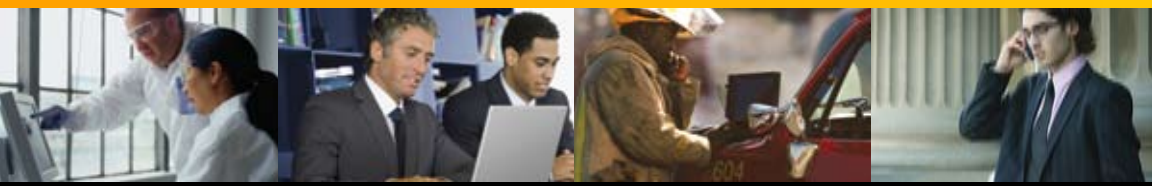


A HOW-TO GUIDE

For IT Security in Government

Information on Seven Key Public-Sector Security Challenges

Network Access Control • Messaging Security
Mobile Security • Data Loss Prevention • Endpoint Security
Managed Security Services • IT Policy Compliance

Produced by GOVERNMENT TECHNOLOGY
SOLUTIONS FOR STATE AND LOCAL GOVERNMENT IN THE INFORMATION AGE

For additional copies or to download this How-To Guide, please visit:
http://go.symantec.com/securitybook

For more information on security, please visit:
http://go.symantec.com/howtoguide

A HOW-TO GUIDE

For IT Security in Government

Table of Contents

Facing Today's Security Challenges

Safeguarding government data and computing resources has never been more complex. Public-sector security officials are responsible for protecting a network of people and information that extends beyond their control. Public work forces rely on multiple network-connected devices — many of them easily portable and extremely powerful — to go about their daily business. Agencies share data with a multifaceted web of government and third-party partners.

At the same time, the threat landscape is changing. Virus attacks have gone underground as their perpetrators, no longer interested in fame, go after confidential data that can lead to financial gain. Theft of sensitive identity and financial information now is a serious criminal enterprise, with a corresponding increase in the sophistication of cyber-attacks.

In this environment, public-sector enterprises must constantly be vigilant about protecting their networks and data to maintain daily operations and public confidence. Citizens trust government with their personal information, and keeping that data secure is of paramount importance.

In this guide, we identify key security challenges and provide solutions and best practices to address them. On the following pages, you'll find practical advice on preventing data loss, addressing policy compliance, securing network endpoints, controlling network access, improving mobile security, strengthening messaging security and choosing a managed security provider.

Symantec's immense data-gathering effort gives it unique insight into real-world security threats and solutions. The company has 2.4 million decoy e-mail accounts that help it study the latest developments in malicious activity. And with more than 40,000 Internet sensors around the world, Symantec experts analyze incidents and threats 24/7. With this guide, Symantec aims to keep readers informed with up-to-date information on the current threat landscape, plus other trends affecting security.

Security breaches can cost a fortune — not just financially, but also in negative publicity and lost confidence from citizens. Productivity losses can be hard to quantify, but they too are real. And regulatory fines can also hurt.

Knowledge is power. The first step in improving security is to understand the risks and vulnerabilities. In these fast-changing times, that means gaining knowledge and implementing solutions *today*.

Chapter 1: Network Access Control

With the significant increase in the numbers and types of endpoints accessing an organization's network, providing security for the entire network has never been more challenging than it is today. Due to this rapid proliferation of endpoints, it's no longer acceptable to provide unchecked access to an organization's network.

Network access control, when done properly, provides the peace of mind that comes with knowing an organization has complete, end-to-end control over access to its network.

A COMPREHENSIVE CHALLENGE

Networks consist of an organization's managed systems (owned and procured by the organization) — in addition to contractor systems, guest systems, public kiosks and partner systems. Administrators often have little or no control over the management of these vastly different endpoints, yet they are expected to keep their networks secure and available.

Added to that is the ever-expanding number of hotspots, kiosks, mobile devices and other types of users. Providing access to networks has become an "anytime, anywhere, anyone" scenario. Networks also need to provide access — both on-site and remote — to both managed computers (owned by the organization) and unmanaged computers (owned by individual workers).

In general, today's networks are much more open than they've been in the past, and that automatically increases an organization's risk. Maintaining network integrity is a constant, daily challenge. Having proper network access control is more important than ever before.

Good network access control is not an isolated endeavor. It's a complete, ongoing process that includes constant, real-time monitoring. The following are some key best practices.

Discover and Evaluate Endpoints — This should occur as endpoints connect to the network — before they access resources. The security system should evaluate new devices connecting to the network according to minimum IT policy requirements. Although most organizations check for antivirus, anti-spyware and installed patches before allowing network access,

the security system should go deeper than that and look at things like registry entries, running processes and file attributes.

Provision Network Access — Full network access should only be granted after systems are evaluated and determined to be in compliance with IT policy. Noncompliant systems should be quarantined and given limited or no access to the network.

Remediate Noncompliant Endpoints — Automatic remediation of noncompliant endpoints should quickly bring them into compliance. If an organization chooses, it can supply information to the user for manual remediation.

Proactively Monitor Compliance — Adherence to policy is a full-time issue. An endpoint's compliance status can change on a moment's notice. Any breach, however brief, can spell disaster for an organization's data security. Thus, security systems should monitor endpoints continuously so any change can be discovered and addressed immediately. Network access privileges should be altered immediately in the case of noncompliance.

STRENGTH AND FLEXIBILITY

A network access control solution that offers numerous enforcement and integrity check options, and works with any operating system or network vendor provides organizations with the strength and flexibility they need to easily and quickly deploy a network access control solutions without having to go through costly network infrastructure upgrades.

