MANAGING TECHNOLOGY RISKS IN BANKS MANAGED SECURITY SERVICES/OUTSOURCED SECURITY – A PERSPECTIVE

Sujit Christy CISA, CISSP, B.COM

Today's fast-paced business environment has become increasingly complicated due to pressure from government and industry to meet ever-growing regulatory and business security compliance requirements in many countries. These requirements have increased in scope and number with many large companies having undergone compliance audits and assessments for Sarbanes-Oxley (SOX), Gramm-Leach-Bliley (GLBA), and the credit card industry. To date, companies have spent billions collectively to meet the vast requirements. Now that the initial rounds of audits have taken place, companies are looking for ways to make their compliance activities more cost-effective.

Computer and network security has been viewed as an engineering problem, and banks including other organizations have tried solving it through application of technologies. The approach is failing even though technologies continue to improve; the security of internet continues to decline. The real problem is not of technology, but of process. Network security is no different from the real world security. There is no magic defense against crime in the real world, yet we are all reasonably safe. The correct paradigm is "risk management". Strong counter measures combine protection, detection and response. The way to build resilient network security is with vigilant, relentless, and adaptive experts (people, not technology).

For the past eleven years, the Computer Security Institute (SCI) has conducted an annual computer crime survey. In 2006, 52% of the respondents reported "unauthorized use of computer systems". 38% said that they had no such unauthorized uses, and 10% said they did not know. The number of incidents was all over the map, and the number of insider (employees) versus outsider incidents was roughly equal. The attacks ranged from telecommunications' fraud to laptop theft to sabotage. What is more interesting is that all of these attacks occurred despite the wide deployment of security technologies. The final consequences are staggering. Only about 313 respondents, less than half the number of the previous year, were willing and could quantify their losses, and those totaled to $53 million. From under 400 companies! In one year! This is a big deal.

1. Importance of Internet Security

Most of things we do in the real world, we want to do on the Internet: conduct private conversations, keep personal papers, sign letters and contracts, speak anonymously, publish digital documents and conduct banking transactions. All these rely on the integrity of the information. All of these things require security. Computer security is a fundamental in enabling technology of the Internet; it's what transforms the Internet from an

academic curiosity into a serious business tool. The limits of security are the limits of Internet. No person or business is without these security needs.

The risks are real. Everyone talks about the direct risks; theft of trade secrets, customer information, money. People also talk about the productivity losses due to computer security problems. What is the loss to a bank if its email goes down for two days? Or if ten people have to scramble to clean up after a particularly nasty intrusion or a worm attack? There are media reports which have quoted worldwide losses high as $10 billion due to ILOVEYOU virus; most of that is due to productivity losses.

More important are the indirect risk: loss of customers, damage to brand, loss of goodwill. Regardless of how million credit card number theft at Egghead.com turned out, some percentage of customers decided to shop elsewhere. In the aftermath of the Microsoft attack in October 2000, the company spent much more money and effort containing the public relations problem than fixing the security problem. The perception that their source code was untainted was much more important than any effects of the actual attack.

European countries have strict privacy laws; companies can be held liable if they do not take steps to protect the privacy of their customers. The USA has similar laws in particular industries – banking and health care. We have not yet seen shareholder lawsuits against companies that failed to adequately secure their networks and suffered the consequences, but they are coming. Can bank officers be held personally liable if they fail to provide for network security? The courts will be deciding this question in the coming years.

As risky as the Internet is, banks have no choice but to be there. The lures of new markets, new customers, new revenue sources, new business models are just so great that the banks will flock to the Internet regardless of the risks. There is no alternative. This, is why computer security is very important.

2. Security and Risk Management

Ask any network administrator what he needs security for and he will describe the threats - an endless list. The traditional paradigm of computer security is born out of the computer science mentality: figure out what the threats are, and build technologies to avoid them. The conceit is
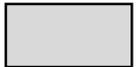
that technologies can somehow "solve" computer security, and the end result is a security program that becomes an expense and a barrier to business. This paradigm is wrong. Security is a people problem, not a technology problem. There is no computer security product or even suite of products as magical security dust, imbuing a network with the property of "secure". It cannot be done and it is not the way banks work. Banks manage risks. They manage all sorts of risks including market risk and credit risk; network security is just another one. There are many ways to manage risks. The choices in a particular situation depend on the details of that situation. And failures happen regularly. Hence risks should be managed to reduce the damage.

