SYS-CON

A Lingua Franca for Security and Development

information STORAGE+ SECURITY journal

www.ISSJournal.com

In This Issue:

VOLUME: 3 ISSUE: 1 2006

E-MAIL: A PORTAL FOR SPAM, VIRUSES, AND SECURITY BREACHES

Are You Ready?

Yesterday's point-solution is no match for today's blended threat—and you can't expect your enterprise IT security experts to be a 24/7 clean-up crew. But you can count on Surf ontrol's Enterprise Protection Suite to deliver unequaled protection against every threat—traveling through every entry point—every time.

It doesn't matter whether it's spam, spyware, phishing, viruses or a specialized day-zero hybrid. Nor does it matter whether it comes from inside your organization, or from outside company walls. The Surf ontrol Enterprise Threat Protection Suite delivers a powerful unified threat management solution, securing Web, e-mail and IM/P2P traffic—from the network gateway to the user desktop. Plus, it's backed by Surf ontrol's 24/7 Adaptive Threat Intelligence Service™. Now you're ready.

FREE 30-day trial **www.surfcontrol.com/go/blended** | 1 800.368.3366

Enterprise Protection Suite
Web, E-mail, IM/P2P, Mobile

Enhance Security
Manage Usage Policies & ompliance
Increase Productivity
Reduce osts & Administration

SurfControl
Adaptive Threat Intelligence™
First to Detect First to Protect™

SurfControl®
Enterprise Threat Protection

information
STORAGE+
SECURITY
journal

Subscriptions

Call 888-303-5252 or 201-802-3012
www.sys-con.com or subscribe@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

Striking the Right Balance

NETWORKED STORAGE IS A SERVICE NOT A PRODUCT

BY PATRICK HYNDS AND BRUCE BACKA

STORAGE IS STILL one of the most costly and fastest-growing aspects of everyone's network and is likely to remain so for some time. Every network user is a storage user. We're all part of a community that shares the costs and the benefits of this expensive resource. Storage management can be a challenging task. There's so much hardware, so many alternatives, and so many issues that it's easy to get lost in the details and fail to see the forest for the trees.

Networked storage is a service not a product. While hardware is necessary for you to provide the service, successful storage management requires a good customer experience, not expensive hardware. Your users are bound to you and the level of service you provide. They can't purchase a unit of storage and take it home with them, nor can they buy storage from another supplier and install it on your network. So we have to treat our users as a customer of our services, not a customer of some product.

The elements that lead to success in the service business are different from those that lead to success in a product business. In particular, service customers want to be a part of those processes that affect them. They want to participate on an on-going basis with the things that will affect them, and it's this participation that leads them to accept and embrace the outcome they get.

The challenge to us, then, as the managers of storage in a cost-constrained world, is to create a high-touch experience for our end users that keeps them continuously engaged at a price we can afford while safeguarding these same resources. Security is in direct conflict with our desire to service the customer because it's limiting. Striking the balance between customers who are happy with the accessibility of the service (storage) and keeping it safe and available only to authorized users is the key. Any product or policy must be evaluated on how well it serves these competing goals as they each map to your organization's needs.

About the Editors

Patrick Hynds is the Microsoft Regional Director for Boston, the CTO of CriticalSites, and has been recognized as a leader in the technology field. An expert on Microsoft technology (with, at last count, 55 Microsoft certifications) he is experienced with other technologies as well (WebSphere, Sybase, Perl, Java, Unix, Netware, C++, etc.). A graduate of West Point and a Gulf War veteran, Patrick has experience in addressing business challenges with special emphasis on security issues involving leading-edge database, Web, and hardware systems. phynds@sys-con.com

Bruce Backa is the founder of NTP Software. He has acted as chief architect, technologist, and project manager for assignments involving large-scale technology and implementation strategies. Bruce has held the positions of director of technology and business research for the American Stock Exchange (AMEX) and director of technology for American International Group. He has also been responsible for the architecture, implementation, and management of a worldwide client/server networking infrastructure for a Fortune 10 company. bbacka@sys-con.com

A Lingua Franca for Security and Development

THE INDUSTRY NEEDS A STANDARD

BY PRAVIR CHANDRA

CHOICEPOINT, CARDSYSTEMS, LEXISNEXIS, Polo Ralph Lauren. The headlines in 2005 were littered with cases of high-profile security breaches and customers, partners, and government are increasingly holding businesses accountable for the security of their applications. Poor application security can result in heavy downstream remediation and management costs, as well as productivity problems, hits on revenue, compliance issues, and damage to corporate reputations.

Unfortunately, most organizations are so busy playing catch-up with security that they neglect their application security problems. They have invested in network-perimeter protection, application-security gateways, and manual software audits. But these approaches are largely after-the-fact solutions that don't target the root cause of security: security flaws in the underlying software.

The Weak Link in the Security Chain

Application security is an enormous, poorly addressed vector of risk for many of the world's largest organizations. For example, overt problems in software — such as SQL injection, session hijacking, and buffer overflows — are caused by extremely common coding mistakes. Although they are easily corrected, these security defects often go unchecked during the software development lifecycle. As a result these vulnerabilities provide an avenue for many of the most common attack types against corporations — attacks that result in millions of dollars worth of productivity losses, data theft, and the like.

So how big is the application security problem? Gartner estimates that approximately 70% of all attacks happen at the application layer, and that it's vastly less expensive for all involved — including the development organization and the customer — to remediate vulnerabilities during development rather than post-deployment. Most security breeches that lead to identity theft, network outages, data loss, or Web site defacement have a root cause in a security flaw that was the result of poorly written code.

As a result, application security is an important emerging requirement in software development. Beyond the potential for severe brand damage, potential financial loss, and privacy issues, risk-aware customers such as financial institutions and governmental organizations are looking for ways to assess the security posture of the products they build or purchase. These kinds of organizations ultimately plan to hold vendors accountable for security problems in their software.

It's clear that security administrators and development teams agree that the best long-term answer to the security problem is to fix these common problems and make software intrinsically more secure. Unfortunately, this is much more easily said than done.

Who Likes Change?

Addressing the application security problem effectively is difficult because the traditional software development lifecycle doesn't deal well with these concerns. This is because software developers lack structured guidance — the few books on the topic are relatively new, and they only document collections of best practices.

Also, development organizations generally prefer to focus on core functionality features, addressing security in an ad hoc way during development. But given their limited security experience, developers typically provide a minimal set of services. This usually results in over-reliance on poorly understood security technologies.

For instance, secure sockets layer (SSL) is the most popular way to provide data confidentiality and integrity services for data traversing a network. However, most SSL deployments are susceptible to network-based attacks because the technology is widely misunderstood. People tend to treat SSL as a drop-in for traditional sockets, but when used that way, they skip critical server authentication steps. Proper authentication is usually a highly complex process. Organizations that deploy technologies such as SSL and Java are often susceptible to a false sense of security.

To add to the problem, while most security professionals recognize some of the common pitfalls, they are unable to communicate clearly with developers and can't implement changes to the development lifecycle. Unfortunately, most organizations don't even see the language gap between developers and traditional

security professionals. They don't realize that asking developers to add security to a product already in development is akin to asking an automaker to install seat belts, airbags, and a steel-enforced, rollover proof cabin in a car after it's hit the assembly line. This ignores the fact that software development is a process and that the only way to impact the quality of the end product is by changing the development process.

A result of the typical shoestring approach to software security is the so-called "penetrate and patch" model. Organizations cross their proverbial fingers, hoping that security problems won't manifest themselves and defer most security issues to when they appear — which is often well after software deployment.

Of course, bolting a security solution on when a problem is found is just as nonsensical as adding a reliability module to fix robustness problems after the software is developed. Again, industry research has examined the costs of addressing security issues at various points during the development lifecycle and clearly shows that the cost of deferring security issues from design all the way to deployment is as much as 10 times greater than the cost associated with traditional reliability bugs. This is largely due to the tremendous overhead that accompanies vulnerability disclosure and actual security breeches.

Security professionals want to help developers write better code, but have always lived in a world where the generally accepted solution is to simply throw more software at a new security problem. The most recent example of this reactionary nature of the security market is the proliferation of spyware and the resulting emergence of the anti-spyware market. Organizations have become accustomed to finding medicine to treat the symptoms of the security disease rather than trying to cure it altogether.

In what may be the most telling sign that the industry's efforts are misguided, recently published research from the SANS Institute shows that hackers and virus writers are now aiming at the actual security products that corporations use to protect themselves. Anti-virus applications are among the most targeted pieces of software by hackers now that operating systems seem to have stopped some of the bleeding.

So hackers are now attacking the software that protected our software. Does this mean that we're supposed to add yet-another layer? Are we going to deploy new software to protect the software that was protecting our software? Confused? Don't worry; you're not alone.

Identifying the Problem

Organizations need to realize that development professionals live in a world vastly different from security professionals. Development is a process-driven discipline where steps and roles are extremely well defined and upsetting the process can result in product development and shipment delays — an outcome that can make management, sales, and even shareholders very unhappy. Development organizations are driven by time-to-market and new feature pressures, not by the need to write more secure code. Only in the most high-profile cases do security breaches result in some sort of action being taken by the development organization to rectify the situation during development.

Security has reached the mainstream conscientiousness of all areas of business and society. Compliance requirements — including Sarbanes-Oxley and other regulations — have moved security to the top of the board's agenda in every large company. High-profile thefts of personal information like those at ChoicePoint and CardSystems have put security back in the media spotlight as a top consumer concern. Isn't it time that security moved into the one area where it can make the biggest difference for all vendors of software, builders of applications, and the people that use them?

Security administrators and developers have to work together to push security into the early stages of the software development lifecycle to address the root cause of the overall security epidemic. To do so, organizations are going to have to build consensus among security, development, and management that better application security is a priority. Unfortunately, most don't know where to start.

Bringing Development and Security Together

There are several steps that organizations can take to get started down the path to better application security. These include:

1. Institute awareness programs: Educate the organization on what's important, why, and who is accountable.
2. Establish assessment strategy: Determine what the inspection process will be and how the results are to be analyzed.
3. Establish security requirements: Ensure that security requirements have the same level of "citizenship" as all other "must haves."
4. Define and monitor metrics: If it's not measurable, progress is impossible to determine.
5. Implement secure development practices: Defined security activities, artifacts, guidelines, and continuous reinforcement must become part of the culture.
6. Build vulnerability remediation processes: If it's bad and you find it, you must be able to assess and contain the exploitation potential and collapse the problem.
7. Publish operational guidelines: The safe-handling procedures for the security of an operational system; if a problem is discovered and the system can't be fixed immediately, the team must be informed of its options.