Key Benefits of Strong Network Access Control

With proper network access control, most organizations can expect to see several benefits:

- reduced propagation of malicious code, such as viruses, worms and spyware;
- lower risk profile due to increased control of endpoints;
- verifiable, real-time compliance information;
- verification that security investments, such as antivirus and client firewalls, are properly enabled; and
- greater network availability and reduced disruption of services for end-users.

Chapter 2: Messaging Security

With e-mail, instant messaging (IM) and Web collaboration rapidly gaining importance in the daily work world, it's more vital than ever for organizations to keep the data within these messages secure. Much of an organization's critical information travels through e-mail. IM is increasingly used for business. Online collaboration too is becoming more popular.

These messaging tools have become essential for day-to-day operations. Organizations cannot afford to have problems with them. Security for messaging should be just as solid as it is for any other area in IT.

The rising dependence on e-mail for mission-critical work means it will continue to be a big target for virus writers, hackers, spammers and phishers. All e-mail should be scanned and controlled. It's important to understand how e-mail affects both network security and risks to the business of any organization, large or small.

Data leakage, spam, viruses and other malware are all concerns for messaging security. Threats are always evolving. Organizations need powerful filtering in place to block unwanted content from entering their networks. And they must ensure their information is not transferred inappropriately.

STAYING PROACTIVE

With the proper protection, organizations can block and filter malware from both e-mail and IM with the same application. They can also reduce downtime by proactively detecting and quarantining suspicious attachments before official antivirus definitions become available. And they can get real-time looks at e-mail and IM traffic on the messaging infrastructure with powerful monitoring and reporting.

Spam is at an all-time high. For some organizations, it can be 95 percent of the e-mail volume they receive. Phishers are always trying to steal personal information. A growing concern lately is content control. Since many government entities deal with sensitive data, such as Social Security numbers or other personal information, they must be concerned about such confidential or sensitive data leaving their boundaries via messaging.

As more information is shared via messaging systems than ever before, organizations need to ensure they're taking especially good care of their most critical data. For strong security, organizations should keep a few guidelines in mind.

Take a Multi-Tiered Approach — It's crucial to have security in several tiers throughout a network. This works well because it attacks the security problem in several different places. The perimeter is just as important as the inner workings. These things are just as critical to messaging security as they are to an organization's overall security.

Protection should be placed as far out on the edge of a network as possible. Initial layers should reduce the volume of what subsequent layers must deal with. The more filtering of spam and viruses that occurs outside the internal messaging servers, the better. Eliminating useless or virulent messages at the outset conserves resources and preserves efficiency further down the stream.

From endpoints through gateways and into servers, there should be security at every point. That way, problems can be isolated before they create larger impacts to the entire network, and internal threats can be spotted as easily as external ones.

Fit Messaging Security Into the Big Picture — It's best to have a holistic security system that seamlessly fits messaging security within the larger protection system. The big picture should cover antispam, antivirus and compliance for all messaging, not just e-mail.

Integration Is Best — Organizations should take an integrated approach whenever possible. Using one vendor is best. When security involves multiple vendors, several user interfaces and numerous subscriptions, the complexity and the costs make security much more difficult to manage. With just one interface, administrators can go in and easily create policies that will be consistent over e-mail, IM and the Web. This saves time in managing messaging security, which results in lower costs.

Accurate Intelligence Is a Must — Organizations must stay on top of the latest threats. Attackers have "grown up" in recent years, conducting their activities in a more organized and businesslike way. They have their own SMTP servers, they create bots to do their bidding, and they are more likely to be after financial gain than they were in the past. They also are smarter about staying "under the radar" and not causing suspicious traffic peaks.

Attackers are always changing tactics and trying to stay ahead of security filters, as they did when they started using images for spam and phishing. Once again, they capitalized on a vulnerability and found a new way to get in the door. Given the resourcefulness of attackers, it's more important than ever for organizations to have an accurate view of the current threat landscape at all times.

Use IP Reputation Analysis — Analysis of IP reputation is a powerful aid. Security experts can determine whether the reputation of an e-mail's source is good or bad. If a particular sender has a bad reputation, its attempts to connect to a network should be rejected at an early stage. This is another reason to have an integrated solution; if e-mail from a certain sender has a bad reputation, IM content from that same sender should also be blocked.

Have Solid Compliance Policies — In addition to cutting down on viruses, spyware and spam, solid security will also help tremendously with enforcing compliance policies. Organizations should stop unauthorized data exchanges, both internally and externally. They must know when messaging is being used in an acceptable manner.

Is sensitive data being properly encrypted? Should multimedia files be allowed from certain overseas locations? With numerous publicly reported breaches and e-mail becoming more crucial to getting things done, compliance has risen in importance in recent years. A serious breach can be extremely costly, especially in terms of bad publicity if it happens within a government agency.

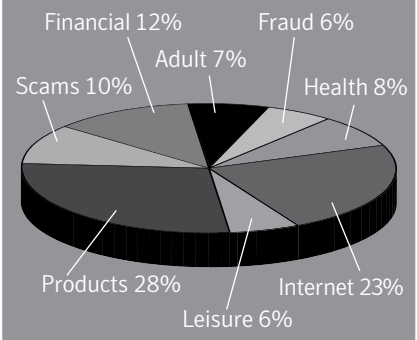
It's important to have security that watches content being sent via messaging tools both within an organization and without. Although sensitive data can be shared by some employees, there will certainly be others who aren't authorized to send or receive it. Security administrators should be able to detect unauthorized content and stop it from getting away.

