SYS-CON

An A–Z of Storage+Security: Rewrite the Lexicon 〈3

information STORAGE+ SECURITY journal

www.ISSJournal.com

In This Issue:

VOLUME: 2 ISSUE: 1 2005

Digital Life Cycle Management 〈26

WHEN THE "BEST OF BREED" ISN'T ALWAYS BEST

Inside! 〉 Articles from *Sarbanes-Oxley Compliance Journal*

$5.99US $6.99CAN

01 〉

0 71486 01793 6

information STORAGE+ SECURITY journal

President and CEO
Fuat Kircaali fuat@sys-con.com
Vice President, Business Development
Grisha Davida grisha@sys-con.com
Group Publisher
Jeremy Geelan jeremy@sys-con.com

Advertising
Senior Vice President, Sales and Marketing
Carmen Gonzalez carmen@sys-con.com
Vice President, Sales and Marketing
Miles Silverman miles@sys-con.com
Advertising Sales Director
Robyn Forma robyn@sys-con.com
Advertising Sales Manager
Dennis Leavey dennis@sys-con.com
Associate Sales Managers
Kristin Kuhnle kristin@sys-con.com
Dorothy Gil dorothy@sys-con.com
Kim Hughes kim@sys-con.com

Editorial
Executive Editor
Gail Schultz gail@sys-con.com
Associate Editors
Nancy Valentine nancy@sys-con.com
Jamie Matusow jamie@sys-con.com
Natalie Charters natalie@sys-con.com
Online Editor
Martin Wezdecki martin@sys-con.com

Production
Production Consultant
Jim Morgan jim@sys-con.com
Art Director
Alex Botero alex@sys-con.com
Associate Art Directors
Louis F. Cuffari louis@sys-con.com
Richard Silverberg richards@sys-con.com
Tami Beatty tami@sys-con.com
Andrea Boden andrea@sys-con.com

Web Services
Information Systems Consultant
Robert Diamond robert@sys-con.com
Web Designers
Stephen Kilmurray stephen@sys-con.com
Matthew Pollotta matthew@sys-con.com

Accounting
Financial Analyst
Joan LaRose joan@sys-con.com
Accounts Receivable
Stephen Michelin smichelin@sys-con.com
Accounts Payable
Betty White betty@sys-con.com

Customer Relations
Circulation Service Coordinators
Edna Earle Russell edna@sys-con.com
Linda Lipton linda@sys-con.com
Monique Floyd monique@sys-con.com

Editorial Offices
SYS-CON Media,135 Chestnut Ridge Rd.
Montvale, NJ 07645
Telephone: 201 802-3000 Fax: 201 782-9638

Worldwide Newsstand Distribution
Curtis Circulation Company, New Milford, NJ

For List Rental Information:
Kevin Collopy: 845 731-2684
kevin.collopy@edithroman.com
Frank Cipolla: 845 731-3832
frank.cipolla@epostdirect.com

Newsstand Distribution Consultant
Brian J. Gregory/Gregory Associates/W.R.D.S.
732 607-9941, BJGAssociates@cs.com

SYS-CON MEDIA
The World's Leading i-Technology Publisher

From the Group Publisher

An A-Z of Security and Storage

IT PROFESSIONALS, TECHNOLOGISTS, AND BUSINESS LEADERS REWRITE THE LEXICON

BY JEREMY GEELAN

SPARE A THOUGHT FOR THE COMPILERS OF DICTIONARIES IN THE DIGITAL AGE. Technology is always moving beyond the confines of the alphabet.

If you were given only 26 choices, for example, what would you list as the chief concerns of IT professionals today? In the storage space alone, there have been more product announcements from suppliers of storage systems in the past six months than in the previous two years. And in the security space, not a week – sometimes not even a day – goes by without a new offering..

So, what should today's i-technology abecedary look like? A for Authentication, B for Backup, C for Clustering, D for Denial-of-Service, E for Encryption…

How about A for AIT (Advanced Intelligent Tape) or D for DAS (Direct Attached Storage)? And what about B for Bots, which are siphoning and transmitting sensitive information from compromised PCs, receiving and spreading malware updates, and being used in distributed, denial-of-service attacks on a wider scale than ever before.

Should F be for Firewall or Fibre Channel, H for Host-Based Security or HIPAA?

By the time you get to S you'd literally have to abandon all hope of narrowing the choices: SAN, Sarbanes-Oxley, SNIA (Storage Networking Industry Association), SNMP, Spam, SSL…Why, with just 26 choices you'd probably never even reach U for USB Drives, V for Virtualization, or W for Worms. Let alone Z for Zero-Day Attacks.

Then would come the colloquies like "Disaster Recovery," "Utility Storage," "IP Spoofing," and the like. Never mind SAN/NAS/RAID, less familiar acronyms are arriving thick and fast, like DHS (Department of Homeland Security), SEP (Security Experts Panel) and even new institutions – like the Internet Storm Center (ISC), an all-volunteer early warning Internet global monitoring organization (http://isc.sans.org/).

Often, amid this slew of technologies and innovations, each new approach seemingly spawns a secondary headache – such as the trend towards networked. IP SANs, which many see as likely to unleash security problems since those who would seek to do harm are so familiar with the IP protocol.

Some say that, in the great scheme of things, neither storage nor security is a front-burner issue – business is. Certainly it is true that, as a recent report noted, IT professionals are often embroiled in operational and tactical considerations, with little time or resources left over for a more strategic approach, and so an understanding of where the storage-security nexus fits in the overall business puzzle is important. But the devil is in the detail, and detail is what we will bring you in each issue.

Here at *ISSJ* we will cover what's new, what's best, and what's next in the ever more important nexus of security and storage. We'll look at key issues, such as whether open-source software means better security or worse.We'll ask where information lifecycle management is going; we'll explore every aspect of storage networking; we'll drill down into NAS management and object-based storage.

What's needed, *ISSJ* articles will show, is a careful, business-based balance between security and storage. Even the most sophisticated SAN isn't much use if it isn't secure – audit regulations require that companies not only log and archive critical data, but also that they do this securely.

As Lenny Heymann, general manager of NetWorld+Interop said, when we unveiled our preview issue at the Networld+Interop Conference & Expo in Las Vegas: "Today's IT buyer is taking a very pragmatic approach to networking purchasing decisions, and really scrutinizing the full range of implications those technologies might have for their company – so discussions about storage should absolutely include related security issues."

The security-storage nexus is here to stay. So is *Information Storage & Security Journal.*

About the Author

Jeremy Geelan is group publisher of SYS-CON Media, and is responsible for the development of new titles and technology portals for the firm. He regularly represents SYS-CON at conferences and trade shows, speaking to technology audiences both in North America and overseas.

jeremy@sys-con.com

A Storage Management Perspective on Sarbanes Oxley

BY JIM DAMOULAKIS

MENTION STORAGE IN the same breath as Sarbanes Oxley and the immediate reaction of senior management might be to hide the checkbook. Invariably a vendor is making a pitch on how the latest, and greatest, WORM-enabled, opto-magnetic, network replicated gizmo is going to solve all of their problems. SOX has become the latest in a line of vehicles to which vendors have hitched their wagons in order to sell more gear (remember the Y2K buying frenzy?). The sad truth of the matter is that you could have the greatest technology in the world and still miserably fail a compliance audit.

The Storage Manager's Dilemma

Don't get me wrong – vendors are not solely to blame. To quote that great American philosopher Pogo, "We have met the enemy and he is us." Many organizations procrastinated before giving serious consideration to SOX, particularly to Section 404's compliance requirements, and now are scrambling at the last minute to address these issues. Of course, the IT organization ends up bearing the brunt of this and, to a large extent, is unprepared to deal with it. Kept largely in the dark as finance, legal, and compliance departments met with consultants and formulated policies, it is now expected that IT will come through, in the 11th hour, with a miracle to somehow implement systems to meet the regulation's directives. The instinctive reaction within IT may be to pick up the phone and call their vendors to see if anyone has a Sarbanes Oxley solution to sell. And they do – sort of.

Within the IT infrastructure organization much of the burden of SOX is borne by the storage management group, which is responsible for data protection and recovery. Unfortunately, in many environments storage management is hamstrung by a lack of visibility into the requirements of SOX. This is symptomatic of a larger scale problem: lack of visibility into the value of data that IT manages. Most data these days is stored on disks, backed up, and sometimes even replicated. Too often, from a storage management perspective it is treated in the same manner regardless of importance or value. Data often has not been classified to differentiate high value data from low value data. And certainly, the storage manager has no idea of what data is SOX-critical. When given a directive to manage SOX data, in desperation, they turn to their vendors.

The vendors then offer technology components that could potentially be incorporated into a solution to a data retention problem. These include primary, secondary, and tertiary storage systems, robotic tape libraries with WORM tape technology, associated networking components, and software to manage all of these devices. Unfortunately, vendors typically cannot sell storage managers what they really need: a set of management and operational processes that can demonstrably ensure internal storage infrastructure controls are compliant with the specifics of the auditing framework being followed within the environment.

Storage and Section 404

Why the emphasis on process? This past November, Section 404 of the Sarbanes Oxley Act went into effect. Among other things, it requires a company to file an internal control statement with its annual report that includes "an assessment, as of the end of the most recent fiscal year ... of the effectiveness of the internal control structure and procedures of the issuer for financial reporting." Essentially, the government is demanding not just that the data be retained, but that companies provide some evidence that they are managing and protecting this information in an appropriate way that ensures compliance - i.e. show us some proof!

While the primary IT-specific impact of Section 404 falls on those groups responsible for financial applications, the IT infrastructure, particularly storage and data protection, is also feeling the effect. At a minimum, storage groups must identify and document processes and establish reporting capabilities to demonstrate that storage management policies and processes are in compliance. From a regulatory perspective, storage-specific activities fall under the category of "general controls", activities that support applications and ensure that systems are reliable and data is protected.

What aspects of storage management must be considered and what needs to be done? Specific areas include:

> Data protection, including data security and the management of backup/restore operations
> Data availability, including policies related to the access to and retrievability of data, both current and from archival sources
> Data recovery, including the ability to recover data in the event of a disaster

Activities in each of these areas include:

> Ensuring that policies exist, are documented, and blessed by legal and compliance
> Processes are validated against policies to ensure that they support them, that they are documented, and that they are followed
> Reporting processes and tools in place that provide evidence;
> A validation process - testing of controls and the accuracy of reporting information

The Upside of SOX

Many storage organizations perceive working toward SOX compliance as a disruptive task adding unnecessary burden to an overworked staff. This is a likely sign of a poorly prepared organization. In reality, many of the activities associated with SOX compliance are things that already should be done as standard policy in a well-run organization. IT audit frameworks, such as COBIT® (Control Objectives in Information Technology) refer to adherence to "good practice", and many organizations have internal goals to meet "best practice" standards. Much of the basis for a SOX-compliant storage infrastructure is following best practices. Activities such as defining standard operating procedures and providing reporting and metrics to support those procedures is simply good practice. Specific activities, such as data classification and recoverability testing, are essential to meeting critical needs of the business as well as for compliance. In other words, if a storage organization is doing the things that it is supposed to be doing, it will not have an extraordinary difficulty in meeting its SOX demands. And if it is not, then the SOX compliance effort can be viewed as a golden opportunity to fix those problems and have the opportunity to better meet the needs of business users.

Where to start

The first step for storage management is to develop a basic SOX competency. This could come from several places and should consist of understanding the law itself, its impact on the organization, and specifically what it means for storage management.

To ensure understanding of organizational requirements, storage management must rely on the appropriate corporate functions: compliance, risk management, finance, and legal. More challenging is the process of interpreting corporate policies and guidelines and turning them into practices that are actionable by IT. A data retention directive, for example, can be acted upon and implemented in a number of ways. Determining which is most appropriate is not always easy. It is likely to be the responsibility of IT to help identify such issues and to be in a position to recommend appropriate courses of action, further underscoring that IT can add value to the SOX compliance process by working closely with other corporate functions. The combined effort between the policy makers and the technical experts will ensure that the actions taken will best meet the compliance needs of the organization.