These basic steps are not the cure-all for application security woes, but they're a good start. Working to rid applications of vulnerabilities involves an agreed-on lingua franca in the software industry. The industry needs to develop a standard for integrating security processes, roles, and artifacts into the existing application development lifecycle with minimal pain and impact on time-to-market.

Even if the approach is modular and takes time to implement, a communications standard will still mark an all-important first step to improving application security. Such a standard is a must if we're going to truly change the way software is developed and impact the overall quality of software. ■

About the Author

Pravir Chandra, chief security architect and co-founder of Secure Software, wrote Network Security with Open SSL, the leading reference book for the world's most popular Open Source cryptographic toolkit.

chandra@securesoftware.com.

Protecting Your Information Assets

THE CROSSROADS OF DATA STORAGE AND DATA SECURITY

BY PAMELA FREDERICKS AND JAMES E. GEIS

EVER SINCE THE introduction of Open Systems into the data center, a problem has been brewing. Too often, the storage environment isn't seen as an area with security considerations. Until recently, corporate security policies rarely considered the data center storage environment; sometimes there was no real link between the two. Security was managed at the operating system level or within applications, and a storage location was seen as purely a physical hardware issue with little bearing on user access or security controls.

However, this is no longer true. By making it much easier to share and access resources, Open Systems architecture has brought data storage and data security considerations to a crossroads: storage security. Not to be confused with information security — which seeks to protect data from unauthorized access, misuse, or theft — storage security refers to the controls surrounding the storage devices and networks that house and deliver that information. Storage security concepts (and the control objectives) parallel those of information security; but some of the risks are new, because the control points and terminology are new.

A storage security mindset requires including the storage environment in the security agenda. For example, those entrusted with storage management roles today are confronting decisions related to data sensitivity, encryption, retention, and the overall integrity of information. And yet, while the storage administration role is responsible for many tasks that have a direct impact on security, privacy, and compliance, those entrusted with storage management roles are likely to operate just under the radar of the information security department, the corporate auditor, and those monitoring regulatory compliance. Storage administration must move from being viewed as a tactical operation to part of strategic information security initiatives.

Likewise, the creation of a storage management control policy is a critical element in achieving an organization's overall security objectives. Compliance has shone a very bright light on how IT manages its controls, with numerous and often unexpected impacts. It is bringing together business and IT disciplines that had never been linked in the past. For example, no one realized that Sarbanes-Oxley would reach into the IT department quite as radically as it did, or that HIPAA security and privacy regulations would affect almost everyone.

Closing an Open Gate

Open Systems have made it much easier to share and access resources, but have at the same time created entirely new complexities for the data center. Digital information access is part of our daily lives now; corporate files and databanks, many of which contain personal data, are regularly accessed from airports, coffee shops, hotel lobbies, and living rooms…from all over the world.

This ease of use creates new security and storage challenges now that personal details, such as a social security number, mother's maiden name, address or credit card numbers can become the entry point to ruined credit, identity theft, and public disgrace for the organizations that allowed it to happen. Frank Abagnale, subject of the book and film *Catch Me If You Can*, once said that all he needed was any three pieces of information about someone, and he could find out everything else about them from the Internet. Given the massive quantities of personal information potentially at risk, the possibilities are staggering.

Meanwhile, corporate data is, in some cases, doubling every six months. At the same time, demands for — and thus replicas of — this data are proliferating exponentially, in multiple locations, greatly complicating the security paradigm. Accordingly, how and where information is stored and accessed, and whether it should be archived and for how long, are now strategic legal decisions. These factors have led to the demand for more sophisticated methods to ensure adequate security and recovery so all of the bases are covered.

What Is Storage Administration?

A definition for paper records management from almost 25 years ago could also describe today's sophisticated information management technology.

A records management program exerts control over the creation, distribution, retention, utilization, storage, retrieval, protection, preservation, and final disposition of all types of records in an organization.[1]

Information today is typically housed on various storage mediums that are accessed through networked storage protocols. In most cases, a dedicated network interconnects the storage-related resources for all operating systems and applications to share. This complexity in connectivity devices enables data transfers at gigabyte-per-second rates and is intrinsically more fault-tolerant should a component or path fail. Business requirements now dictate the elimination of all single points of failure.

Because the storage environment includes hardware devices and multiple

Forum XWall™ Web Services Firewall - Reinventing Security

Security should never be an inhibitor to new opportunity: Forum XWall™ Web Services Firewall has been enabling Fortune 1000 companies to move forward with XML Web services confidently. Forum XWall regulates the flow of XML data, prevents unwanted intrusions and controls access to critical Web services.

Visit us at www.forumsys.com to learn more about how you can take your next leap forward without increasing the risks to your business.

FORUM SYSTEMS™ – THE LEADER IN WEB SERVICES SECURITY

modules of specialized software to configure and monitor the environment, the storage administrator must perform several functions that may cross over into the realm of information security. These include:

- *Classification*. Information must be stored based on its requirements for availability, recoverability, performance, authenticity, security, integrity, or retention.
- *Physical storage*. To ensure that data arrives at its destination, it must be organized and placed correctly across multiple devices. If done incorrectly, data could be overwritten, corrupted, or lost.
- *Logical storage*. Data stores are coordinated on various mediums (storage tiers) in multiple facilities or locations, each potentially having their own access controls
- *Administrative Privilege*. Physical and logical protection of the management consoles, utilities, and tools that can allow direct manipulation (and access to) data
- *Privacy*. Ensuring that encryption is applied where and when appropriate

Converging Classification

In a security context, asset classification categorizes information according to its requirements for confidentiality depending on the potential impact of disclosure or loss. This helps to identify the protection level that should be assigned, with the end goal being that information is secured based on its value and sensitivity. Typical categories are Restricted or Confidential, Internal or Proprietary, and Public or Unclassified. Security is assigned based on who will access the information. Varying privilege levels include *administrator*, *privileged user*, *general user*, and *no access*.

Storage managers are likely to classify information with an emphasis on how it is used, who needs it, and its recovery requirements. Information may be deemed, for example, mission-critical, business-critical, essential, non-critical, or disposable. From the storage perspective, value equates to need (i.e., which applications or platforms use this information), overall business importance, and recovery capability.

Organizations may also have specific privacy classifications, especially in healthcare (which must comply with HIPAA requirements for protected health information, or "PHI"), or when customer data is maintained (personally identifiable information, or "PI"). The privacy or compliance officer's responsibility for properly locating and identifying information in these categories is currently being highlighted due to a proliferation of laws mandating notification if PI security is breached. International data protection laws also require strict control of personal information. And public expectation of PI security whenever a company maintains customer information is increasingly the norm.

Clearly, the best classification level for each type of information must be based on all of these factors. An information classification taxonomy has to be developed that converges multiple perspectives on information storage and access into a single set or matrix of categories. The storage administrator has to stay informed and in close synchronicity with both the security and privacy communities. This will foster sharing about information requirements and ultimately be more effective at protecting the organization's interests than it would be if the storage administrator maintained only a single perspective.

Securing and Controlling the Risk Points in an Networked Storage Architecture

Do internal or external audits include the storage environment when a general controls review is conducted? Probably not. But from a security perspective, storage technology is an application with many of the same access and security control requirements as any other, perhaps more. Accordingly, the following questions should be considered in audits:

Where and what is the networked storage architecture?

Risk points exist in every storage protocol regardless of the transmission medium and regardless of whether the data is "in flight" or "at rest." Both physical and logical security must be considered. As with any data center resource, the physical location of the equipment should be evaluated to ensure that it's protected from unauthorized access. For SAN (storage area network) technology, which is often deployed over extended distances, all geographically disparate storage device locations should be checked for potentially different physical access control procedures.

Network architecture includes the equipment that will transport the data to the SAN. Ethernet ports also exist on the storage devices, servers, switches, routers, and other equipment that transports, houses, and moves information. Ports can be restricted to ensure that unauthorized nodes and other machines are prevented from accessing the data.

Access to management consoles is a key risk area. These may be in- or out-of-band management frameworks, either employing native protocols in the SAN or using IP-based communications. Remote access to SAN devices and consoles should also be evaluated, and may be via VPN (virtual private network) or through other tunneling technologies. These management software vulnerabilities are being addressed in the convergence of the Common Information Module (CIM) and Web-Based Enterprise Management (WBEM) into the Storage Management Initiative Standard (SMI-S) that's being driven by the Storage Networking Industry Association.

Who can access the storage environment?

Storage administrators can access the actual data on storage devices just as a database administrator can access database tables. The number of administrators must be limited and must have assigned backup personnel. Vendors and other third parties may retain access for support or troubleshooting purposes, and if so, appropriate authentication, access, and logging must be enabled. Others in IT who can access the storage environment should be identified, and the circumstances under which they may do so must be documented.

What controls are in place?

Security controls for networked storage should take a classic approach that includes physical, technical, and administrative security elements. First, authentication must be implemented on two levels: for the equipment in the storage network and for the individuals who will access it. Switches and hubs themselves must be authorized and properly authenticated before they are allowed to join the networked storage environment. In a SAN, each switch or director needs a list of the World Wide Names (WWN) of every element authorized to access the environment, and a set of parameters that will be used to verify the identity of all the elements that belong. Storage administrators and other users must then be authenticated via a unique account name and password. Two-factor authentication should be considered, especially for access to management consoles. Passwords are everywhere: on the storage devices, switches, consoles, software. Any vendor-

There's an easier way to protect your data.

Every 12 seconds, a P□ is lost or stolen—most with confidential or sensitive information. In today's stringent environments with laws and compliance issues all around us, protecting your data is a priority that no one can afford to live without.

Fortunately, keeping data safely locked away is easy with SafeGuard® from Utimaco. Unauthorized users can't access, read or decipher protected data, and authorized users won't be inconvenienced or inhibited in any way.

SafeGuard keeps them out with industry-leading authentication, including pre-boot authentication for eTokens, Smart□ard and Biometric identification systems. That's just the first line of defense. The entire hard disk's contents are protected via any of 10 worldwide industry standard encryption algorithms. And because SafeGuard encryption works in the background, users will never know it's working.

Utimaco also has security solutions to protect PDAs, smartphones, files and folders, and emails, as well as LANs, servers and storage, email gateways, embedded systems, digital signatures and stamping.

Protect your crucial data with Utimaco. Risk management has never been so easy.

For more information on how we can help you protect your mobile data visit our website at **www.utimaco.us** or call us at 1-877-UTIMA O.

Try a free demo of our latest SGE4.20 with FIPS mode and omputrace compatibility.

utimaco®
safeware
Security made simple.

default passwords should be changed, and company security standards should dictate account and password expiration and composition requirements.

