

Successfully Mitigating Corporate Risk

Executive Summary

Organizations are scrambling to adhere to numerous and often-conflicting internal policies, government regulations, third-party mandates and industry best practices pertaining to security. The sheer complexity of the security landscape has created a new “super-risk”: the heightened likelihood that one or more pieces of equipment will be misconfigured or fall out of date with the latest rules or software patches, situations that create corporate vulnerability. Successful risk mitigation in this multifaceted environment requires centralized policy setting and event correlation, frequent risk assessments and audits, and a structured, cohesive approach to updating worldwide equipment, which are all described in this paper.



Complexity is its Own Risk

It is imperative to circumvent configuration errors and policy violations not only to avoid legal liability, fines and other infringement penalties, but also to protect your organization's overall integrity, reputation and brand. Yet mitigating corporate risks has become a multidimensional discipline that requires policy setting and enforcement on many planes. The resulting complexity is becoming one of the largest security challenges that enterprises face today.

There are different types of security breaches to protect against which require different tools. Among them:

- Network breaches exposing the network to other forms of attack
- Data theft, including over-the-network data hijacking
- Malware that causes servers, PCs or virtualized applications to misbehave or become the source of other types of attacks
- Denial-of-service (DoS) attacks that render data unavailable or block network access to authorized users

On top of these threats, a number of industry and regulatory factors, described below, are complicating the security landscape.

Outside Regulation

Organizations are required to comply with varying customer privacy regulations that differ from state to state and country to country. Then there are third-party regulations specific to particular vertical markets. For example, the Payment Card Industry (PCI), an association of credit card companies, sets consumer privacy standards for retailers and others who accept credit cards for payment, a subset of which fall into the IT and networking domains. The PCI doesn't hesitate to impose fines and other penalties for infringements.

Similarly, the Health Insurance Portability and Accountability Act (HIPAA) sets strict mandates for organizations to protect patient privacy in the healthcare industry, and the Gramm-Leach-Bliley Act requires financial institutions to keep consumers' personal financial information confidential. Compliance with such third-party regulations is subject to audit and often requires documentation describing the compliant security measures that are in place and the exact process for changing them. The rules also often mandate that businesses conduct a regular review (weekly, monthly, quarterly or yearly) of security event logs.

Best Practice Standards

On top of these considerations, many companies bolster their security efforts by following industry-standard IT security management best practices, detailed in International Standards Organization (ISO) 27000 series documents. In doing so, of course, each organization puts its own special safeguards in appropriate segments of its network to protect its intellectual property (IP), confidential data and customer information, and to enforce a business continuity plan. But aligning with industry best practices does create still another "layer" of security rules to follow.

Contributors to Security Complexity

- **Dissimilar government regulations from geography to geography**
- **Third-party compliance mandates**
- **ISO 27000 series security management best practices**
- **New Web 2.0 social networking channels entering the organization**
- **Frequent releases of software and security patches requiring constant updates**

Virtualized Data Centers and Cloud Computing

Virtualization and cloud computing are quickly growing popular for their efficiencies in simplifying the IT infrastructure and responding to dynamic traffic, hosting, computing and storage needs. However, having infrastructure in the cloud can create vulnerabilities and leave enterprises open to DoS attacks. In addition, great care must be taken in the configuration and implementation of network designs. Extensive auditing should be completed to help ensure there are no security gaps in the design.

Moving to a virtualized datacenter means moving to two-tier security. In addition to securing physical hosts, now the virtual machines (VMs) on each server also need their own security. Enterprise security teams will need to deploy security tools that account for devices that might change addresses frequently in response to changing workloads, rather than relying on security appliances that protect only the static hardware resources in traditional datacenters.

New Channels into the Organization

Most recently, Web 2.0 technologies have thrown another wrinkle into the security landscape. Twitter, Facebook, YouTube and other popular social networking venues weren't even on corporate radars a year ago. They have now infiltrated the corporate environment for legitimate business and marketing reasons but frequently spill over to employees' personal use.

In short, they create another channel into the organization. Ideally, that channel will be used to improve business awareness and operations. But it is one that could also open up a new avenue for mischief or data theft and make it easier for employees to share sensitive information externally. Social networking sites, for example, are often used to launch phishing scams.

