Securing Against Insider Attacks

David M. Lynch

We are all creatures of habit; the way we think and the views we take are conditioned by our education, society as a whole, and, at a much deeper level, our cultural memories or instinct.

It is sometimes surprising how much the past can unconsciously affect today’s thinking. George Santayana famously observed, “Those who cannot remember the past are condemned to repeat it.” But when it comes to IT security, a better way of thinking might be, “Those who fail to understand the impact of the past on their thinking may find themselves somewhat exposed.”

The integration of the Internet — a public network — into the communication framework of most organizations has significantly changed the way IT security is implemented in virtually every business environment. And up until now, the primary basis for most security strategies to deal with this has been the “moat and castle” model: a strong perimeter is established that divides the environment into a trusted interior and untrusted exterior, with security focused on establishing the perimeter, enforcing access control strategies, and securing data as it flows from exterior to perimeter.

This approach to security is hardly new. Tribal defense is a tried and trusted remedy for a hostile world and has at its base a survival trait that has served us well for millions of years, right back to the time when prehistoric man first started to walk upright and cluster together into groups for defense against a very hostile world.

THE TRUSTED TRIBE

The instinct toward tribes is well established in the human psyche (as any parent of teenagers can attest), and although this has been a well-founded and successful strategy in the past, this way of thinking can create problems when it finds its way into IT security planning.

One of the primary foundations of our tribal instinct relates to trust, and it is externalized quite simply: if you are a member of my tribe, you can be trusted, and if you are not a member of my tribe, you should be viewed with suspicion.

This instinct worked well when tribes were based in limited geography, common

DAVID M. LYNCH joined Apani Networks as vice president of marketing in early 2005. He has more than 20 years of diverse and successful executive experience in the high tech world, primarily focused on new business startups and operational turnarounds. David started his management career at Digital Equipment Corporation and since 1995, he has focused on growing businesses in the security marketplace, holding vice president of marketing positions at Kyberpass Corporation, Rainbow Technologies, and Array Networks.
culture, and strong familial ties. But in today’s context, this instinct emerges as, “Folks who work for my enterprise are trusted, whereas folks outside the enterprise are not.” This is human nature at its most profound and, like a lot of instincts, has served us well over the years, both as a race and as individuals. It may very well explain one of the more puzzling aspects of IT security.

THE INSIDER VS. THE OUTSIDER

Since the very first IT survey on cyberattacks, one fact has remained almost constant: a greater percentage of attacks come from the inside (from “trusted” folks) — 60 to 70 percent — than from the outside (the “untrusted” folks). Or, to put it another way, roughly twice the number of attacks come from the inside vs. the outside.

This is factual, historical data, and yet a disproportionate amount of IT security spending has traditionally focused on keeping outsiders out rather than protecting against insider threats. And when this issue is discussed with IT managers today, it is not uncommon for senior managers to become visibly upset with the notion that in today’s world you need to secure both sides of the perimeter; the idea that “you need to protect against insiders” or that “insiders can’t be trusted” bothers them.

In many ways this is understandable. We are dealing with instinct here; something that operates at the gut level, making it sometimes physically uncomfortable to even consider the concept that the tribe cannot be implicitly trusted. Cyber-security surveys consistently note that even when an internal attack occurs, it frequently goes unreported.

When such attacks were affecting only an individual firm, this may have been okay. But the nature of the game has changed recently; the game has acquired referees.

THE GAME HAS CHANGED

Electronic commerce and the Internet changed the way we do business. It has truly made the world a smaller place. Organizations of all sizes now operate globally, collecting and processing orders electronically and routinely collecting personal information from their customers.

As more and more business is done electronically, the value of this “electronic identity” has increased exponentially, and the emergence of electronic identities combined with information repositories and unprotected internal networks is a major reason why identity theft is one of the fastest growing crimes worldwide.