Encryption is mostly implemented voluntarily, but is increasingly viewed as a standard when transmitting sensitive information on a network (on either a DMZ connected to a public network or internally) and is more frequently being mandated by legislation. Where has encryption been deployed in the storage network? Encryption may be in effect for passwords and data in transit or at rest. Cryptographically secure communication between Fibre Channel devices protects data in transit through the network, but will not address the security of data that is stored on a device. Encryption algorithms commonly encountered in a networked storage infrastructure could include DES, Triple DES, AES, SFTP, SHA, SSL, and SSH.

Change control is another control point that shouldn't be ignored. Changes made by storage administrators should follow IT change control processes with approvals required prior to change or patch implementation. And as with other platforms, a test environment should be implemented. Policies should be enforced against changing data directly on a SAN outside of established enterprise change processes.

Which WWNs are logged in the SAN, and are logs reviewed for any changes in access, zones, or LUN masking? Who audits the environment? Does the security staff or auditors know where these logs are housed and how to obtain or request this log data? If the environment is breached, would it be detected before, during, or after the fact? Storage administrators may need to be included in the part of the Computer Incident Response Team formed to manage incident response. Real-time monitoring, logging, audit trails, and subsequent review of output can provide various windows into SAN activity.

Achieving Security Through Storage Management Control Policy

The need to create and enforce information and storage management policies is clear. But to do this, organizations must understand the complete set of information storage requirements. A common-sense approach will go a long way toward serving business information needs, but a more comprehensive method may be required to address and meet compliance and security requirements.

"CARD"

New information is generated every day, creating new resources to be managed and new protection and storage requirements. Without a clear and defining policy, storage administrators may be unaware of compliance issues that may apply to different kinds of information. "CARD" (Creation, Access, Retention, Deletion) is an intuitive way of viewing the storage information lifecycle and defining supporting policies that may be needed. Information is created, then stored, protected, and accessed for some period before it is, or can, be deleted.

Creation: Thinking about how and why information is created will in most cases define the what and where of its storage requirements. Most of the rules for storage, security, privacy, and access can be made at the point at which the information enters the company. If the time is taken to properly classify information at the beginning, the roadmap for storage, protection, and privacy will fall into place. Backup, recovery, and access requirements can also be defined at the beginning of the information lifecycle.

An information or data "owner" should be appointed to be responsible for classifying information. Often the information security function will have identified owners or approvers throughout the company. When new applications or databases are brought into production, the owner should determine a suitable classification based on information storage, security, privacy, and recovery requirements.

Access: Once classified, decisions regarding the "who" described above can be determined. Access lines can be clearly divided in two ways: first, internal users versus external (non-employee), and second, privileged versus non-privileged access. Access requirements will be influenced by "where" factors, with possibly different access profiles depending on where the networked storage is located or the technology used. Performance attributes may also evolve, having an impact on security or availability requirements.

Retention: The length of time records must be retained to satisfy legal and regulatory requirements is often contained in a policy defined by the legal or compliance department. Again, changes will occur and the storage retention policy must be resilient enough to accommodate this fluctuation. If information is transitioned to other storage mediums (or physical locations) during the retention period, the security paradigm must be continued.

Deletion: And the final question, when is information no longer needed? When can it be flagged for removal and any of the supporting processes be altered (including access, encryption, or monitoring)? This is especially important with any sensitive or personal information, which should be retained only as long as necessary or required by law. When deleted, all copies on all storage mediums should be destroyed. This includes centrally managed or distributed data stored on disk, tape, desktop and laptop drives, and PDAs, etc.

The Crossroads of Information Storage and Security

Storage technology has enabled incredibly fast and efficient information access and replication, which presents a new set of challenges and complexities. The compliance focus of the past several years has made information management more complex, creating new requirements for archiving, retention, and deletion. Information management will be better able to meet these requirements as it becomes more closely aligned with the information security framework. ■

About the Authors

Pamela Fredericks, CISSP, CISM, CIPP, has extensive experience in internal, corporate information security management and administration as well as external consulting. As senior technical consultant at Forsythe, Pamela focuses on security controls and information privacy, with particular emphasis on security management through the creation of IT policies and guidelines that fulfill security, audit, and legal compliance requirements.

James E. Geis is director of storage solutions marketing for Forsythe (www.forsythe.com). Geis developed Forsythe's unique information management framework — the roadmap Forsythe uses for information and storage consulting engagements. He manages Forsythe's professional services practice focused on information policy, information lifecycle management, tiered storage, operational backup and recovery, and data replication and archiving.

www.forsythe.com

Reference

[1]Maedke, Wilmer; Robek, Mary; and Brown, Gerald. (1981). Information and Records Management, Second Edition. Glencoe Publishing Company.

I couldn't believe how little Paul, a Fortune 1000 CIO, knew about what was going on within his storage environment...

(On which he had spent millions.) And he was panicked. That's why we were talking. The platform that he had promised the executive committee would last five years was almost exhausted. He didn't know why the resources were being depleted so fast, or who was consuming all the space.

Perhaps most unsettling, he didn't know what to do about it. But he knew he had to do something in the next 12 months or his job would be at stake.

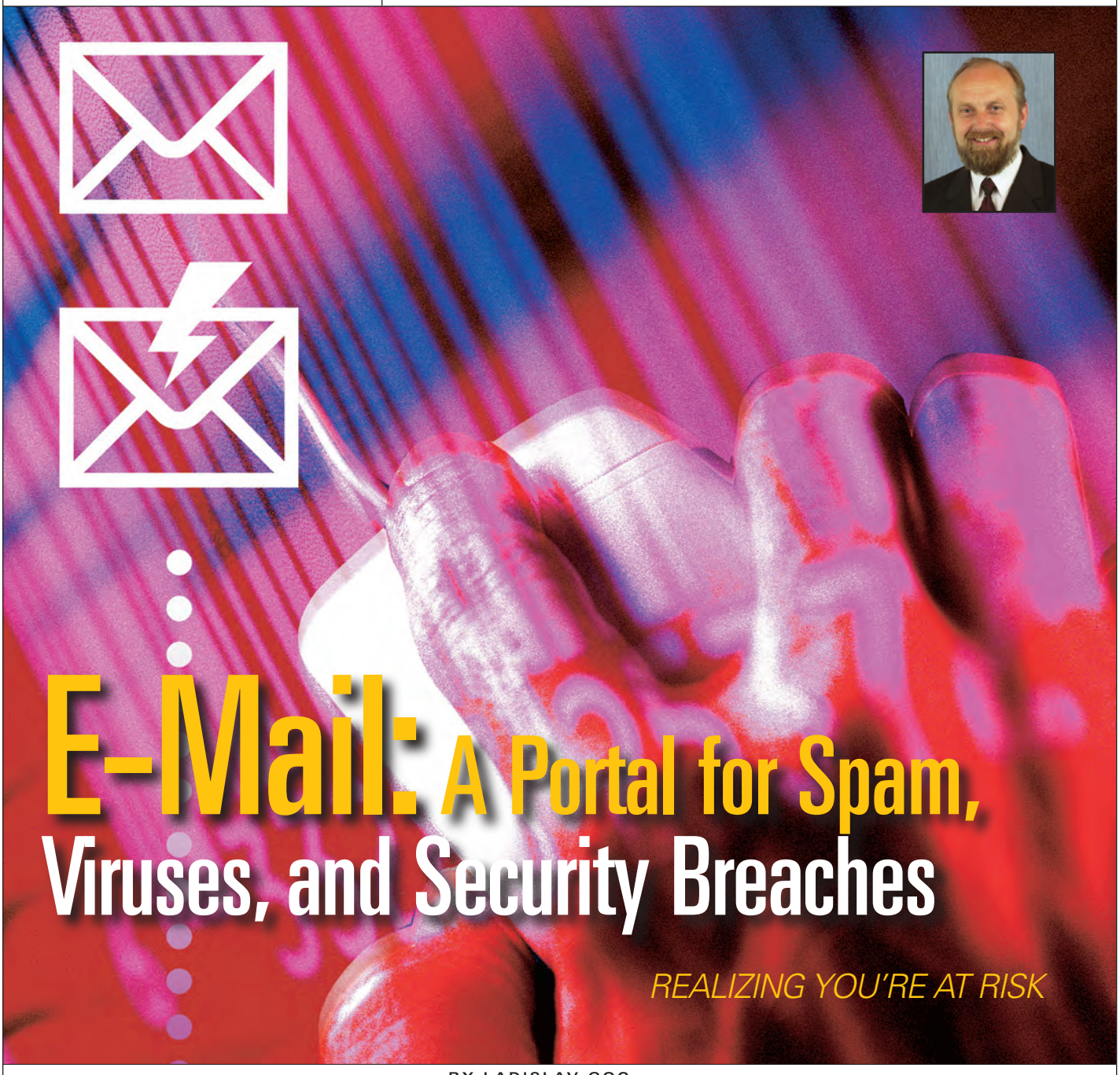
> *"Storage hardware and data growth continues at a phenomenal rate, consuming more and more of the IT budget. Consequently, storage capacity management tools are a critical component to address this run away growth."*
>
> **Ray Paquet**
> **Managing VP, Gartner, Inc.**

Paul took me aside after hearing me speak about storage management at a recent conference. His question was, in essence, "Can you save my job?" I confessed that I didn't know about his job, but said that I *could* help him figure out what was going on in his storage environment and what to do about it. I've seen this problem dozens of times. Paul's situation is by no means unique, but it is also unnecessary. Anyone can learn what's going on in any storage environment. The technology exists — and has for years — to give you whatever level of insight you need. I told Paul that we should install NTP Software Storage Modeling & Analysis (M&A) in his environment to give him all the information he needed — and more. Literally over night, NTP Software Storage M&A would tell him who was using what part of his storage resources and give him the data he needed to charge them for that use. Over time, Storage M&A would reveal patterns of use and project future consumption.

While it's too soon to know Paul's ultimate fate, he already knows who his primary consumers are and what they're doing with his storage. He knows which volumes and platforms are at greatest risk. And he has early projections for his needs in the coming year.

Take the first step to understanding your environment completely...

http://ntpsoftware.com/Paul



E-Mail: A Portal for Spam, Viruses, and Security Breaches

REALIZING YOU'RE AT RISK

BY LADISLAV GOC

OVER THE LAST 15 years, the Internet has revolutionized legitimate business communications supplanting the venerable fax machine and creating its own marketing infrastructure. Nowhere is that revolution more prevalent than in the wide acceptance of e-mail as a way to maintain communications between individuals and corporations.

The ability to attach documents and instantly transfer them from one site to another is an incredible time and money saver. It's also a wide open invitation for unscrupulous people and organizations to harvest the information that is so freely transmitted from site to site.

