

Security at Microsoft

Technical White Paper

Published: November 2003

CONTENTS

Executive Summary	1
Introduction: OTG Mission and Priorities	2
Microsoft IT Environment	3
Security Environment	3
Security Principles	4
Trustworthy Assurances	5
How OTG Manages Risk	6
Risk Management	6
The Microsoft Corporate Security Group Risk Management Framework	7
Components of Risk Assessment	8
Data Classification	8
Risk and Controls	9
Security Ecosystem	10
Security Vectors	10
A Risk Management Example	11
Enterprise Roles for Risk Management	13
Security Group Organization	14
Using Risk Management to Create Security Solutions	17
Securing the Network Perimeter	17
Securing the Network Interior	20
Securing Key Assets	22
Monitoring and Auditing	23
Conclusion	25
For Further Information	27

EXECUTIVE SUMMARY

Microsoft is committed to sharing its internal IT security practices in order to help its customers successfully secure their environments. This paper describes what the Microsoft Corporate Security Group does to prevent malicious or unauthorized use of digital assets at Microsoft. This asset protection takes place through a formal risk management framework, risk management processes, and clear organizational roles and responsibilities. The basis of the approach is recognition that risk is an inherent part of any environment and that risk should be proactively managed. The principles and techniques described in this paper can be employed to manage risk at any organization.

The interdependent security initiatives, strategies, and technologies that Microsoft has deployed were implemented in a number of phases. The essential enabling technologies described in this paper run on Microsoft® Windows Server™ 2003. However, most of the technologies were developed when the infrastructure was based on Microsoft Windows® 2000 Server, and can be implemented on Windows 2000 Server. All of the technologies and deployments continue to mature based on evolving security requirements, future strategic plans, and product testing and validation requirements.

This paper is intended for enterprise technical decision makers, security operations staff, and infrastructure engineering staff. It is not intended to serve as a procedural guide. Each enterprise environment is composed of unique circumstances. Therefore, each organization should adapt the approaches, designs, processes, and best practice recommendations described in this paper to meet its specific needs. Note that for security reasons, the domain names provided are for illustration only and do not necessarily reflect actual names.

INTRODUCTION: OTG MISSION AND PRIORITIES

Microsoft Mission:

Enable people and businesses throughout the world to realize their full potential.

OTG Mission:

Proactively deliver IT infrastructure and applications that exceed defined expectations of our clients, customers, and partners—making it easy to work anywhere at any time.

Microsoft Corporate Security Group Mission:

Prevent malicious or unauthorized use of digital assets that results in the loss of Microsoft intellectual property or productivity by systematically assessing, communicating, and mitigating risks.

The Corporate Security Group reports to the Operations and Technology Group (OTG). Prior to examining the Corporate Security Group, it is useful to understand the Microsoft and OTG missions, as well as OTG's IT priorities and IT environment.

The Microsoft company mission is to *enable people and businesses throughout the world to realize their full potential.*

OTG is a highly customer-focused organization with the related mission to *proactively deliver IT infrastructure and applications that exceed defined expectations of our clients, customers, and partners—making it easy to work anywhere at any time.*

The phrase "exceed defined expectations" in OTG's mission reflects an emphasis on service measurement and analysis. This part of the mission is based on the tenet that "you cannot manage what you do not measure." For example, in the IT operations area, expectations are documented in the form of service level agreements. The service level agreement metrics are reviewed monthly in a CIO "scorecard."

OTG's IT priorities are as follows:

1. Be Microsoft's first and best customer
2. Provide intellectual leadership
3. Set a coordinated IT strategy
4. Run a world-class utility

Be Microsoft's First and Best Customer

The primary business of Microsoft is software design. Consequently, OTG has a mission that is unique among global enterprises. For example, in addition to running the enterprise IT utility, OTG plays a strategic role as one of the Microsoft early adopters by testing and deploying Microsoft software before its release to customers. In addition to benefits Microsoft realizes through product feedback from testing for scale and load in a real-world production environment, these evaluation efforts must provide tangible business benefits to Microsoft. For example, as of October 2003, OTG ran the corporate infrastructure on Windows Server 2003 with approximately 4,200 servers deployed (which include 800 infrastructure servers and key line-of-business applications). In addition, the corporate website, www.microsoft.com, has over 600 servers running Windows Server 2003. Internal real-world evaluation activities drive a very high rate of change in the environment, with many more deployments to servers and desktop computers than is typical at enterprises of comparable size.

Provide Intellectual Leadership

OTG drives the early adoption of technologies that help define the Microsoft vision of the leading-edge IT professional, developer, and information worker. OTG also provides product feedback to the Microsoft product development groups.

Set a Coordinated IT Strategy

OTG leads the process that defines and delivers high-value IT solutions at both the business-unit level and the enterprise level. Setting strategy is a critical OTG function because the IT infrastructure is centralized, whereas line-of-business application development is decentralized. Although application development occurs independently in each business unit, OTG provides centralized support for applications, hosting in the data center, and

architectural guidance and standards (including security standards).

Run a World-Class Utility

A unique challenge for OTG is to deliver on all the previously mentioned priorities while providing world-class availability, reliability, and cost-effectiveness in a global environment that includes high client expectations and technically skilled users.

The Corporate Security Group, OTG, and Microsoft missions are aligned in several ways. For example, measurement is key to successfully fulfilling both the Corporate Security Group and OTG missions. Additionally, the Corporate Security Group focus on productivity and intellectual property is necessary to support the Microsoft company mission, which is focused on people and businesses. Through this alignment, the Corporate Security Group has effectively partnered with business owners throughout Microsoft to develop an appropriate security strategy.

Microsoft IT Environment

Another factor to consider when understanding the Corporate Security Group's approach to security is the IT environment. OTG operates a large and dynamic IT environment that is critical to the success of Microsoft. OTG is responsible for managing IT services for more than 55,000 employees and more than 300,000 computers that span over 400 sites worldwide on an around-the-clock basis. Over 300 of the sites are sales and marketing offices distributed in major worldwide cities. IT-managed infrastructure exists at over 200 of those sites.

The early deployment of technology and continual growth at Microsoft result in a highly dynamic environment. This environment houses more than 1,600 line-of-business applications that range from a single SAP R/3 instance used globally to specialized departmental or even workgroup applications for groups such as research, product support, and product development. OTG provides support and tracking for all line-of-business applications. Additionally, e-mail is a mission-critical application at Microsoft. Approximately 8 million e-mail messages a day flow to and from the Internet, and 4 million e-mail messages a day circulate internally.

The Microsoft corporate network is the world's largest experimental computer network. Although a variety of network protocols are run for development and testing purposes on the Microsoft corporate network, the environment is primarily Transmission Control Protocol/Internet Protocol (TCP/IP) based. It employs a high-speed (170 gigabits per second) asynchronous transfer mode (ATM) backbone over Synchronous Optical Network (SONET) to move massive amounts of digital data and voice messages.

Security Environment

Microsoft operates in an extremely active and challenging security environment. Challenges include the following:

- Each month, Microsoft experiences approximately 100,000 intrusion attempts.
- Each month, Microsoft probes, scans, and quarantines over 125,000 virus-infected e-mail messages.
- Microsoft has unique IT environments for product development, testing, and support, which require special security.