The system should have numerous options for how to deal with each instance. For example, an offending message could be deleted, quarantined or allowed while also being flagged.

Set Up Internal Content Filters — Internal issues also should be addressed by messaging security. Content filters can be set up to eliminate employees' exposure to objectionable content, such as racially insensitive or other inflammatory material. In the interest of keeping a sustainable workplace environment, government has been especially aggressive about blocking negative content from reaching employees and going beyond its boundaries.

Global Spam Categories

Spam category data is collected from messages passing through the Symantec Probe Network.



Source: Symantec Spam Monthly Report, February 2008

BETTER SECURITY, BETTER PERFORMANCE

Integrated, multi-tiered messaging security goes a long way toward making all of IT work better for an organization. Blocking malware and other threats at the edge of the network brings better performance. When a system isn't wasting CPUs processing and storing thousands of unnecessary messages, the network runs more smoothly and has less downtime.

Sound messaging security is an important piece of the security puzzle. There are a lot of pieces, and the better they fit together, the more productive the organization.

Chapter 3: Mobile Security

Mobile devices — in particular laptops, handhelds, PDAs and smartphones — can be taken just about anywhere. The mobility of these tools makes them a great productivity aid. However, they can also expose an entire organization to data-security threats.

With the rapid increase in the number of mobile workers, there are more end-points than ever before. Laptops, smartphones and other mobile devices also are being used by a growing variety of end-users. This includes people who aren't always part of the organization — contractors, guests and temporary workers, for example. This pushes the security boundary out further than it's ever been before and increases the risks.

There are numerous risks to having inadequate security for mobile devices. First of all, a mobile breach can be just as damaging as a wired breach. Mobile devices have similar access to resources as wired devices.

VPN technology is common in laptops and it's becoming more widespread in smartphones, so these mobile devices can have the same connectivity when outside the brick-and-mortar environment as when inside. This puts all kinds of data — including customer, financial and personal information — at risk for the entire organization.

These portable electronic devices access the same data on an agency's network as desktops, but they're storing it offsite. And the devices are so small and light, they're more susceptible than desktop devices to loss or theft.

A NEW, EASY TARGET

Overall, the mobile security threat landscape is in its infancy, but the threats are growing both in number and sophistication. Smartphones, especially, are of increasing concern today. With their ability to function almost like a PC, they're powerful tools. They're rapidly increasing in number, and they're quite different from other devices that have been around longer.

Security for smartphones is improving, but it's not as mature as it is for laptops and desktops. Many organizations don't yet have the means to manage smartphone security. In fact, IT security policies usually cover servers, desktops and laptops, but often there's no specific mention of smartphones or other types of mobile devices.

Managers often don't realize how much data — or what kind of data — is stored on smartphones. It's the first time a device like this has been widely deployed. Employees commonly purchase smartphones for personal use, but they also use

them at work for storing important enterprise data. The fact that an organization's data now often resides on devices it doesn't own presents a new challenge for security specialists.

Since smartphones carry much of the same data as laptops, they're generally considered the next big target for hackers. The acceptance of smartphones as a useful new tool is similar to the way laptops caught on a few years ago. The difference is that smartphones, with smaller price tags, are taking off much faster than laptops did. Smartphones are expected to out-ship laptops for the first time this year. Security efforts need to catch up.

Although it's tempting to make an analogy between smartphones and laptops, there are some important differences.

Most laptops run on some version of Windows in enterprise environments. Installation and support processes are typically well established and easier to implement since most users have a common system configuration. Smartphones, however, use numerous operating systems. There are unique challenges in managing each separate platform. Many IT specialists who are responsible for smartphones often don't yet have a frame of reference for these platforms because they don't have much experience with them.

To get a better handle on security for mobile devices, several best practices should be observed:

Now, Not Later — The number of mobile endpoints is rapidly increasing. It's best to improve security for these sooner rather than later. Smartphones are becoming increasingly popular for daily work. Managers must address the security issues around smartphones as soon as possible. That's also the case for any other mobile devices, such as laptops.

Know Where Your Data Is Stored — Too often, managers don't even realize where their data is stored because employees store an organization's data on laptops, flash drives and smartphones. With new ways to take an organization's data beyond its borders, managers need to know what kind of data is stored on the various mobile devices that have access to the network.

Expand the Organization's Definition of Endpoints — Do your policy guidelines cover smartphones? Do they include mobile devices in general, or stop at laptops? Many managers are discovering their current definition of an endpoint doesn't include smartphones, which is dangerous.

Treat Mobile Devices as Regular Endpoints — Management should give smartphones as much security attention as more traditional endpoints, such as laptops and desktops. Smartphones certainly can hold the same kind of data, so they should be treated as simply another endpoint that needs protection. Organizations should strive for centralized management, reporting and regulatory compliance across all endpoints, including mobile ones. Smartphones, like other devices, should have antivirus technology, firewalls and encryption.

Have Password Protection on Smartphones — Smartphones often aren't password-protected, making it easy for someone who finds or steals a smartphone to access confidential data. Compromising information, such as e-mails, files, contact information, text messages, calendars, etc., can be damaging to an organization. It can also mean a compliance breach that requires public disclosure.

Don't Lose Smartphones — It sounds almost too simple, but it's important to keep track of them. Phones are lost 15 times more frequently than laptops. Every time a phone is lost, there is instant risk to the data stored on it. Hackers who get into a system through a smartphone can disrupt an organization's network and its business just as easily as they can from any other endpoint.