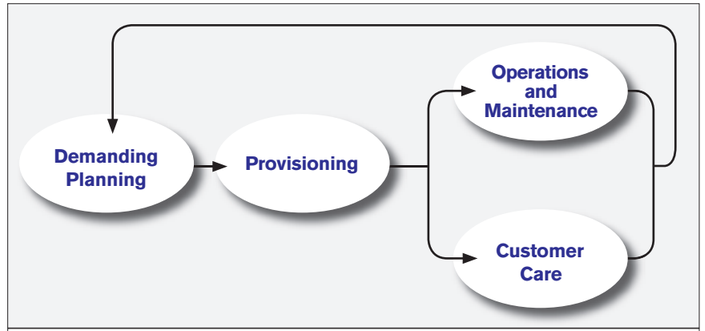


Figure 1: The GlassHouse Strage Management Lifecycle℠

In order to be able to add value, one also must be familiar with the guidelines that auditors are likely to be applying, as well as other related IT frameworks and methodologies. Specifically, for SOX initiatives, storage management should become familiar with COSO and COBIT. For further support, general-purpose IT frameworks such as ITIL (IT Infrastructure Library) may be helpful. Unfortunately none of these guidelines or frameworks specifically addresses storage management. Therefore, it will be necessary to translate policies and directives from business to IT to storage. Let's look at how this might be done.

COSO provides the necessary high-level guidelines for establishing sound corporate governance. The areas of focus defined by COSO include:

> Control Environment: the so-called "tone at the top", detailing specific corporate standard and objectives
> Risk Assessment: specifies the relevant areas of concern that must be addressed by governance policies and practices
> Control Activities: identify the corporate policies, practices, and procedures needed to meet compliance requirements (and, hopefully, business objectives, as well)
> Information and Communication: details the data required, the frequency of reporting, and the channels of communication required to ensure compliance
> Monitoring: covers the activities required to oversee and evaluate that the entire process is being followed and that it is meeting the intended requirements.

The first level of translation from COSO-specified corporate guidelines to IT activities and areas of focus can be accomplished through the COBIT framework, from the IT Governance Institute. COBIT identifies 34 areas of IT-specific governance and control organized into four domains:

> Plan and Organize
> Acquire and Implement
> Deliver and Support
> Monitor and Evaluate

It should be noted that COBIT is not exclusively focused on compliance. It is designed to provide an auditing framework for sound IT management. Therefore COBIT also addresses cost and efficiency concerns that go beyond the scope of compliance but are very much within the scope of business needs.

Translating to Storage

The next step is to applying COSO and COBIT principles to storage infrastructure by initially assessing how well the storage infrastructure is addressing risk, as well as by examining relevant storage processes and making a determination as to whether they are meeting corporate objectives. To do this requires analyzing storage operational processes, mapping these processes to compliance, governance, and business policies, and determining whether requirements are being met.

Unfortunately, neither COSO nor COBIT discusses storage specifically. Thus a translation layer, typically developed by the storage management group, is needed. . For our clients, GlassHouse Technologies provides this translation through a storage-specific best practices framework called the Storage Management Lifecycle. The SML describes the end-to-end operational activities required to effectively

and efficiently manage a storage environment. Figure 1 details the highest-level SML domains, which encompass over 200 activities and focus areas. This framework provides a direct mapping to COSO and COBIT that can serve as a guide for focusing storage activities to appropriately support compliance initiatives. The SML provides a necessary link between storage activities and corporate policies.

A reasonable approach to establishing this link is to focus on the COSO Risk Assessment, Control Activities, and Monitoring areas by conducting a risk and process assessment of the storage environment. A minimum list of questions that the assessment must address includes:

> Does the storage organization have documented processes to address critical areas such as data protection, data security, data availability and recovery?
> Are these processes being followed?
> What levels of monitoring and reporting capabilities are in place to provide assurance that critical data is being protected and can be retrieved in accordance to corporate requirements?

Within each of the critical areas, questions should investigate the quality of each of the processes:

> Do backups complete successfully? Are appropriate measures taken to ensure that media is recoverable? Does the organization test application recoverability (in addition to file recoverability)?
> Is there a data archiving process in addition to the daily backup process? Is appropriate meta-data information being retained to enable timely retrievability?
> How effective is the Disaster Recover process? Is ensuring that DR plans are up-to-date considered in the normal change management process? Are regular DR tests performed?
> How secure is data "at rest"? What processes are in place to ensure that data stored on physical media (disk, tape, or optical) is be protected in accordance with corporate policies?

In our practice, we have adapted the Software Engineering Institute's Capability Maturity Model (CMM) (see Figure 2) to assess SML processes within storage organizations. Generally, in order to meet compliance requirements an organization must be at a minimum maturity level of three for most activities and at a maturity level of four to meet control point requirements for critical tasks.

CMM Level	Name	Description
1	Initial	Ad-hoc, reactive, "firefighting"
2	Repeatable	Proactive, trained people
3	Defined	Documented, standardized products and procedures
4	Managed	Metrics for deliverables and processes
5	Optimizing	Continuous improvement with feedback

Figure 2: Capability Maturity Model

The assessment produces an analysis detailing which processes are critical to the area under consideration, such as compliance, and specifically identifies the gap between where the organization is today and where it needs to be. The gap analysis then leads to the development of a corrective action plan to address shortcomings in a prioritized fashion that will form the basis for a compliance-readiness roadmap.

The specific storage-related control points and tasks will depend upon specific guidelines identified by the compliance office, auditors, or other appropriate committee, and may vary based on the selected audit framework. Typical control points related to data protection will focus on areas related to the backup-restore and disaster recovery processes, and may include:

> Media management tracking, including offsite tape handling and inventory
> Backup success reports for SOX-critical applications
> Restore logs
> Disaster recovery planning, including maintenance, review and testing processes
> Disaster recovery application assignment and review process
> Data retention policies and verification process
> Data expiration policies and verification process

Taking Action

From the risk and process assessment, the next step is to take action. In most instances, this means addressing those activities identified as shortcomings in the assessment. This includes developing and documenting standard operating procedures. This is not a trivial activity and will require a significant investment in time from the staff, both with regard to actual development as well as testing, validation and acceptance.

Monitoring and reporting is also a significant challenge. The existing tools and technologies may only provide a subset of the data required, or may be in a form that is difficult to validate from an auditing perspective. For example, most backup applications can report on the success or failure of backup and restore activities, but they typically provide this information from the perspective of individual servers. There is no report detailing the status of a particular application. This mapping of servers to applications is an additional task that needs to be done to determine whether critical SOX-related data is adequately protected.

Finally, the SOX-compliance effort is not a one-time event. Storage environments are highly dynamic. Data growth rates of 50-100% annually are the norm in many organizations. Ensuring that, as additional storage is added, this new data continues to be managed in accordance with SOX policies is an ongoing activity. Strong adherence to and regular review of provisioning, configuration management, and change management activities must become part of the standard operating procedure.

If this effort is approached properly, the outcome will be more than just an infrastructure that can pass an auditing team's inspection. It will result in a storage organization that is better able to respond to users because data value is understood, and a storage organization that is more efficient because it has better documented, more repeatable processes. It will also provide a methodology for focusing technology investments specifically where they are needed and can be justified in terms the business can appreciate.

Compliance is not only the right thing to do, it's good for you too.

About the Author

Jim Damoulakis is CTO of GlassHouse Technologies, the leading independent provider of storage services.
jimd@glasshouse.com

Enterprise-Wide Intrusion Prevention: Network Security's Next Generation

STOPPING ZERO-DAY ATTACKS, COMBATING EVOLVING SECURITY THREATS, AND ADDRESSING INTERNAL SECURITY

BY BRENDAN HANNIGAN

NEW SECURITY THREATS are growing in frequency, sophistication, and danger. While perimeter-focused security can mitigate risk from known attacks, real protection comes from identifying and reacting to any new threat the instant it hits your network.

This article looks at enterprise-wide intrusion prevention, a technology recognized by network and security experts as the smart way to combat the many threats facing security managers every day. We'll show how it replaces outward-focused security products with an approach that embeds security throughout the enterprise network.

What Is Enterprise-wide Intrusion Prevention? Why Do I Need It?

Continued innovation has created many ways to protect against known threats. We evaluate every new attack that hits, spending valuable time analyzing and creating defenses that protect against major worms, viruses, commonly-known hacking vulnerabilities and other threats. Yet a malicious attacker can change only a few lines of code and the same worm, or Trojan will slip right by the reactive signature or patches developed to stop the original. Hackers creatively find new ways to breach traditional signature-based security defenses. Ongoing changes and upgrades in network infrastructures, Web services, and new software continue to create vulnerabilities and opportunities for exploitation.

Perimeter-focused security, which blocks attacks coming from outside, is no longer enough. IT staff really need to understand what constitutes normal network behavior, identify inconsistent behavior, and fix it so business can proceed. Enterprise-wide intrusion prevention profiles network behavior across the extended enterprise, flags anomalies, isolates the source of the issue or attack, and offers a choice of corrective measures to resolve or mitigate the threat. The net gain comes from faster reaction to breaking threats and shortened time to resolution. Business processes suffer little or no impact. That translates into increased uptime and efficiency combined with decreased operational costs and losses.

How Do I Use Surveillance, Analysis, and Control?

Enterprise-wide intrusion prevention technology models traffic flows, transactions, and network activity and analyzes them to learn what normal behavior, including run-rate activity spikes, looks like. It detects aberrations – changes in traffic levels, communication patterns, or other anomalies that serve as an early warning system for malicious activity – whether from an external attack or internal misuse of the network. Pinpointing suspicious behavior, this technology isolates the source of the anomaly and offers several means of resolution to fix the problem before it causes damage.

Successful enterprise-wide intrusion detection requires a three-tiered approach of surveillance, analysis, and control. Surveillance recognizes malicious activity, catching even the most insidious low-and-slow probes of network defenses without sounding false alarms based on every traffic spike. While firewalls and other appliances provide a limited view from a single point in the network, this technology looks across the entire network.

Behavioral analysis is the key to understanding and applying what is learned from network surveillance. Enterprise-wide intrusion prevention taps both real-time and historical views of network activity to model the behavior of users, applications, servers, and network resources. The latest technology includes a classification engine that profiles network behavior and identifies normal behavior over time. It understands the dynamic complexities of modern networks, recognizing normal and acceptable behavioral changes as safe. It raises an alarm when it perceives potential threats based on deviations from the baseline. Unlike traditional IPS, this technology does not rely on a signature to identify a malicious internal user or an evolving worm. Behavioral analysis recognizes everything from the abnormal behavior caused by a new attack or hacking attempt, to internal threats such as insider scams and stealth attacks. It even finds policy violations among network

Top 10 Benefits of Enterprise-wide Intrusion Prevention

1. **Provides an enterprise-wide security system:** Holistic enterprise-wide view of security goes beyond segment-based, perimeter-focused point products.
2. **Stops external threats:** Provides the first (and often only) defense against the proliferation of zero-day, blended, and internal threats, without the time delays or alarm overload of signature-based systems. This means identifying and locating worms, Trojans, denial of service, and blended/hybrid threats quickly and providing automated resolution.
3. **Enforces internal policies:** Exposes and locates internal threats so you can stop them quickly and eliminate future problems, whether from violation of internal policies or intentional misuse. Such misuse wastes resources and exposes enterprises to unnecessary legal and security risk.
4. **Ensures regulatory compliance:** Provides monitoring, detection, alerts, and audit trails to comply with new regulations and compliance issues that demand IT participation.
5. **Avoids legal risks and liabilities:** Provides the processes and information to protect your organization against risks and liabilities such as lawsuits from illegal file sharing of copyrighted material, lawsuits from accidental disclosure of confidential information, and penalties for noncompliance with regulations.
6. **Improve operational efficiency:** Identifies problems quickly, isolating the source of network bandwidth issues or security threats to speed resolution without additional staff.
7. **Secures the "perimeter-free" network:** Protects open, distributed networks from potential threats for the most advanced defense of infrastructures that can't rely on perimeter security solutions.
8. **Eliminates breaches from mis-configured systems:** Identifies network misconfigurations quickly and effectively, isolating the source to close vulnerabilities and conduits for hackers.
9. **Provides live window of network activity:** Gives network and security administrators an instant real-time view into network behavior, along with access to terabytes of data. It identifies issues in real time and archives a complete audit log of activity without costly additional storage requirements.
10. **Combines network and security analysis:** Integrating asset discovery, vulnerability data, and observed network profiling provides context-sensitive detection of known events. Pivoting between security and network data simplifies the process of finding, fixing, and preventing threats.

users who use P2P file sharing and instant messaging, as well as any type of network misuse.