- Most Microsoft employees are highly technology literate and routinely explore the limits of the tools available to them in order to improve product quality.

This combination of factors—an evolving security landscape full of potential vulnerabilities operating across a large and dynamic IT environment—presents a challenging array of variables for a security organization to comprehend, organize, and address. The Corporate Security Group developed mechanisms to comprehensively understand, communicate, and prioritize security problems in order to facilitate an effective decision support capability. This decision support system is guided by security principles in an effort to deliver assurances about the security of the IT environment.

Security Principles

Security principles are fundamental concepts used to design, develop, and operate secure systems. The Corporate Security Group categorizes security principles as shown in Table 1. Each category in the table represents a key area in which to evaluate security.

Table 1. Security Principles

Category	Security principle
<p>Organizational:</p> <p>Directed to management's commitment to risk management and security awareness</p>	<p>Manage risk according to business objectives</p> <p>Define organizational roles and responsibilities</p> <p>Invest in secure design</p> <p>Commit to secure operations</p>
<p>Users and data:</p> <p>Includes authentication, user privacy, and data authorization</p>	<p>Manage to practice of least privilege</p> <p>Base decision on data classification and fair use</p> <p>Enforce Privacy and Personally Identifiable Information protection</p> <p>Ensure data integrity</p> <p>Monitor identity assurance</p> <p>Build in availability</p>
<p>Application and system development:</p> <p>Dedicated to the design and development of secure systems</p>	<p>Build security into the life cycle</p> <p>Design defense in depth</p> <p>Reduce attack surface</p> <p>Keep it simple</p>
<p>Operations and maintenance:</p> <p>Encompasses people, processes, and technology to build, maintain, and operate secure systems</p>	<p>Plan for system maintenance</p> <p>Enforce secure configuration and hardening</p> <p>Monitor and audit</p> <p>Practice incident response</p> <p>Verify disaster recovery</p>

The Corporate Security Group uses security principles to:

- Enable customers and partners to understand and incorporate security concepts in

their design, development, and operation of secure systems.

- Organize and communicate security policies, requirements, and guidelines across Microsoft.
- Improve the way security problems are communicated both internally within the company and externally to Microsoft customers.

These security principles influence the decision support system and guide the delivery of assurances about the state of security in the IT environment of the corporate network.

Trustworthy Assurances

The Corporate Security Group created the “Five Trustworthy Assurances” as a mechanism to capture presumptive expectations that every member of the IT environment has about security. These assurances are used to communicate where OTG can and cannot commit to protecting digital assets. They also allow the organization to holistically evaluate its success in reaching the goal of providing trustworthy digital assets to corporate users. The trustworthy assurances are one component of a decision support system. The five assurances address availability, privacy, and security as fundamental elements in risk analysis.

The Five Trustworthy Assurances that OTG provides for the IT environment are as follows:

1. My identity is not compromised.
2. The resources I need are secure and available, defined as follows:
 - **Secure.** Free from tampering, free from unauthorized access.
 - **Available.** Free from security vulnerabilities, available per service agreements.
3. My data and communication are private.
4. I understand my role and I am accountable for my responsibilities to ensure a secure environment.
5. I receive timely responses to the risks affecting me.

To provide these assurances, the Corporate Security Group uses a risk management approach. Risk management is the process of identifying, evaluating, and mitigating risk on an ongoing basis. A risk management approach to security recognizes that the cost of security must be balanced against business needs. Microsoft uses a risk management approach to systematically evaluate and prioritize security risk, supporting an effective decision support capability.

How OTG MANAGES RISK

The remainder of this paper focuses on how the Corporate Security Group manages risk, how the IT environment is divided into manageable components, and what Microsoft does internally to prevent malicious or unauthorized use of digital assets. Where available, links to detailed information are provided.

Risk Management

Risk management provides organizations with a consistent, clear path to organize and prioritize limited resources to manage risk to the business. The benefits are realized by developing a cost-effective control environment that drives down risk to an acceptable level.

Figure 1 shows the overall risk reduction through application of the risk management framework.

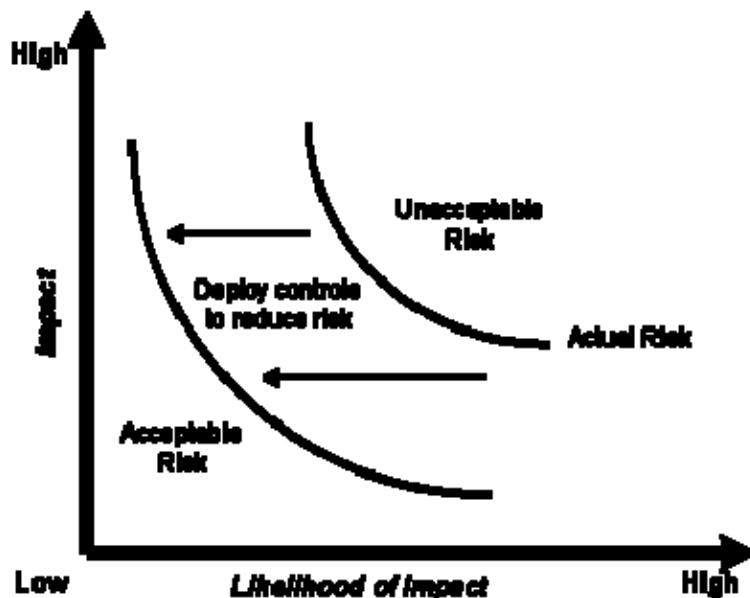


Figure 1. Risk management summary

The definition of acceptable risk, and the approach to manage risk, varies for every business. There is no right or wrong answer; there are many risk management models in use today. Each model has tradeoffs that balance accuracy, resources, time, complexity, and subjectivity. The Corporate Security Group risk management model is a combination of various approaches, such as pure quantitative analysis, return on security investment analysis, qualitative analysis, and best practice approaches.

To organize and prioritize efforts for mitigating risk to Microsoft digital assets and adopting security controls, the Corporate Security Group developed a framework based on a traditional risk management model.

The Microsoft Corporate Security Group Risk Management Framework

Investing in a risk management process—with a solid framework and defined roles and responsibilities—prepares the organization to articulate priorities, plan to mitigate threats, and address the next threat or vulnerability to the business. To better manage security risks, the Corporate Security Group follows a traditional risk management approach consisting of an iterative four-phase process:

1. **Assess risk.** Execute a risk assessment methodology to evaluate risk.
2. **Define policy.** Develop security policy to mitigate risk.
3. **Implement controls.** Organize people, processes, and technology designed to mitigate risk, as justified by a cost/benefit analysis.
4. **Audit and measure.** Monitor, audit, measure, and control environments for effectiveness.

Figure 2 shows the steps in the Corporate Security Group risk management framework.



Figure 2. Risk management framework

The first phase in the framework is to assess risk by performing a risk assessment. To perform the risk assessment, the Corporate Security Group uses the security principles as a guide across each category.

The second and third phases define and implement security controls. Security controls can be technology implementations (smart cards, or network segmentation through IPsec) or can be behavior policies (prohibiting use of unauthorized modems).