Consider MDM — Mobile device management (MDM) can provide more diligence in protecting mobile devices from security threats. MDM is a fairly new tool that provides monitoring and administration specifically for mobile devices.

Whether large or small, most organizations face the same security risks, and the growing use and variety of mobile devices creates a constant challenge for security professionals. Using the right technology and best practices, organizations can protect themselves from the risks presented by mobile devices.

Where Is Your Organization's Confidential Data?

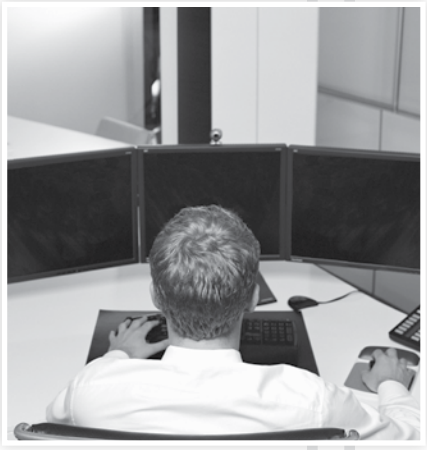
1 in 50 network files contains confidential information.
1 in 400 messages contains confidential information.

Devices most likely to contain sensitive data:

Chapter 4: Data Loss Prevention

Data loss prevention is on more people's minds these days. With security breaches being widely reported in the media, increasing numbers of endpoints and increasing information sharing among workers, the need to secure all kinds of data is becoming more important.

Government regulations are now a big part of data loss prevention, with both state and federal governments requiring more data protection. And with the rapidly growing number of mobile devices being used, people have become the endpoints. The workers themselves — not the computers — are the new security perimeter. Organizations now must protect much more than a finite number of connected computers.



In these fast-changing times, the key is to discover and protect confidential data wherever it's stored or used. That includes all endpoints, and all network and storage systems. It includes machines owned by the organization and machines owned by employees who use them for work. Organizations are allowing more people outside their boundaries — such as contractors, guests, vendors and temporary employees — to access their networks. The data being used by those people must be protected too.

Organizations must protect against malicious behavior and unintentional breaches by insiders, and they should prevent data from exiting any network gateway or endpoint. No matter where data lives or where it's going, it must be secured.

While many government agencies have a good handle on data loss prevention, others do not. It often comes down to upper-level management, and its particular interpretation of what data security is. More education is sometimes required, and that should be an ongoing process. It's also important to have the right tools to work with.

Automation can be a big help when it comes to knowing where the sensitive data is — and what to do with data that's found in the wrong place. Policy-based automation is becoming increasingly popular as organizations work toward better data security. And IT professionals are looking harder at how to prevent data loss across entire organizations, for all data types and all device types.

GOVERNMENT REQUIRES MORE

The key trend affecting data loss prevention these days is the fallout from several data security breaches that were widely reported in the media in recent years. Until these

occurred, the emphasis had always been on securing the network from hackers. While malicious code and other such threats are still a factor, the focus has shifted.

In recent years, there have been more than 230 breaches disclosing more than 90 million individual data records. More than half of these were due to "insiders," people working with or within the agencies responsible for the data. Of insider breaches, less than 1 percent are malicious. Most often, breaches occur through inadvertent actions or broken business processes.

Recent government regulations, such as the Federal Information Security Management Act, and directives from the Office of Management and Budget have mandated better security for federal government data. However, these are broadly written and leave much to interpretation. Thus many government agencies aren't sure what to do regarding these.

Many have said it would help if the regulations were more prescriptive. It's difficult to enforce policies that people can't agree on. For example, government agencies don't agree on what the federal definition of personally identifiable information (PII) is, which makes it harder for the issue to be addressed. PII has become a hot topic because people are concerned about personal information being exposed to hackers. Government agencies would like to find a way to certify that PII is not stored on laptops or other machines.

Although there are vagaries accompanying the government mandates, the good news is that the regulations are spurring more interest in data security in general. More people are taking it seriously, and that's better for everyone.

PROLIFERATION OF ENDPOINTS

Many experts agree that not enough security attention is being paid to the rapidly expanding number of endpoints. There are now more places than ever before from which a user can connect to a network — coffeehouses, hotels, airports, kiosks and more. There are also more mobile devices — smartphones, laptops and PDAs, for example.

Smartphones in particular are a concern because sales are skyrocketing. They're being used more and more on a daily basis — and they're easily lost or stolen. Also, the security environment for smartphones isn't as mature as it is for other endpoints, which means the risk to organizational data is increasing as more smartphones are used.

One effort that could help with the dizzying number of endpoints is the combination of identity management with data loss prevention technology. Identity management would allow an organization to associate permissions with every

possible use/device combination, and data loss prevention would provide classifications of data and where that data is, where it's going, and how it's being used. For example, if User A borrows User B's laptop for a while, the system would recognize that and allow User A his or her appropriate access to the laptop depending on what type of data and what User A was doing with the data. Such an identity management and data loss prevention system would be extremely helpful in protecting sensitive data.

Also, more organizations are showing an interest in encryption. However, not all of them are using it correctly. While some organizations choose to encrypt everything, it's often smarter to look specifically at what type of data is stored, and where it's stored. That way, an organization can encrypt the sensitive data only and leave the rest alone.

Don't forget encryption alone does not solve the data loss prevention problem. Encryption helps to secure data that may be stored on a stolen laptop but what about the sensitive data that is sent via e-mail or downloaded to a USB device? Data loss prevention is about protecting the data wherever it is stored or used — across endpoint, network and storage systems.