3. Business Case for Security Monitoring

Few years ago a firewall was needed for security on the Internet. Back then, no one had ever heard of "denial-of-service" attacks shutting down Web servers, let alone common gateway interface scripting flaws and the latest vulnerabilities found in many off the shelf and in-house built software applications. But in recent years, came intrusion detection systems, intrusion prevention systems, public-key infrastructure, smart cards and biometrics. New networking services, wireless devices and the latest products regularly turn network security upside down. Every year there is new research, technologies, products even laws. And every year over the last 50 odd years, it has got worse. It is no wonder CIO's cannot keep up. What's amazing is that no one can either.

Network security is an arms race, where the attackers have all the advantage. First, potential intruders are in military strategies call "the position of the interior"; the defender has to defend against every possible attack, while the attacker only has to find one weakness. Second, the immense complexity of the modern networks makes them impossible to properly secure. And third, skilled attackers can encapsulate their attacks in automatic programs, allowing people with no skill to use them.

The way forward is not more products but better processes. We have to stop looking for the magic preventive technology that will avoid the threats, and embrace processes that will let us manage the risks. That does not mean more prevention; it means detection and response.

On the Internet, this translates to constant monitoring of the network. Monitoring also means vigilance; attacks come from all over and at all the times. It means experts need to continuously monitor with the tools and expertise at hand to figure out what is happening. Implementing an intrusion detection system onto a network and handing a system administrator a mobile phone, is not monitoring.

Prevention systems are never perfect. No bank ever says "Our safe is so good that we do not need an alarm system". Detection and response are how we get security in the real world, and it is the only way we can possibly get security on the Internet. CIOs must invest in monitoring services if they are to maintain security in the networked world.

4. What is Managed Security Monitoring?

This means a trusted third party i.e., Managed Security Services Provider, watches over the network. Watching is done by real people: expert security analysts monitor the systems 24 hours a day. The Managed Security Services Provider takes the existing security devices and software, and leverages their potential, with a powerful combination of unmatched technology and proven expertise. The result is the network is protected from today's growing risks by a real time, full time security solution. The value is a unique combination of people and technology. The security analysts are highly trained and qualified experts who understand the need to protect the business assets. Managed security service companies can monitor networks, manage security devices, scan networks, implement organization's security policies, install security devices, and more. Some companies offer similar services, often tied to particular products or suites of products. Sometimes outsourced network security comes in a package with other outsourced network services.

Outsourcing network defenses may seem like an odd idea. Doing so means handing over the keys to an enterprise to some stranger. Yet security outsourcing is becoming popular to the point of becoming a fad. More and more companies are outsourcing their network security. This trend is driven by one truism: there is no other way to deal with the shortage of skilled computer security experts, the increasing requirements for businesses to open their networks, and the dangerous threats to an environment. For the Internet to succeed as a business tool, security has to scale. *Outsourcing is how it will do that.*

In reality, there's no dichotomy. Hiring a trusted third party to handle the network security can be less risky than building its own expertise inside the bank. And it most definitely can be both cheaper and more effective.

The primary argument for outsourcing is financial: a bank can get the security expertise it needs much more cheaply by hiring someone else to provide it. Take monitoring, for example. The key to successful security monitoring is vigilance: attacks can happen at any time of the day and any day of the year. While it is possible for banks to build detection and response services for their own networks, it's rarely cost-effective.

On one hand, the promises of outsourced security are very attractive: the potential to significantly increase network's security without hiring half a dozen people or spending a fortune is impossible to ignore. On the other hand, giving over the network security to another company feels like it should be inherently risky. But if the decision to outsource network security is a difficult one, the decision of precisely what to outsource seems impossible.