The third element, control, empowers security and network professionals to enforce network behavior. Simply identifying an anomaly is not enough; corrective measures must be taken as soon as possible. New attacks and security threats continue to hit every network with increasing sophistication – and far greater danger. The control element offers a variety of mechanisms for fixing or mitigating the problem. With a choice ranging from automatic remediation to full operator intervention, administrators can address the most critical issues first and focus their valuable time where it's needed most. These systems can address different types of activities in different ways, and are flexible enough to enforce network behavior based on unique customer use. After all, some parts of the network are more critical than others, and different types of threats require different approaches to resolution. Advances in enterprise-wide intrusion prevention technology give IT staff options they have never before enjoyed.

Where Does Enterprise-wide Intrusion Prevention Fit In My Security Strategy?

In a crowded security market, every vendor hypes a different technology as the most critical element of a layered security defense. So where does enterprise-wide intrusion prevention fit in your security strategy and network architecture?

This technology incorporates security event feeds and network traffic flows from your existing infrastructure to leverage its data completely. But the most direct value it provides, and the primary reason people choose these systems, is to address the critical flaws of traditional signature-based technologies: addressing internal security concerns and stopping subtle blended threats and zero-day attacks. The bulk of ongoing security expenses, and the biggest nightmare for security and network managers, is identifying, reacting to, and cleaning up damage from the "next big attack." No other technology matches the ability of enterprise-wide intrusion prevention to defend against new attacks that are as unpredictable as they are inevitable. It serves as the first-responder product for identifying, understanding, controlling and fixing any new attack.

About the Author

Brendan Hannigan, executive vice president of Marketing & Product Engineering, brings over 16 years of industry experience to Q1 Labs. Before joining Q1 Labs, he was vice president of marketing at Sockeye Networks (a route-optimization firm acquired by Internap), where he led all marketing and product management functions. As director of network research at Forrester Research, he oversaw the firm's most successful practices, covering enterprise networks, security technology, and public network services.
info@q1labs.com

USB Flash Drives – Ready To Go Corporate?

CORPORATIONS SHOULD START REGARDING USB DRIVES AS COMPANY-CONTROLLED DEVICES

BY NIMROD REICHENBERG

YOU WOULDN'T CONSIDER buying a laptop at your nearest consumer electronics store and bringing it into the office to work on, right? What about a RAID disk or a CD drive? – didn't think so. Yet one device that nearly everyone buys privately and keeps in their ockets these days to store both their personal data and confidential corporate data is seldom controlled or secured by the corporation: USB flash drives.

The staggering growth of USB flash drives, from 5 million units sold worldwide in 2002 to 46 million units in 2004 (Source: Gartner), has left many IT departments at odds on how to best tackle this useful, yet potentially risky appliance. Some companies still opt to ban USB drives in their organizations, using anything from a simple policy and procedures to physically welding all USB ports. However, this approach is a short-term stop-gap measure, at best. Most companies, having realized the benefits of using USB flash drives and the fact that they are here to stay, are now looking for solutions to enable their secure deployment and usage.

Corporations should start regarding USB drives in the same way that they treat notebooks, blackberries and other mobile appliances – as company-controlled devices. This implies that these devices should be purchased by the company and configured to adhere to the company's security policy before being issued to employees. Furthermore, the company should be able to set and enforce a policy on non-company issued devices. Employees using unsecured USB flash drives and other portable storage devices pose two serious and almost unrelated sets of risks, either unintentionally or deliberately. Unintentionally, they subject companies to a myriad of risks related to the data stored on their devices when they use them on non-company controlled machines, and the potential introduction of malware when they plug the devices back into a network PC. Deliberately, employees can unlawfully extract data using mass storage devices. Both of these types of risks must be overcome for a secure deployment of USB flash drives.

Overcoming Risks

Unintentionally, employees put their companies at risk the moment they step out of the office. A single misplaced or stolen USB drive can expose companies to severe regulatory and commercial implications. But problems do not stop here - plugging the device into a PC at home or at the business center introduces even more risks – viruses can infect sensitive files, spyware can capture sensitive data and even an innocent application such as a web browser can cache behind critical corporate data. In a recent AOL/National Cyber Security Alliance, 67 percent of home users either had no anti-virus protection or have not updated their protection within the past week. An average number of 93 spyware/adware programs were found on respondents' machines.

What should an IT manager be looking for in order to manage and control the security of these devices? Today there are numerous solutions from hardware to software to assist IT managers with identifying a solution. Some criteria to consider when identifying a solution could include high-grade encryption to ensure data protection. Drives that allow for secure remote access should also be considered, including 2-factor authentication and endpoint security technology that wipes cookies, temporary files, and leaves no traces of work behind so users can safely plug into non-company issued computers.

Companies have begun looking into enterprise-ready USB drives such as Xkey (www.xkey.com), which includes strong authentication and data encryption, as well as on-board anti-virus protection and other security applications to ensure that no unintended traces of work are left behind. Biometric USB flash drives, which require a fingerprint swipe in order to view their content, are also slowly gaining momentum in the enterprise environment.

Deliberately, employees can unlawfully extract data using mass storage devices. If the scene from Al Pacino's 2003 movie "The Recruit," in which a cleverly concealed USB drive was used to steal CIA secrets did not bring this risk into alarming focus, maybe Gartner's study dated July 2004 will. It cited portable storage devices are "ideal for anyone intending to steal sensitive and valuable data" and warned that they can be used to bypass perimeter defenses such as firewalls and antivirus protection at the mailserver. Gartner unequivocally recommends that companies forbid the use of uncontrolled, privately owned devices with corporate PCs. Companies should examine software solutions such as Reflex-Magnetic's Disknet Pro (www.reflex-magnetics.co.uk) or SecureWave's Sanctuary Device Control (www.securewave.com), that enable IT departments to monitor ports and specify which devices are allowed inside the organizations, while banning all others.

Summary

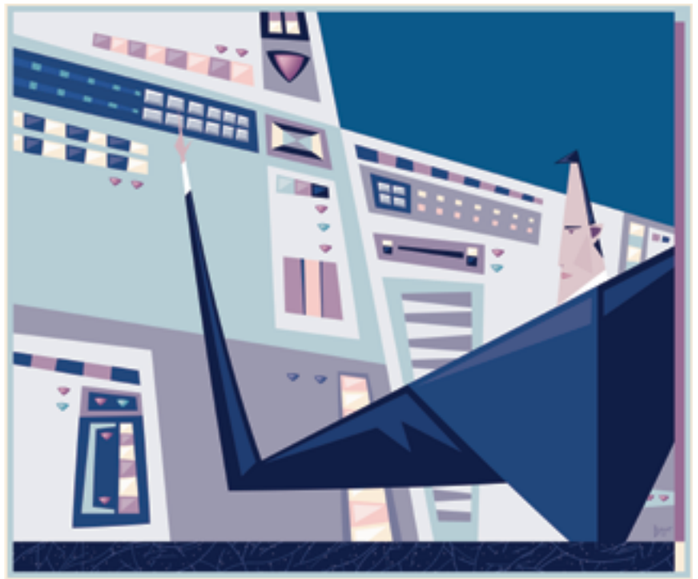
The value of portable storage devices in today's business environment is clear. Equally clear is the initiative corporations must take to integrate these devices with their storage and security policies. Federal regulations such as Sarbanes Oxley and HIPAA will not forgive the unmonitored and unsecured flow of confidential corporate information. With the help of these new secure USB products and applications, neither should you. ■

The Storage Security Problem

… AND HOW TO PROTECT YOUR NETWORK

BY HIMANSHU DWIVEDI AND ANDY HUBBARD

STORAGE NETWORKS HAVE BECOME critical components of corporate computing environments. Regardless of the type of storage technology, these networks have been designed as if the storage environment and all of the components are already secure because security is provided by other networked systems. Most storage vendors, storage application developers, and storage network designers/engineers operate under the false and dangerous assumption that storage networks are both safe and protected from malicious activity. What's true is that storage networks are just as safe as any other unprotected network. It takes only a single exposed entry point for an attacker to gain access to a storage network and compromise everything the organization is trying to protect.



Elements of Security

There are several basic elements to consider when discussing security. The typical security elements that must be addressed by any secure solution are authentication, authorization, auditing, integrity, encryption, and availability/stability.

Most storage product vendors support these elements to some degree, but not in any uniform, standards-based method. Typically, product vendors focus on only a single component of a storage network, so they only provide for selected elements of security based on a single scenario. This limited focus has a direct impact on the user's environment as a whole.

A complete and secure storage solution must address each element of security. The solution must also address the growth and evolution of the storage environment. In order for products to function together, the newer versions often operate in some form of backwards-compatibility mode. This effectively reduces the security of all of the storage products to that offered by the oldest, and most likely, the weakest version.

The problem doesn't end with backwards compatibility. The storage network environment includes network and host elements that are part of the overall corporate computing environment and may even provide backbone functionality (in the case of switches). These elements are often overlooked as part of the overall security posture.

Overlooked items in terms of security include the storage products themselves as well as any other networking or host equipment that is used to make the environment function. If any one of these elements can be replaced, Trojaned, or subverted, then the entire environment is at risk. While lesser degrees of security may be applied to an environment that is fully contained or localized, the decision to do this and the assumptions made about the design must be understood and recorded. Otherwise, future environmental and functional design changes may fail to take previous design assumptions regarding security into account.

Security and the SNIA Shared Storage Model

By addressing security in the context of the layering scheme of the SNIA Shared Storage Model, we can easily identify areas where the elements of security can be applied.

If we break the model down into its component parts we can begin to identify where elements of security should be applied to the SNIA Shared Storage Model (see Figure 1). Determining whether or not one or more of the elements of security may be required for the individual layer and how that security is going to be achieved is the important part.

Applications

Applications are used to run storage devices, manage storage components, move data, and perform any one of a host of other functions needed for the devices and products in a storage network to function. In effect, every component that makes up a storage network is made up of applications. Therefore, each application must be examined in the context of its ability to be used to attack or defend the storage network. The determination of how security applies to individual elements of the storage network will most effectively be made at the application level.

File/Record Layer

Without proper authentication, authorization, auditing, integrity, and availability the components of the file/record layer would easily allow an attacker to bypass security in a number of ways.

Typically, the components of the file/record layer have many of the elements of security built into them. The issue is that the elements of security within these components can be safely ignored if functionality is the only consideration. Databases and file systems are often configured "out of the box" with little in the way of applied security options enabled. This is due primarily to the fact that default installations do not require that either the database or the file system it uses be configured in any way other than simple defaults.

Whether CIFS, NFS, SQL, FTP, or some other proprietary protocol is used, there are risks with the types of communication that are routinely established in the file/record layer of storage networks. These protocols are integral to the file/record layer components and their security components for their ease of deployment and with which disparate systems can be integrated into a shared environment.

Block Aggregation

The interoperability and compatibility issues that come from integrating disparate host, network, and device components often introduce new security challenges within the block aggregation layer. Each of these components requires some level of security to function safely and properly. These components must address security at both an individual as well as a unit level. These components may all come from different vendors that have made different design assumptions. The overall storage network design may call for certain component level capabilities that simply do not exist within the component used.

Storage Devices

By themselves, storage devices are basically inert objects that await commands from some form of controller (disk, server, storage, etc.). Yet they can understand device drivers, they can understand function calls, and they can establish communication to other devices. Therefore, it is important to understand how these devices function and how they could be compromised. For example, an attacker could use this capability to install rogue applications in virtually any location on a storage network – because that rogue application could interface directly with the storage devices.

Authentication

Authentication methods for storage networks like Simple Name Servers, basic end-user authentication, and hard-coded username/password combinations are simplistic and easy to defeat.

Authentication should encompass not only the users of storage systems, but also the devices and applications with which the storage system interacts. In many environments, any component of the storage network can be replaced or added without authentication. And in others, storage applications can be introduced into the environment with no form of authentication other than communicating with the appropriate protocol or utilization of an accepted SDK or API.

Storage networking components can be easily attacked due to weaknesses within their authentication mechanisms. Even environments that have deployed advanced forms of authentication can be attacked if the implementation of these mechanisms is faulty. The strength of any authentication mechanism is based on the quality of the implementation and the strength of the credentials. If the credentials are weak, or if authentication data is exposed due to faulty implementation, the mechanism itself can and will be defeated.

Authorization

In the case of pure networking components, the authorization components are built into the networking gear and may or may not be tied into the advanced authentication/authorization systems that are in common use in larger networks today. In the case of multi-vendor storage networks, there is a wide variety of authorization implementations due to the wide variety of storage hosts, storage devices, and the file system and database components.