BEST PRACTICES

With all the changes occurring in the area of data loss prevention, organizations should take a fresh look at what they're doing. Some best practices follow.

Protect All Data — Don't forget about data stored on USBs and smartphones, and within e-mails and instant messages. Government employees use many tools and devices, and they all should be addressed. It's about protecting the data, wherever it's stored or used. That goes for endpoints, network systems, storage systems, file servers, databases — everything. It should all be a priority. This is especially important because of the way people work today, sharing data with others like never before.

Always Go for Accuracy — Organizations need to accurately detect every possible threat to their data. There should be no false positives. The security system should accurately monitor and detect issues for all data types, data endpoints and network protocols.

Have Solid Reporting in Place — Reporting is very important. It's a valuable tool for finding broken business processes. It helps educate both higher-level managers and employees in general. Good reporting can ultimately reduce the number of security incidents. Some organizations have seen risk reduced by 90 percent after turning on automated notification. Reporting should be done across the organization,

and allow users to aggregate data, give high-level views to senior management, drill down for more information, and see how the organization is performing on regulatory compliance.

Designate Various Classifications of Data — All data should be categorized to designate what type of data it is, where it is, how it can be used and where it can be sent. Scans should provide specific details about the type and location of sensitive data stored on file servers, document and e-mail repositories, Web content and applications, databases, laptops, desktops and other data repositories. Data should be quarantined or relocated if it's out of place.

Control Data at the Endpoint — Organizations should be able to discover sensitive data stored on endpoints and then prevent the data from being inappropriately used, sent out or copied to storage devices, such as USB drives, CDs or DVDs.

Maximize Encryption — It's best to use encryption only when necessary — for sensitive data. It can be wasteful and costly to encrypt everything. A lot of information is fine just the way it is.

Secure All Databases — Analyze all data accessed from databases, and check for unauthorized access to sensitive data. Have an audit trail in place for database activities. Look for anomalous database activity from both authorized and unauthorized users.

Scan and Monitor Laptop Data — This can be a challenge because laptops are offline much of the time. That can be done, however, by automatically scanning e-mail archives and disk backup files to find confidential data that was previously pulled from the network to a laptop. Scanning should cover a complete inventory of which laptops have sensitive data on them. For exposed data, appropriate steps should be taken to remove, encrypt or relocate the data.

THE WAY IT IS

In today's demanding world of data security, the best solutions are those that combine traditional network-based technology with broad, deep endpoint protection. Data loss prevention has become a serious business, and government organizations should make sure they're giving it due attention.

Any organization wants to keep the trust of the public and comply with government regulations. The best way to do these things is to ensure data loss prevention measures are implemented. It's not just the machines or the network that needs protecting — it's the data itself that should command attention now.

Chapter 5: Endpoint Security

There's a double challenge these days when it comes to keeping IT network endpoints secure. Not only are there more endpoints, but also more types of endpoints.

A primary way for attackers to obtain unauthorized access is by exploiting endpoint vulnerabilities. Endpoints include servers, desktops, laptops and other mobile devices, such as smartphones and PDAs. To protect those endpoints, organizations need a solid framework of security measures. This should include antivirus, antispyware, desktop firewall, intrusion prevention and application and device control.

Cyber-attackers have become more organized, businesslike and efficient. They're better than ever at escaping detection and finding new entry points into a system. They're now more interested in financial gain than in fame, so they've gone further underground. They're constantly developing new ways to access organizations' systems and data.

As the number of endpoints continues to increase, so does the risk. Attackers go after both known and new vulnerabilities. While it's more productive for an organization to provide increased network access to workers, it also presents attackers with more potential entry points. Simply put, organizations must be more diligent than ever before in protecting their endpoints.

ENDPOINT SECURITY = PROTECTION + COMPLIANCE

Traditional measures, such as antivirus and antispyware programs, are no longer enough. Viruses, worms, Trojan horses and unknown dangers are growing in number and complexity. Thus the potential for a security breach is expanding dramatically.

Today's workers need instant access to data, and the amount of data that's shared — both within and across organizations — has increased. Endpoints can be onsite or remote. They can be full-time staff, guests, contractors, temporary workers, business partners, auditors and others. And they're accessing the network from more locations — coffeehouses, airports or hotels, for example — and from more types of computing devices than they have in the past. More sharing means more endpoints are affected, and that means an increased risk profile for an organization. The speed at which information travels today provides a perfect opportunity for an infected computer to infect other computers extremely rapidly. Protecting all the endpoints associated with a network is vital.

In addition to protection, endpoint security should also provide a solution for compliance. Endpoints should comply with an organization's IT policies. Security mechanisms must be running and properly configured according to an organization's guidelines. Attackers can find vulnerabilities if an endpoint device is not properly configured.

A NEW BREED OF ATTACKER

Previously attackers focused on disrupting services and gaining fame or notoriety. That's changed. Now most attackers focus on financial gain, going after sensitive or personal data, such as credit card information or passwords.

Their methods have also evolved. Gone are the days of the noisy attacks that were reported in the newspapers. Hackers now try for silent attacks, which they hope to carry out without ever being noticed. Malware writers often create targeted attacks and have a business model behind them. They are more organized than in the past.

Also, attackers are better at creating automatic variance, so the same attack can look different from one day to the next. Some are creating botnets, where they use infected computers to carry out their commands like robots. It's harder to trace the hacker through this network of unsuspecting users. And it's even more difficult given that the unsuspecting person's computer may only be doing the malicious bidding of the attacker two or three minutes a day, to minimize chances of detection.