Staffing for security expertise 24 hours a day and 365 days a year requires six full-time employees - more, if you include supervisors and escalation personnel with specialized skills. Even if a bank could find the budget for all of these people, it would be very difficult to hire them in today's job market. If hiring them is difficult, retaining them would be an even harder challenge. Security monitoring is inherently erratic: four weeks of boredom followed by eight hours of panic,

then seven weeks of boredom followed by six hours of panic. Attacks against a single organization don't happen often enough to keep a team of the caliber needed engaged and interested. This is why outsourcing is the only cost-effective way to satisfy the requirements.

Medical care is a prime example of outsourcing that we can use for comparison. Everyone outsource healthcare, in the sense that people don't act as their own doctor; nor does anyone hire a private personal doctor. Certainly cost is a factor in their decision to outsource, but there's more to it than that. One may only need a doctor twice in the coming year, but when he needs one, he may need him immediately, and he may need specialists. Out of a hundred possible specialists, he may need two of them - and he has no idea beforehand which ones. He would never consider hiring a team of doctors to wait around until he gets sick. So individuals outsource their medical needs to a hospital. Similarly, it makes sense for a bank to outsource its network security needs to a variety of experts.

The benefits of security outsourcing are enormous. Aside from the aggregation of expertise, an outsourced monitoring service has other beneficial economies of scale. Managed Security Services providers can more easily hire and train its personnel simply because it needs more employees and it can build an infrastructure to support them. Managed Security Services providers also have a much broader view of the Internet. Managed Security Services providers can learn from attacks against one customer, and use that knowledge to protect all of its customers. And from their point of view, attacks are frequent.

Vigilant monitoring means keeping up to date on new vulnerabilities, hacker tools, security products, and software releases. Managed Security Services providers can spread these costs among all of their customers. To return to our medical care analogy, one can get better medical care from a doctor that sees patient after patient, learning from each one. To an outsourced security company, network attacks are everyday occurrences and its experts know exactly how to respond to any given attack, because in all likelihood they have seen it many times before.

5. What to Outsource

There are, however, limits on what a bank should outsource. The bottom line is that a bank won't outsource everything, because some things just don't outsource well. Things that don't outsource well are often too close to business, or they're too expensive for an outsourcing company to deliver efficiently, or they simply don't scale well. Knowing the difference is important. Think about healthcare again. We all know what aspects of medical care we like: the ambulance picks us up in seconds and rushes us to the hospital, a team of medical experts spares no expense in running tests to figure out what's wrong and in doing whatever it takes to cure us. And we all know what aspects we don't like: ill-equipped and ill-staffed hospitals, Medical Officers telling us that we can't have that particular test or that a specialist isn't warranted in this case. The aspects of outsourced healthcare we like, involve immediate access to experts. Any medical emergency requires experts, and the faster they can pay attention to us, the better off we'll be. The aspects of outsourced healthcare we don't like, involve control of the process. Our healthcare is our

responsibility, and we don't want someone else making life and death decisions about us. Network security is no different. Don't outsource control of the process.

What a Managed Security Service Provider cannot do is determine how IT security interacts with business. For example, a Managed Security Service Provider can detect when a hacker is inside a corporate network and what he's doing, but won't know the business ramifications of different responses. Managed Security Service Provider can detect an insider attacking a network, but does not know whether he's malicious or performing authorized testing.

Customers who run highly secure networks would rather disconnect from the Internet than have a hacker wandering around. Other customers who generate far too much revenue from their Internet connection to disconnect for even a minute require responses that keep them operational. Managed Security Service Providers work best when they can work with their customers, combining their expertise with their knowledge of the business processes.

6. How to Choose an Outsourcer

Choosing an outsourcing partner is difficult, because it's hard to tell the difference between good computer security and bad computer security. But by the same token, it's hard to tell the difference between good medical care and bad medical care. If we're not health experts ourselves, we can sometimes be led astray by bad doctors that appear to be good. So how do you choose a doctor? Or a hospital? We should choose by asking around, getting recommendations, and going with the best we can find. Medical care involves trust; we should to be able to trust our doctor.