Because e-mail is so prevalent and accepted it's taken for granted that unless there's some sort of "virtual wiretap," the information that flows over the Internet is secure and accessible only to the sender and receiver. That explains why sensitive information is sent without hesitation over the wire. And yet, access to a company's mail system is a lot easier than most people realize. Even the simple fact of knowing that individual A is in contact with individual B can be of paramount importance in our litigious society.

Reading other people's mail has become an industry in itself. Going to Google and typing in "Sniffing Tools" will bring up over a million and a half sites that offer software that allows people to "sniff" out various activities on any

network. These include packet analyzers, penetration testing, packet capture, encryption analyzers and breakers and many more.

At Risk Mail

When is the mail most at risk? To be honest, e-mail is always at risk. It can be read while in transit over the Internet, it can be read from the LOG files in the servers at either end of the transmission, and it can be picked up in the recipient's e-mail server storage. It's important to understand that unlike regular snail mail or the older fax machines, e-mails don't have a physical form that requires copying for reading. On the Internet, all data is instantly digitized and can be reassembled into its component parts anywhere it lands or is picked up.

E-Mail 101

To understand how accessible e-mail is, a brief explanation of the system is in order.

When a sender sends a message to a recipient, the following steps occur: The mail goes from the sender's computer through a client system (Outlook) to the sender's mail server (SMTP Service). The default configuration in most cases is a plain vanilla SMTP protocol that sends the e-mail over the Internet in an unencrypted format.

This is the easiest stage for an e-mail reader to use the "sniffing tools" that are so widely available. They can be installed in a number of ways on the e-mail sender computer by using available viruses from the Internet.

Sniffer has become a special name for network monitor and analyzer software; it also usually stands for a means of collecting data and information. ISS defines sniffer as a tool that uses the network interfaces of a computer to capture data packets whose destination is other computers. It's clearly a high jacking tool thinly disguised as an analytical tool.

The e-mail goes from the sender's computer to an ISP server, again using an SMTP service. Here the risk of interception increases because a sniffer can be installed by a virus or the ISP itself is monitoring the e-mails that go through its servers for legitimate reasons or otherwise. There are parts of the world where e-mail monitoring is a government prerogative covered by specific laws. China and the United States regularly keep an eye on e-mail traffic to catch subversive activities. Recent legislation makes it very clear how important access to e-mail services is in collecting data used to ferret out conspiracies.

ISPs also regularly capture e-mail addresses to promote spamming activities. Face it, spamming is a form of advertising, and the more contacts you can dish up, the more you get paid. The quality of the contacts is irrelevant because we're dealing in numbers. Recent techniques in spamming let unscrupulous advertisers actually mimic users' current recipients and trick them into opening the mail rather than just trashing it.

At this point the e-mail is entirely visible to anyone who has redirected it and is monitoring the server. Even more significant is the fact that unencrypted attachments can be picked up. The two next steps involve sniffers when the e-mail goes from one server to the next, where they often reside for a while before being picked up, opened, and read by the recipient client (Outlook).

In other words, where SMTP is used, the e-mails are vulnerable if not encrypted.

Travel Light Hint

There's one place where we can almost guarantee that your e-mails will be reviewed unless you take precautions, the Cyber Café where you buy time to check on your e-mails. That is a prime area for infection because the computers are open to everyone and access is unlimited. The person who infected that computer can read your passwords and any other information that you type in including credit card information or any confidential documents you send or receive.

Just keep in mind that viruses have been designed to copy data packets, search for passwords, create activity log files, and send the information they harvest to whoever installed them to find that data.

Places You May Not Think About

Curiosity is an insatiable thirst and people wanting to know you will go to almost any length to get the smallest detail. Each mail server that your mail traverses has a LOG file that notes its passage. These LOG files are quite innocent since they are used for legitimate reasons such as checking server usage, statistical analysis of traffic and doing routine maintenance. The LOG files identify problem areas in delivery, speed, and usage.

The problem is that the e-mail server LOG files note where the mail came from and specifically identifies the exact computer that generated the message, how big the delivery was, and which specific computer picked up the message. Note, it doesn't just identify the recipient e-mail address. It provides the name and location of the actual machine that was logged in to get that message. In a very real sense, it tracks where the two parties were at a specific time. That kind of information can't be bypassed or modified since it's generated at the protocol level and can't be cheated.

So anyone with access to either the recipient or sender's server can access those LOG files. Those files provide a complete communications history.

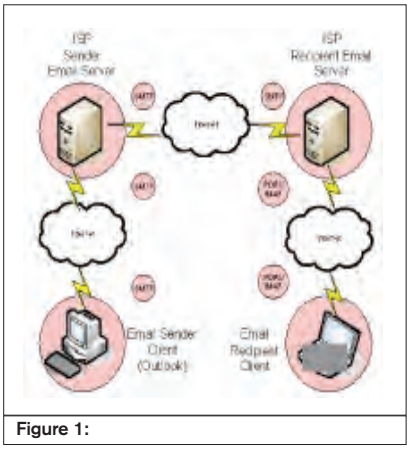


Figure 1:

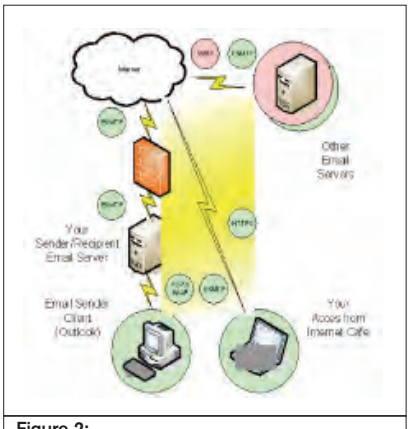


Figure 2:

Recipient E-mail Server

E-mails that arrive at the recipient's server are stored there until they are downloaded and processed. These storage folders are as open to attack as any other section of the e-mail process except for one critical difference, the mail in that server usually stays there in unencrypted form for a long time.

In a POP3 protocol server the mail has a shelf life of several hours to several days, the IMAP protocol allows for several months of storage before being deleted. So anyone with access to the recipient's server has all the time in the world to read the mail.

To make a very simple comparison to snail mail, you put a letter in the mail and unscrupulous mail carriers can access it as long as it's their system. Once they drop it off in your mailbox, anyone with a criminal intent can access it.

How to Get Around the Problem?

The simple answer is to use your own e-mail server located physically in your data center with access restricted to everybody. Using that server you can configure it correctly to protect your clients and company from e-mail tampering on both the sending and receiving end. A company's server is routinely housed near the PBX or even in storage enclosure. These places are wide open to anyone disguised as an electrician, phone company service person or even janitor. If your information is important, put it somewhere where access is limited and open only to authorized personnel.

Install the server just behind the firewall, which allows several layers of protection to be installed safely from outside tampering. If the server is in front of the firewall, nothing you do can protect you from attack. Putting your security systems in front of the firewall creates access to more sophisticated attacks.

In that context you have to install the most sophisticated anti-virus protection you can afford. Be particularly alert to anti-Trojan horse features because they tend to infect the whole computer through the e-mail server. Installing software is a simple operation, but the sheer number of e-mails going through a system can affect the response time of the anti-virus software.

If you have a high-traffic server, consider the fact that your protection can be overwhelmed and will skip messages, randomly select suspicious packets, or slow the whole system to a crawl. With the possibility of up to 20,000 messages going through the server every minute, you may want to consider installing a hardware accelerator to cope with the glut.

Encryption

The best thing you can do is to enable the ESMTP (Extended Simple Mail Transfer Protocol on your server, and most of the more up-to-date e-mail servers support ESMTPT, but be sure to check and see if your server supports the ESMTP protocol, otherwise consider changing your server's software to one that specifically supports the encrypted parameters. The neat thing about ESMTP is that it can transfer all data in encrypted form once you have enabled the TSL/SSL algorithms in the ESMTP which provides endpoint authentification and communications privacy over the Internet using cryptography tools. This ensures that the server is authenticated but the client is uncovered. Going the next step by implementing PKI allows client/server communications that prevent eavesdropping, tampering, and message forgery.

But remember that encryption carries its own risks. The exchange of the decrypting keys is done over the same network as the message. Public keys are usually stored in the user's address book and has to be retrieved from the remote party. The remote party usually publishes his public keys on the Web or sends them as an attachment to his e-mail. However, public keys aren't at risk since they are used only for encrypting messages and private keys are used to decrypt them. Private keys are used for signing. If you sign (with your private key) and encrypt the message (with the recipient's public key) you avoid most security problems.

In long-term relationships, encryption protocols can be set up offline and implemented on a daily random basis. If you control both servers, the keys can be kept safe. There are a number of one-on-one encrypting systems on the market like Kinar. For a small fee they ensure mutually acceptable encrypting between parties. These entail downloading a small software package to decipher the mail and the sender pays for the whole service.

The next step is to ensure that all access to the server is through HTTPS rather than HTTP. This provides one more level of security since the session information is encrypted before transmission using a layer of the SSL you enabled (see above) or TSL. In any case, it allows one more level of protection from eavesdroppers listening or hijacking your e-mails or even the newer man in the middle techniques of capturing e-mails in transit. It's not foolproof since much depends on the installation and the encryption algorithms used, but it does a good job during transmission. It won't protect your data once it arrives in the recipient's server.

Finally make sure that all e-mails and LOG files are stored in your own server where you can control access to them at all times. More importantly you can control who and when access is granted.

The Ultimate Solution

The ultimate solution to ensure that your e-mails are secure is to go to an almost military level of security by encrypting ALL e-mails at the client level. This solution allows secure communications between consenting servers by ensuring encryption from end to end. It also entails setting up complicated encryption systems between peers and should only be considered for the most sensitive data.

Conclusion

There's a lot of interest in what you write and send over the Internet. You transfer information on a daily basis that you may consider useless or relevant to only the recipient, but that information is the gold that data miners are looking for. The e-mail system on the Internet has become the mother lode of all this data. Sophisticated sniffers, server moles, and other traps can be thwarted by taking a few elementary precautions. They can be stopped by taking some complicated precautions. I hope this article will make you consider how open you are, and how to protect yourself.

(In the next article we'll cover how to detect fake e-mails, false URLs, and phishing attempts.)

About the Author

Ladislav Goc started his IT career with FoxBase and became one of the leading European authorities on that database until the company was sold to Microsoft. He founded IceWarp in 1999 to meet the demand for a reliable e-mail platform in the face of the exploding demand for enterprise-level e-mail systems.

The World's Leading Java Resource Is Just a >Click< Away!

JDJ is the world's premier independent, vendor-neutral print resource for the ever-expanding international community of Internet technology professionals who use Java.