The fourth and final phase assesses risk after implementation of the security control to measure effectiveness. This measurement is used to compare the anticipated risk level after implementation of the security controls to actual risk level achieved. This new risk level is used as an input in the next cycle of risk assessment.

Components of Risk Assessment

The first phase of the risk management process, the risk assessment, represents an important step in understanding security problems for the business and prioritizing reduction of risk within available resources. Figure 3 presents the basic components of the risk assessment.

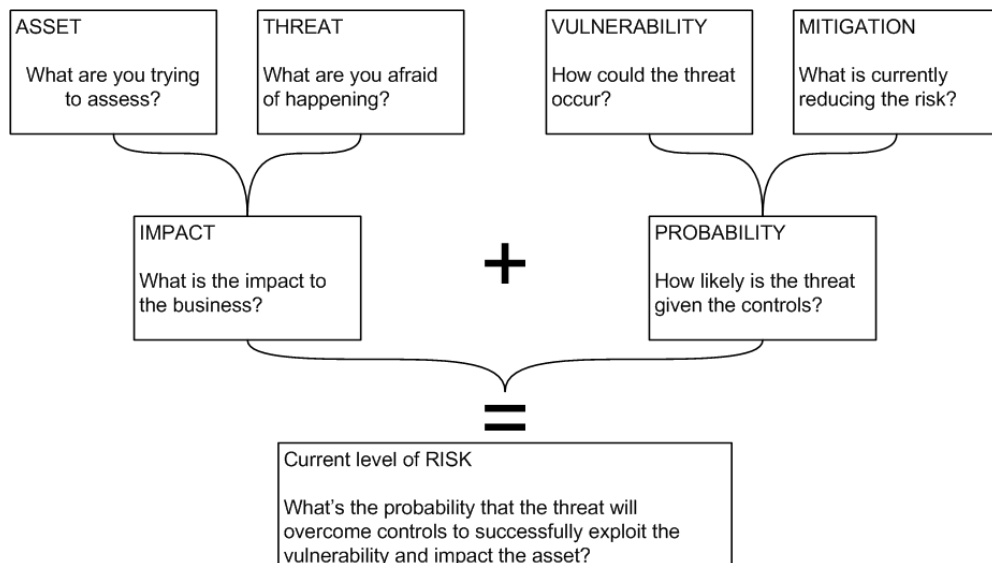


Figure 3. Components of risk assessment

By communicating a consistent structure for evaluating the components of risk, digital asset owners and OTG have a common taxonomy to track progress and contribute to the evaluation process. It is important to note that many stakeholders are required to sufficiently address each component. This is especially true for the more subjective areas of business impact costs, the likelihood of vulnerabilities occurring, and the larger cost/benefit analysis when evaluating new control solutions. Stakeholders can include risk management experts who are involved in calculating risk, security analysts who know specific vulnerabilities and threat probabilities, data owners who understand the value of the digital assets under consideration, and security architects and engineers who can identify potential security controls to mitigate risk.

To better understand “impact” and to apply increasing levels of security controls based on the combination of asset value and risk, the Corporate Security Group developed a classification system to group assets by value.

Data Classification

Not all digital assets carry the same level of value to the business. Some assets are of low value and may not justify the costs of achieving the Five Trustworthy Assurances. Other assets are so valuable that the cost of additional controls to achieve the Five Trustworthy Assurances is justified. The majority of digital assets at Microsoft require the level of risk reduction represented by the Five Trustworthy Assurances.

To organize the reduction of risk to an acceptable level in a cost-efficient manner, the Corporate Security Group categorizes digital assets into data classes. Data classes help

ensure that plans to protect digital assets are cost effective and properly prioritized. In addition, they provide insight into asset impact, which is a key variable in assessing overall risk.

Although several prominent data classification taxonomies exist, the classes used by the Corporate Security Group fit into the following three areas:

- Highest Value class.** Consists of the most valuable Microsoft digital assets. The Corporate Security Group commits to provide multiple strong measures to exceed the Five Trustworthy Assurances. In this class, the cost of additional controls is justified by the business need to reduce the overall level of risk to the assets to a very low level. For example, the Windows source code servers house valuable intellectual property. Compromised source code could lead to a significant negative impact on the company. Increased levels of security controls and costs are therefore justified.
- High Value class.** Consists of the vast majority of desktop computers and servers and most OTG-provided services. For example, file share servers, e-mail infrastructure, and Microsoft operations and planning data are assets within this class. The Corporate Security Group commits to deliver the Five Trustworthy Assurances without any special action on the asset owner's part.
- Low Value class.** Consists of the assets that have relatively low risk and that do not justify costly security controls. For example, some test labs have little valuable data and can accept the risk of potential data loss. In this case, an adequate level of risk reduction may be obtained through basic network controls, scanning for security vulnerabilities, and installing antivirus software. The Corporate Security Group does not commit to providing the Five Trustworthy Assurances for assets in this class but assists in providing a lesser degree of IT services and risk mitigation based on business need, to ensure that assets in this class do not become a risk to higher-value assets.

Risk and Controls

A core tenet of risk management is to match the policy and controls to the amount of risk acceptable to digital assets. Table 2 illustrates how controls are applied based on the data class. As the data class value decreases, so do the number and cost of the controls.

Table 2. Data Class vs. Security Control Examples

Data class	OTG service examples	Security control examples
Highest Value	Highest-value OTG-managed services <ul style="list-style-type: none"> Source code access HR data management 	User: two-factor authentication, explicit user authorization required Device: IPsec required with explicit user and computer authorization
High Value	OTG-managed services <ul style="list-style-type: none"> File sharing Mail 	User: single-factor authentication, authorized user-defined groups Device: IPsec required
Low Value	Basic OTG network services <ul style="list-style-type: none"> Network connectivity for intranet 	Authentication: single-factor, restricted services (for example, service limited to Outlook Web

	browsing or virtual private network (VPN) <ul style="list-style-type: none"> Limited network connectivity to allow compliance checking 	Access)
--	---	---------

No amount of controls can totally eliminate risk. The assumption of some risk is “by design.” Understanding where to add to controls to reduce risk to an acceptable level is the key to achieving a secure IT environment.

Security Ecosystem

Viewed as a whole, an enterprise IT environment can be unwieldy. An enterprise IT environment is characterized by constant change and is not conducive to “one-size-fits-all” solutions for security. The Corporate Security Group approach to this problem is to decompose the Microsoft enterprise into manageable security components that compose the Security Ecosystem. The ecosystem consists of distinct components interacting with each other and the external environment. At Microsoft, the ecosystem is viewed as including five environments: data centers, managed clients, unmanaged clients, remote access clients, and extranets. The elements that define an individual environment include the data, computers, people, and functions that share a common business purpose. Dividing the enterprise IT environment into these five components allows Microsoft to organize security risk into smaller, more targeted areas.

Security Vectors

After the individual components of the ecosystem are identified, a framework is needed to decompose those components into groupings that aid the Corporate Security Group in identifying vulnerabilities and targeting security controls for the components. The framework that the Corporate Security Group uses consists of the following five vectors:

- **Network.** Data transport and infrastructure devices.
- **Host.** Operating system and core services (for example database servers, Web servers, mail servers, file shares).
- **Application.** Internally and externally developed applications.
- **Account.** Device or user credentials associated with identity.
- **Trust.** Administration models mapped to the Active Directory® directory service and certificate-based trusts.