Security outsourcing is no different; we should choose a company we trust. To determine which one, talk with others in your industry or ask analysts. Go with the industry leader. In both security and medical care, you don't use a little-known maverick unless you're desperate. In any outsourcing decision that involves an ongoing relationship, the financial health of the outsourcer is critical. Look for companies that are leaders in their field, have a strong history of security services, and don't try to do everything.

7. The Future of Outsourcing

Modern society is built around specialization; more tasks are outsourced today then ever before. We outsource fire and police services and food preparation (restaurants). In general, we outsource things that have one or more of three characteristics: they are complex, important, or distasteful. In business, we outsource tax preparation, payroll, and cleaning services. Outsourcing security is nothing new: all buildings hire another company to put guards in their lobbies, and every bank hires another company to drive its money around town.

Computer security is all three: complex, important, and distasteful. Its distastefulness comes from the difficulty, the drudgery, and the 2:00 a.m. alarms. Its complexity comes out of the

intricacies of modern networks, the rate at which threats change and attacks improve, and the ever-evolving network services. Its importance comes from this fact of business today: companies have no choice but to open up their networks to the Internet.

Doctors and hospitals are the only way to get adequate medical care. Similarly, outsourcing is the only way to get adequate security on today's networks.

8. Reasons to Outsource Security

- Security Device management and monitoring can be mundane and tedious. Expertise is expensive to find and difficult to maintain. Outsourcing Security tasks relieve the talented staff of the day-to-day grind.

- The best in-house information misses the big picture. In-house analysts only see their own data. A trusted Security Service provider correlates data from thousands of devices and the Internet infrastructure to map trends, anomalies, and better identify security threats with threat data gathered from researchers.

- Threats don't go on vacation or take holidays. Global, fully-staffed Security Operations Centers (SOCs) or Global Command Centers (GCCs) mean highly trained security professionals are monitoring the infrastructure.

- Information security is patchy and contradictory, a moving target. Understanding the impact of evolving threats and the changes required to protect against them has become increasingly difficult. Enterprises need help making better decisions to reduce cost and complexity and more effectively manage risk.

- Security tools come in a box; security solutions don't. Even the best security tools require people to configure, monitor and manage them. A security solution begins with highly trained people using best-of-breed tools for security prevention, detection and response to help ensure malicious traffic is blocked without blocking benign traffic.

- Bank's operational costs may escalate with each new security initiative. Outsourcing security services to a vendor-neutral provider lowers operating costs for recruiting, training and retaining staff for 24/7 security organizations.

- Bank's worry about every threat, hack, virus, or worm that might attack. A Managed Security Service Provider monitors threats 24/7 so bank's doesn't have to.

- Non-compliance is a business risk. Whether the banks know the regulations or not, is liable for security breaches and non-compliance.

- Find out how well the security initiatives are doing. The banks have invested a lot of money in technology and people, yet the threats and the regulations constantly evolve.

- Strategic outsourcing keeps banks focused on their core business.

9. Regulatory Compliance and Managed Security Services

Banks face rising costs and increasing complexity related to regulatory compliance. In addition to government and industry-specific regulations, business partners, suppliers, and customers have security policies and practices that require compliance and validation. Few banks have the in-house resources to implement all aspects of the type of program required for due care and due diligence.

10. Problem: Cost and Complexity of Maintaining Compliance

With changing regulations and new vulnerabilities & threats discovered daily, regular assessments serve only as a foundation for compliance. Maintaining and documenting compliance in an auditable format requires 24/7 monitoring, secure archiving, and reporting systems mapped to the requirements of key standards.

11. Solution: Outsourcing Managed Security Services

By outsourcing the resource-intensive tasks of 24/7 monitoring and maintaining compliance, banks stay focused on core, value-producing activities. Commonly outsourced Managed Security Services (MSS) include:

- *Log monitoring*: The ability to log, track, and analyze user and system activity is often critical for preventing, detecting, responding to, and remediation security breaches. A number of standards and regulations also require third-party archiving and storage of log monitors to audit IT controls.