SYS-CON MEDIA

ONLY $69.99

ONE YEAR
12 ISSUES

Subscription Price Includes FREE JDJ Digital Edition!

www.JDJ.SYS-CON.com

or **1-888-303-5282**

OFFER SUBJECT TO CHANGE WITHOUT NOTICE

Information Security Assurance

WHY THERE'S NO SINGLE SOLUTION

BY FIONA PATTINSON

INFORMATION SECURITY ASSURANCE is a topic that has developed quickly over the last few years. Drivers for its rapid development include the development of computers at the pace of Moore's Law during the information revolution of the last century. Motivation for interest in the topic stems from the more recent Internet revolution, the focus on critical infrastructure related to Homeland Security, the increased emphasis on corporate governance, and the increasing awareness of privacy matters as society recognizes the dangers that accompany IT advances.

No wonder we occasionally see confusion, and more disturbingly, inappropriate use of standards, schemes, and activities in the security assurance arena. Below is the information security ecosystem in a way that will clarify and demystify some of the key factors and the certification frameworks in common use for information security.

Information security is a pervasive concept. It transcends every aspect of an organization, system, product, component, even protocols. We have to consider information security at every point. In our society, we must consider it as an important aspect of our organizations and their departments, systems, applications, people, protocols, algorithms, and equipment.

There is no single solution to the information security assurance problem. In the software engineering world, Fred Brooks wrote, "There is no silver bullet." He asserted no single software engineering development will produce an order of magnitude improvement in programming productivity. Over the years, this assertion has turned out to be quite true, and I contend this notion is equally true for information security.

There's no silver bullet for information security and, so we must approach the problem with a pellet gun. Symptomatic of such an approach is the variety of frameworks and certifications used to provide assurance at different points in the system. This article discusses the frameworks available and commonly used in the U.S. that offer a certification of some kind and are relevant to the commercial sector. However, there are many other excellent frameworks and schemes apart from those mentioned. Please note, the discussion is general and the specific examples chosen illustrate the information security taxonomy of today.

This "pellet gun" or "piecemeal" approach to information security has the benefit of being very flexible. Existing frameworks can meet the requirements of governments, commercial businesses, and other organizations. However, the approach brings its own risks. One of the major risks is the reliance of each piece on its environment. You might have the strongest, most robust cryptographic algorithm in the universe, but if the staff writes the pass phrase in a text file, it's not secure. You might have an application that has security certifications galore, but if it runs on a system administered by a blackmailing kleptomaniac, it's not secure. You might have a properly accredited system, but if the computer room door isn't locked, or there is no disaster recovery plan, it's not secure. You might have a perfect IT environment, but if the business is run by corrupt people, well, it's just not secure. These scenarios highlight the importance of providing an appropriate environment as a starting point for security.

A quick review of the much-used and often misused term "security assurance" reminds us security assurance is just that: an assurance, or a level of confidence, that things are as we said they should be. There are no absolutes. There is no such thing as perfect security. All we can offer is the ability to make an assessment of how likely it is that things will go wrong. We hear over and over again about "the weakest link." The truth is it's rare to have only one weak link. It's more likely that we have several of them in our "chain." The link that actually fails depends on the particular stresses and use we put on the chain.

To gain any assurance at all, you must trust the person or organization making that assurance. Some important qualities of the assuror are:

- *Independence* (Assurance is *not* influenced by relationships, fears, etc.)
- *Competence* (Assuror must be competent to measure the assurance.)
- *Trustworthiness*

At this point, the third tier of assurance comes in. Accreditation of those making assurances is a way of federating trust. You only need to have trust in one accreditation organization, and then you can call on that organization to tell you who can be relied on to make assurances.

For example, Cryptographic Module Testing laboratories and Common Criteria Testing Laboratories are accredited by the National Voluntary Laboratory Accreditation Program to provide assurance. For ISMS (Information

Security System standards) (ISO/IEC 27001:2005, which used to be BS 7799-2), certification bodies are accredited by accreditation organizations such as the U.K. Accreditation Service (currently there is, no U.S. accreditation organization).

At the highest levels of security, we observe legislation often governs the environment for information security. This legislation can be at the local, state, or national level. Sometimes political or ethical agreements are made at an international level. (For example, the OECD (Organization for Co-operation and Development) guidelines for information security resulted from a G8 conference.) These guidelines are the agreed-on principles that permeate through the various layers and facilitate consistency.

Figure 1 shows some key U.S. legislation, key drivers for information security, the growth in the number of hosts, and selected key events.

Given information security is pervasive, it's not surprising much of the legislation that's having a substantial effect on information security in the U.S. isn't dedicated to the topic, but is embedded in legislation that tackles a wider issue. One example of such legislation is the Sarbanes-Oxley Act of 2002, which includes a requirement for internal controls in Section 404 and which has led to many certification schemes, including those linked to the financial sector (SAS/70) and more general schemes, including CobIT and BS 7799-2 (now ISO/IEC 27001). Another example, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), has been phased in over a number of years, and currently specifies some fairly detailed Information Security requirements for the health industry. However, while the standards' requirements are mandatory, no independent certification scheme was identified with the legislation, nor has an independent certification scheme developed in the years since its enactment. Several commercial entities offer certification schemes, but without a *trusted accreditation scheme*, the independence, competence, and even trustworthiness of commercial providers are often in doubt.

In the U.S., legislation and other policy manifestations have made certification mandatory for providers of products to federal agencies. Examples include DOD Directives #8500.1 and #8500.2; Presidential Decision Directive and 63 Homeland Security Presidential Directive #12.

We also see voluntary regulation in certain industry sectors, where frameworks for security are agreed on, often internationally. An example of such regulation is the ICAO specifications that are being used for passports throughout the world.

A framework specifying an ISMS fills the area between the legislation and the organization. Such a framework uses a risk management approach, and the applicable requirements from legislation, regulation, and others specific to an organization. For the commercial world and for an international company, having an organization certified as conformant with ISO/IEC 27001:2005 provides independent assurance from an accredited certification body that the organization's ISMS conforms to the standard. The standard is process-based and easily integrated with other management system standards such as the Quality Management System (ISO/IEC 9001) or the Environmental Management System (ISO/IEC 14001). (This standard used to be called BS 7799 and includes ISO/IEC 17799.) Certification to this scheme brings a baseline assurance to an organization's customers, partners, and suppliers. It proves the organization followed industry best practices and it can therefore contribute to a defense in case of litigation. This type of certification has even been the vehicle for negotiating a reduction in insurance premiums.

ISO/IEC 27001, in conjunction with ISO/IEC 17799, also ensures that the correct controls are specified and applied to the operation of IT systems. It ensures that the IT systems including operating systems, applications, and network equipment are installed, operated, and patched, that changes are properly managed, and that the systems are de-commissioned according to the program in place.

People are involved in information security at every level. They are IT system users, operators, architects, programmers, testers, auditors, and many other roles. The recent realization of the extent of these roles has prompted a growing popularity in general certifications such as the Certified Information System Security Professional (CISSP) by ISC2 and its specialist certifications. This certification is notable because the ISC2 organization is accredited as conforming to ISO/IEC 17024, which specifies general requirements for bodies that certify people in any occupation. This accreditation brings some assurance about the quality of the certification.

Proprietary training schemes for certifications also exist. These certifications are tied to commercial products, and aim to ensure people using the products have the requisite training and knowledge to do so effectively. For example, Cisco has several certifications for its products, including Cisco Certified Network Associate (CCNA), Cisco Certified Network Professional (CCNP), Cisco Certified Design Associate (CCDA), Cisco Certified Design Professional (CCDP), Cisco Certified Internetwork Design (CID), Cisco Building Remote Access Networks (BCRAN), and Cisco Installation Maintenance Cisco Routers (IMCR).

The processes to include information security during the engineering phase aren't forgotten either. The Systems Security Engineering Capability Maturity Model (SSE CMM) and its ISO counterpart (ISO/IEC 21827) are used to assess the maturity of an organization's processes. This maturity can be formally assessed by third-party auditors who, again, provide assurance the process can be trusted.

There are several other options for achieving information security assurance for operational IT systems. In the U.S., the NIST standards that have been developed in support of the Federal Information Security Management Act of 2002 (FISMA), focused on assuring IT systems are installed and operated properly.

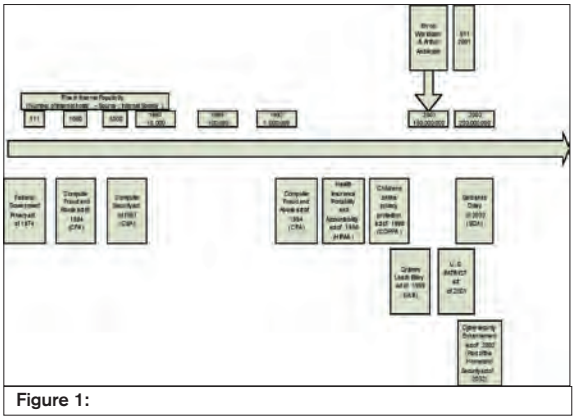


Figure 1:

These standards take a systems-centric viewpoint. They are firmly aimed at (U.S.) federal systems in an environment where certain assumptions about the organization responsible for operating them can be made. These standards are of excellent quality and are free to all; however, no "certification" scheme exists outside the federal world. In the world of government IT systems, we find the terminology used is different. In this framework, the term "accreditation" is used to designate an IT system that has been assessed and approved for use.

At the moment, the full scheme, including certification and accreditation of the systems, is applied only to federal systems, but because it has been successful, there's active interest and movement in bringing this scheme to the commercial world.

Building a secure system, including a variety of diverse components such as operating systems, network equipment, and applications, requires knowledge of the assurance to be gained from each component and how those components can be securely composed into systems. To do this, a flexible framework is needed – one that can be used to assess more complex items. These items might include elements we can't or shouldn't write standard specifications for such as operating systems, large database applications, one-of-a-kind products, or even simpler elements for which a standard specification doesn't exist.

To address this problem, security experts have defined a set of security criteria that can be applied to an item and evaluated. A variety of national frameworks existed including ITSEC in Europe and the Orange Book (part of the Rainbow Series) in the U.S. Over time, these and other frameworks merged and became the "Common Criteria," an international standard that defines a methodology and language that ensures consistency and conformity is defined. It offers adaptability and flexibility. Products are evaluated, and emphasis is placed on ensuring the results are comparable. This comparison is the all-important validation aspect of the process. In any assessment, it's important to define the boundaries, and build a specification of what is to be tested before the evaluation can begin. In the Common Criteria scheme, this specification is called a Security Target and is the most critical document in the process. There's no standard specification; instead, each project must build its own. (In fact, some partial standard specifications exist that can be included in a Security Target. These are known as Protection Profiles.)