An individual component of an ecosystem and the five vectors is represented in Figure 4.

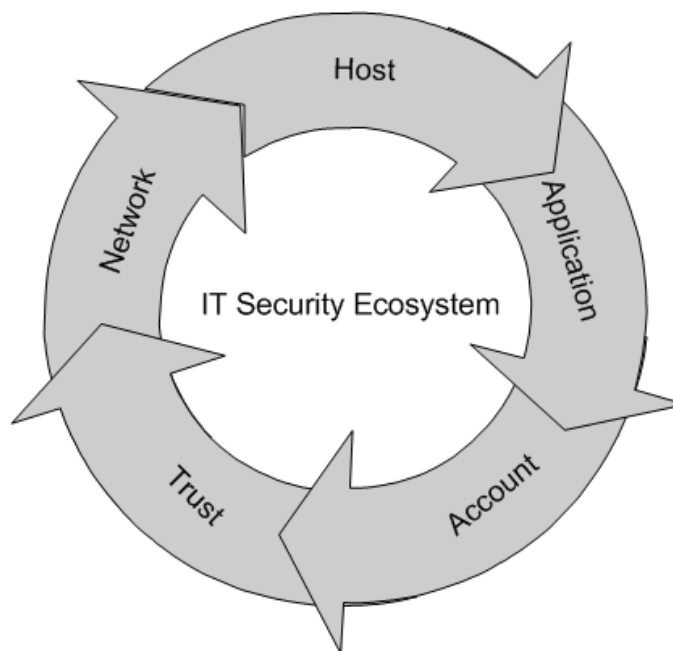


Figure 4. Ecosystem Component and Five Vectors

The concepts of an ecosystem and five vectors allow the Corporate Security Group to organize the security problem space. With a risk management framework in place, ecosystem components can be evaluated independently for risk and can be targeted independently for appropriate security controls.

The ecosystem, the five vectors, and a risk management approach combine to yield risk assessments that are appropriate to an individual ecosystem component's business requirements. For example, in evaluating the risks of remote users connecting to the corporate network, several controls were put in place as a result of the assessment of the five vectors. Threats were identified in four of the five vectors, including the following:

- Host: unauthorized access to data on another computer
- Application: unauthorized access to internal applications through the remote computer
- Account: unauthorized access to credentials that may be used to expand or escalate privileges
- Network: denial of availability through network flooding from the remote computer

A Risk Management Example

In this section, OTG's "Network Segmentation with IPsec" project is used as an example of how the Corporate Security Group uses the risk management process—from identifying a particular risk to actually deploying a technical countermeasure to mitigate that risk. This initiative is referred to as the IPsec project.

The goal of the IPsec project is to group corporate network hosts into two broad categories: managed computers and unmanaged computers. This logical segmentation works to mitigate risks posed to OTG-managed computers by ensuring that network-level access is allowed only from devices that meet OTG security requirements and by denying, by default, access from unmanaged devices. OTG defines its managed computer population as those

computers that are joined to OTG-managed Windows Active Directory domains that are subject to OTG monitoring and patching mechanisms. Many of the unmanaged devices on the Microsoft network are primarily used for product testing, debugging, and/or private lab use and are not joined to OTG-managed domains. Corporate IPsec policy specifies Kerberos as its preferred authentication mechanism and also enables the use of computer-based digital certificates as a secondary authentication mechanism.

In the IPsec project example, the Corporate Security Group determined that OTG-managed computers were exposed to unnecessary threats resulting from network layer attacks launched by unmanaged computers on the Microsoft corporate network. A risk assessment measured the threat and probability of impact. Next, detailed security requirements were developed to address this risk. Infrastructure architects and network engineers then considered and compared control alternatives and determined that logical segmentation through IPsec was the best technical solution. A project implementation team was formed, and the IPsec deployment began. The effectiveness of the solution in mitigating identified risks will be assessed during implementation and after completion of the deployment.

Risk assessment for the IPsec project included the following:

- *Asset:* Protecting digital assets in the Highest Value and High Value data classes.
- *Threat:* Unauthorized access, compromise of data integrity “over the wire,” and information gathering that may lead to an expanded attack.
- *Impact:* Microsoft suffers lost revenue and reputation from stolen or damaged data and intellectual property. Microsoft employees lose productivity.
- *Vulnerability:* Attacks may occur from network-level threats such as buffer overflow attacks, exploit of unpatched vulnerabilities, and exploit of system misconfiguration. Hackers could also compromise unmanaged computers, which in turn could be used to attack managed computers.
- *Current Controls:* Antivirus software, screening routers and firewalls, patch management, centrally managed security configurations, and other measures.
- *Probability:* High. Even with current controls, attacks have occurred and will likely happen again.
- *Current Level of Risk:* There is a medium to high probability that within the next year, a successful attack will occur that could compromise the High Value and/or Highest Value data class.

ENTERPRISE ROLES FOR RISK MANAGEMENT

The Corporate Security Group plays a key role in prioritizing risk and measuring compliance. However, it is important to recognize the contribution and ownership of other operating groups and stakeholders. To maintain independence between the Corporate Security Group and the operating functions, OTG defined roles to determine the optimal balance of separation of duties while encouraging collaboration across groups.

Table 3 outlines the roles and responsibilities in managing risk in OTG. The deliverables in the table are based on the IPsec project example.

Table 3. Risk Management Roles

Task	Organization ownership (role)	IPsec project deliverable
1. Identify and prioritize IT risks across the organization.	The Corporate Security Group has primary ownership.	The Corporate Security Group delivered a list of identified and prioritized risks to managed computers from unmanaged computers.
2. Define security policy to reduce risk to an acceptable level.	The Corporate Security Group has primary ownership, leads the collaborative process across OTG and business owners to define appropriate policy.	The Corporate Security Group delivered a security requirements document that specified segmentation between managed and unmanaged computers to mitigate identified risks.
3. Develop solutions to reduce risk.	Engineering and OTG Operations are primary owners, with Corporate Security Group contribution.	Infrastructure architects and network engineers designed a solution based on IPsec technology. Operations implements, deploys, and monitors the IPsec project.
4. Operate the solution effectively.	OTG Operations has primary ownership.	All support tiers were trained and the support process was put in place.
5. Audit and monitor to measure compliance.	The Corporate Security Group enforces policy.	During and after the deployment phase, the Corporate Security Group audited and evaluated the effectiveness of the solution.

Figure 5 shows the organizational mapping of each role to a deliverable at each step of the risk management process.