User, application, and system authorization are all critical to the security of the overall storage environment. Administrators must ensure that authorization information is not lost during transit from the originating system (the storage client) through some form of intermediary (a storage controller, caching engine, etc.) and eventually to some form of storage device. It is also important to ensure that the credentials that are associated with user access are appropriately understood by all elements of the storage environment and that they can be acted upon (i.e., user rights, disk quotas, or specific file system attributes).

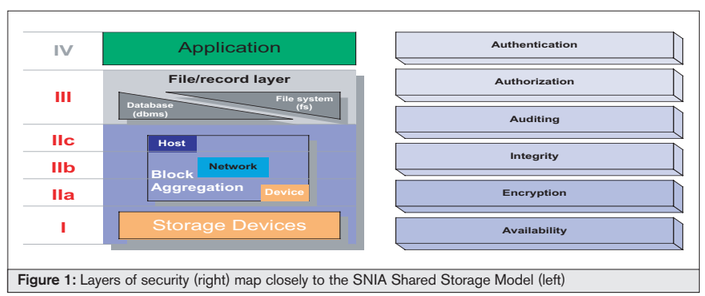


Figure 1: Layers of security (right) map closely to the SNIA Shared Storage Model (left)

Authorization works best when it reflects discrete roles, which encompass users, devices, and applications within the environment. Controls around authorization must be designed with the overall environment in mind. This makes it difficult for administrators of existing storage networks, especially early adopters of storage technologies, as many of the components that currently exist may have been inherited and therefore may not be fully understood.

Failure to identify how and when objects or resources need to be accessed during design will result in lax or nonexistent access controls or authorizations. For example, access to critical files, especially log, temp, cache, configuration, and database files must be closely guarded and limited to privileged accounts. If these files are not protected with proper access controls, or if the access controls can be bypassed in some way, users can essentially gain access to data that may allow them to elevate their privileges.

administrator should create a mechanism to allow containment of a remote logging device for the storage network to identify trends, anomalies, and suspicious activity. Most storage products today relegate logging and log reporting to other components of the storage network. While many storage applications and storage products have some capability to capture and display log information, standards and formats are inconsistent, and the amount and quality of detail vary widely.

Many systems are completely proprietary in nature, making the import and export of logging data into a third-party system difficult. As with other networks, many storage network environments support only limited logging capabilities, and administrators tend to accept the default configuration. In other cases logs are not properly protected or may be accessed by users, even those with limited privileges. Malicious attackers know this, and take advantage of both the product's default logging features (which are limited) and

that integrity has been maintained over time. While storage solution vendors provide some means for ensuring integrity through their product offerings, the integrity of the system remains open to compromise because there is no accounting for the integrity of the networking or switching components that provide the storage system's foundation.

To the trained security professional (or malicious attacker), these network components are obvious attack points. If the storage vendors don't provide helpful security guidelines for the secure deployment of their components, their customers are at risk.

The integrity of the components of the storage network and the configuration of those components is just as important as maintaining data integrity. If an attacker can Trojan or replace a component of the storage network, then he/she can force nearly any change that is desired into that network, up to and including capture or destruction of data.

"Security plays a vital supporting role in enterprise storage networks"

Auditing

The ability of the systems within the storage environment to capture and retain log information pertaining to access and modification of data is paramount to the security of the overall environment.

All storage network components must be able to capture and maintain log information, either remotely or locally; this includes networking components, hosts, storage devices, and storage applications. While these various components of the storage environment may capture and record log information in different ways, they must have the capability to log pertinent information in context.

Additionally, the ability to log both remotely and locally is important for trend analysis and shared security infrastructure. In order to understand security threats and manage security breaches, the average administrator's reluctance to change them. As a result, attacks sometimes go unnoticed. This dynamic presents opportunity for attack of both storage technology (hardware and software) as well as the networking gear that supports the storage network (routers, switches, and hosts).

Sometimes the simplest solution is the best one. Since the de facto standard for logging of information throughout the computing industry is syslog, it would be ideal for storage network components and applications, in the future, to have some means of delivering log information in this format.

Integrity

It goes without saying that storage security must not in any way compromise the storage environment or the data it manages. This requires that the system provide some means to confirm

Encryption

Data encryption for storage networks is still in its infancy. Few storage network architectures take advantage of the benefits of encryption, which can be blamed to some degree on design considerations and functionality tradeoffs when encryption is put to use. The process of encrypting data can be very costly and the tradeoffs significantly impact the performance of any network. Encryption brings with it the requirements to both protect encryption keys and escrow them in the case of a catastrophic system failure. While a malicious user may attempt to steal an encryption key and thus be able to steal usable information from a storage network, it is a far greater risk that in the event of a system failure the loss of an encryption key could render all data upon a given disk array completely irretrievable.

Assuming design considerations and functionality issues are resolved, encryption is not a security panacea. Encryption can protect against data theft, prevent certain forms of hijacking of data, protect network traffic, and even prevent attacking systems from successfully communicating with intended targets. However, encryption cannot protect against the willful destruction of data, which can still be deleted or tampered with in a fashion that will render it useless.

As a security best practice, storage environments must have the ability to encrypt data both in transit and at rest. Since storage environments can be used in many different ways and can have many different customers, steps should be taken to ensure that data is encrypted before it even reaches the storage network. This does not remove the responsibility for providing this capability from the storage vendor, but it is also good practice on the part of the eventual end-user of the environment. This is especially important for users of shared storage environments.

Availability/Stability

Availability and stability of systems are hallmarks of successful products. Unless alternatives are limited or non-existent, users will not put their faith in products that are regularly unavailable or are often thrown into an unstable state. Many storage solutions are susceptible to simple denial of service (DoS) or flooding attacks. The likelihood of these attacks occurring is reduced only by the location of the storage network. As storage networks proliferate, they have a tendency to migrate towards the edge of corporate networks, increasing the likelihood that they come under attack. Furthermore, DoS attacks and flooding attacks are common methods used to force systems into an unstable state or force systems to invoke a down-level protocol. This can be part of a larger attack that necessitates the target being weakened in some way. Smart attackers can target relatively unprotected storage networks in order to compromise other corporate information networks or assets.

Overall system security is a requirement for any environment in order to guarantee availability and stability. If the environment cannot resist even simple attacks, then it cannot be maintained in an available state. In the case of some storage network and some storage product designs, availability is addressed by simply supplying more of the same resource to the resource pool. This will not protect the storage environment from automated attacks or malicious mobile code; it will simply result in more of the same type of resource being damaged. The end result will still be a storage network that is unavailable.

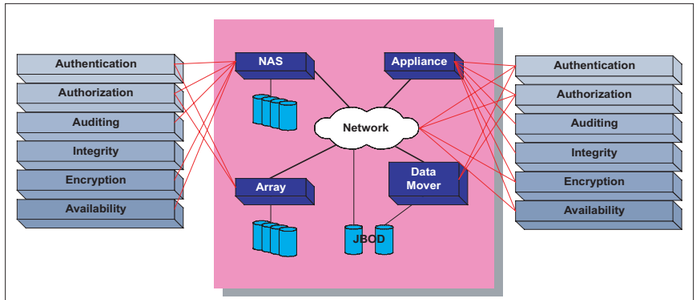


Figure 2: Security elements in storage network design

Elements of Storage Design

Storage network design must take security of both the environment and the data into account. Figure 2 describes a simple storage design that spans multiple networks, and presents configurations that enable communication for this type of network along with potential security risks.

Storage Network Design

As the demand for storage technology increases, it makes economic sense to combine the benefits of storage networks with those of existing network investments. Without proper planning, doing this can actually have negative effects on the security of the existing enterprise network.

Some aspects of a storage network design may look similar to an Out-of-Band (OOB) management network. In these cases the storage network may effectively transit many different security zones, providing attackers with access to a transit network that bypasses security from externally attached networks into the core. Most attackers understand the basics of network management, of which storage solutions may be considered a part, and know how to take advantage of the protocols and applications used to communicate between these systems and environments.

As stated previously, the storage devices and applications may not be the ultimate target of attack, but their vulnerability to attack may make it easy for an attacker to reach resources on the attached enterprise network. In this case, attackers rely on the fact that administrators may cut corners in order to make multi-vendor networking and storage technologies work together.

The converse may also be true. In environments that have grown to depend on storage technology, it is quite possible to introduce connectivity into the storage environment from unanticipated sources. This is a danger in any network, but even more so in storage networks, as many of the components of storage technology within them are critically dependent on the security of the storage environment being maintained.

Product Functionality/Interoperability

Interoperability and functionality are issues that have plagued network and host systems for years. In the case of storage networks it is again an issue of balancing security needs with system requirements of stability, functionality, and performance. Some storage products require such specific configurations that the introduction of some security technologies has a deleterious effect on system performance. In the case of a localized storage network the risks of allowing some protocols or some types of system configuration are relatively limited as the environment is known and well contained. But, when an environment of this type is expanded or connected to other networks, the previously acceptable risks become security nightmares.

Many storage products actually introduce considerable security risks to a network if all of the functionality of the product is enabled. Some simple examples of this are Web-based management, SNMP-based management, and the use of a large number of ports for communications between product components. Fortunately, each of these issues is easily resolved, but in some cases they require additional layers of protection and design. Many of these issues could easily have been prevented by the vendors through more secure product design.

Additional issues arise when product vendors base their product design on third-party solutions. For example, storage controllers are dependent on the base operating system upon which they run. If that OS is taken down frequently due to patch administration and upgrades, the stability and functionality of the storage solution are reduced.

The problem of product maintenance quickly becomes extremely complex. If the vendor is responsible for support of both the storage component and the supporting infrastructure (the OS) component, then that vendor must devote resources to both understanding the patch cycle of the components and managing each product's maintenance schedule. The vendor must also develop methods of updating the product in a fashion that is easily understood by the eventual end user, who may be a storage operations engineer or a systems engineer.

If the vendor product team is not responsible for the maintenance of the component, then both the component and the storage product are exposed to those attacks to which the component may be vulnerable. Unfortunately, it takes only a few days or weeks for attacks to spread among attackers, often leading to a simple attack vector becoming executed against every buyer of a given product line, while the victim companies await the fix or patch from the vendor.

Applications

Storage applications cover the implementation of everything from commercial off-the-shelf (COTS) applications to proprietary applications developed in-house, to software development kits (SDKs) and application programming interfaces (APIs) used to enhance storage solutions. These applications represent major components of the inner workings of the storage environment. As a result, they are all the more attractive to attackers and have become the favorite targets.

Application attack techniques have advanced exponentially in the last few years. Unfortunately, quality engineering, testing processes, and security awareness within software development teams has failed to keep pace. Developers of storage solution software and storage applications, both commercial developers and in-house development teams, often fail to consider what would happen if an attacker gained direct network access via the storage application or device.

Conclusion

Security plays a vital supporting role in enterprise storage networks. As storage networks proliferate and become more integrated within the enterprise network, companies need to put appropriate security plans in place to adequately protect intellectual property. By viewing security as a system of interconnected processes and technologies, companies can still provide appropriate support for requirements such as functionally, throughput, and design simplicity.

This security storage provides a foundation for security professionals who need to understand security issues as they pertain to storage networks. The Security Storage Model puts security in the context of storage and makes it easier for the average storage administrator to include security issues in the design, creation, implementation, and maintenance of any storage network without incurring unnecessary overhead, negatively impacting functionality or compromising the integrity of the data.

About the Authors

Himanshu Dwivedi is a regional technical director at @stake, Inc., where he leads the Storage Center of Excellence (CoE), which focuses research and training around storage technology, including Network Attached Storage (NAS) and Storage Area Networks (SAN). Himanshu is considered an industry expert in the area of SAN security, specifically fibre channel and iSCSI security. He has given numerous presentations and workshops regarding the security in SANs, and currently has a patent pending on a storage design architecture that he co-developed with other @stake professionals (U.S. Patent Serial No. 10/198,728).
hdwivedi@atstake.com

Andy Hubbard is a regional technical director at @stake, Inc., and has been a computer security professional for the past seven years. While at @stake he has worked on projects that range from security assessments and secure design of security infrastructures for Fortune 1000 companies to training and curriculum management for @stake Academy. His most recent projects have included product assessments for a variety of storage and enterprise management software products, focusing on functionality, ease of use, and resistance to internal attack.
ahubbard@atstake.com

Looming Danger

THE NEWEST ASSAULTS TARGET APPLICATIONS AND DATABASES

BY AARON NEWMAN

INEVITABLY, INTRUDERS' MOST attractive targets have the weakest defenses. Therefore, it shouldn't be surprising that enterprise applications and databases are increasingly coming under attack from the kind of threats once associated mostly with operating systems and desktop applications.