- *Intrusion detection and prevention systems management and monitoring*: As the complexity and scope of network threats grows, installing network security technology does not guarantee protection or compliance. A bank must be able to detect and prevent intrusions with 24/7 monitoring and management of intrusion detection and prevention systems.

- *Firewall management and monitoring*: Despite the implementation of firewall technology, most banks continue to suffer from unauthorized access due to insufficient firewall

management. Outsourcing firewall upgrades, configuration management, rule-set changes, and health monitoring protects a critical component of network security without taxing in-house resources.

- **Vulnerability management**: Some scanning and assessment requirements apply to Internet applications as well as network and operating systems. Manual testing by experienced professionals combined with automated technology helps identify the breadth and depth of vulnerabilities.

Outsourcing provides significant benefits when you calculate the cost of recruiting, training and retaining information-security compliance expertise, and maintaining a reliable, scalable infrastructure to support 24/7 management and monitoring of network security.

12. How Managed Security Services Providers Help

Managed Security Services Provider apply their people, processes, technology, and intelligence to securing a bank's critical infrastructure as required by regulations and business needs. The bank's staff stays focused on strategic business initiatives while Managed Security Services Provider security analysts monitor and manage critical devices 24/7 with real-time analysis and a consolidated portal view across the entire infrastructure.

12.1 Value of Intelligence

A security breach can cost a bank dearly in lost time, compromised data, and brand equity damage. These costs add up to lost revenue and may result in fines or other business costs. As vulnerabilities increase and the time from vulnerability identification to exploit continues to shrink, having accurate, actionable intelligence becomes more important everyday.

12.2 Problem: Prioritizing Response

Information can tell that vulnerability exists or that an event has occurred in the environment. Alerts from vendors or the network community may tell about a new threat. But too many false positives and too many alerts from the extend network resources obscure the threats that matter most. To help ensure critical-system availability and protect information more effectively, bank's need proactive, actionable security intelligence tailored to business needs.

12.3 Solution: Proactive Intelligence

Actionable intelligence comes from a rich layering of intelligence sources, expert analysis and effective data correlation to provide advanced warning of a threat, identify the likelihood of attack and the risk to critical systems. Many banks fail to use the first layer of intelligence - the data

within the bank's own systems, because they cannot correlate data between sites and across disparate systems.

The next layer of intelligence goes beyond individual organizations to correlating data across multiple organizations, industries, and regions. Managed Security Services Provider, with thousands of devices under their management, uses correlation and trend analysis to identify attacks on particular industries such as financial services providers or on specific devices to help clients respond.

These first two layers of intelligence tell a bank what has happened or is happening. Proactive intelligence comes in advance of an event. To know what's coming requires early identification and verification of vulnerabilities, as well as a way to measure the criticality of a threat, and steps for remediation.

13. Why the Value of Intelligence Matters

Information security is no longer about managing and monitoring devices. Threats can originate anywhere in the world and wreak havoc on the operations and reputations of banks anywhere. Better intelligence helps reduce false positives and prioritize remediation to reduce the potential harm to a bank.

14. Compliance: A Business Opportunity

The United States is witnessing increased regulation of business process-oriented laws including the Sarbanes-Oxley (SOX) Act of 2002, the California Senate Bill 1386, Database Protection Act (SB 1386) of 2001, and the Gramm Leach Bliley (GLB) Act of 1999.

Each of these laws imposes strict requirements on enterprises to establish or identify, document, test and monitor "internal control" processes. Most of these processes, are supported by increasingly sophisticated information technologies. Being unprepared can cost banks more than money - under Sarbanes-Oxley, jail time is possible for non-compliant executives.

SOX, GLB, and SB 1386 all have data privacy and protection in common. Each has varying requirements but all share the following common enterprise mandates:

- **Security Policies**: Well-defined policies for data privacy and protection discourage the government from imposing their own standards - the least desirable of all situations.