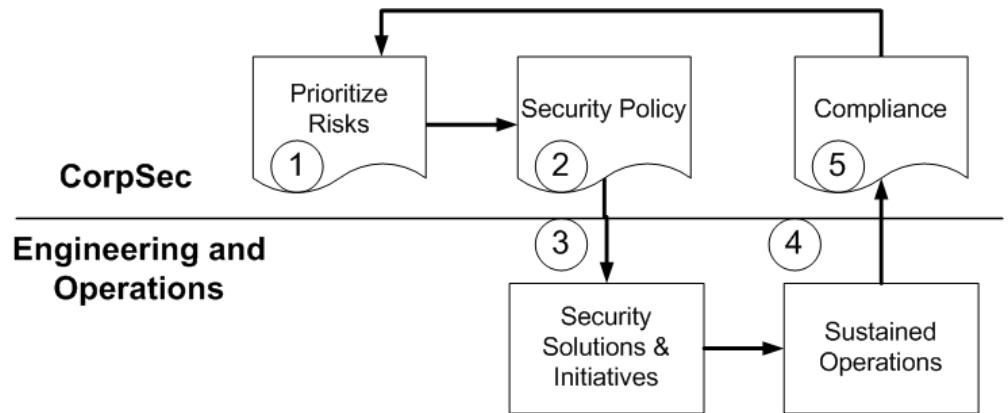


Figure 5. Tasks and organization roles in the risk management process

The risk management process benefits from clearly defined roles and responsibilities because translating security risk into appropriate control solutions is complex. Many organizations and groups are involved, and it is important for each to understand the parameters of its contribution to achieving and maintaining an effective security control. Security specialists are often needed to evaluate and communicate risk to the business. However, the accountability to protect and maintain digital assets ultimately resides with the asset owner.

Security Group Organization

The Corporate Security Group mission is to *prevent malicious or unauthorized use that results in the loss of Microsoft intellectual property or productivity by systematically assessing, communicating, and mitigating risks to digital assets*. A team of trained professionals is required to manage enterprise IT security risks. The Corporate Security Group defines its organizational roles as shown in Figure 6.

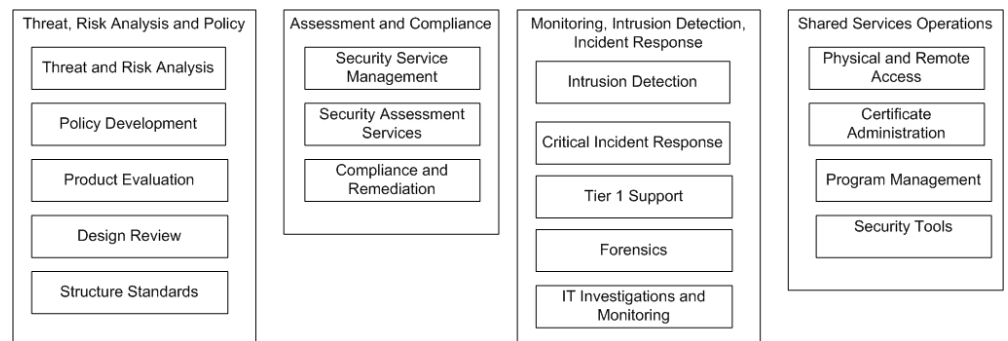


Figure 6. Microsoft Corporate Security Group teams and roles

Threat, Risk Analysis and Policy

The Threat, Risk Analysis and Policy team serves as the single, authoritative source for security policy, risk assessment, and ownership of the risk management framework.

This team assesses and prioritizes IT assets, risks, and mitigations across present environments. The team also manages the process to analyze and manage future risks and mitigations. Primary responsibilities include:

-
- Develop a single, authoritative source for security policy and requirements. Ensure that all policies can map to mitigations of risks identified.
 - Be Microsoft's best security customer through early adoption of Microsoft and third-party security products.
 - Provide a consistent, scalable security design review process that provides threat assessment and secure design consulting, including subject matter experts throughout the Corporate Security Group.
 - Drive security standards for high-risk areas.

Assessment and Compliance

The Assessment and Compliance team consists of subject matter experts across all aspects of security auditing and real-world threat assessments. Primary responsibilities include:

- Security service management: Improve the security of key environments by defining security requirements; developing policy; and driving auditing, monitoring, and remediation plans.
- Security assessment services: Help secure critical IT assets in compliance with security policies and standards through the delivery of premium IT security assessment services. For example, the Attack and Penetration Team provides real-world threat assessment auditing and consulting services across all layers of the ecosystem, including controls on the network, host, application, trust, and account levels. The team's objective is to measure the effectiveness of OTG security controls against highly skilled internal and external threats and then assist in developing cost-effective risk mitigating solutions.
- Compliance and remediation: Ensure that accounts, trusts, hosts, and networks within managed environments comply with Corporate Security Group policies by systematically identifying vulnerabilities and driving remediation with owners.

Monitoring, Intrusion Detection, and Incident Response

The primary responsibilities of the Monitoring, Intrusion Detection, and Incident Response team include:

- Intrusion detection: Monitor activity and events across environments.
- Critical incident response: Respond to and remediate against network intruders across environments.
- Tier 1 security support: Provide rapid response/resolution to smaller virus/network attack issues.
- Forensics: Provide host digital evidence recovery services.
- IT investigations and compliance monitoring as follows:
 - Investigate all reported unauthorized network access.
 - Investigate all unauthorized instances of peer-to-peer file sharing.

Shared Services Operations

The Shared Services Operations team is responsible for supporting security infrastructure and access management. Primary responsibilities include:

-
- Develop and manage a responsive U.S. Physical Access and Global Remote Security Access program.
 - Manage the public key infrastructures with centralized client support, including:
 - Smart card issuance.
 - Tier 2 and Tier 3 support and troubleshooting.
 - Card access issuance.
 - Solution design with crypto focus.
 - Public Key Infrastructure (PKI) certificate support and troubleshooting.
 - Program manage Corporate Security Group initiatives to drive mitigations for the top information security risks.
 - Manage security tools.

USING RISK MANAGEMENT TO CREATE SECURITY SOLUTIONS

When initiating a risk management program by using the framework described earlier in this paper, Microsoft (like other enterprises) faced myriad security risks. OTG evaluated risks across the five ecosystem environments and five vectors and organized risk mitigation tactics into four execution groups as follows:

- **Securing the network perimeter.** Plugging holes in the network perimeter so that intruders and malicious code cannot easily access the network.
- **Securing the network interior.** Managing user accounts, policy, and client and server security configuration inside the network perimeter.
- **Securing key assets.** Ensuring that key assets are secured and regularly checked for vulnerabilities.
- **Monitoring and auditing.** Enforcing compliance on an ongoing basis.

The formation of the execution groups resulted in identification and implementation of several projects and tactics, such as the Network Segmentation with IPsec project. OTG's approach combined the projects and tactics to achieve comprehensive defense-in-depth security.

In 2000, the Corporate Security Group created a PKI that established a foundation that has been used by many of these projects. The PKI hierarchy built by OTG is made up of three tiers: an offline corporate root authority, offline subordinate authorities, and multiple online enterprise issuing authorities. The offline root authority is a self-signed entity and is the anchor of all PKI trust. This authority is used solely to subordinate other intermediate authorities. These intermediate authorities are then used to subordinate online issuing authorities in multiple network and Active Directory environments throughout Microsoft. The issuing authorities interact with Active Directory and are responsible for the issuance of all certificates to users and systems.

Securing the Network Perimeter

The aim of securing the network perimeter is to block as many attacks as possible before they can gain access to the network. To accomplish this, OTG used targeted tactics and initiatives to deploy the solutions described in the following paragraphs.