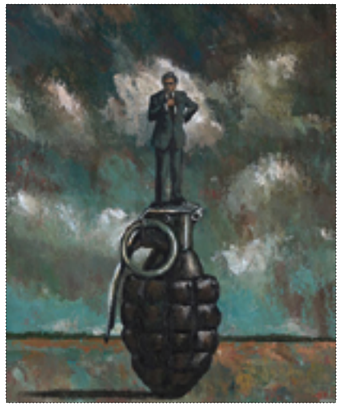
As a result of this trend, most large organizations have already installed anti-virus software, firewalls and even intrusion detection systems (IDSs) to protect their networks and host operating systems. But by comparison, enterprise-class applications have received relatively little attention, on the assumption that they are protected by firewalls and other defenses at the network perimeter. Yet these applications and databases are the major reason enterprises invest in IT in the first place, and the data they contain are often the enterprise's most valuable assets. Indeed, an enterprise without database security is like a bank with locks on the doors and armed guards by every entrance, but no vault.

Though a critical component of a layered defense, firewalls cannot detect and stop the new class of threats now being directed at applications and databases. Another widely deployed tool, intrusion detection systems, performs only passive monitoring and after-the-fact forensics rather than preventing attacks.

Organizations need to bring the same level of protection to applications and databases that they apply to servers and networks, with solutions that can automatically detect and respond to application-level threats in real time, and that are granular enough to provide access for customers and business partners while keeping attackers out.

Requirements for Enterprise-Class Application Security

What capabilities, then, are required to provide true security for the application layer? For a proven framework, look no further than the methodology organizations



have already successfully applied at the network and host operating system levels. Just as at the host and the network perimeters, application-aware security solutions must provide vulnerability assessment, real-time intrusion protection, and encryption. To achieve these goals, such application-level tools must provide:

> ***Audit/Proactive Hardening:*** The system must audit the status and configuration of all application components and perform security tests and proactive hardening of such components while producing detailed security audit reports before and after application deployment. It must also ensure all current patches have been installed; default passwords have been changed; and recommended security configurations (such as changing the default ports on which applications run) have been implemented. As with the network and host OS, assessing the vulnerability of application components is the bedrock upon which any security strategy is built. Without it, an enterprise cannot either proactively minimize risk or gauge ongoing compliance with its security policies.

> ***Real-Time Protection:*** The ability to detect and block attacks as they happen. Not only are more hackers creating more attacks than ever, but the mal-ware they create is spreading more rapidly than ever. Further exacerbating this threat is the window of opportunity left open for intruders before the new vulnerability can be properly repaired. Given today's rapidly propagating threats and the time needed to deploy patches, organizations require real-time protection to complement the proactive hardening provided by ongoing vulnerability assessments.

Attacks can begin at any time. Another growing threat is from "zero-day" attacks which target vulnerabilities before their existence is published and before patches are available for them. This threat exemplifies the need for behavioral-based intrusion prevention systems that can detect, and block, application-level attacks for which there is no known signature to scan for, nor any patch to apply.

Not all security threats are created equal. Some will pose more severe threats than others; and some threats will be of greater danger to some types of organizations than others. For this reason, administrators must be able to tune their response to the danger posed by the security threat for their specific enterprise.

> ***Encryption:*** The ability to encrypt the most sensitive data as a "last line of defense" even if the database itself is compromised. Encryption also prevents unauthorized access to data by legitimate users. For example, a database administrator needs administrative access to the application in order to grant, revoke or change users' access rights, but should not be able to see, change or copy the actual information in the database, such as customers' credit card numbers. Any such encryption solution must be transparent to the application components it protects, meaning that the encryption will still function even as needed changes are made to individual components.

> ***Internal and External Protection:*** The ability to detect and protect against application or database attacks from inside as well as outside the firewall. Many organizations focus their security attention on attacks from outside the organization, and believe that a secure perimeter (such as firewalls) will eliminate most threats. But Gartner, Inc. estimates that 70 percent of security incidents that cause loss (rather than mere annoyance) to organizations involve insiders. Since an insider has trusted access to corporate systems, he or she is (by definition) inside the firewall – meaning that perimeter-based defenses will never see their attacks.

> ***Multi-Tier Protection:*** The ability to protect against attacks at any tier of the IT infrastructure, including the Web front-end, the application and middleware, and the back-end database. Hackers increasingly are creating "blended" attacks that might use a port scan to find a way into a Web front-end, a password dictionary attack to gain illegal access to an application and a SQL injection attack against the database itself. Application-level security must work to protect every tier of the IT infrastructure.

> ***Enterprise-Class Infrastructure:*** A unified scanning infrastructure that works in a common fashion and provides the same capabilities within each tier of the application environment. As organizations move towards flexible, service-based IT architectures, applications may run on any number of tiers (or platforms) throughout the enterprise. The number, and nature of tiers on which an application depends may change unpredictably as business or technical needs change. Organizations cannot afford to pay skilled personnel to monitor multiple security scanning tools, nor can their networks afford the bandwidth it takes for those scanners to look for threats and report their results. Just as with network and host-level security tools, organizations need scalable, enterprise-class application security tools that can grow to meet their future needs.

> ***Distributed Management/Centralized Reporting:*** The ability to delegate the responsibility for and the work involved in, monitoring and managing application and database security across geographies or business units, while providing for centralized reporting of audit results. Modern businesses outsource more work than ever to consultants, contractors, or business partners such as distributors or contract manufacturers. An application-level security system must be flexible enough to delegate responsibility to such outside entities for keeping their portion of shared information systems secure. Even within a single organization, multiple business units, divisions or geographies must cooperate in keeping data secure, and take responsibility for securing that data. At the same time, however, the security infrastructure must provide a single, centralized security audit to provide for centralized accountability and enforcement of security processes.

Summary

Applications and databases form the core of an organization's information technology infrastructure. Without the business processes they support (such as sales, marketing, manufacturing, distribution and accounting) and the data they hold (such as customer names, production status, credit card data, and account histories) the business cannot function. Yet applications and databases have been alarmingly neglected within the enterprise compared to the security provided for networks and servers. Organizations that understand the importance of their applications and databases recognize the need for proactive, dynamic tools that can find and stop attacks on applications and databases before they cripple the enterprise. Fortunately, hard-earned experience securing the network provides a ready-made blueprint for an effective approach to securing enterprise applications: vulnerability assessments, real-time intrusion protection, and encryption at the application layer.

About the Author

Aaron Newman is co-founder and the chief technology officer of Application Security, Inc. (AppSecInc). In his current role, Newman is responsible for defining the overall AppSecInc product vision. Widely regarded as one of the world's foremost database security experts, Newman is the coauthor of the Oracle Security Handbook, printed by Oracle press. Visit http://www.appsecinc.com/techdocs/whitepapers.html, to read "Protecting the Crown Jewels: An Enterprise Class Approach to Application Security," and other white papers in full by Mr. Newman.

anewman@appsecinc.com

Wake Up!

THE INSIDER THREAT CAN BE THE MOST DANGEROUS

BY JONATHAN BINGHAM

THE SECURITY INDUSTRY has a massive problem. Despite a constant flow of patches, millions spent on firewalls and IDS, and updated security procedures, we're still plagued by the insider threat – malicious hackers infiltrating networks using legitimate, but stolen, credentials. As long as there are ways for malicious hackers to find "legitimate" ways into your network – and there are dozens of easy ways – networks will continue to be compromised.

There are two distinct insider threats. The most well known, but less damaging, involves rogue employees wandering around their company networks. Some of these employees are just curious, but others are malcontents looking to inflict damage or benefit financially. They steal documents when moving to a new job or maybe pilfer a few proprietary reports. This damage is localized and can often be contained and controlled. Regardless of the scope, the actual individual is classified as an "unsophisticated"threat to your organization. This is nothing different from the disgruntled employee during the 1970s who grabbed a file out of the file cabinet and sold it to the competition. How do you solve this problem now and then? Access control. Lock it up and only give the keys to the trusted individuals that need access to accomplish their job.

The other class of insider threat shakes the very foundation of a company and costs it millions of dollars. This is the case of sophisticated and malicious hackers or a technically proficient rogue employee who attempts to control the network. These are covert compromises that resemble the infiltration techniques of moles or spies. These kinds of internal breaches – technically internal compromises – are happening with greater frequency. In this case, if the target of the malicious hacker or rogue employee is the research results or formulas critical to the company's success, it is certain to be under lock and key; access is granted only to the select few that need it. Back in the 1970s this was easier to restrict. The individual would physically come to the controller of the information and request access. If there was merit to the request, it was granted. In today's digital world, we have supplemented the "person" with technology to streamline the process and give access to individuals who may not even be in the same location. These access control technologies depend on the user being who they say they are. For example, Chief Scientist Jane Doe from Research and Development at XYZ Biotech Company can see the formulas she is creating to cure cancer. The access control lets Barbara in. The database the data resides on decrypts the information so she can use it. Only problem here is, Barbara isn't actually Barbara anymore. She is a malicious hacker that has compromised her system, gathered her credentials, and can now bypass all access control precautions designed to restrict unauthorized access. In this case the technology worked perfectly. The only problem is it failed to protect the data.

Recent headlines prove that these internal compromises are not as uncommon as many security vendors would lead their buyers to believe. In the last six months, the industry has witnessed Cisco, Ingram Micro, Acxiom , Lowe's, and BJ's Wholesale all going public with insider threat security compromises. More than 10 universities have disclosed similar breaches in the same time period. These compromises were sophisticated and covert operations conducted by malicious hackers, possibly cyber-terrorists, who purposely set out to seize control of the network and the information it contained – be it credit card numbers, secret source code, or sensitive personal and financial information.

And those are just the known examples How many of these compromises have never been disclosed? How many malicious hackers are inside enterprises right now and those enterprises have no idea that an illegal squatter is camped inside their network?

If it's scary now, it's only the tip of the iceberg.

Vendors have deliberately misled the industry into thinking that traditional perimeter defenses can be repositioned on the inside. They are wrong and have created a dangerous climate of hype and misunderstanding that inevitably leads to a frustrating and glaring lack of security.

Hype

That every vendor wants to tackle the insider threat should come as no surprise. The security market is saturated with ways to stop intruders from getting in, but what about after they breach the perimeter? Are they really going to attack the inside after they have already gained legitimate access? Don't count on it.

Because of the risk to companies, solutions to the insider threat can receive heightened priority in security budgets. It's natural that companies want to capture this revenue. However, in the rush they try to force fit technologies not designed for insider compromises into the internal network. If you put an IDS on an external network it's attack detection. If you put it on the internal network it's intrusion detection? Academically this makes sense, but read between the lines. On the outside you attack to get it (if you even need to). Once on the inside, you were successful at penetrating the network. You are now an intruder. Now here's the leap. Intruders and attackers don't behave the same way... What does that mean? Simple, renaming attack technology intrusion technology is lipstick on the bulldog – it doesn't work. Subtle changes mean all the difference, right?

Misunderstanding

With the hype machines in full swing, it's no wonder that security professionals feel overloaded. They already have to worry about so much going on outside and inside their networks. They have employees who do silly or outright inane things that pose problems. They are also crunched and trying to sort out what they need to secure their networks. It might seem like a full time job for two people.

When being secure meant having a VPN or a firewall, new products and services were easily categorized. Now, as threats become more involved and as the areas needing protection broaden, the market has responded by shoveling new solutions, not adequately defined. This gives CIOs and CTOs a false sense of security. They think their IDS system protects the inside, but in reality it doesn't.

Vulnerability

The simple fact is that dressed up IDS systems, anti-DDoS and firewalls do little to combat the Insider Threat effectively. If a sophisticated hacker can bypass them on the outside, there is nothing to suggest that the same technology renamed for an insider solution will do any better in a new environment.

Products that rely on profiling user behavior are easily duped if a malicious hacker illegitimately gains access to an internal network.

Products that use baselines – such as most popular anti-DDoS – will govern in pre-existing compromises and at best, point you in the direction of changes in network traffic.