For low-level components, a standard specification can be (relatively) easily agreed on. As long as the item *conforms* to that standard, you have assurance the item is at least as good as the standard. This method is fine and works well for simple components. Good examples of items in this class are cryptographic algorithms. As long as they're implemented correctly, then you have all the assurance the specification promises.

However, there are two instances in which assurance can be lost. First, the specification we defined might not be very good. In this situation, expert cryptographers are needed to help create a good one. If the specification hasn't been inspected by a large body of experts, we have much less assurance, which is why proprietary cryptographic algorithms are so often bad news. Second, the specification must be implemented correctly. When NIST gathered statistics about the number of flawed implementations of its approved algorithms, it was startedled to find that approximately 25% were not implemented correctly. If the algorithm isn't implemented correctly, then we can't have ANY assurance from it. So unless your chosen algorithm is a) assessed as being a good algorithm in the first place, and b) validated as being implemented correctly, you can't offer your customers any assurances.

This model works well for items that are simple enough that a) a detailed specification can be written and implemented, and b) a tight boundary can be defined.

Security-related conformance testing schemes in the U.S. include the Cryptographic Algorithm Validation Scheme (CAVS), Cryptographic Module Validation Program (CMVP), and the NIST Personal Identity Validation Program (NPIVP). Within these schemes, there is generally a clear specification and very often the exact tests for conformity are pre-defined. (FIPS 140-2, the standard defining security requirements for cryptographic modules, these tests are known as derived test requirements.)

Another risk of the piecemeal approach is composability; the process of integrating various components evaluated separately is difficult. For example, taking an application that was evaluated with high assurance and running it on an operating system that is also of high assurance doesn't necessarily mean the system is of high assurance. Security experts need to look at the interfaces between the two components and other aspects of the system to ensure that no new vulnerabilities exist; there might be gaps in the frameworks and specifications. In addition, having the products and systems evaluated takes time and is expensive. The cost is no suprise when you consider that security is a quality item. Paying a premium for high-quality items in cost and time-to-market is a well-known phenomenon.

Raising the bar for information security assurance is needed. As the media shows us time after time, various vulnerabilities exist for all of us, from identity theft to the potential vulnerabilities in our nation's critical infrastructure or in electronic voting systems, just to name a few. To reduce our risks and ensure our security, we have to rely on multiple frameworks to identify whether our information is secure. An assurance can give us some comfort, but only if it's given by someone we trust. Security certifications, especially those that work in conjunction with a trusted accreditation scheme, can help provide that trust by ensuring the assuror is independent, competent, and trustworthy.

Find out more about:

- atsec at http://www.atsec.com
  CISSP at http://www.isc2.org
- Common Criteria at http://niap.nist.gov/cc-scheme/ and http://www.commoncriteriaportal.org/
- Cryptographic Module Validation Program at http://csrc.nist.gov/cryptval/
- FISMA at http://csrc.nist.gov/sec-cert/
- ISO/IEC 27001 (BS 7799-2) and ISO/IEC 17799 http://www.xisec.com
- ISSA at http://www.issa.org

About the Author

Fiona Pattinson serves as Common Criteria (CC) lab manager for Austin, Texas-based atsec information security, an IT security consulting and evaluation services company. She manages the atsec Cryptographic Module Testing Laboratory (CMTL) and the forthcoming atsec ISMS Certification Body (CB). Fiona is an evaluator for CC and also a senior consultant. She is a Certified Information System Security Professional (CISSP) and Certified Software Development Professional (CSDP).

ENGAGE AND EXPLORE...

The Technologies, Solutions and Applications that are Driving Today's Initiatives and Strategies...

CALL FOR PAPERS NOW OPEN!

SOA WebServices Edge 10th International conference+expo 06

The Sixth Annual SOA Web Services Edge 2006 East - International Web Services Conference & Expo, to be held June 2006, announces that its Call for Papers is now open. Topics include all aspects of Web services and Service-Oriented Architecture

Suggested topics...

- *Transitioning Successfully to SOA*
- *Federated Web services*
- *ebXML*
- *Orchestration*
- *Discovery*
- *The Business Case for SOA*
- *Interop & Standards*
- *Web Services Management*
- *Messaging Buses and SOA*
- *Enterprise Service Buses*
- *SOBAs (Service-Oriented Business Apps)*
- *Delivering ROI with SOA*
- *Java Web Services*
- *XML Web Services*
- *Security*
- *Professional Open Source*
- *Systems Integration*
- *Sarbanes-Oxley*
- *Grid Computing*
- *Business Process Management*
- *Web Services Choreography*

CALL FOR PAPERS NOW OPEN!

2006 ENTERPRISE> OPENSOURCE CONFERENCE+EXPO

The first annual Enterprise Open Source Conference & Expo announces that its Call for Papers is now open. Topics include all aspects of Open Source technology. The Enterprise Open Source Conference & Expo is a software development and management conference addressing the emerging technologies, tools and strategies surrounding the development of open source software. We invite you to submit a proposal to present in the following topics. Case studies, tools, best practices, development, security, deployment, performance, challenges, application management, strategies and integration.

Suggested topics...

- *Open Source Licenses*
- *Open Source & E-Mail*
- *Databases*
- *ROI Case Studies*
- *Open Source ERP & CRM*
- *Open-Source SIP*
- *Testing*
- *LAMP Technologies*
- *Open Source on the Desktop*
- *Open Source & Sarbanes-Oxley*
- *IP Management*

Submit Your Topic Today! www2.sys-con.com/events

Sponsored by

WebServices JOURNAL | XML JOURNAL | .NET DEVELOPER'S JOURNAL | eclipse developer's journal | WebSphere JOURNAL | information STORAGE+SECURITY journal | wldj | JDJ | LINUXWORLD MAGAZINE | MX developer's journal | asp.netPRO | SD Times | CoDe | Software Test & Performance

*Call for Papers email: jimh@sys-con.com

Attention Exhibitors:
An Exhibit-Forum will display leading Web services and OpenSource products, services, and solutions

For Exhibit and Sponsorship Information ► Call 201 802-3066

An Information-Centric Approach to Information Security

DATA SECURITY IS A PROCESS, NOT A PRODUCT

BY DENNIS HOFFMAN

SUCCESSFUL BUSINESSES EXECUTE simultaneously on three fronts: sustained revenue growth, continuous cost control, and comprehensive risk management. Driven by a significant rise in public awareness of information security breaches, the discipline of risk management is under increased pressure to protect the information assets of the business better. This pressure has resulted in a great deal of confusion about the best course of action, and more than a few ill-considered measures have been put in place. But businesses need not fret. The solution comes in a process they already understand, albeit with an intuitive reorientation of traditional thinking.

Information protection is already a core element of most businesses' risk management strategies. IT departments all over the globe have accumulated expertise and established best practices for protecting their information from disasters such as hurricanes or from operating failures such as those caused by human error. They have also worked to ensure the integrity of their most important data, making sure they can replace damaged or corrupt data with backup copies. But a third dimension to data protection exists that to date has received less attention than availability or integrity: data confidentiality. In the face of increasing threats in this area, confidentiality lapses can't continue. To bring this "third leg" up to par, we need to understand why it hasn't gotten the same level of attention.

The reality is that despite the millions of dollars in corporate investment in IT and information security information simply isn't secure. Two factors explain this state of insecurity. First, security is fundamentally a process problem, not a technology problem. Without a comprehensive, well-designed set of policies and procedures underpinning an organization's information security efforts, even the best technology will fail. Secondly, up until now, securing information has meant securing the infrastructure that surrounds it – networks, servers, applications – anything but the information itself. To be effective, we have to focus on securing the information assets themselves. When we re-orientate our thinking, taking an information-centric approach, the solution becomes familiar and clear: Information security is fundamentally an information management problem, and success hinges on making security an integral element of an organization's existing information management discipline and processes.

In recent years many businesses have gone through a fundamental reassessment of their approach to managing information. With the volume of information growing by 70% annually in large corporations (and faster in small businesses), it no longer makes sense – if it ever did – to manage all information in the same way. It's simply too expensive and too resource-intensive to treat all information equally. The most important information should have the highest levels of service: performance, availability, integrity, and now, confidentiality/security.

Today many organizations pursue an information-centric IT strategy called Information Lifecycle Management (ILM). It helps them manage different information differently, based on the changing value of the information to the business. They classify all their information assets into logical groups, from the lowest to highest requirements for speed of access, availability, retention, and security. ILM lets them not only better match the right type of IT resources to the requirements of the business, but acknowledge the dynamic nature

of information, tracking its movement throughout its lifecycle from creation to deletion or archiving. Organizations today manage information selectively and dynamically.

An information-centric approach to information security reorients our thinking about key security questions. Consider, for example, the issue of what is secured. As we've noted, most of the investment in information security has been made in a sea of point-products aimed at securing specific IT resources such as networks, applications, servers, operating systems, and personal devices. But information is dynamic, not static. It moves throughout and between these resources and ultimately outside the scope of the specific product protecting them. A successful information security strategy will recognize the movement implied in the lifecycle of information and protect the information itself, not just the stationary IT resource supporting it.

Another issue in dire need of re-evaluation is where to focus the protection of information. As we've noted, information security isn't a product; it is a process and a system, a comprehensive approach to securing the path of each piece of digital content from the point of creation or entry into the corporation's information flow to deletion or permanent archiving. Most of the investment in information security has been concentrated on the network perimeter. Securing the outer defenses, the thinking went, will protect everything inside the business. Well, that approach didn't save the Trojans, and it's clearly far from sufficient today due to the widespread sharing of information inside and outside of the business. The increase in information-based teamwork and enhanced collaboration with partners and customers helped businesses grow revenues and control costs. But the more businesses share their information, the bigger the challenge is in protecting and securing it. To continue to benefit from investments in information technology, they needn't stop the productive flow of information inside and outside of the business. Only an information-centric approach, not a perimeter-centric view, permits this.

CEOs should mandate a comprehensive overview of the information assets of the corporation then develop and implement an end-to-end information security strategy that will be integrated with how they manage information. This detailed plan of action must encompass all points of access, storage, and movement of information. It must also integrate all the various activities touching in one way or another on securing and protecting information – from encryption, to disaster recovery, to digital rights management, to backup, to compliance. This information-centric approach to information security makes data protection comprehensive, and ensures that emerging business risks are successfully mitigated. ■

About the Author

Dennis Hoffman is the Vice President of Information Security at EMC Corporation

Data as Baggage

TRAVEL LIGHT, TRAVEL FAST

BY JOHN WEBSTER

IT'S OFTEN SAID that IT administrators in general, and storage administrators in particular, are highly risk-averse. Clearly that's the case today. Look for a moment at any one of the surveys that seeks to understand the most pressing issues on the minds of those are tasked with the stewardship of enterprise data. These surveys point to data protection, security, system reliability and availability, and responsiveness to regulatory agencies and corporate governance as top priorities. Hot products these days are continuous data protection (CDP), disk-to-disk-to-tape (D2D2T), and e-mail archiving solutions. Storage-based data encryption solutions are now getting a thorough examination as well. Managing risk is a prime mover in the storage industry.