Shift to Mobile and Wireless Networking

Traditional network borders and their associated protections are melting away as volumes of enterprise users move to wireless networking – cellular or Wi-Fi or both – to stay connected and productive while mobile. Methods for securing mobile devices, encrypting both confidential data stored on mobile devices and over-the-air data and credentials, and protecting the corporate network from mobile intrusions such as hacks or malware have emerged as a bona fide sub-discipline of mobile device management, or MDM.

In general, the “consumerization” of information and networking technology has opened – and will continue to open – new avenues into and out of companies, many of which will be used strategically to benefit the organization. As new variations of Web 2.0 applications and mobile networks continue to emerge, security becomes a living, changing discipline that needs constant care and tending. No longer is a “set and forget” approach possible.

The Challenge of ‘Keeping Up’

These factors have created a complex, multifaceted security environment that has become a risk in and of itself. The higher the level of complexity, the greater the number of security layers and the more diverse staff expertise that is required for management and mitigation. As new software patches, bug fixes and security updates are issued from software and networking equipment companies, there is an ongoing requirement to keep pace, which can quickly overburden operations staff and require additional equipment and software investments. And if IT staffs responsible for different aspects of the infrastructure – say, security and application server administrators – don’t work in tandem, some components might get updated while others don’t, creating vulnerability.

For example, a breach occurred in an infrastructure company that had a firewall protecting the Internet connection at a small satellite office. The firewall had not been updated in four years. A command was sent to bot software in the corporate network causing sensitive corporate information from a Lotus Notes database to be sent overseas daily to an unauthorized recipient in a high-risk country. The company had hundreds of firewalls that needed to be kept up to date and was struggling to keep pace with the constant software and security patches that were required. Updating this small office firewall fell through the cracks and jeopardized the security of the company’s and its customers’ information.

Because of such situations, the fundamental question CIOs and others involved in IT security are asking is: How do I accurately create, enforce, filter and correlate all these policies, events and potential violations so I have a clear picture of my security situation at any given time? Their multipronged goal is to make sure the company is always in compliance with various regulations and to curb threats to the confidentiality, integrity and availability of their IP and data.

In addition, mitigating risks requires a top-down management approach where rules are written based on policies that come from upper management. An understanding of security policy should exist across all levels and be part of the corporate culture. Security needs to be an integral part of the operation of the business to help reduce risks.

How to Reduce Risks

The first step is to look at the big picture and assess each data asset in terms of privacy and criticality. This is essentially the same exercise required for business continuity and disaster recovery planning, in that the goal is to protect data from being stolen, compromised or inaccessible – situations that would all have an adverse impact on your business. So both data security and business continuity assessments can be done at the same time.

AT&T writes custom algorithms for enterprises based on United States Department of Homeland Security cyber security alerts and modifies them based on individual corporate risks, vulnerabilities and policies – all as part of the security event and threat analysis that AT&T offers to customers.

There are three primary requirements for getting a handle on your overall security landscape and mitigating risks:

- Regular risk assessments
- Simplification and centralization of tasks
- Policy setting and enforcement

Let’s take a quick look at each.

Risk/Vulnerability Assessment

To conduct a risk and vulnerability assessment, the first step is to engage a set of management tools that are able to discover everything – all network devices, servers, storage devices, software – running on the corporate network. You have to first know what’s out there in order to determine if all components are up to date on policy, relevant compliance mandates and regulations and software patching.

Fortunately, network discovery and security tools have grown quite sophisticated over the past several years. They have been enhanced to collect mounds of security event data out of network and server equipment network-wide, which they spit out in extremely lengthy reports containing granular details about all network activity.

Now that all this information can be captured, however, the bigger challenge has become figuring out how to do something meaningful with it. That requires harnessing it, prioritizing it and organizing it – and doing so rather quickly. Much of the event information captured is irrelevant or duplicated. So it’s important to be able to filter the information so that real and imminent risks are found quickly and that precursors to attacks are identified, allowing the business to avert them before they cause costly problems.

Filtering can be accomplished by writing customized algorithms that separate superfluous information from anomalous activity. Analysis of the data is based on known attack types and traffic history, both within the enterprise and on the open Internet. Many companies do not include a broad view of security issues that have been impacting networks on a global scale as part of the analysis. They also lack data gathering tools, such as analysis software, that help capture and prioritize alert data.

To keep equipment up to date, enterprises must also have the ability to complete multiple device and device-type correlations and conduct regular vulnerability scans. These capabilities require diverse expertise and manpower.