Firewalls are exploited through covert data channels – specifically Reverse HTTP tunnels. These tunnels basically flip the role of client and server, allowing the server to make requests of the client. Information is often smuggled out of organizations this way taking advantage of the very technology designed to protect.

Action Points

So where does this leave the security professional toiling away in frustration?

> ***Recognize the problem.*** Start to look for technologies that are built for specific threats. Watch out for old products that are chasing the hype as they repackage last month's solution in a new box to address your current problems.

> ***Embrace breakthroughs.*** If you are looking for internal problems you need to understand the threat. If malicious hackers and rogue employees don't attack on the inside, don't protect internal networks with attack technologies. Focus on technologies that are resistant to constant updating and customization.

Conclusion

Compromise detection examines the root causes of internal breaches as they develop. It applies a counter-espionage model to find network spies, similar to hunting for a mole in the CIA or FBI. Unlike other technologies, compromise detection was actually built for the express purpose of guarding the internal network against the insider threat.

The good news for security professionals is that real solutions exist to help protect against the most determined and well-armed adversaries. It's up to all the vendors involved to communicate that message. Remember, you may have locked up all the file cabinets, but the malicious hackers and rogue employees have all the keys. ■

About the Author

As President of Intrusic, Jonathan is responsible for the strategic direction and day-to-day operations of Intrusic. Since its inception Jonathan has been leading Intrusic as it introduces a next-generation security product to market. Jonathan identified the demand in the marketplace and assembled a talented team of security and business professionals to execute on this need. He brings to Intrusic his experience at Forrester Research, where he assisted companies in applying the strategic research relevant to their business needs. While at Forrester, Jonathan identified the need for a security solution addressing the Insider Threat.

jbingham@intrusic.com

Digital Life Cycle Management

WHEN THE "BEST OF BREED" ISN'T ALWAYS BEST

BY DAVID CONFALONIERI

EVERY ORGANIZATION IS confronted with the question of how best to manage digital identities in order to effectively control access to and use of its IT application resources. To grasp the extent of this challenge, consider the stages of an identity's lifecycle, and the processes, practices, and tools needed within each stage.

In this context, identity management is basically defined as the tools and processes related to the efficient, secure, and auditable creation, use, maintenance, and deletion of digital identities. The diagram shows a lifecycle comprised of five core stages, establishing the relationship between Create, Use, Maintain, and Delete; underpinning them all is a consistent Audit mechanism that provides visibility into the what, when, where, and how of that identity's activity in each stage.

It is critically important to recognize the interdependence between each stage in the identity lifecycle. In other words, changes in technology or processes within any one stage are likely to have repercussions on the others. This is why it is imperative that identity lifecycle management initiatives focus as much on the linkage between lifecycle stages as the processes within any one stage. In the end, disjointed identity lifecycle management results in operational, information security, and regulatory compliance problems.

This interdependence between lifecycle stages highlights the need for a turnkey technology approach for identity management, one that provides tight and consistent linkage between the processes of each stage. To date, however, vendors have generally promoted and attempted a "best-of-breed" approach in this arena. This is evidenced by the large number of vendors who provide stand-alone products targeted at individual functions within the lifecycle, such as password management, user account provisioning, directory integration tools, single sign-on, and reporting and audit tools.

Even so-called suite providers may in actuality be best-of-breed product providers. In many cases, each element in the suite is actually fully stand-alone, having been developed separately, at different times, and/or by entirely different companies who have since either merged or OEM'd their product to each other.

While the best-of-breed technology philosophy has merits when addressing

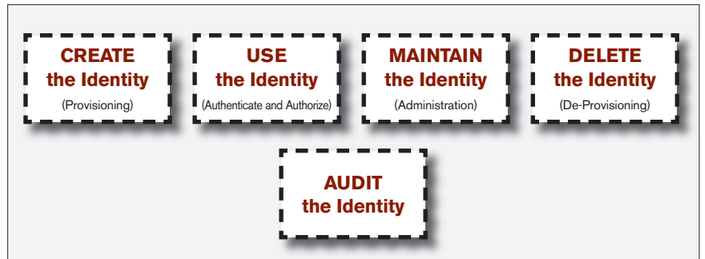


Figure 1: Lifecycle of a Digital Identity

independent, singular problems, it is not well suited for environments with highly interdependent processes that require cohesion; matrixed organizational structures with many shared resources; and sensitivity to the delays that extensive field integration can cause. The identity lifecycle is one such environment where the best-of-breed point product approach will be problematic, for two primary reasons. First, point products are typically functionally oriented, rather than business-unit oriented. This makes providing a complete lifecycle management ecosystem an enterprise-wide proposition rather than a business-unit endeavor. Second, "chaining" point products across lifecycle stages will present greater integration burdens and risks than a cohesive, end-to-end product that establishes a consistent construct for the entire lifecycle.

The Critical Need For Identity Lifecycle Management

As stated above, disjointed and inefficient identity lifecycle management results in a set of interrelated operational, information security, and regulatory compliance problems. Taken together, these form the Secured User Management challenge that needs to be addressed by an identity, access, and audit management infrastructure.

Operational Challenges

This class of business problem concerns itself with operating metrics such as administrative cost burden, personnel productivity, and user satisfaction. In the user management context, examples of operational challenges stemming from poor identity lifecycle management are:

> ***Inefficient and error-prone user account provisioning:*** Each application owner defines a different procedure for account enrollment and approval. The user is burdened with navigating and "walking through" each unique procedure. Furthermore, multiple accounts need to be created, one for each independent application. Depending on the application, the process may be automated or manual, so the time to commission the user is bound to vary. Finally, the fragmented nature of provisioning makes effecting changes to an employee's role and associated privileges a time consuming endeavor.

> ***User frustration with large number of passwords:*** Each independent application requires its own password, whose format is likely to be unique to that application. The end user, overwhelmed with managing multiple and differing passwords, winds up driving excessive help desk costs for resets and renewals. Beyond the hard costs of help desk, from both a brand and customer relationship management standpoint, it is inappropriate to burden users with multiple passwords.

> ***Fragmented system administration:*** Independent applications, implemented on a range of platforms, make it extremely difficult to have a consolidated measurement of administrative overhead across users and applications.

Information Security Challenges

This class of business problem relates to the establishment and enforcement of security policies and standards across the IT environment, particularly in the area of user authentication and authorization. In the user management context, examples of security challenges stemming from identity lifecycle management are:

> ***Inconsistent digital credential policy:*** Each application defines its own standard for credential traits (e.g. strength of password, frequency of password changes).

> ***Weak Authentication:*** Burdening users with a large number of passwords leads them to weaken the password mechanism. At best, users pick simple passwords that they can easily remember. Unfortunately, these passwords are also easy for hackers to crack. Worse, many users write their passwords down and store them in unsecured work areas. The business case for an identity management solution must address the cost of risk associated with having such points of weakness in authentication control.
> ***"Orphan" Accounts:*** The other side of inefficient and error-prone provisioning is an equally problematic de-provisioning hurdle. In this case, the lack of consistent and reliable de-provisioning of a user account results in "orphan accounts", which could be covertly exploited by persons with malicious intent, including former employees and unhappy insiders.

Compliance and Process Integrity Challenges

If these operational and security issues were not enough, there is now a third challenge, which is arguably more compelling than the first two: legal and regulatory compliance. The enactment of numerous regulations, including Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA), is placing a significant strain on business, IT, and auditing resources across the enterprise. Compliance with these regulations demands that controls be defined and enforced to protect the integrity, privacy, and confidentiality of systems and data.

In the context of identity management, this requires that an organization be able to provide a full accounting of each user's activity. At a minimum, this means knowing who has access to which resource, and then tracking when each user accessed each resource.

This class of business problem relates to accurately and cost-effectively collecting and processing data about users' access and activity on IT applications. Examples of challenges stemming from a lack of effective identity lifecycle management are:

> ***Incomplete user data:*** Legacy applications, particularly those without authorization engines, cannot collect granular data on user access patterns. Responding to an auditor's request for such data is therefore impossible.
> ***Fragmented user access data:*** Each independent application collects its own data, in its own repository, using its own rules. Even after the time is spent gathering this data from each application, the process still yields disparate presentations and reports.
> ***No audit report facility:*** Varying (perhaps non-existent in some cases) capabilities in terms of report generation make it practically impossible to provide a single, consolidated audit report of all user activity across all applications.

Identity Lifecycle Management Functions	North America Business Unit	Marketing Department	R&D Division
Audit Reporting	Integrated Platform Approach		
Credential Mgmt			
Delegated Administration			
Single Sign-On			
Authorization Policy			
Account Provisioning			
Directory Integration		Best-of-Breed Point Product Approach	

Figure 2: Point Product vs. Integrated Platform Deployment Approach

Tackling Identity Lifecycle Management

The above discussion highlights the business problems associated with managing digital identities. Due to their interdependence, any solution must be able to concurrently address these operational, information security, and compliance challenges. The strategic question to be answered, then, is whether a best-of-breed (i.e. point product) or integrated platform solution is more appropriate.

The best-of-breed approach to the problem involves selecting a set of point products and undertaking a field integration project to embed them into the enterprise's IT infrastructure. Conversely, an integrated platform approach involves deploying a single infrastructure product that powers all of the identity, access, and audit management services needed in an end-to-end identity lifecycle management system.

A key difference between the two approaches is the way in which they are deployed. A point product is, by definition, focused on delivering a single function (or set of related functions), such as account provisioning or password management. As shown in Figure 2, a point product can be thought of a deploying horizontally across business units. An integrated platform, on the other hand, inherently incorporates all the services needed for identity lifecycle management, and can therefore be regarded as deploying "vertically" within each business unit. Hence the earlier statement that a point product is functionally oriented, while an integrated platform is business-unit oriented. This has important ramifications in the design and deployment strategy for a secured user management solution.

What attracts buyers to point products is their promise of ease of deployment, since a point product is focused on only one business function at a time. This at first may appear simple enough, but if the processes and resources impacted by the point product are shared by multiple business units, then deployment of the product may require a cross-enterprise coordination effort. This has both technological and political implications. When considering a point product, therefore, determine if it can be deployed within a contained area, without drawing in a broader set of constituents.

Ironically, that creates its own challenges. If a point product is really so contained in its reach, experience shows that each individual department will be tempted to acquire whichever product they prefer. This ultimately leads to the company owning a host of products, doing essentially the same thing, deployed throughout the enterprise.

Perhaps the most important ramification of a best-of-breed approach is the amount of field integration that would be needed to chain all the point products into a seamless and efficient identity lifecycle management system. Each product's data scheme, input and output requirements, and configuration flexibility will impact the integration effort. Configuration flexibility, for example, comes into play when two products have some functional overlap. The integration effort will need to determine which product's native functionality will be used, while disabling the other's equivalent functionality.

Another critical integration consideration relates to auditing and reporting. Point products and even some product suites may present multiple log repositories and variable reporting capabilities that would need to be harmonized through integration. Given the regulatory pressures facing enterprises today, it is imperative that an efficient and accurate identity event auditing and reporting mechanism be established. In this way, the cost and risk of auditing will be mitigated as much as possible.

Overall integration effort, cost, and schedule and technical risk need to be carefully assessed, accounting for the complete set of point products that will ultimately be needed for an end-to-end identity management solution.

As shown in Figure 2, the integrated platform approach enables a "vertical" deployment model. That is, it can tackle either the entire enterprise or a business unit at a time. The primary benefit of this approach is the flexibility to rapidly commission the complete identity management ecosystem within a business entity. The result is the ability to show return on investment early in the process, without having to wait until the solution has been placed into production enterprise-wide.

Another key benefit of an integrated platform approach is its inherently lower cost and risk of integration. With all of the key functionality natively built in to the product, the linkages between the lifecycle stages are automatically made strong. Finally, one product platform powering the entire lifecycle management process translates into one security architecture and one consistent administrative and auditing system, thereby maximizing the efficacy of the solution in addressing the operational, security, and compliance challenges mentioned above.

Conclusion

Enterprises are increasingly compelled to design and deploy a Secured User Management solution that concurrently addresses the operational, information security, and regulatory compliance challenges associated with management of users' digital identities. Due to the interdependence between identity lifecycle stages, an integrated technology platform approach is better suited than a best-of-breed product approach for tackling these business problems.