- **Security Processes**: Demonstrating policy in action with people using technology in a predictable manner to protect data from attackers.

- ***Robust Audit Trail***: The foundation of evolved process, where regulators require evidence of what happened to justify why events need not be reported.

- ***Preventative Measures***: Encryption, digital signing and real-time detection of attacks all serve to pre-empt attacks on data.

15. Doing the Homework

When considering any Managed Security Service Provider, (MSSP) be sure to address the following considerations:

The Service Level Agreement (SLA) may be the single most important part of any Managed Security Services contract. The SLA is going to define the roles the bank and the prospective MSSP is going to fill. As such, a bank must understand exactly what they are expected to do, and what the MSSP is agreeing to do. Working with outsourcers boils down to due diligence and that includes a stringent review of SLAs and other agreements related to security management, monitoring, incident response and documentation. Banks have to ensure, via SLAs, that response time and escalation processes meet their needs. Banks have to get the outsourcers to agree to security tests, including detailed audits and penetration testing exercises. And the banks have to make sure they have instituted security processes, including authentication, access control and auditing."

With security SLAs, there are two areas of primary concerns:

- **Access to the Bank's Systems**

  First, the SLA should specify what in bank the MSSP can and cannot access. A bank may be reluctant to share any of its secrets - or access to the secrets with anyone, no matter what their credentials are. That's what security is all about. With an SLA, banks have to balance two key considerations. The MSSP must have sufficient access to do the work being paid for and at the same time, banks must feel comfortable about the access being granted to the MSSP. If the bank is uncomfortable with the level of access, the bank must carefully think through what is to be accomplished and why the MSSP needs the access. This is a mini-risk assessment in itself.

- **Information and behavior during an attack**

  The SLA should also specify who will do what, in the event of an attack. An MSSP's response can vary widely from post-attack audit notification to on-the-spot consultation to full responsibility for real-time response. Defining these roles and responsibilities is critical. At the same time, the bank must recognize that anything the MSSP doesn't do is up to the bank to perform. Any limitation in the MSSP's response puts an additional burden on the bank. In addition, make sure that bank will be getting reports as frequently as you need

them and with the level of detail appropriate for the bank and it's environment. The SLA may also specify contact personnel in both organizations and other such information. Such details may seem unnecessary at first, but the more specific the SLA (within reason), the better the bank will be protected in the long run.

Cost Another natural concern is the cost. The good news is that economies of scale allow even highly regarded MSSPs to set prices within the grasp of even modest budgets. The secret is scaling. If a service provider is monitoring 10,000 networks, adding your's isn't going to require a major upgrade in resources. Thus, monthly fees as low as $1,000 are not unusual; at the higher end, the bank can expect to pay about what it would pay 6 salaried IT professionals to monitor the network 24/7. Of course, cost also depends a great deal on what services are availed. Simple monitoring and notification is usually least expensive, since it's largely automated. Analysis costs more, depending on the level. Response costs more still, since that almost always involves human decisions and actions. Most MSSPs charge a monthly or yearly subscription fee that entitles a bank to a certain level of service. The fee often depends on how many servers the providers are protecting, how many extras selected, quality of service and speed. There may be an additional fee for initial analysis of the security posture or non-routine customization.

Typically, banks can test the waters by outsourcing something simple and non - critical. Then gradually add more services as the confidence in the provider grows. Look for MSSPs that allow such incremental changes in your coverage.

16. Getting What You Pay For

A short list of outsourceable security services includes intrusion detection and perimeter scanning, VPN and firewall monitoring/management, antivirus/content protection and data/file encryption services. Some of these areas are better fits than others as outsourcing candidates: malicious code protection, for instance. Antivirus managed services, such as those offered by McAfee.com, operate under the assumption that virus threats change so rapidly that it requires professionals focused totally on the task. On the other hand, most companies manage their e-mail and file-encryption applications in-house.