Smart Cards for Remote Access

More than 65,000 Microsoft workers worldwide gain access to Microsoft corporate e-mail accounts, files, and computer network resources through remote access—for example, by using direct dial and VPN. OTG manages more than 250,000 remote access connections each week. To manage threats from malicious users, OTG implemented two-factor user authentication by using smart cards. Two-factor authentication significantly increases the assurance that remote connections are initiated by valid users. Over 65,000 smart cards have been distributed worldwide to the workforce. For more information about the implementation of smart cards for remote access, see <http://www.microsoft.com/technet/itsolutions/msit/security/smtcrdcs.asp> and <http://www.microsoft.com/technet/itsolutions/msit/security/smartcrd.asp>.

Secure Remote User

Unmanaged computers connecting to the network from remote locations can compromise a

company's overall network security. Unmanaged computers are those for which the organization's IT professionals cannot control the operating system security settings, the installation of security patches, or specialized security software. The organization's group policy does not extend to these computers. As a consequence, they frequently are missing critical security patches or are otherwise not configured according to IT security policies and standards. Under the Secure Remote User (SRU) initiative, remote access connections to the corporate network are permitted only if the device is validated as meeting security requirements. Group Policy settings require remote users to connect by using Connection Manager with customized profiles and scripts that perform system configuration checks, update antivirus software and signature files, enable Internet Connection Firewall, disable Internet Connection Sharing, and enforce the use of a minimum Windows version (Microsoft Windows XP Professional Service Pack 1 at the time of this writing).

Secure Wireless Access

OTG has deployed more than 4,000 wireless access points (APs) worldwide, including over 2,100 in the Puget Sound region. The APs enable wireless network connectivity to more than 30,000 employees. Before each user can access the wireless network, he or she must be uniquely authenticated through the 802.1X client authentication protocol, which is built into Windows XP Professional and the Windows Server 2003 family. In addition, Pocket PC 2002 is 802.1X capable with selected wireless local area network (WLAN) hardware. As of this writing, the implementation uses Extensible Authentication Protocol (EAP)/Transport Layer Security (TLS) with certificates as the authentication method. Computer account certificates and/or user account certificates are used. Each wireless session between a user and/or device and the wireless network must be uniquely encrypted. Users and devices must both be periodically reauthenticated during a wireless session. By policy, non-OTG-managed wireless access points, called "rogue" APs, are prohibited on the corporate network. Like many enterprises, OTG scans for rogue APs and is evaluating automated detection and management technologies. For more information about the secure WLAN at Microsoft, see the technical case study *Mobility: Empowering People through Wireless Networks* at <http://www.microsoft.com/technet/itshowcase>.

Perimeter Messaging Firewall

Enabling e-mail access over the Internet for mobile employees through services such as Outlook Web Access (OWA) and Outlook Mobile Access (OMA) requires servers that are accessible to both the Internet and the corporate network. To reduce the risk of intruders gaining unauthorized access, OTG deploys Microsoft Internet Security and Acceleration (ISA) Server 2000 Feature Pack 1 in front of front-end servers running these messaging services. The front-end servers are homed on the corporate network and are not connected to the Internet. Instead, the server running ISA Server connects to the Internet and to the corporate network. Users are connected to the external interface of ISA Server, but the behavior is as if they are directly connected to the front-end server. This approach provides defense-in-depth coverage of systems that connect to the corporate network over the Internet, removing those systems from direct risk of Internet attack by placing them behind a firewall. Configuration includes hardened firewall security settings, network isolation, application filtering, and protocol filtering. For more information about ISA Server, see <http://www.microsoft.com/firewall>.

E-Mail Antivirus

OTG's approach to managing virus risk goes beyond filtering software alone. The layered defense includes deploying antivirus software on all desktop computers, servers, e-mail gateways, internet gateways, and Personal Digital Assistants (PDAs). Computer Associates eTrust is used on all desktop computers and fully managed servers, except the gateways, which run Trend Micro InterScan Viruswall and also Brightmail software. About 5 million inbound e-mail messages are scanned every day. On average, 800 viruses are stripped per day, and approximately 2.4 million junk e-mail messages are filtered per day.

Secure Extranet and Partner Connections

OTG maintains extranet environments that connect to a variety of business partners. Microsoft cannot guarantee that the physical and IT device security standards enforced internally are also enforced on devices owned and used by external partners. As a result, these devices—typically used to conduct business and exchange information with Microsoft—can be used to exploit vulnerabilities, attack Microsoft, and put Microsoft assets and intellectual property at risk. Therefore, OTG targeted the following four initiatives at securing the extranet:

- **Smart Cards for Administrators.** The theft of a domain administrator's credentials can jeopardize the integrity of an entire domain. Risk associated with this threat can be mitigated by requiring smart cards on domain controllers and selected "High Security" member servers located on the extranet. ("High Security" servers are defined as servers that require additional controls because either the data they contain or the harm that can be caused by their compromise is substantial.) Smart card readers are installed on domain controllers and these servers. A flag is set on administrator accounts to require smart cards for interactive logons.
- **Vendor Network Retirement/Migration/Remediation.** Network and server security in vendor networks was not compliant with security standards and was challenging to manage due to the number of environments and the architecture of vendor networks. Therefore, the services residing on those networks were audited, and the service owners were identified. As a result, most business partner applications are now hosted on the extranet. Vendor connections have been either re-homed to the extranet or migrated to the Internet. Network and vendor connections have been decommissioned such that all partner connections are owned and managed by OTG. This gives OTG the ability to end connections in any Microsoft-owned partner environment immediately and at any time.
- **Partner Account Security.** Microsoft assets were at greater risk on the extranet because of external exposure and delegation of user management tasks. As a result of this project, all partner accounts now must be owned and managed by OTG and adhere to all account and password policies applied to accounts on the corporate network. In addition, local member server accounts can no longer be created in partner environments. All partner local administrator accounts on all OTG-managed servers were consolidated by requiring a unique password for local administrator accounts and by requiring a single local account for maintenance by OTG personnel. Shared account vulnerabilities were mitigated by restricting the use of shared domain accounts for services, and by restricting service use of domain administrator privileges. Unused new accounts after 30 days were deleted and inactive accounts were disabled. Disabled accounts were restricted from interactive logon, from logon as a service or batch job, and

from the ability to log on across the network. Credentials were restricted to their intended logon rights, and inactive partner accounts and shared partner accounts were eliminated.

- **Eliminate Direct Vendor Connections.** Partners are now required to authenticate themselves at a perimeter access control point prior to gaining access to the Microsoft corporate network. Access is limited and enforced to only those systems and network resources required by vendors to conduct their business with Microsoft. The perimeter access control points are implemented through ISA Server firewalls in combination with Remote Access Policy (RAP) restrictions available with Internet Authentication Service (IAS).

Securing the Network Interior

The aim of securing the network interior is to ensure strong authentication and authorization for users and computers on the corporate network. To secure the network interior, OTG deployed the solutions described in the following paragraphs.

Reduce Shared Service Account Vulnerabilities

Applications use services (a type of background process) to perform work on, or obtain information from, a server. Prior to Windows 2000, services accessing resources on a network were required to use a domain user account in order to authenticate themselves to each remote server they used. Tools are available that allow administrators of a given computer to expose account user name and password information for all services configured on that computer.