About the Author

David Confalonieri, director of marketing of Secured Services, Inc., oversees product management and marketing of Identiprise, a complete Secured User Management solution, whose distinctive architecture provides a comprehensive digital identity lifecycle management system, deploying identity, access, and audit functionality across all enterprise applications, rapidly and non-disruptively.
dconfalonieri@secured-services.com

New Trends in Vulnerability Detection

ACCURATELY DETERMINE YOUR SECURITY EXPOSURES

BY RON GULA

IF YOU ARE responsible for finding vulnerabilities on large or small enterprise networks, you are faced with a variety of political and technical challenges in doing your job. Fortunately, there have been a variety of new developments in the art of enterprise vulnerability detection that make use of new and old technologies.

The Old Model

Traditionally, corporations schedule yearly vulnerability assessments which are conducted by an internal security team or a third party. These teams use vulnerability scanners to discover the network and the underlying security issues. They use this information to attempt to compromise key systems to demonstrate security weaknesses.

This approach is still in use by many organizations today, but mostly to fulfill a requirement for third party audits. However, these audits can have an impact on operational servers. It is very common for penetration teams to inadvertently crash key servers such as databases, as well as stress network infrastructure such as DNS (domain name system), switches, and routers. Very often, the way vulnerability scanners discover network devices and services can crash network hardware or systems that are not robust. Legacy or outdated machines are particularly susceptible to such crashes.

Although the results of these scans are useful, they are only a snapshot of any network's weaknesses at a given point in time. They do not capture the subtle changes that a network undergoes each day, such as a vulnerable host being added to a DMZ (demilitarized zone).

Instant, Continuous, and Daily Scanning

To get a near real-time view of what is on the network, many organizations are simply scanning more often. Most vulnerability management solutions allow for either daily scanning or continuous scanning. As new systems and vulnerabilities are discovered, alerts can be sent directly to security and operational network teams.

This approach has several positive implications. First, it is very accurate. Any host on the network with a known vulnerability should be discovered. Second, any host or network device that is fragile and easily crashed by scanning will be discovered very quickly. Once these issues are remediated, the network itself will be more robust and resistant to network scanning, as well as worm outbreaks.

An emerging trend is to scan hosts as they are added to the network. For example, if a laptop is plugged into the network, the port that it is connected to is only allowed to talk to a vulnerability scanner. Once a scan of the new laptop is completed, it is allowed to enter the network if no vulnerabilities are found.

Asset-Based Alerting

Some organizations, politically, cannot afford to conduct daily scans of their network infrastructure. An alternative to performing a vulnerability scan is to subscribe to feed of new vulnerability information that is classified by asset types. For example, a company may subscribe to a service and request vulnerability information on Windows 2000, HP-UX 10, Solaris 9, and Red Hat Enterprise 2.1. As new vulnerabilities emerge for these operating systems, the company is notified.

This type of service is very efficient and has no impact on the operational network. However, there are many limitations to this approach. First, the accuracy of the service is totally dependent on what asset information is requested. It also does not take into account any changes to the network. Second, the fidelity of how systems are configured also needs to be taken into consideration. Someone may have 250 RedHat Enterprise 2.1 servers, but 50 of them may be running Apache 1.3, another 50 running Apache 2.0, and 10 of those may be running a MySQL database. If the vulnerability subscription service does not allow for this fidelity of asset descriptions, a false sense of security may result.

An additional variation on this type of method is to use the results of old vulnerability scans to estimate when new vulnerability checks will likely find vulnerable servers. For example, a vulnerability scan may detect 500 Microsoft IIS Web servers. A day later, a new vulnerability check may be available to detect a slightly different Microsoft IIS Web server security issue. Based on the results from the last scan, it may be possible to automatically estimate that some or all of those 500 Web servers are also vulnerable to the new security issue. This type of technology allows security managers to estimate how often they need to scan and make political arguments for launching those scans. If daily scans are already in progress, this sort of technology is not needed.

Passive Vulnerability Discovery

A very recent technology that has been introduced to the market is a set of network traffic analyzers which produce very accurate lists of vulnerabilities. They are commonly known as passive vulnerability scanners. These solutions are deployed much like a sniffer or network intrusion detection system. The technology works by analyzing network traffic to produce a list of active clients and servers, determining which ports they are browsing, the types of applications in use, and vulnerabilities associated with those applications. Very often, these solutions observe how low-level network connections occur to make an accurate guess as to the underlying operating system.

Passive vulnerability detection technology has huge political advantages as there is no impact on the networks that are being monitored. If someone installs an additional server to a DMZ, a passive detection system will observe and report it as soon as it starts to communicate on the network. With an active scan, the system would not be discovered until the next scan was completed. If the system disappeared before the next active scan, it would never be discovered. For this technology to work properly, it is dependent on network traffic. If a backup DNS server is installed and no one makes use of it, the passive technology will not see it.

Although the initial reaction to passive scanning may be that active scans are more accurate, this is often not the case. Most active scans are highly tuned. They look for a limited port range or a specific range of network addresses. They also only look for server-side vulnerabilities. A passive scanner waits for any network traffic and observes both sides of the network session to identify both the client and server.

A practical example of this is the outbreak of the Sasser worm. This worm placed a daemon on port 5554. Before the outbreak of Sasser, this was not a port normally scanned by vulnerability scanners and a worm would likely not be discovered by daily port scans or vulnerability sweeps. However, a passive technology would readily identify new activity on the port. Similarly, with the rash of security alerts occurring in Microsoft e-mail and Web clients, the only way to really audit a network for these vulnerabilities is to get onto the host and see which clients are in use. With a passive technology this information can be gathered directly from the network traffic.

Host-Based Configuration Checking

Security teams are also beginning to deploy technologies that assess the vulnerabilities and configurations of systems directly on the hosts being monitored. Traditionally, most security teams maintain an adversarial relationship with server administrators because they are continuously pointing out problems and creating work for them.

This type of perception is changing. A wide variety of host-based technologies exist which can be deployed with or without agents that give highly accurate reports about vulnerabilities, configurations, and compliance issues. Instead of pointing out long laundry lists of vulnerabilities, these technologies can be used to show which systems are in compliance with audit standards such as Sarbanes-Oxley.

Conducting an audit of access lists and configurations is a huge undertaking for most server administrators. If the security team can do this with an automated tool, it saves an immense amount of time for the administrators. The security team also has the benefit of knowing the exact configuration and patch level of the systems being monitored. This allows them to also be much more accurate in recommending an efficient solution when attempting to mitigate known vulnerabilities.

Conclusions

Each of these technologies has a variety of political and operational advantages and disadvantages. Choosing one, some, or all for your vulnerability assessment needs can result in more accurately determining your security exposures as well as increasing the ties between the security team and network administrators.

About the Author

Ron Gula is the CTO and co-founder of Tenable Network Security, which produces active, passive, and host vulnerability management solutions. Ron is also the original author of the Dragon IDS.

rgula@tenablesecurity.com

SOX & Storage

THE ABCs

BY DAVID BREISACHER

BECAUSE OF TODAY'S emphasis on stakeholder accountability and changing oversight structures, business management is more answerable than at anytime in the past for assuring the accuracy, protection, and access to, financial and other business transactional information. This is creating a partnership of responsibility between the IT domain and the organization's executive management. Recent actions of lawmakers and industry regulators are hitting hard at recordkeeping practices, with specific requirements for the long-term collection and safeguarding of, and quick access to, reams of vital information of all types. As you are probably aware, the Sarbanes-Oxley (SOX) Act mandates changes in financial and corporate reporting, delineates rules for the retention of documents of all types, and provides stiff penalties for the alteration or destruction of records. The act is far-reaching, applying to securities broker-dealers and all companies listed on the U.S. securities markets.

The SEC is requiring that publicly traded companies with market capitalizations over $75 million meet major SOX compliance directives by November 15th of this year (smaller market cap organizations have until July 15th of 2005 to comply). Failure to meet these deadlines can result in substantial financial penalties for corporations, and/or fines and imprisonment of up to 20 years for CEOs and other corporate officers. In practice, the portions of SOX regulations dealing with the implementation of improved records management and protection processes will fall heavily on IT. In order to achieve compliance, additional investments in storage devices, specialized software, new types of media, and enhanced records management controls will be necessary.

We at GST, as storage solutions specialists, believe we have a responsibility to the business community to depict what we believe are the best storage management options that can lessen the burden and cost of SOX compliance as it relates to the collection, protection, archiving, and validation of enterprise data. Because SOX regulations pertaining to recordkeeping demand that stored data not be altered in any way, solutions more often than not will include a computer storage component. This storage component must be one that can be easily customized for your enterprise environment and is affordable, otherwise it won't be implemented even if it fulfills SOX and other requirements. For every "perp walked" exec that goes to jail on TV, there are others that watch and are not moved by it. Beyond government threats of jail and fines, there needs to be the wherewithall to get there in a reasonable fashion, otherwise there could be wholesale non-compliance.

We believe one storage technology that can bring affordable relief to the SOX landscape is a magnetic recording methodology called Write-once, Read-Many (WORM). How WORM functionality might best be implemented to address evolving storage requirements to meet SOX (and an onslaught of similar regulatory actions) is presented below as the A(Assessment), B (Backup & retention), and C (Compliance) of SOX and storage.

(A)ssessment

SOX and other regulations outlining a prescription for backup and restore strategies, records archiving, and long-term data retention are planted squarely in the midst of the computer storage industry. So, too, are the associated requirements that data custodianship be of a non-alterable and non-erasable nature, which has affected the type of magnetic storage media used. The requirements to safeguard more data for longer periods, add e-mail and instant messaging under records management control, and to maintain secure duplicate backup data sets off-site means that storage practices at most organizations will need to be modified both in terms of expanded capacities and new capabilities. To comply with the new regulations, all retained records must be indexed and this index must be easily searchable in order to furnish requested data to oversight agencies on demand. Moreover, a new requirement to report all attempts to modify or delete a stored record will require considerable strengthening of processes affecting enterprise-wide electronic recordkeeping Retaining records for extended periods of time (10, 20, or 30 years) presents a technical challenge for ensuring the retrieval of these records, since both storage media and computer hardware used to read and write onto this media is constantly evolving; with tape backup systems being replaced every three to five years to add capacity and newer functionality, it is difficult to imagine that a stack of tape cartridges or optical disks recorded ten to thirty years ago could be read by the current tape or disk hardware. Accomplishing all of this, while at the same time providing for better access, stricter security controls, and detailed record-keeping of actions dealing with backup files, becomes a formidable assignment for the CIO (chief information officer) and is forcing organizations to overhaul their storage policies and develop methods to save records in a more permanent and protected fashion

However, as daunting as this all seems, SOX should not be considered a burden, but rather a benefit. While compliance with this legislation may repurpose time and money away from other IT projects, upgrading the internal controls over vital recordkeeping should be an ongoing corporate mission and a high-priority, with or without SOX deadlines looming in the not-to-distant future. At GST, we believe each organization must conduct an enterprise-wide assessment of its storage management landscape as the first step in determining what must be done to meet mandated compliance standards in a way that adds value to the rest of the organization.

For those organizations that have already focused on governance, the assessment will show that SOX compliance won't be a disruptive element, as many of its directives would have already been implemented to some degree. For others, the assessment will be a wakeup call and an opportunity to upgrade storage and backup methodologies, disaster recovery practices, and storage management processes, which have been neglected and fallen behind current practices after years of lean budgets and staff cutbacks.

(B)ack Up and Retention

Backup, duplicate, and archive everything! OK, maybe not everything, but close. All employee individual workstations must now be an intricate part of enterprise backup processes, including all e-mail and instant messaging communications, which must be treated as business records. Long-term record-retention policies and the guarantee of the integrity of those records (with verifiable audit trails) plus swift access to all retained data by government agencies and industry overseers are important keys to SOX compliance.

SOX doesn't specify the use of a specific storage technology to accomplish its criteria for long-term data retention and availability on tamper-proof media with verifiable audit trails. WORM magnetic tape functionality, built into new WORM-enabled drives and WORM data cartridges, is the most sensible solution in many cases. WORM identifies a storage technology that includes built-in protection against writing over or erasing any data stored on the media. If additional data or revisions are recorded, they are appended at the end of the existing records on the media, thus creating a continuous audit trail of record additions, changes and deletions. WORM tape drives and cartridges provide the best mix of high performance, high capacity, unalterable backup and long-term retention of data at an affordable cost. WORM functionality is also available on optical disk drives and magnetic hard drives, however both of these options have major drawbacks today. Optical disk's technical properties restrict capacity, performance (speed), and come with a high cost-per-megabyte (million bytes) of stored data. Magnetic disk drives (hard drives) are impractical in terms of easy removal for remote long-term storage due to their lack of portability. WORM tape media provides higher capacities of up to 1.3 terabytes (trillion bytes) and increased performance of up to 280 gigabytes (billion bytes) an hour at a lower cost-per-MB than either of the other options.