With sensitive data being a big target for hackers today, keeping endpoints secure should be a primary concern for governments. As endpoint security has become more complex, it's important to examine ways to protect your organization's endpoints. Following are some key best practices.

Find One Solution — Too often, organizations use different solutions for different types of endpoints. It's best to use one provider for all endpoint security. With several different solutions, management becomes inefficient and time-consuming. And the increased complexity leads to higher costs.

The Best Solution Combines the Core Technologies — antivirus, antispyware, firewall, intrusion detection and intrusion prevention as well as device and application control. It also manages endpoints of all kinds of devices, ideally from a single console. From one management console, it's also easier and more efficient to set and enforce security policies across an entire organization — including all its endpoints.

Use Behavioral-Based Methods — Security techniques are always evolving, and this new method studies and reacts to the behavior of potential threats. By finding both good and bad behavior, a more complete picture is developed, and a wider range of threats can be dealt with proactively.

Advanced Threat Prevention — It's no longer enough to just have the traditional security measures against the usual malware. It's important to have advanced tools that can protect against the most sophisticated attacks that evade traditional security measures, such as rootkits, zero-day attacks and mutating spyware.

Deny Specific Activities — An organization's endpoint protection should allow it to deny specific device and application activities that the organization has designated as high-risk. It also should be able to block certain actions based on the user's location. It's best if the organization has many options, so it can configure its security system to meet its specific needs.

Take a Proactive Approach Overall — With the increasing number of endpoints and attackers finding more complex ways of getting into a system, it's vital to have proactive security. This is the best defense against new attacks — and against those not yet created.

NEW ERA FOR ENDPOINTS

The number of endpoints has exploded. That, combined with increased data-sharing and more mobile devices, makes endpoint security more important — and more difficult — than ever before. The challenge now is to allow more workers — even those outside organizational boundaries — to have more access to information while providing greater security.

As the threat landscape continues to become more complex, managing endpoint security becomes more expensive and time-consuming. With proper endpoint security from a single vendor, however, an organization can realize a lower total cost of ownership. Administrative overhead can be reduced, and costs associated with managing multiple products should be lower. A unified approach simplifies administration, allowing for a better process for updates, licensing, maintenance and training. Better security at a lower cost is hard to beat.

Chapter 6: Managed Security Services

With a myriad of ever-changing threats springing up and new technologies constantly arriving, it's amazing that an organization can keep tabs on all its IT security issues. The reality is many organizations — both public and private — aren't up to the task by themselves. They're simply unable to keep pace with the crush of information and amount of technology necessary to truly protect themselves.

By bringing in a dedicated outside expert to manage their security affairs, government agencies can benefit in numerous ways: lower costs, better reporting, stronger analysis and quicker response to attacks of all kinds. Perhaps most important, assistance from a managed services provider lets an agency stay focused on its own core business. Too often security issues distract organizations from their chief business missions.

With today's complex network environments and limited resources, it's simply too difficult and costly for most government organizations to deploy information security on their own. To eliminate potentially costly security gaps and vulnerabilities, an organization should hire a managed services provider and get the best of both worlds — better security and more efficiency.

COMPLEX THREATS

Security threats are rapidly evolving. Attackers are becoming more adept, and they are always striving to stay one step ahead of security measures. Attacks have become more complex and are more likely to be "under the radar" as attackers learn to disguise their activities — and there are always new threats to identify and eradicate. New risks to an organization's data appear almost daily. The right managed services provider will have a thorough, up-to-date view of the current threat landscape.

An increasingly mobile government work force complicates matters. There are an ever-expanding number of endpoints that must be protected. There are also regulatory compliance issues and internal content polices related to who can share what data with whom. At the same time, more data is being shared among agencies within jurisdictions or between separate government jurisdictions. Data-sharing will continue to expand, which will increase security risks.

Now more than ever, immediate analyses of security attacks — and response to those attacks — are of vital importance. These issues must be addressed while the business moves forward and everyone has access to the data they need to do their jobs.

In the wake of well publicized data breaches in recent years, managers know all too well a breach can lead to negative publicity and erode confidence among an organization's customers. A breach can also result in costly recovery efforts and regulatory compliance penalties.

COMPREHENSIVE BENEFITS

Despite security's growing importance, few organizations can afford to maintain the staff that real security requires. It's too costly to train and retain qualified employees. It's also impractical for staff members to look at all the necessary security information 24/7.

From a resource management standpoint, it would be an improvement if managers didn't have to deal with these kinds of issues. It's more cost-effective to have managed security services from an outside source. It saves an organization money, allowing it to allocate those funds to other mission-critical items.

Managed security services maximize the value of an organization's investments in IT infrastructure and enable employees to work solely on the core business missions. This improves the efficiency of an organization and its processes. And it's all done while improving the level of security.

WHY CHOOSE MANAGED SERVICES?

A managed security services expert can provide an agency with real-time, 24/7 management and monitoring of security infrastructure and activities. This includes firewalls, servers, routers, intrusion detection, intrusion prevention and much more. The services can even examine logs of numerous types of servers, including file, application, database and Web.

Working with a managed security service provider gives an organization customized protection against a wide variety of threats, plus guidance for dealing with the most complex attacks.

Managed services should ideally provide an agency with a unique blend of elements that far outshines its own ability to protect itself. This should include state-of-the-art technology, experienced personnel, proven processes and continuous threat intelligence that few organizations possess themselves.

Log Monitoring — For example, a key benefit of managed security services is the monitoring of security logs. Focused on the expert analysis of security logs, it takes a closer look at network and server activity. Log monitoring gives a more detailed look at security information with a trained eye. It's a different skill set than what's required to manage firewalls.