OTG implemented a project to convert many services to use the LocalSystem operating-system-owned account present in Windows 2000 and later operating systems. Applications using services that required domain-level administrative privileges or that did not support computer account authentication used alternative configurations. These configurations included using unique accounts and passwords on each computer, treating the computer on which the service operates as a “High Security” server, or configuring applications by using services on multiple computers to minimize management overhead on a case-by-case basis.

Consolidate Local Administrator Accounts

When the domain membership of an OTG-managed server is damaged or unverifiable, administrative activities must be performed directly on the server through the use of a local administrator account. OTG maintained at least four such accounts on each OTG-managed server for this purpose. This situation created a vulnerability whereby the compromise of a single local administrator account could expose many other OTG-managed servers. To mitigate this risk, a unique password requirement for all local administrator accounts was mandated. In addition, a single administrator-level account (for each server and each domain) was mandated, accompanied by the removal of additional local administrator accounts on those servers.

Eliminate Weak Passwords

Intruders can take advantage of weak passwords and blank passwords (such as “administrator”, “admin”, “password”, computer name, or null) by using password cracking techniques to facilitate unauthorized access. After an intruder gains access with a user (or system) account, the intruder effectively gains unlimited access to network resources. An approach of employing scans to identify these accounts and notify owners to rectify was slow

(36 hours for a scan) and inefficient (only half of the accounts were remedied).

To improve the results, the Corporate Security Group deployed an internally developed scanner tool that conducts an automated, scheduled process that continuously identifies accounts with weak or blank passwords, and then generates a new strong password for those accounts and concurrently resets the password. The Corporate Security Group also created a server configuration requirement for OTG-managed servers that mandates strong password selection and use. Widespread deployment of Windows XP will assist in the reduction of this security exposure by not allowing users to connect remotely to a system if the local administrator account password field is null.

In addition, to ensure strong password management, OTG runs a custom password filter—Passfilt.dll—at the domain level for domain user accounts. For more information about Passfilt.dll, see “Installing and Registering a Password Filter DLL” at http://msdn.microsoft.com/library/default.asp?url=/library/en-us/security/security/installing_and_registering_a_password_filter_dll.asp. This password filtering was moved into the operating system security components for Windows 2000 Server and Windows XP Professional. Strong password enforcement can be enabled on Windows 2000 Server, Windows Server 2003, and Windows XP Professional through the system administration tools.

Migrate Windows NT 4.0 Domains to Windows 2000 Active Directory

Although a great number of corporate domains had migrated to Windows 2000, there were many Microsoft Windows NT® version 4.0 domains still in existence that had a trust relationship to the corporate network. Computers and user accounts residing in those Windows NT 4.0 domains could not be effectively managed by OTG because Windows NT 4.0 does not support Active Directory.

OTG launched a project to upgrade Windows NT 4.0 domains to Windows 2000 or later, retire the Windows NT 4.0 domains, or have the domains’ trust to the Corporate network removed. Taking these steps strengthened the infrastructure by enabling OTG to deploy and support OTG security policies, settings, configuration, and software on all computers running Windows 2000 and later and on user accounts in domains with trusts to OTG-managed domains. These actions also ensured consistent application of security directives across all computer and user accounts, provided the ability to accurately identify unique users and computers, and provided the ability to identify groups of users and computers.

Smart Cards for Administrators

A project is underway to mitigate security threats to highly privileged accounts and important infrastructure servers—such as domain-level administrator accounts, domain controllers, and Source Depot servers—by implementing two-factor authentication through smart cards. There are two major parallel efforts in this project. The first effort is to make the target servers capable of supporting interactive logon with an account that uses a smart card (includes deployment of the necessary hardware and certificate utilities). The second effort is to identify the administrators who must own a smart-card-enabled, domain-level administrator account and to create and deploy such accounts. This effort includes an in-depth analysis to refine the administrator account model, reduce the number of such accounts to a minimum without adverse impact to operations, and then identify which accounts require a smart card.

Segment the Network by Using IPsec

OTG uses IPsec to group devices on the Microsoft network into two broad categories: managed computers and unmanaged computers. This logical segmentation works to mitigate risks posed to OTG-managed computers by ensuring that network-level access is allowed only from devices that meet security requirements and by denying, by default, access from unmanaged devices. OTG defines its managed computer population as those computers that are joined to OTG-managed domains and that are subject to OTG monitoring and patching mechanisms. Many of the unmanaged devices are primarily used for product testing, debugging, and/or private lab use.

The project to segment the network by using IPsec has two phases. In the first phase, approximately 150,000 managed desktop computers and servers were configured to use IPsec without blocking any communications from unmanaged computers. Phasing the deployment allowed implementers to focus on IPsec technology issues in the first phase. Deployment of the second phase is now underway, and OTG is gradually changing the IPsec policy to implement segmentation and block inbound connections from any unmanaged computer. The IPsec policy specifies Kerberos as its preferred authentication mechanism and also accepts the use of computer-based digital certificates as a secondary form of authentication.

Securing Key Assets

To ensure that key assets are secured and regularly checked for vulnerabilities, OTG deployed the solutions and requirements described in the following paragraphs.

Managed Source Code

Microsoft source code is a high-value digital asset. However, there was no formal, targeted enterprise-level service for managing the security of source code. There was redundant infrastructure and personnel, in addition to inconsistent processes.

OTG has implemented a project aimed at creating a common, centralized, and professionally managed enterprise-level service for secure management of source code across each business group at Microsoft. The goal of the project is to reduce the risk of compromise of source code integrity and confidentiality by unauthorized users. Components of this project include the following:

- Creation of a separate, secure network forest
- Restriction of local administrator account privileges on Source Depot servers
- Elimination of services and batch jobs run from authorized Source Depot accounts
- Use of data center patch management and antivirus processes to enforce remediation and audit for unpatched vulnerabilities
- Addition of event management software and intrusion detection software to Source Depot servers
- Location of the Source Depot servers in a secure data center facility

Source Code Server Segmentation

At one point, any computer on the corporate network could access Source Depot servers at

the network layer. This situation created a vulnerability where compromise of a single computer on the corporate network could potentially lead to penetration of one or more Source Depot servers.

OTG implemented a project to restrict the computers that can access Source Depot servers to only those whose users need access. IPsec technology was used for authenticating and authorizing access to source code servers. Computer accounts for developers who need Source Depot server access are registered and added to security groups that—in concert with IPsec, Kerberos, and the “access this computer from the network” local policy user rights assignment—are given controlled access to the required Source Depot servers.

Secure Domain Controllers

In the corporate environment, there were many servers that consolidated infrastructure, end-user, and tools services on a single server. OTG launched a project in which servers enabled as domain controllers are regularly audited to confirm appropriate configuration—that is, that they are limited to providing infrastructure services, such as domain controllers and global catalogs servers, DNS, DHCP, and Microsoft Systems Management Server (SMS). Domain controllers are permitted to run services to provide monitoring capabilities (such as SeNTRY and Microsoft Operations Manager), and may provide backup of domain controller state information. Any remote server employed to back up domain controller state information requires a higher degree of security. In keeping with the security principle of minimal service configuration, services that allow end users to place files onto a server enabled as a domain controller are prohibited. In keeping with another best practice of minimal service configuration, servers enabled as domain controllers are not configured with Internet Information Services (IIS).