Over the past year, millions of consumers have been exposed to potential identity theft in major breaches at a variety of banks and other organizations. For example:

- Data broker Acxiom Corp. experienced data theft by an insider that cost it $5.8 million, including employees’ time and travel expenses, security audits, and encryption software. The insider involved, contract employee Daniel J. Baas, was sentenced to 45 months in prison in March 2005 for stealing password files.
- ChoicePoint said in February that thieves using stolen identities had created 50 dummy businesses that pulled data including names, addresses, and Social Security numbers on as many as 145,000 people. As a result, its stock dropped from $48 a share the day before the announcement to around $39.
- In May 2005, Wachovia Corp. and Bank of America Corp. notified more than 100,000 customers that their financial records had been stolen by bank employees and sold to collection agencies. At the time of writing, investigators are still looking into the case, which may involve the unauthorized sale of data on nearly 700,000 customers of various banks.
- In the same month, CardSystems Solutions Inc. confirmed it suffered a “security incident” in which an “unauthorized individual” infiltrated the computer network and may have stolen up to 40 million credit card numbers.
Bank of America Corp. lost computer tapes containing financial data on 1.2 million federal workers. In June 2005 a box of computer tapes containing personal account and payment history information of clients of Citifinancial, Citigroup Inc.’s lending unit, went missing while being shipped to a credit bureau through a third party. The tapes contained names, Social Security numbers, account numbers, and personal history of customers in the United States and affected some 3.9 million customers.

This list was pulled together from a quick scan of recent news, and sadly, it is just the tip of the iceberg.

The California Department of Consumer Affairs reported on May 27, 2005, that since the state’s notification law (more on this later) went into effect in July 2003, it has been aware of 61 significant breach notifications, each involving an average of 163,500 individuals.

The rate at which confidential information is being exposed has forced governments to get into the act and start regulating the security of confidential information held by businesses, forcing organizations to reevaluate their “trusted” vs. “untrusted” environments. Significant aspects of these new laws include specific penalties for non-compliance and the legal requirement for organizations that suffer any form of breach to disclose the fact immediately.

Before these privacy laws went into effect, reports of data theft never made the newspapers. These laws now make it mandatory to disclose, and almost universally, the markets react to these disclosures aggressively, as we saw with the ChoicePoint incident when its stock price dropped (and stayed there) almost 20 percent overnight.

IT security is no longer simply an IT concern; it now affects the boardroom and beyond.

In the United States, where a number of discrete federal laws (e.g., SOX, HIPAA, FISMA, and GLBA) address this issue, it is the states that are leading the charge, with nearly two dozen currently debating or having recently passed new legislation, including a tough North Dakota law that took effect June 1, 2005, that forces companies to reveal unauthorized access to information that is commonly found in phone books.

California was one of the first to enact a law that uses the threat of civil lawsuits to goad companies into disclosing when a digital break-in or data theft exposes customers in the state to identity fraud. But in the first six months of 2005 alone, laws went on the books in Arkansas, Georgia, Montana, North Dakota, and Washington. Similar pieces of legislation in Florida and Illinois are awaiting governors’ signatures, and Indiana lawmakers passed legislation that would require state agencies to notify residents if their Social Security numbers are divulged.

The fines laid out by some of the state measures are substantial. The Florida statute would fine companies $1,000 for each day they fail to disclose a data breach to their customers, and after the first 30 days, companies would be hit with monthly fines of $50,000. Montana, on the other hand, would fine companies up to $10,000 per violation for failing to disclose a security breach that endangers customer data. Companies also could face criminal charges if they take steps to hide consumer data thefts.

Georgia’s new law went into effect in April, the one in Washington activates July 24, and Arkansas’s goes live August 12. Montana residents will see protection starting in March 2006, and in North Dakota, where most laws go into effect August 1, state lawmakers made their law effective June 1, 2005, by declaring the bill an “emergency measure,” requiring passage by at least a two-thirds vote in both houses.
soon be forced to set their overall policies to satisfy the state with the most stringent law.

Currently that is North Dakota, where a law signed in April 2002, and which took effect in June 2005, goes far beyond the California statute in its classification of what constitutes personal identifying information. As previously noted, companies doing business in North Dakota will be required to disclose a data theft if they lose track of any customer information — including information not generally considered private, such as names, addresses, or telephone numbers.

To resolve this issue, there are now a number of moves afoot to enact a federal data protection law, similar to those in Europe or Japan. It looks like this will be based on the California 1386, which narrows the definition of personally identifiable information to a person’s name along with either their Social Security or driver’s license number or their financial information and does not require companies to disclose a security breach if the data compromised in the break-in was scrambled with encryption technology.

DEFENDING AGAINST INSIDERS
Either way, the issue of insider attacks is one that most organizations will need to address. A new study, The Insider Threat Study (ITS): Computer System Sabotage in Critical Infrastructure Sectors, conducted by the Secret Service National Threat Assessment Center (NTAC) and the Carnegie Mellon University Computer Emergency Response Team (CERT) and published in May 2005 (http://www.cert.org/archive/pdf/insidercross051105.pdf), goes beyond the “how many” statistic and looks at the nature of insider attacks, who are causing them, and why.