This deep analysis of security logs can aid an organization in many significant ways, including identifying threats to the organization as well as helping demonstrate compliance. The thorough attention that comes with log monitoring is usually impossible for organizations to handle themselves and is best performed by a knowledgeable managed services provider.

Attack Detection — A good managed services provider can also advise an organization quickly when an attack occurs. What happened? Who was likely behind the attack? Was it specifically targeted at my organization? An experienced analyst can best answer these and other questions. This expertise can also help an organization quickly modify its security posture when reacting to a changing threat environment or in response to evolving attacks.

Real-Time Attack Analysis — All the data in the world is meaningless if management doesn't know what it means. A strong managed security services provider with years of experience can analyze the data quickly and accurately and then provide meaningful insight into even the most elaborate attacks. From there, specific recommendations for response can be made. This kind of real-time guidance is invaluable. The process can also incorporate customized escalation procedures that address an organization's unique requirements.

Reporting — After security events are identified and remediated, organizations need to understand what has occurred on their networks, both in real time and from a historical perspective. Managed security services can provide meaningful reporting that provide an understanding of the threats seen against the organization.

Improved Compliance — When it comes to regulatory compliance, many organizations are finding huge benefits from managed services. The managed services provider can provide compliance reporting that meets an organization's unique needs. Furthermore a good managed services provider should map compliance policies against applicable regulatory guidelines and keep management informed about compliance issues that arise. By covering an organization's regulatory and auditing mandates, managed services can head off potential penalties.

Threat Remediation — Remediation is another area where organizations can reap major benefits from using managed security services. For example, a threat could impact just one version of one operating system, among numerous versions and systems in use by an organization. Good remediation allows the organization to quickly know where the problem is and what action should be taken.

Remediation can often be quite complicated, and fast action is critical. It's at those times that managers will be glad they're working with an expert.

Cost Control — Cost is another key factor to consider. Many organizations, when they pencil out the cost scenarios, find that managed services are much less expensive than developing and building out a security operations center internally. Lower costs coupled with increased expertise makes the proposition an obvious win for most organizations.

CHOOSING A PROVIDER

When it comes to working with an outside provider, an organization should look for a partner it can trust and ensure the partner can meet expectations and business objectives.

Find a Trusted Partner — An organization should have a good comfort level with the managed services provider it will be working with. It should choose a service provider with a good reputation.

Outline Expectations — In addition to going with a company that has a good reputation, an organization should have a solid service-level agreement in place so that both parties have a clear understanding of the level of service that will be provided.

Align Security with Business Objectives — It's important to find a provider that can align its security activities with an organization's unique business goals. An organization should be able to get the information it needs on a regular basis. For example, it should be able to view the change requests to a firewall at any time. If it wants to know the number of security incidents by level of security, or by classification, it should be able to view this information immediately.

Having the information, and the ability to drill down for even more detail, enables management to provide actionable information to upper-level managers or financial teams. This allows everyone to see the value that managed services have brought to an organization.

Most organizations could use effective information security to maintain the integrity of valuable corporate assets, enable compliance with industry regulations, and ensure business continuity and public trust. Strong security should be about helping an organization meet its business goals at all times.

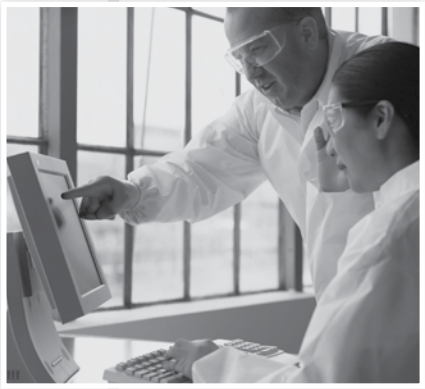
The key to finding peace-of-mind security is arriving at the perfect combination of people, processes and technology. With today's complex, ever-evolving threat landscape, that's most likely to happen with managed security services.

Chapter 7: IT Policy Compliance

IT security breaches have been headline news many times in recent years. No government agency wants to be mentioned in those headlines. That's one reason governments have been paying more attention to security policy compliance. By practicing good policy compliance, organizations adhere to both internal policies and external regulations set up to keep networks and data secure. Proper compliance results in a more secure, better-managed IT environment.

Policy compliance involves creating and managing IT policies, assessing controls and looking for vulnerabilities. It also deals with prioritizing, monitoring and responding to security events properly, and reporting on security and compliance status. Compliance is about measuring overall security against internal and external standards.

While regulatory requirements can be a big factor in compliance, it's mostly the potential business impacts that make organizations strive to do better at it. There are simply too many negative impacts when compliance isn't done properly.



Any security vulnerability that can be exploited could impede an organization's ability to deliver services that are key to its mission. The core business can't be done if IT is greatly impacted by a security attack.

The organizations that are best at policy compliance are those that link it closely with their core missions. That helps them prioritize their efforts and spend wisely when it comes to giving compliance its due attention. Since there are never enough dollars for an organization to do everything it wants to do, allocating funds for policy compliance is most effective when compliance efforts are aligned with the organization's overall goals.

A COMPLEX PROCESS

Compliance might seem like a simple, straightforward proposition, but it can actually be quite complex. There are many facets to it, and it can mean different things to different people at various levels within an organization. An IT operations person will have a different perspective than a financial manager. There are high-level directives. And there are specific rules addressing the smallest security details.

Policy compliance is not a one-time-only endeavor. It changes constantly, and that's why governments must stay on top of it. Policy management is a process, just like any other business process that needs attention within an organization.