Sony Electronics incorporated WORM functionality into their Super-AIT (SAIT) and AIT (Advanced Tape Technology) tape drives. These WORM drives operate with special versions of SAIT and AIT data cartridges. The WORM option is added to the AIT family of tape drives through firmware stored in the WORM data cartridge's Remote Memory-in-Cassette chip making these drives multifunctional ... Sony's SAIT drives accept either WORM or standard (writable/erasable) tape media.

By incorporating WORM functionality into a tape backup solution, we gain the time-tested benefits of tape which are capacity and performance with native capacities up to 500 GB with 30 MB/sec transfer rates (1.3TB capacity with a 78MB/sec transfer rate using 2.6:1 compression). Long-term durability (estimated shelf-life of WORM media is over 30 years), portability (tape cartridges can be easily removed and stored offsite), and the lowest cost of ownership of any WORM media (well below $1/GB) lead us to conclude that tape backup systems with WORM functionality will be the most prevalent SOX-compliant backup technology. Since WORM media protects against over-writes, revisions, or erasing of the stored data. long-term safe storage of retained records is ensured so long as the tapes are protected from environmental damage. On all storage media with WORM, the functionality provides advanced search techniques for easy and quick indexing and access to all stored data. Consequently, WORM meets these records management requirements of SOX and other SEC regulations.

The next challenge is to ensure a fail-safe backup process that won't fail in the middle, and to get the backup media off-site as quickly as possible. GST developed Server-Transparent Media DuplicationTM (SMTDTM) which is a process to ensure that backup media creates two identical backup sets during the backup operation with no extra workload placed on the server. This SMTD, commonly called mirrored backup, delivers identical sets of backup media on GST's dual-drive and mirrored library backup products.

GST's Mirrored Backup Technology using SMTDTM permits identical sets of backup tapes to be created simultaneously during the backup operation. Following the backup, one backup set is retained on-site for any rapid restores that are needed, while the second identical set is safely removed to a secure remote site that can either be a disaster-proof vault or a Disaster Recovery Center.

Another unique capability of mirrored backup configuration (all of which use two tape drives for writing backup tapes or for reading them during a backup restore process) is called Fail-Safe Backup/Restore. During a Mirrored Backup, if a drive fails for any reason, the tape controller attached to both drives continues to write data to the second drive, completing the backup (or restore) process. You can then go off-line to make the duplicate set of tapes needed for the DR center.

(C)ompliance

Once duplicate data sets are created on WORM media, the recorded data cannot be altered or erased due to the write-once functionality of the cartridges. The AIT and SAIT WORM media will last for 30 years when stored in accordance with Federal Guidelines and with practices stated by the maker of the WORM media used (Sony Electronics in the case of AIT and SAIT tape). Both the AIT and SAIT drives are able to read and write earlier generations

of the tape technology (called backward compatible) and write data that future generations of the same tape technology will be able to read (forward compatibility). Thus, the data is guaranteed retrievable after long-term retention, even as new generations of the tape technologies (AIT and SAIT) begin to replace older generations. This meets the SOX requirements that multiple copies of the data be maintained in their original condition for extended time periods and be available to regulators on demand. But all of this only satisfies the part of the records management compliance guidelines pertaining to how data is written to storage media. Another part of SOX compliance is assuring that the physical security of the media be safeguarded. The best way to protect against physical loss or unauthorized removal is to place duplicate copies of records on separate media and place the media in separate locations. Furthermore, access to the location where the media is stored must be tightly controlled. SOX requires that any attempt to alter or erase a stored record be documented. With controls over access, procedures can be put into place to track by whom and when files are accessed and any attempts to alter or remove data on the stored media, and to record unauthorized removal or attempts to remove the media itself from the storage area.

Other smart steps to take that ensure compliance with SOX records retention regulations and avoid the risk of incurring stiff penalties, are to select tape drives and media with the highest reliability ratings. Both MTBF (Mean Time Between Failures) and Head Life Expectancy are longstanding storage industry measurements of drive reliability. For example, the SAIT-1 drives used in GST's tape subsystems and libraries have an MTBF of 500,000 hours and a magnetic head life expectancy of 50,000 hours. Likewise, a good reliability measurement for media is the number of passes a cartridge can endure under heavy usage. The WORM SAIT-1 media is certified for error-free operation for up to 30,000 end-to-end passes.

Sony's WORM drives support both traditional rewritable cartridges and WORM media, facilitating storage policies that dictate when WORM media is to be used and when rewritable cartridges can be used. "Tape continues to be a desirable format for archival storage, and the addition of write-once solutions allows companies to economically meet their storage needs as well as comply with mandates for record storing," noted Fara Yale, Research Vice President at Gartner Dataquest. The SAIT and AIT WORM tape drives and media are designed to meet the SEC's regulatory safety, security, and integrity requirements for electronic storage. Use of WORM media eliminates accidental and intentional erasure of data, enables time and date authentication, and facilitates quick search and retrieval of archived files (most files can be retrieved in about a minute) to support regulatory audits. The managing of the backup process and archival media is greatly simplified and controls and security strengthened by selecting a tape backup solution with a high capacity. For many sites, today's high-capacity tape cartridges (up to 1.3 TB of data when using data compression) permit an entire daily backup to fit on a single data cartridge, making it easy to ship that single cartridge to a Disaster Recovery or remote vaulting site each day and simplifying cataloging, labeling, storing retrieving, and media management.

The Sarbanes-Oxley Act is designed to protect stakeholders -- those with risk tied to an enterprise's performance, which most often includes the organization's shareholders, employees, partners, and customers. Shareholders expect an accurate picture of performance to be delivered in a timely manner. Employees expect continuous operations. Partners, such as financial institutions, require reliable financial reporting and accounting processes. Strategic allies expect delivery of service/products in accordance with contractual agreements. All of these stakeholders are at risk when an organization's financial reporting, controls, and business processes are suspect, inaccurate, or unverifiable. All are served by Sarbanes-Oxley compliance along with associated regulations and oversight organizations.

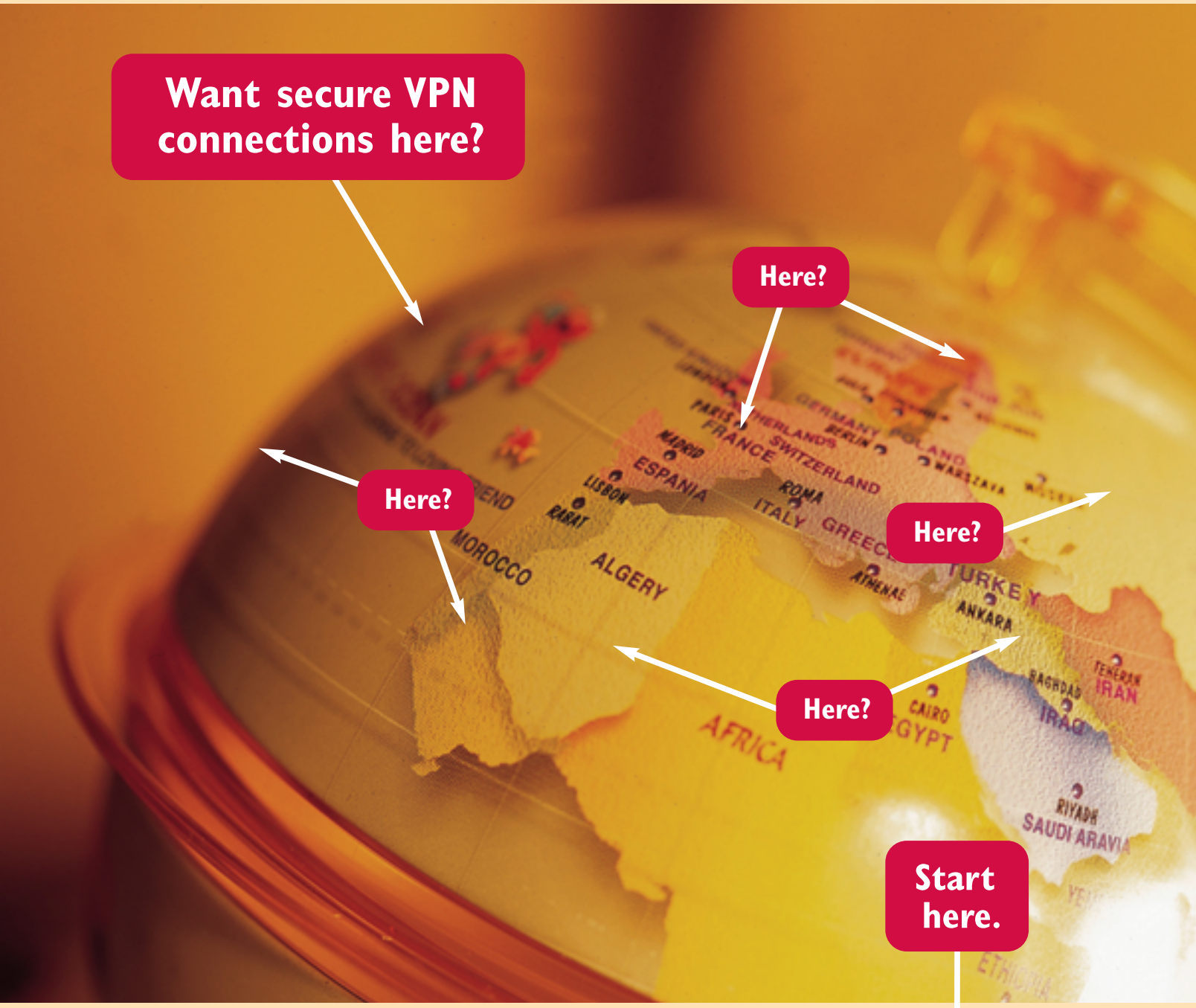
SOX, however, also provides benefits to the complying organization. The corporate responsibility and increased disclosure directives demand that time, energy, and resources are used to upgrade records management, which often means IT operations. Because storage upgrades of software and devices may have to be installed, and improvements made to backup and archival processes to meet compliance requirements, IT operations will be improving business productivity along with financial and accounting reporting. Everyone benefits.

Once a SOX compliance plan for records backup and retention is developed and implemented, rehearsals and reviews on a regular basis are necessary to ensure that plans are continuing to meet compliance objectives. Fully working and tested recordkeeping procedures and compliance plans are the antidote for protecting business processes against obsolete practices and non-compliance leading to stiff fines and even jail time.

"Fully working and tested recordkeeping procedures and compliance plans are the antidote for protecting business processes against **obsolete practices and non-compliance leading to stiff fines and even jail time.**"

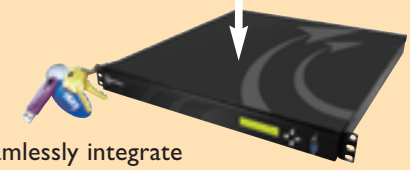
About the Author

David Breisacher is CEO/Chairman at GST, Inc. GST engineers, manufactures and markets tape backup and recovery solutions that include single and dual-drives, autoloaders and tape libraries with a variety of currently used tape technologies including AIT and SAIT, the only current tape technologies with WORM functionality. In addition to founding GST, David has founded several other successful computer companies, including BCC Technologies, a manufacturer of eServer disk, tape and memory devices. A visionary for the storage industry since the early 90s, David's market insights and predictions guide the research conducted at GST.



iKey iGate

Easy remote access doesn't have to mean easy hacker access!



A remote access VPN with SSL is the easiest way to get everyone up and working quickly and securely. With SafeNet's iGate server protection, you also have the option of adding iKey USB authentication. Together they seamlessly integrate to form the industry's only high assurance SSL VPN platform, combining integrated 3A security and application level control with powerful user authentication. Plus an access and control interface that gives you instant authorization and authentication. So if you'd like the ease of a remote access VPN with SSL—without the security worries—call SafeNet today.

Call 1-800-696-5308 to be SafeNet sure.
www.safenet-inc.com/igate

SafeNet®
The Foundation of Information Security

APPLICATIONS - AUTHENTICATION - REMOTE ACCESS - ANTI-PIRACY - LICENSE MANAGEMENT - VPN/SSL