Monitoring and Auditing

Attackers continue to threaten computer networks. However, many organizations focus resources at reacting to attacks after they occur rather than anticipating and preventing attacks. The ongoing success of security policies, services, and initiatives relies on the ability to enforce their compliance. OTG’s monitoring and auditing tactics focus on improving tools to make compliance monitoring and auditing more effective. To accomplish this tactic, OTG deployed the solutions and requirements described in the following paragraphs.

Network Intrusion Detection

A continual increase in hacker intrusion attempts prompted the focus on a tactic to expand and improve the Corporate Security Group’s Network Intrusion Detection System (NIDS) to monitor perimeter attacks on the corporate network. This initiative follows a strategy of using two layers of intrusion detection. The outer layer (NIDS) allows the Corporate Security Group to track and monitor attacks and connection attempts from outside the network, while the inner layer—Host Intrusion Detection System (HIDS)—allows for detection of breaches from the outer layer.

The use of two detection layers substantially increases the overall value for identifying, tracking, isolating, and stopping network intrusions. However, a NIDS system implemented in 1999 struggled to keep pace with expansion of the corporate network. A later initiative improved the OTG NIDS capability in the following ways:

-
- It improved the ability to see all external network attack attempts in near real time, to store network attack information to identify attack patterns and trends, and to collect evidence of the attacks.
 - It improved the ability to define and use custom signatures for network intrusion detection.
 - It created centralized command and control of network intrusion detection sensors.

OTG manages intrusion detection with a number of third-party and internally developed programs and tools, including Microsoft Audit Collections System (MACS), BlackICE and RealSecure from Internet Security Systems, and proxy traffic monitoring and antivirus software.

Vulnerability Management

OTG's approach to computer vulnerability management begins with regular active vulnerability scanning and auditing. A systematic vulnerability management solution has been developed to ensure compliance and manage remediation in all Microsoft environments and includes coverage of network devices, hosts, applications, trusts, and accounts. The tools, and the process that surround their use, are known internally as Secure Environmental Remediation (SER). OTG's solution audits environments and drives them to acceptable levels of risk tolerance. Tolerance limits are developed with environment owners prior to allowing each new environment to access the network. New environments are subject to rigorous and consistent compliance and remediation operations. Success metrics and noncompliance reporting are delivered to both OTG management and environment owners.

Security Patch Management

Microsoft regularly releases patches to correct vulnerabilities in operating system and user applications. OTG management of devices includes management of security patches. All computers must maintain the security patch compliance levels deemed critical by the Corporate Security Group. To ensure this compliance, the Corporate Security Group monitors and ensures consistent and timely installation of operating system and application patches, enforces the application of security patches without end-user or operation intervention, and prevents end users from disabling security patch management without an approved exemption. OTG relies on Microsoft SMS 2003 as the primary tool to track and enforce compliance. OTG uses SMS 2003 to silently install patches on desktops and servers that have passed the compliance deadline. Additional tools include Windows Update to remind server administrators and desktop users to manually install patches, e-mail messages with patch installation links and instructions to help users manually install patches, and logon scripts for rapid deployment of emergency patches. For more information about SMS 2003, see <http://www.microsoft.com/downloads/details.aspx?FamilyId=959EE7D6-7DDF-409A-9522-7D270BDCF12A&displaylang=en> and <http://www.microsoft.com/smsserver/>.

CONCLUSION

The Microsoft Corporate Security Group has succeeded through a strategy that is guided by a formal risk management framework, processes, and clear roles and responsibilities. The framework is fundamental to understating the specific actions OTG has taken to provide security. The examples of what OTG has done to mitigate risk are meant to illustrate core controls that are used to secure Microsoft. Over time, the Corporate Security Group has developed an effective framework to secure a Windows environment, though this approach is just one of many possible approaches to effectively secure a Windows environment. Through direct experience, the Corporate Security Group learned that a formal risk management framework and process were necessary to cost-effectively mitigate risk to digital assets.

The Corporate Security Group organizes around a risk management approach. Rather than performing vulnerability assessments after an incident has occurred, the Corporate Security Group uses a formalized risk management framework to continuously evaluate the current risk profile—that is, to identify risk, prioritize risk, and re-evaluate risk. The continuous evaluation of risk provides decision makers with the necessary data to make good business decisions that balance risk against the costs of security controls.

Within the formal risk management framework, the Corporate Security Group strives to develop a cost-effective control environment to achieve an acceptable level of risk. Acceptable risk is an organization-specific determination; the level of acceptable risk for an organization may differ from the level at Microsoft, based on that organization's unique characteristics.

As part of the effort to organize and prioritize risk, the Corporate Security Group uses a data classification system that helps focus on the highest level of risk first and the lowest levels of risk last. Data classification systems vary by organization but are an essential part of the risk-prioritization process.

The Corporate Security Group created the “Five Trustworthy Assurances” to communicate where it can commit to protect digital assets and where it will not, or cannot, provide security assurances. The five assurances are fundamental to the analysis of risk in each data classification. A key part of a risk management program for any organization is defining assurances and to whom these assurances are provided.

Changes in technology over the past several years continue to put a strain on the traditional security divisions of securing the network perimeter, securing the network interior, securing key assets, and monitoring and auditing. These four divisions become less important as technological advances and business relationships blur the line between “inside” and “outside” the network. As a result, the Corporate Security Group is moving away from these groupings toward new ways of approaching security by using the Microsoft risk management process.

Moving forward, the Corporate Security Group's approach to security risk management will build on Windows-based security controls complemented with network-based security controls when appropriate. Policy enforcement technologies such as Windows Rights Management are expected to play an increasingly important role in augmenting security controls, such as Internet Connection Firewall in Windows XP Professional and antivirus software. Creating a “virtual security perimeter” with technologies like IPsec and Internet Connection Firewall will help keep corporate devices secure no matter where they are located. And increasingly, the Corporate Security Group will move the authentication

infrastructure away from using weak password-based authentication to strong two-factor authentication through smart cards. For example, smart card authentication has already been deployed for VPN access and administrator access to “High Security” server assets.

Computer resources cannot be made completely invulnerable. Risk is an inherent part of networks. It is therefore important to implement a risk management process that identifies cost-effective security controls to mitigate these risks. Risk management provides organizations a consistent, clear path to organize and prioritize limited resources to manage risk to the business. The risk management methodology used by the Microsoft Corporate Security Group can be used by any organization. The end result of an effective risk management program is a set of security controls that mitigate overall risk to a level the organization deems acceptable.

FOR FURTHER INFORMATION

To view additional IT Showcase material, please visit

<http://www.microsoft.com/technet/showcase>.

For information about authoritative security guidance for the enterprise, go to

<http://microsoft.com/technet/security/bestprac>.

Microsoft Security Notification Service is a free service that notifies subscribers through e-mail when new security bulletins are released. This service provides accurate information that can help you protect systems from malicious attacks. To register, go to

<http://register.microsoft.com/regsys/pic.asp>.

For any questions, comments, or suggestions on this document, or to obtain additional information about Microsoft IT Showcase, please send e-mail to showcase@microsoft.com.