There are two key trends making compliance even more of a challenge. One is the increase in mobile workers and devices. The other is additional regulations from government.

Certainly the increasingly mobile work force makes compliance more difficult. With more endpoints, devices and people involved, there is that much more to watch. There are devices not owned by the organization pulling data off the organization's network. Is your organization's policy consistent with that of contractors you work with? That's just one of many questions that must be asked. This all makes compliance more complex than it was before.

REGULATORY TIMES

The tricky part about external regulations — those required by law — is that there are often multiple sets of regulatory guidelines for any given agency or department. A health department, for example, will have different legal requirements than an engineering department.

These days, a key requirement is for the protection of personally identifiable information. There is a lot of congressional scrutiny around this type of information, making it a huge driver for many organizations. As a result, many are putting more money and effort into compliance around data security.

Security policy compliance is a dynamic, fast-changing activity. Security threats are constantly changing, but any organization can keep up with things if it observes a few best practices, such as:

Have a Compliance Mindset — Policies don't enforce themselves. Everyone involved must do his or her part and realize the value of good compliance practices that go well beyond minimum requirements. The result can be a more secure environment and more control of the organization's assets.

Link Compliance to Delivery on Your Mission — The organizations most successful with compliance are those that find a way to tie compliance directives to their business goals. Keeping these closely linked improves the chances for successful projects — and in getting more funding for future projects.

Have Infrastructure That Lets You Automate — Organizations should try to drive the human cost out of compliance efforts. They should try to automate as many tasks as possible. That can lead to more efficiency and lower costs.

Know Which Regulatory Mandates Relate to Your Organization — The Federal Information Security Management Act is aimed at protecting the federal government's investment in IT. The Health Information Portability and Accountability Act seeks to

secure electronic health information, such as patient medical records. There are numerous state and federal laws requiring IT security compliance. Do you know which apply to your organization?

Be Able to Demonstrate Compliance — Government entities should be able to show that they're compliant consistently and regularly across the organization. Some find that although they're complying with everything in the proper manner, they don't really have the data to prove it. Organizations must be able to show they are compliant with everything they should be.

There are three key parts to demonstrating compliance: 1) show you have a good, thorough policy in place; 2) collect data over time to show you're complying uniformly and regularly; and 3) demonstrate that the policy is effective.

When it comes to the last item on that list, it's important to constantly monitor the agency or department's performance against the policy. Many factors can complicate that, such as new threats, technology changes or personnel turnover. Thus, organizations must be especially diligent about regularly measuring their compliance performance. Is the policy effective? If not, where are the gaps and how can they be closed?

Constantly Evaluate Risks to Your Mission — Threats are always evolving. Hackers never stop trying new ways to get around security. Every organization should be aware of the latest trends within the threat landscape and have a process that's constantly evaluating the risks to its particular mission.

GOVERNANCE AND COMPLIANCE

Policy compliance is closely related to IT governance. Compliance has much to do with defining, controlling and governing security efforts. How should an organization respond to security events? How should it keep its records? These are just two of many questions organizations must answer in setting up their internal policies. And they must address the regulatory mandates as well.

Some organizations don't even have uniform policies within their own operations. Various divisions could be doing compliance in different ways, for example. Government enterprises need a framework of policies, supported by proven processes and best practices, maintained with regular use of automated tools.

Managing security policy compliance is not just about checking necessary items off a list. The reality is that compliance is a complex, fast-moving, important factor in the ability of any organization to deliver on its business functions — and compliance demands ongoing attention.

Improving Your Organization's IT Security

- ❏ Use in-depth defense strategies. This calls for multiple, overlapping, mutually supportive defense systems to guard against single-point failures in any specific technology or protection method. This should include regularly updated antivirus, firewalls, intrusion detection and intrusion protection systems on client systems.
- ❏ Test security to ensure adequate controls are in place.
- ❏ Always keep patches up to date, especially on computers that host public services and are accessible through the firewall, such as HTTP, FTP, mail and DNS services.
- ❏ Enforce an effective password policy. Passwords should be a mix of letters and numbers, and should be changed often. They shouldn't consist of words from the dictionary.
- ❏ Consider implementing network compliance solutions that help keep infected mobile users out of the network (and disinfect them before rejoining the network).
- ❏ If malicious code or some other threat exploits one or more network services, disable or block access to those services until a patch is applied.
- ❏ Isolate infected computers quickly to prevent the risk of further infection within the organization. Perform a forensic analysis and restore the computers using trusted media.
- ❏ Configure mail servers to block or remove e-mail that contains file attachments commonly used to spread viruses, such as .VBS, .BAT, .EXE, .PIF and .SCR files.
- ❏ Train employees not to open attachments unless they are expected and come from a known and trusted source. Clicking on links or attachments in e-mail or IM messages may expose computers to unnecessary risks.
- ❏ Be aware that security risks may be automatically installed on computers with the installation of file-sharing programs, free downloads, and freeware or shareware. Employees should not execute software downloaded from the Internet unless it's been scanned for viruses.
- ❏ Ensure that only applications approved by the organization are deployed on desktop computers.
- ❏ Have emergency response procedures in place. This includes having a backup-and-restore solution to restore lost or compromised data in the event of a successful attack or catastrophic data loss.
- ❏ Turn off and remove unnecessary services.
- ❏ Educate management on budgeting needs for security.

For additional copies or to download this How-To Guide, please visit:
http://go.symantec.com/securitybook

For more information on security, please visit:
http://go.symantec.com/howtoguide