Centralization = Simplification and Reliability

All of the data collected, from both public-facing devices as well as internal devices, should be centrally analyzed to provide a holistic view of the enterprise. The objective should be to simplify the information to help enable faster alerts that are prioritized based on the needs of the business and allow for appropriate responsiveness based on the threat or vulnerability detected.

One of the most reliable ways to do this is to collect event data through a consolidated view of gateways and firewalls (equipment that sits at the intersection of disparate networks, such as between LANs and WANs and between the WAN and the Internet) and then correlate it in a central location. Whether this function is handled in-house or is outsourced, cross-device correlation and aggregation of network event data into a holistic view significantly reduces risk by helping you anticipate when events are going to happen, and it allows you to be proactive about defusing them before they cause harm to the organization.

This is a philosophy being used by telecommunications and government agencies. By centralizing and filtering superfluous information, DoS attacks and spam become more apparent and can be identified quickly. This enables the enterprise to react faster to the event and prevent a catastrophe that might otherwise impact the whole company.

Strong discovery tools or third-party discovery services should have the ability to sift through hundreds of millions of alerts, filter out those that are irrelevant and pare the data down to 100 or 200 events that a network analyst should examine. From there, the analyst should be able to settle on 50 critical events that need attention.

Getting to the point where a network analyst has a manageable number of critical events to focus on is a critical step toward simplification of the complex, holistic network security landscape. Having local IT staffs working out of sync with those in other sites is a recipe for creating vulnerability.

Still, multinational companies have to address different rules and regulations in different countries. This can result in the requirement for different firewall policy settings between networks. In addition, firewall patches are issued regularly, and most large IT departments tend to patch and upgrade equipment in a priority order. This process often results in low-priority locations rarely, if ever, getting touched. A location with a firewall that hasn't been upgraded in several years, in effect, is equivalent to having a location with no firewall at all. It can become a policy violator and a point of entry into the business's overall network and IT infrastructure.

For these reasons, it is highly recommended to centralize the management, upgrading and policy setting of corporate firewalls, even if the policies differ. It's all too easy for local staff to make a change in response to an individual or local request and immediately throw the whole security infrastructure out of whack.

Similarly, it's recommended that there is a specific change management procedure implemented with a limited number of people having permission to authorize changes, and then having those changes made centrally by pre-identified personnel only.

The centralized change management function may be simplified by outsourcing to a large entity that has economies of scale, the latest tools and dedicated security experts who can assess and update the entire network as one cohesive entity. To do this internally would require hiring experts in every country, knowing what type of information can be sent to and from every country, and maintaining a centralized party who would take a holistic view of each country's policy and create a centralized policy that works for all.

Policy Setting and Enforcement

Many of today's firewalls and firewall services combine a number of security functions into one piece of equipment or service. There are multiple "layers" to these functions and those that are engaged and enforced in each firewall depend on the networks between which each one sits (WAN service and private network, private network and the public Internet, public servers and the private network, and so forth). They also depend on the vulnerability/risk associated with that network segment.

One type of policy might be to engage intrusion prevention tools, whether in software, appliance or service form factor, to scan traffic flows for certain signatures indicating an anomaly. Shortly after a virus, worm, Trojan horse, spyware or other form of malware has been discovered and documented, firewall and security software makers quickly create and send patches to their equipment, which is then on the lookout for these known signatures and automatically filters them from traffic flows. This is why it is critical for all equipment to stay abreast of the latest patches; new threats are emerging all the time.

Security programs can also simply look for any "unusual" activity – for example, an unusually high number of communications requests on a particular server or other machine that could make it so "busy" as to eventually render it inaccessible to users.

User access lists and authentication will likely be role based and might differ from country to country, industry to industry, based on the collection of internal best practices and regulatory requirements that a given organization must follow. The same is true for what data gets encrypted, whether it's data on a PC hard drive or running over the network using an IPSec or Secure Sockets Layer (SSL) VPN private "tunnel."