Many MSSPs offer monitoring/management services for perimeter security devices: VPNs, firewalls or other network elements. One fundamental question for the bank is what precisely should be monitored. Banks may engage an MSSP to watch only a particular piece or class of equipment. Internet-based technology permits much of monitoring to be done remotely and in real time. Some providers configure the security devices to send the logs to the Security Operations Center which is non-intrusive in manner. Most monitoring services acquire data in real time, nipping budding problems before they bloom. However, some services don't look at real-time data. Clearly, such services cannot respond to crises as they occur, but specialize in postmortem log analysis, forensics and incident response.

For large banks, MSSPs must cut down a mountain of input data, primarily with automated filters. Most of the logged data is routine and irrelevant. "Some 98 percent of all breach 'attempts' are actually false positives," viz., somebody made a mistake, the software gagged or someone accessed the wrong port.

The tricky part is determining whether the remaining 2 percent are real attacks or something else, and that's where automated filtering falls short. "It takes a person, not a product, to interpret this information correctly. Services that are entirely automated are unlikely to provide the deep and sophisticated insights that human - staffed services can.

Some security service providers lock their client into a single technology or product. They are, in essence, resellers for that product. However, most banks are more interested in a security solution than a security product. Make sure the MSSP can deal with multiple products, technologies and approaches.

Many services providers (including e-Cop, Verisign and ISS) make a point of handling a variety of the more popular products. It's more likely that such companies will find a technology match that makes sense for bank's situation, rather than trying to shoehorn the enterprise into their product. This is especially important if the bank has a security policy in place; the service provider should be able to incorporate the policies into their monitoring or management program. The point is, the banks should not want a "one-size-fits-nobody" plan.

Now, what if a bank does not already have a security policy in place? The bank can either develop a policy before proceeding with outsourcing, or can adopt the security service provider's policy as the bank's own ad hoc policy. The danger with this is that the policy may not really fit the operating needs, in which case the bank could seek the assistance of the provider.

Some MSSPs look beyond the computer data at the bank's setup and procedures for good reason. Many problems arise from people: human errors or actual internal threats. Approximately, 80 percent of firewall breaches are due to internal causes that is a disgruntled employee or an honest mistake.

17. See a Good Analyst

Analysis of input data, including possible attacks, runs the gamut of depth and sophistication. For example, e-Cop uses CESM (Cyclops Enterprise Security Manager) to recognize threat patterns, often using suggestive data from several sources. The proprietary data-mining techniques uses to extract patterns from data that may indicate threatening situations - much as a physician analyzes symptoms and lab tests to make a diagnosis and recommend a course of treatment. Ultimately, a human being must look at the data, and any automatic analysis of it, and interpret its meaning. The result is usually a severity level assigned to an incident. The provider staff doesn't have to look at the low-severity events - and that is what makes managed security services scaleable and affordable.

18. Getting a Response

Some MSSPs don't actually respond to threatening situations - and some banks like it that way. Banks may be uncomfortable with a third party acting for them in a confrontational situation; they would prefer to assume the responsibility themselves. In such cases, the provider may advise the bank about their options. Some providers simply will not work with banks who don't have adequate resources to respond properly. For instance, some MSSPs won't touch a bank that has fewer than three servers to handle failover properly.

A similar situation exists with those banks that don't want monitoring of any kind: that's simply their idea of security. All they really want is to be able to contact a provider in times of need and get advice about how to handle it. Some help banks develop policies, remedy existing problems, lay a foundation of security and prepare for future incidents.

When a situation does arise, the bank can contact MSSP for suggestions. This may involve stepping the bank through a response, or coming onsite to deal with the problem directly. The bank has control throughout. If security service providers do handle responses, they usually have a hierarchy of predefined reactions, based on the severity of the problem that they can offer in real time. Part of the bank's SLA with the provider defines specific responses to predefined symptoms. Obviously, response is integral to those providers that place their own hardware in the line of fire.

Just because the provider handles the response, however, doesn't mean the bank is out of the loop: The bank's SLA may specify that they are to be consulted before any action takes place. The fast, free, accessible Web makes it relatively easy for MSSPs to provide responses to problems remotely. Some services notify the bank when things are going wrong, explain the situation and the options available, then wait for the bank's instructions on how best to proceed. Others are more direct.