The Insider Threat Study (ITS)
The ITS focused on the people who had internal access to information systems and perpetrated harm using them. Incidents in which the insider’s primary motivation was financial gain or theft of information or property were not included as part of this report.

The study examines each incident from a behavioral and a technical perspective, combining the Secret Service’s expertise in behavioral and incident analysis with CERT’s technical expertise in network systems survivability and security.

Overview of the ITS Findings. The ITS’ examination of incidents of insider sabotage found that most of the insiders who committed acts of sabotage were former employees who had held technical positions within the organization, and the sabotage was not simply a nuisance. Most involved organizations identified financial losses, negative impacts to their business operations, and damage to their reputations. (See Table 1 for a summary of findings.)

---

<table>
<thead>
<tr>
<th>TABLE 1</th>
<th>Summary of Insider Threat Study</th>
</tr>
</thead>
<tbody>
<tr>
<td>A negative work-related event triggered most insiders’ actions.</td>
<td></td>
</tr>
<tr>
<td>The majority of insiders planned their activities in advance.</td>
<td></td>
</tr>
<tr>
<td>When hired, the majority of insiders were granted system administrator or privileged access, but less than half of all of the insiders had authorized access at the time of the incident.</td>
<td></td>
</tr>
<tr>
<td>Insiders used unsophisticated methods for exploiting systemic vulnerabilities in applications, processes, and/or procedures, but relatively sophisticated attack tools were also employed.</td>
<td></td>
</tr>
<tr>
<td>The majority of insiders compromised computer accounts, created unauthorized backdoor accounts, or used shared accounts in their attacks.</td>
<td></td>
</tr>
<tr>
<td>Remote access was used to carry out the majority of the attacks.</td>
<td></td>
</tr>
<tr>
<td>The majority of the insider attacks were detected only once there was a noticeable irregularity in the information system or a system became unavailable.</td>
<td></td>
</tr>
<tr>
<td>Insider activities caused organizations financial losses, negative impacts to their business operations, and damage to their reputations.</td>
<td></td>
</tr>
</tbody>
</table>
The impetus for most attacks was some form of negative work-related event, the most frequently reported motive was revenge, and the attacks were clearly a planned activity.

Although the insiders tended to be technical people, and some sophisticated attack tools were also employed, 87 percent of the attacks used very simple user commands that didn’t require any advanced knowledge. Most of the attacks were made using relatively unsophisticated methods that exploited systemic vulnerabilities.

The report identifies complete areas where the trust implicit in the trusted environment worked against the organization and actually made it easy for attackers to complete their sabotage. This included the ability to compromise computer accounts, to create unauthorized backdoor accounts, or simply to use shared accounts in their attacks.

In 60 percent of the cases, the insider compromised an account to carry out the attack. These compromises included the use of another’s username and password (33 percent) or the use of an unauthorized account created by the insider (20 percent). In 92 percent of these cases, there were no indications of suspicious activity related to the account before the initial incident.

The majority of attacks took place outside normal working hours, and in many cases the attackers used a security element (remote access) against the organization, even after the individual had ceased to work for the company. The environment of trust also made the sabotage difficult to detect, with the majority of attacks detected only once there was a noticeable irregularity in the information system or a system became unavailable.

**Characteristics of the Insider Attacker.**
Although insiders in this report tended to be former technical employees, there was no identifiable demographic “profile” of a malicious insider.

In fact, the profile of the perpetrators matches the normal employee distribution of any modern organization, and attackers included currently employed, as well as recently terminated, contractors and temporary employees. Ages ranged from late teens to retirement and included both men and women. The positions held included programmers, graphic artists, system and network administrators, managers, and executives. The only common characteristic was that all these incidents of sabotage were committed by “insiders” — individuals who were, or previously had been, authorized to use the information systems they eventually employed to perpetrate harm.

Key insider characteristics were as follows:

- At the time of the incident, 59 percent of the insiders were former employees or contractors of the affected organizations and 41 percent were current employees or contractors. (See Figure 1.)
The former employees or contractors left their positions for a variety of reasons, including being fired (48 percent), resigning (38 percent), and being laid off (7 percent).

Most insiders were either previously or currently employed full time in a technical position within the organization.

