for encryption and digital identity verification. The remaining chapters of this shortcut guide will delve into details of how to accomplish this.