Providers must walk a fine line when it comes to response. Yes, they must defeat attacks, but not in such a way that it interferes with normal enterprise operations. Even a "shut down immediately" response should get the system up and available again as rapidly as possible i.e., "seat belt" style of response: preventative, but unobtrusive. Occasionally, follow-up to a response is necessary. If attacks from one source persist, it may be necessary to specifically block that source. Sometimes the seriousness of an attack may necessitate escalating the matter with law enforcement authorities. Gathering forensic evidence might also be necessary. "Clearly, an attack is more serious if it originates from a competitor than from a student".

19. Score Card

MSSPs supply regular reports to customers, and with good reason: If the providers are doing their job well, the customers may have no notion that any attacks have ever been attempted. Periodic reports noting incidents and responses are often an eye-opener, and let the customer know what they're paying for.
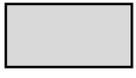
In addition, since MSSPs see so many similar situations, they can typically offer solutions for problems an enterprise may be experiencing. These suggestions may be as obvious as reminding customers of necessary patches or recommended configuration parameters for their systems. It may involve consulting the provider's database of similar environments to determine best practice procedures for the customer.

Recommendations may take a more proactive stance; the provider may suggest changes to hardware, software and procedures that will help to prevent future incidents. Again, this is based on both the previous experience of the provider and their perception of threats for setups like the client's. Some providers can even offer predictions. If their analysis shows a trend in either the types of attacks (in general) or in the pattern of events on the customer's system or both they may be able to predict the likelihood of a certain type of attack. They would also be likely to issue recommendations that would head off such attacks before they occur. Look for this capability to become more widespread, and more in demand.

20. Outsourcing Outlook

It's no secret that outsourced and managed security services are a growing trend. The Internet and e-commerce are creating a rising demand for security. In addition, the atmosphere of mergers and acquisitions make it necessary to secure cobbled - together legacy systems that may have no overarching security scheme. Plus, there's a limited supply of qualified personnel. It makes sense to go to a specialist to handle specialized problems.

21. Conclusion

Network security risks will always be with us. The downside of being in a highly connected network is that we are all connected with the best and worst of society. Security products will not "solve" the problems of Internet security, any more than they "solve" the security problems in the real world. The best we can do is to manage the risks: employ technological and procedural mitigation while at the same time allowing businesses to thrive.

Computer security equals vigilance, a day-to-day process. It's been thousands of years, and the world still isn't a safe place. No matter how fast technology advances, alarms and security services are still state-of-the-art.

The key to effective security is human intervention. Automatic security is necessarily flawed. Smart attackers bypass the security, and new attacks fool products. People are needed to recognize, and respond, to new attacks and new threats. It's a simple matter of regaining a balance of power: human minds are the attackers, so human minds need to be the defenders as well.

On the day you're attacked, you want the best possible defense. It's not enough to give the job to your overworked system administrators or in-house security staff. You need the best, and

you need them immediately. This is why you hire an MSS company: because they can defend you better.

MSS combines people, processes and products to create a security environment for the chaos of modern business networks. The reality of today's Internet makes MSS the most cost-effective way to provide resilient security.

MSS people are network security experts and security analysts are uniquely qualified by their tools, training, and experience to watch entire network, not just a few security devices. They're backed up by the best security experts in the world. They're vigilant, watching your complete network 24x7. They're relentless in protecting your assets. They are adaptive, always one step ahead of the newest hacker group, product vulnerability, or attack tool.

MSS improves a network's security immediately, today. It tells you whether your security is working - and saves you when it isn't. Better than a vulnerability assessment, better than an audit, better than installing more security products, MSS gives you the security you need to keep your business moving ahead. It's the first thing you need to do.

Anyone can install a security product, carry a pager, and pretend to monitor a network; MSS marries the best people and the best processes to provide complete security, resilient security, a level of security unmatched anywhere.