Most of the insiders (77 percent) were full-time employees of the affected organizations either before or during the incidents. Eight percent of the insiders worked part time and an additional 8 percent had been hired as contractors or consultants. Two (4 percent) of the insiders worked as temporary employees and one (2 percent) was hired as a subcontractor.

Eighty-seven percent of the insiders were employed in technical positions, which included system administrators (38 percent), programmers (21 percent), engineers (14 percent), and IT specialists (14 percent). (See Figure 2.) Of the insiders not holding technical positions, 10 percent were employed in a professional position (e.g., editors, managers, and auditors). An additional two insiders (4 percent) worked in service positions, both as customer service representatives.

**FIGURE 2** Breakdown of Insiders

<table>
<thead>
<tr>
<th>Position</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>System admin</td>
<td>38%</td>
</tr>
<tr>
<td>Programmers</td>
<td>21%</td>
</tr>
<tr>
<td>Engineers</td>
<td>14%</td>
</tr>
<tr>
<td>IT specialists</td>
<td>14%</td>
</tr>
<tr>
<td>Professionals</td>
<td>10%</td>
</tr>
<tr>
<td>Service reps</td>
<td>4%</td>
</tr>
<tr>
<td>Professionals, 4%</td>
<td></td>
</tr>
<tr>
<td>System admin, 38%</td>
<td></td>
</tr>
</tbody>
</table>

Impact of These Attacks on the Business.

In many ways, by virtue of their knowledge of the organization’s systems or databases, insiders pose a more substantial threat than “outsiders.” And so it is not surprising that although most organizations identified financial losses and damage to their reputations as results of the attacks, the study found that 75 percent of the organizations experienced some form of impact on their business operations, including:

- Severed communications due to networks, routers, servers, or dial-up access being shut down
- Blocked sales due to blocked sales applications or deleted sales records
- Blocked customer contact due to modified customer passwords
- Damaged or destroyed critical information assets, such as proprietary software, data, computing systems, and storage media necessary to the organization’s ability to contract work, produce product, or develop new products
- Damaged supervisory integrity, including exposed personal or private communications embarrassing to a supervisor

It is important to remember here that incidents in which insiders’ primary motivation was financial gain or theft of information or property were not included as part of this report.

Protecting against Insider Attacks — Study Recommendations. The study recommends a layered defense strategy consisting of policies, procedures, and technical controls. For IT security specifically, it recommends the following:
1. **Restrict remote access** to where remote access is allowed for e-mail and non-critical data; limit access to the most critical data and information systems to those employees physically located inside the workplace.

2. **Restrict system administrator access** to the smallest group possible and closely log and monitor all such access on a regular basis.

3. **Collect information for all remote logins**, such as login account, date/time connected and disconnected, and IP address.

4. **Monitor failed remote logins**, including the reason the login failed. If authorization for remote access to critical data is kept to a minimum, monitoring can become more manageable and effective.

Let’s look more closely at each of these recommendations.

**Restrict Remote Access**

The ITS noted that the predominant means of insider attack was remote access. This is an example of where the focus on external threats has let organizations down. Remote access products focus on two things: access control and privacy. Simply put, they encrypt data transfer in the open and restrict access to “authorized users.” Most take the form of gateways where, once individuals connecting have been authenticated, they are allowed access to inside the perimeter, where they can freely roam; and for those with a technical background, the roaming is easy.

The study suggests that organizations restrict remote access to e-mail and noncritical data and that access to the most critical data and information systems be limited to those employees physically located inside the workplace. Unfortunately, this is another example of where what has worked in the past is affecting how we view security in the present. This approach would indeed work if everyone still “went to the office” to get their work done.

According to a study by Nemertes Research, 90 percent of employees don’t work at headquarters, and there’s been an 800 percent increase in virtual workers — employees based in different geographies from their managers and peers — in the past five years.

Organizations today are almost universally in part virtual; IT, sales, support, and even executives may be scattered around the world. The IT perimeter is getting stretched to the degree that it can be difficult to determine where the “workplace” really is. All of which makes it next to impossible to limit access to the most critical data and information systems to those employees physically located inside the workplace.

**Restrict System Administrator Access**

Restricting system administrator access to the smallest group possible is a good idea, but no matter what happens, there has to be some group of system administrators out there. And although only 17 percent of the insider events studied involved individuals with administrator access, given the population of an average environment, this means that it is just as likely that an attack will come from this group as from any other; and attacks from this group have a higher chance of success because these insiders typically have a higher level of access and knowledge than the average group member.