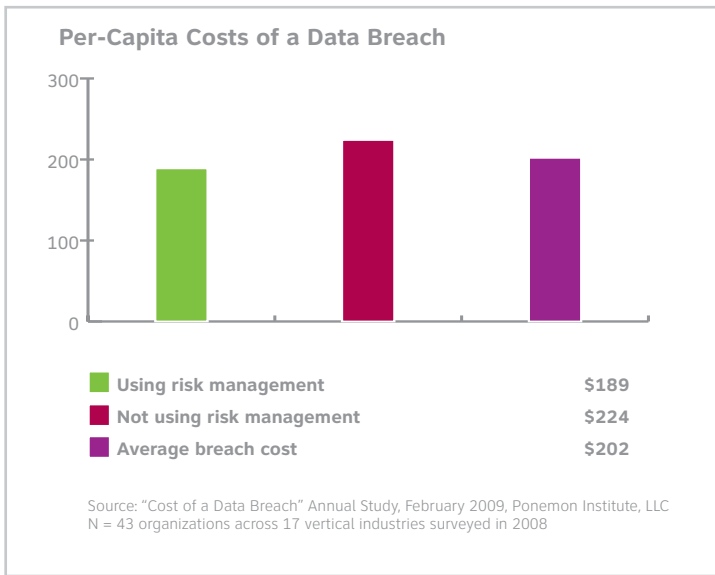
Using a Trusted Third Party

At this point in time, it has become not only challenging but nearly impossible for large, multinational corporations to stay on top of all the necessary, but ever-changing, policies and security settings worldwide that need to be constantly enforced, assessed and audited. A focused and empowered security/network operations center (S/NOC) is required for 24x7 policy and regulatory review, risk assessment, action on imminent alerts and proactive risk avoidance.

Some companies inevitably will continue to attempt to manage and maintain these centers on their own. Such companies will take on the continuing investments required to upgrade equipment, software and staff skills as the landscape continually faces new regulations and threats.

Many, however, will view the state of information and network security as one that has become a discipline in its own right and one that is not a core business function. If given a portal into their own security environments, many organizations find that it makes sense for the continual monitoring, event correlation, assessing and auditing to be

Risk Management Makes a Difference



done by a trusted partner that focuses on the security discipline as part of their core expertise. Such out-tasking partners should be able to process millions of worldwide security events per hour and boil them down into the most important and actionable events.

Third-party security service providers scale worldwide and constantly update their tools and expertise in sync with industry change. In short, for a monthly service fee, organizations can be sure that their third-party S/NOC partner stays on top of the most updated tools and expertise needed to protect the network and IT infrastructure at all times.

In addition, the redundancy needed for business continuity is automatically built in to the outsourcing partner's hardened S/NOC facility, which by definition is automatically set up with equipment redundancy and network circuit redundancy to avoid data loss from downtime.

Conclusion

The sheer number of security threats, combined with the different types of threats and the requirement for different tools to police and mitigate them, have made IT and network security unmanageable for many of even the largest organizations. Throw into that mix disparate regulations and mandates from the world's governments and vertical-industry associations, and complexity itself emerges as one of the biggest risks to corporate data.

Successfully mitigating risks and the liabilities and costs associated with them requires a top-down approach that simplifies the landscape with a centralized view of the whole security architecture. The task requires frequent assessment of what's on the network, understanding whether each component is in compliance with all the policies that pertain to it, and continual patching of all enterprise-wide network equipment to help ensure that no one location becomes a vulnerable channel.

Logging, reporting and filtering millions of network events each hour is a key component of successful risk management so that network security analysts can quickly discover the important events indicating imminent risk and act on them.

It's safer for policy setting, compliance monitoring and upgrading/patching to be handled centrally and enterprise-wide, rather than on a location-by-location basis where staff hurries the process by making changes locally. That willy-nilly behavior can quickly compromise an enterprise's overall security profile.

Some enterprises will inevitably attempt to keep up with the continually changing and growing threats, rules, tools and expertise in-house. However, it can be more effective and less expensive for many to work in partnership with a trusted third party that focuses on security as its core competence and has immediate access to all the latest expertise, tools and equipment necessary to manage the security infrastructure cohesively. Such services generally offer a portal into each customer's own security landscape, reports and alerts. They also follow best-practice processes for policy changes and provide documentation needed to demonstrate compliance with the various and sundry mandates and regulations pertinent to each customer.

About AT&T Security Services

AT&T has a long legacy of developing and managing security services that support a defense-in-depth architecture used to help enforce your security policies. This expertise helps to reduce complexity, reduce costs and provide documentation you can use to validate regulatory compliance. You can count on AT&T as a trusted provider with true global reach for a comprehensive range of security services that provide you integrated solutions to help support your network security environment.

For more information on AT&T Managed Network Services, please contact your local account representative or visit www.att.com/networkingexchange or www.att.com/security.