As a result of observing this heavy concentration on risk management a few years ago, I decided to explore the well-established practice of fiduciary risk management to see if that endeavor had anything to offer the practice of storage management. I ran across something by a fellow analyst named Felix Kloman. Felix writes a newsletter call "Risk Management Reports." It's a monthly compilation of observations and advice that Felix offers to those who manage actuarial and fiduciary risk for a living. Thanks to Felix, I've discovered an emerging research effort into operational risk. Practitioners of fiduciary risk management seek to quantify risk. Future practitioners of operational risk will seek to do the same thing. What's cool about that? IT is included under the category of operational risk. Imagine having an accepted and reliable way to quantify downtime or data loss that both CIOs and CFOs could agree upon. You wouldn't have to quote the widely divergent numbers on this subject offered up by us analysts.

I've also come to adopt an attitude toward risk management that's one of Felix' guiding philosophies: There are really two ways to look at risk. One is the hindsight view, and the other the foresight view. The hindsight view concentrates on protecting what you already have. The foresight view asks you to be constantly on the lookout for new opportunities because, in the final analysis, having little or no foresight is as risky as having no hindsight. Why? Without the foresight to see coming marketplace changes and new opportunities, you're at risk of being run out by a competitor who *does* have that essential foresight. Felix advises his readers to take a balanced approach. Be diligent with hindsight, but don't forget the foresight.

The sad state of affairs in storage management – and IT management in general – is that hindsight often takes priority over foresight. These days, improved backup and e-mail archiving projects often take priority over speeding new applications to a user's desktop. We all moan and groan when Nicholas Carr, author of "IT Doesn't Matter," chastises IT for its irrelevance, but we can't just pass off Nick as an irrelevant academic. We all know there's a kernel of truth in that observation, no matter how hard it is to admit. Irrelevance is what happens when all IT does is protect what it has.

Here's a radical thought: Data is both a blessing and a curse. You have to have it to stay in business. But then the government tells you to save it for years on end. You curse.

Recently I brought my family to a summer resort outside the US for a week. All five of us had one suitcase and one carry-on as we boarded the plane. We watched as other families struggled to get multiple SUV-sized bags (I mean this was LUG-gage) across international borders. Data is essential to business survival and forward motion. No doubt, you gotta have it. However, it can also be luggage with a capital LUG.

Here's a proposal: take steps to *radically* reduce the amount of data you have to lug around. The fewer the number of bits you schlep over system boundaries, the fewer bits you have at risk, and the faster you move to the next new opportunity. Shavingoff 10% isn't going to get you there. Think big. Think 50%.

Shred

It's become fashionable in storage circles to talk about automated, policy-based management. Corporate policies are the most difficult to translate to the storage environment. Why? Because corporate policies are outside the control of the IT department, whereas the other policy sources remain under IT control. Corporate policy makers now include attorneys who want e-mails saved in case of possible litigation and regulatory compliance managers who want

multiple years of audit trails and transaction logs saved for possible governmental review. Storage administrators shouldn't and can't make corporate policy. Yet they must somehow make things happen. And, in the absence of established corporate policy with regard to shredding data, the default position for storage administrators is to save (and therefore LUG) everything.

When corporate policy is clearly understood, the job of translating policy to storage management practice gets easier. However, when corporate policy is unclear — or in some cases nonexistent — IT must somehow force clarity from corporate executives. Otherwise pack those bags. No shredding policy results in big data baggage. Do the residents of mahogany row know that? The executives that really matter here are corporate legal counselors. They have the power to create records-deletion policies that are:

1. Enforceable at the application user level
2. Defensible in court if challenged

Do We Really Have to Store All These Data Bits?

Dare I say this? We all talk about burgeoning data volumes and data growth rates in excess of 70% a year. The standard storage industry response is a call for more efficient management and solutions that enable storage administrators to do more with less. Rarely do we survey the TBs piling up on data center floor tiles and ask, "Do we really have to save *all* these data bits?"

There is little financial incentive for storage vendors to ask this question – a true statement even for software vendors who have no hardware axe to grind but nevertheless price their offerings based on capacity in one form or another. And it's become difficult for storage administrators to pose this question to senior corporate executives who fear the worst from litigious lawyers and government regulators. It's easier just to save everything.

Yet, do more with less is not the only answer. There are ways to move the capacity growth meter away from the red zone. Start by seriously collaborating with corporate legal counsel to establish a clear and defensible records deletion policy.

Travel light, travel fast.

About the Author

John Webster is senior analyst and founder of Data Mobility Group. He is the author of numerous articles and white papers on a wide range of topics, including data convergence, storage networking devices and management, and storage services and outsourcing. He is also the coauthor of a book entitled Inescapable Data - Harnessing the Power of Convergence, published in April 2005 by IBM Press.

jwebster@datamobilitygroup.com

Striking the Balance Between Storage Security and Availability

RULES OF THE ROAD

BY GLENN GROSHANS

EVERY BUSINESS OWNER knows that information is much more than one of an organization's strategic resources. In a very real sense, information is the organization. For IT professionals, there's no shortage of challenges when it comes to protecting and managing such a vital asset efficiently.

The year 2005 was proof that information loss can be detrimental to an organization. Almost every week another organization was involved in a security breach involving valuable corporate data or customer information, several of which involved stolen or lost backup tapes. As a result, high-profile organizations are scrambling to ensure more effective storage security and data protection, while concerns surrounding identity theft continue to mount among consumers.

Adding to storage professionals' anxiety is the amount of data that can be compromised on a single backup tape. Because of the concentrated pool of data it contains, a single tape can compromise more personal information than many of this year's online break-ins.

Any good strategy for data storage protection includes a strategic balance between information availability and information security. IT managers today are tasked with maintaining this balance at a reasonable cost. It's easy to make information completely secure — by locking it up in a safe, for example — but the trick is to ensure that it's available when needed. However, by providing information access, there are always risks, which generally fall into four main categories:

- ***Malicious attacks:*** Cybercrime has moved online and will continue to do so with a variety of tricks, including the latest flavors of worms, viruses, bot networks, and phishing attacks. During 2005, there was a noted shift from pesky virus writers looking for attention to more organized, malicious attackers seeking financial gain.
- ***Human error:*** To err is human, and unfortunately it happens all too often. Employees leave laptops in airplanes, trip over wires, or cause system crashes. Or, as in one high-profile case from 2005, storage tapes are simply lost in transport.
- ***Infrastructure failures:*** IT infrastructures aren't foolproof and all it takes is a power loss or server failure to lose business-critical information.
- ***Natural disasters:*** 2005 also reminded us how quickly natural disasters can strike and bring any business to its knees. According to Gartner, the market research house, 50% of enterprises that lack a recovery plan go out of business within one year of a significant disaster.

A good strategy for effective storage security would take all of these risks into consideration. Data and information on its own isn't valuable to any organization. Applications, servers, and operating systems must be up and running to make use of the information and to maintain the highest degree of information availability and integrity.

As IT managers and storage professionals plan for 2006, storage security should be top-of-mind. By implementing the following best practices, organizations can avoid many of the embarrassing and dangerous storage security incidents that made news last year.

Online Data Protection

Organizations should maintain multiple point-in-time copies of data for uninterrupted operation. And, for a higher level of online data protection, consider replicating to another location in either real-time (synchronous replication), or near real-time (asynchronous replication).

Encrypt Data

Unencrypted data is always going to be subject to some level of risk. A recent survey by the Enterprise Strategy Group found that 60% of storage professionals never encrypt backup tapes and only 7% do so routinely. Storage professionals should focus on encrypting any

data going outside the company or facility. Also ensure that there's a plan for decryption and that the appropriate individuals have access to the encryption keys.

Physical Security Measures

Besides encryption, add another layer of security by using shipping boxes that can't be opened easily when transporting backup tapes. And determine if unused ports to the network are disabled and make sure lockable racks and cabinets are locked. Consider using a backup product that includes a vault option for keeping track of containers full of media. Be particularly careful about securing and encrypting data while it's in transport and keep track of all of the organization's backup tape with a detailed inventory. Create a plan for finding any backup tapes that go missing.

Lockdown Process, Manage Data Throughout the Lifecycle

Storage professionals should avoid retaining backup tapes longer than necessary. One organization kept data longer than required, leaving the information vulnerable; it ultimately resulted in a recent security breach. A plan for managing data and information from creation to deletion will ensure that only the information that's needed remains accessible. Information should be analyzed when it's created or received and then assigned an appropriate policy for management and deletion or retention.

Besides taking the obvious step of not using manufacturers' default passwords for data storage access, organizations should have a clear plan for changing passwords often and use separate IDs and passwords for each user. Storage professionals should also ensure that they are choosing the right storage option for their data. For example, data that doesn't need to be accessed very often can be saved on tape, rather than waste space on more expensive disk-based storage.

Access control is another basic security measure that should be in place within any organization. IT should implement granular control of who can access the data and the applications that manage the data, providing appropriate rights and permissions to various types of data.

Consider Disk-to-Disk-to-Tape

While backing up to and securing tape is important, "recoverability" is even more critical. Organizations should consider a combination of disk and tape-based solutions to ensure the integrity of information. Disk-based solutions provide ease-of-use and recoverability, ultimately ensuring a more effective recovery strategy. Storage professionals should deploy the combination of disk and tape solutions that works best for their organizations and provides the benefits of both technologies.

Compliance Drives Concerns

By implementing these best practices, organizations can gain the trust of consumers by avoiding embarrassing and potentially damaging data and information losses and comply with industry regulations. All public companies are feeling greater regulatory pressure to improve information security because of the Sarbanes-Oxley Act, which includes control over data security as an audit criterion for proper corporate governance.

Laws such as the California Security Breach Information Act (SB-1386) have also called more attention to the problem and increased consumer awareness surrounding identity theft and personal data protection. The California law requires organizations that maintain personal information about individuals to inform those people if the security of their information is compromised. It stipulates that if there's a security breach of a database containing personal data, the responsible organization must notify each individual for whom it maintained information. The far-reaching law affects organizations outside California since it applies to anyone who might have a customer or conduct business with an entity in California. Twenty-six states have subsequently passed laws similar to SB-1386.