**Gather Information**

Information gathering by itself will not prevent sabotage, although it could potentially provide valuable information to determine that an attack is underway, as well as the ability to track the damage done.

**Monitor Failed Remote Logins**

Monitoring failed logins can provide information that an attack is underway, but as the size of the remote access community expands, the analysis task can become onerous.
PROTECTING AGAINST INSIDER ATTACKS — MORE COMPREHENSIVE RECOMMENDATIONS

The ITS sheds some light on the issue of insider attacks, the impact on the organization, and options to protect against an insider attack. It takes a comprehensive view on ways to protect against insider attacks, including education, changes in process, and management awareness, among others.

However, when it comes to specific recommendations for IT security, it falls back into conventional thinking. Information gathering and analysis are key to any security scheme; however, restricting remote access and the size of the administration team, although good ideas, may not be very practical in today’s world.

With governments around the world changing the fundamental rules of the game and establishing themselves as referees to ensure that the rules are followed, it is time for IT security to put the security of the environment inside the firewall on equal footing with the security outside of the firewall. And the first step toward this is understanding and acknowledging that we are all subject to the “trusted tribe” mentality and that it is creating blind spots in our planning and implementation.

Inside the perimeter is not secure in today’s world and the term “trusted environment” is truly a misnomer.

THE POROUS PERIMETER

To add to the problem (and to the urgency), an explosion in outsourcing, mobile computing, and Webified applications has placed a premium on back-office connectivity to anyone, from anywhere, with any device. Perimeter-based security fails because there is no longer a clearly defined perimeter, and it’s often difficult to tell who should have access to the trusted network and who should be kept out.

Wireless networks, remote users, Web services, corporate spies, disgruntled employees, bribed administrators, and socially engineered victims have seen to that.

Hackers can set up rogue Wi-Fi access points near hotspots to trick users into logging on to their networks. Once malicious users have control of a computer, they can plant a key logger that can steal passwords and use it to access the network at will.

Employees and consultants open still more holes. Employees connect their personal machines to organizations’ networks, despite the fact that those PCs are connected to home networks or unsecured wireless LANs. Consultants, business partners, or remote employees may try to access sites within the trusted network, compromising the network with unprotected communications. Over time, company firewalls start to resemble Swiss cheese, as more and more ports need to be opened and unnecessary ports often remain open long after they’re needed; or worse, your “trusted environment” is now connected directly to the Internet through a home or partner link or an unapproved wireless LAN.

PERIMETER DEFENSE IS A LOST BATTLE

IT managers need to rethink security to reduce the risks of these attacks on the trusted network and ensure they do not violate privacy laws, exposing the agency to legal and civil penalties. As E-business extends the definition of “internal” beyond the perimeter, opening internal assets to more and more people and businesses, administrators must be aware that the “trusted” network can no longer be trusted.

A NEW TECHNOLOGY IS NEEDED

Traditional access and privacy products have been focused on the outside of the perimeter and are not well suited to defending inside the perimeter.

Most access control and privacy products on the market today take the form of gateways; once the individuals connecting have been authenticated they are allowed access to inside the perimeter, where they are then free to roam; and for those with a technical
background or prior knowledge of the environment, the roaming is easy.

Gateways by definition are designed to be inserted in the wall and to control the flow. For them to function, all traffic must route through them, which will have a severe impact on the internal network performance. They also have an “inside” and “outside”; encryption happens on the outside but not usually the inside, which means that confidential material will be only partially protected.

What is needed is a fundamental new approach: technology that works effectively with existing infrastructure but that will enable organizations to lock down their internal networks, to define allowable data flows, and to ensure that confidential information is always encrypted — no matter where it is flowing from and to.

To meet the needs of the new referees (the auditors for the slew of government privacy regulations that are already here, with more coming), this technology must be able to cover the whole network, provide an effective audit trail, and report on “out of bounds” activities.

To secure a trusted environment, follow six basic steps:

1. Establish necessary security relationships.
2. Segregate the network into security zones for easier management.
3. Enforce the established security relationships within and across the security zones.
4. Regularly audit the network to ensure that the security relationships are being enforced.
5. Manage and update the security relationships as business needs or compliance issues require.
6. Provide an audit trail and effective reporting to the IT organization as well as regulatory compliance auditors.
Copyright of Information Systems Security is the property of Auerbach Publications Inc. and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.