Conclusion

The demand for an always-on IT infrastructure will increase while threats constantly evolve because of the profit motive. Not only is it important for enterprises to protect their stored data by deploying the best practices, it's of paramount importance that they continue to re-examine their storage security strategy, consider any new information access requirements, ensure regulatory compliance, and keep a few steps ahead of potential data storage loss.

About the Author

Glenn Groshans is director of the Data Management Group at Symantec Corporation.

Cyber-Extortion Is Real –

IS YOUR BUSINESS AT RISK?

BY JOSE NAZARIO

CRIMINAL GANGS ARE increasingly using the Internet to extort money from businesses. Thousands of Distributed Denial of Service attacks occur globally every day and it' vital that senior management wakes up to the very real risk of such an assault.

The rise of the Internet has carried a number of threats in the form of viruses, hackers, worms, and malware. Most companies are aware of these risks and have the appropriate processes and technology in place to mitigate them. But in the last few years these Internet-based threats have taken on a more malevolent and sophisticated nature; virus writing is no longer the pastime of teenagers with too much time on their hands – instead, viruses are now being written for organized cyber-criminals motivated only by money.

Extortion – A Growing Problem

These criminals are increasingly using Distributed Denial of Service (DDoS) attacks. DDoS attacks are launched solely to crash a company's Web site or server by bombarding it with packets of data, usually in the form of Web requests or e-mails. Unlike single source attacks (which can be stopped relatively easily), the attacker compromises a number of host computers that, in turn, infect thousands of other computers that then operate as agents for the assault. These infected host computers, known as zombies or bots, then start flooding the victims' Web site with requests for information – creating a vast continuous stream of data that overwhelms the target Web site preventing it from providing any service.

Every Business Is At Risk

The cost of a DDoS attack can be substantial and it' been estimated that as many as 10,000 occur worldwide every day. DDoS extortion attacks were originally used against online gambling sites. Criminal gangs would initiate attacks that would bring the Web site down just before a major sporting event, inflicting maximum financial damage. Now, however, DDoS attacks are increasingly being used to extort money from all sorts of businesses.

There are numerous examples of DDoS attacks. One of the most well-known happened early last year: The MyDoom virus infected hundreds of thousands of computers before launching an attack on the SCO Group, a Utah-based Unix vendor, that took the company out of business for several days. The motive for the attack has never truly been established. It's assumed it had something to do with the fact that SCO is suing IBM for $5 billion.

DDoS attacks are global threats since the extortionists aren't restrained by traditional borders. Even the greater Manchester police have fallen victim to an assault; recently the chief constable was subjected to 2,000 e-mails an hour in an attempt to crash the force's computer systems. DDoS attacks are also increasingly being used for political purposes. Last Valentine's Day, animal activists set up a chat-room and encouraged people to log on and "chat" at the same time. For every word typed, an e-mail would be sent to target organizations in the vivisection and fur industries in an effort to crash their Web sites.

The reality is that no company is safe. The problem is exacerbated by the fact that DDoS attacks simply don't effect the organizations they target, but can bring down the Internet Service Provider (ISP).

Lack of Awareness Makes Businesses Vulnerable

Despite the substantial damage DDoS attacks can cause, research released by IT company IntY earlier this year revealed an alarming lack of awareness about the threat posed among businesses. According to IntY, more than half of the U.K.'s companies are at risk because the lack of understanding has resulted in a widespread failure to implement the necessary preventative technology. It's vital that senior decision makers wake up to the very real threat posed by DDoS attacks. Failure to do so can have far-reaching consequences.

All businesses with an online arm should implement preventative measures to mitigate the threat of a DDoS attack. Many rely on reactive measures such as blackholing, router filters, and firewalls, but these methods are inefficient, too unsophisticated to protect against

cyber-criminals, or can only be configured to specific external sources.

A Multi-Layered Approach to Defense

While these tools possess crucial security features, they fail to offer sufficient protection against the ever-evolving and sophisticated nature of these assaults. If companies are to ward off a DDoS attack successfully, a truly multi-layered defense system must be adopted. So it's vital to establish a solid relationship with your service provider to ensure that you're aware of the measures available to you to protect your network and online business. Recent research by Arbor Networks revealed that DDoS attacks are the most crippling threat facing ISPs today, yet only 29% of the ISPs surveyed offer their customers security and DDoS service levels agreements.

Because DDoS attacks are launched from thousands of computers around the world, it's essential that companies share information about attacks if they're to be stopped. Such assaults can't be fought alone' A collaborative effort is vital. A number of ISPs including Belgacomm, Cable & Wireless, and COLT have joined the Arbor Networks Fingerprint Sharing Alliance, enabling them to share detailed attack information in real-time and block attacks closer to the source. Once a member company identifies an attack, the other ISPs in the alliance are automatically sent its "fingerprint" so they can identify and remove infected hosts from the network. This enables businesses and their ISPs to stay abreast of security threats as they arise. The alliance is helping to break down communication barriers and its rapid growth marks a significant step forward in the fight against cyber-criminals.

The threat of being blackmailed by organized criminals using DDoS attacks is very real and businesses can't afford to be complacent. Such attacks can bring the largest companies to their knees. However, standalone defenses are insufficient to combat them and a comprehensive approach to security must be implemented. Not only should a multi-layered security strategy be adopted at the enterprise level, but companies must also work with their ISPs to ensure that they too have taken preventative measures.

• • •

Arbor Networks is exhibiting at Infosecurity Europe 2006.

About the Author

Dr. Jose Nazario is aworm researcher and senior software engineer at Arbor Networks.

Intelligent Plastic

THE DESCENDENTS OF A DINERS CLUB CREDIT CARD ARE PROTECTING OUR VITAL ASSETS

BY TOFFER WINSLOW

ENTERPRISES AND GOVERNMENT agencies are using smart card-based credentials more and more. Organizations around the globe are striving to protect corporate information assets, address regulatory compliance pressures, and achieve cost savings and increased security through the convergence of physical and logical access credentials.

To the casual observer, it's easy to think of a smart card as merely a piece of plastic – intelligent plastic, to be sure – but plastic nonetheless. In fact, the evolution of smart card technology reflects a transformation from credit cards to cutting-edge devices whose capabilities have grown exponentially along with chip features and capacities.

Today smart cards protect physical facilities, desktops, networks, applications, and much more. Applications are growing as fast as the forces driving smart card adoption. However, the "smart chip" concept is leaping beyond the confines of the smart card itself. Smart cards and smart chips, along with management solutions that extend enterprise investments, are paving the way for advanced security applications such as enterprise single sign-on.

A Brief History

In a simplistic sense, the smart card was born in the 1950s, when Diners Club introduced a plastic version of its paper charge card. This provided the long-lasting, now familiar form factor, and afforded credit to those who carried it. In a foreshadowing of events that preoccupied the security industry for the next five decades, the risk of fraud and the need for financial controls saw the original plastic card evolve into a machine-readable card. More recently, this evolution has continued into what is now the most common form of electronic payment: the magnetic stripe-embossed card.

The introduction of encryption into the smart card equation was of considerable interest to security professionals. Microprocessors capable of stronger authentication opened up the way for the standalone or challenge-and-response authentication of cardholders without the security risks or infrastructure associated with

magnetic stripe cards. This encryption can be public key, symmetric, or a hybrid approach leveraging digital signatures. The power of encryption and advances in microprocessor technology meant that smart cards now feature chips whose functionality is constantly expanding.

Applications: From ID Badges to Converged Access

Applications for smart chip technology span the gamut from physical security to logical security. The most common physical security applications revolve around access to campuses and buildings. When embedded in a card, smart chips combine the familiarity of the typical ID badge, such as employee photo and company logo, with the authority to access office campuses, specific buildings, and the like.

Logical security – the software safeguards for an organization's systems, including user ID and password access, authentication, access rights, and authority levels – represents the leading edge of smart chip applications. These measures are necessary to ensure that only authorized users can to do certain things or access information in a network or workstation. For example, smart chips in USB tokens or more traditional smart cards can authenticate users on corporate networks, whether on-site or via remote dial-in or virtual private networks (VPNs). They can authenticate everyday users for an application, group of applications, or a Web portal. They can also be used to provide administrators with everything from operating system access to other high-level corporate functions.

Another crucial smart-chip application is the convergence of stronger physical and logical security in the same form factor. For example, a single smart chip-enabled device can let an employee access a corporate campus, enter his or her building, and log on to those portions of the corporate network that he or she is approved to access.

These applications and many others have led to the rapid growth of the smart chip market. In September 2005, Frost and Sullivan predicted a 27.7% compound annual growth rate in North

BY NOW THERE ISN'T A SOFTWARE DEVELOPER ON EARTH WHO ISN'T AWARE OF THE COLLECTION OF PROGRAMMING TECHNOLOGIES KNOWN AS AJAX!

REAL-WORLD
AJAX
ONE DAY SEMINAR

www.ajaxseminar.com

March 13, 2006

Marriott
Marriott Marquis Times Square
New York City

For more information
Call 201-802-3022 or
email events@sys-con.com

REAL WORLD

How, in concrete terms, can you take advantage in your own projects of this newly popular way of delivering online content to users without reloading an entire page?

How soon can you be monetizing AJAX?

This "Real-World AJAX" one-day seminar aims to answer these exact questions...

Led by "The Father of AJAX" himself, the charismatic Jesse James Garrett of Adaptive Path, "Real-World AJAX" has one overriding organizing principle: its aim is to make sure that delegates fortunate enough to secure themselves a place – before all seats are sold out – will leave the seminar with a sufficient grasp of Asynchronous JavaScript and XML to enable them to build their first AJAX application on their own when they get back to their offices.

Jesse James Garrett
Father of AJAX

Scott Dietzen
Creator of WebLogic, Ph.D., President and CTO, Zimbra

Bill Scott
AJAX Evangelist of Yahoo!

David Heinemeier Hansson
Creator of Ruby on Rails

Satish Dharmaraj
Father of JSP, Co-Founder & CEO, Zimbra

Rob Gonda
Best-Selling AJAX Author, CTO, iChameleon Group

Dion Hinchcliffe
Co-founder & CTO, Sphere of Influence Inc.

Ross Dargahi
Well-known AJAX Evangelist & Co-founder and VP of Engineering, Zimbra

Early Bird (Before January 31, 2006)	**$995**
Discounted Price (Before February 28, 2006)	**$1,195**
Seminar Price (After February 28, 2006, and if any seat is available)	**$1,295**

HURRY! LIMITED SEATING THIS SEMINAR WILL SELL-OUT CALL 201-802-3022 TO REGISTER!

Jeremy Geelan
Conference Chair, Real-World AJAX
jeremy@sys-con.com

MEDIA SPONSOR
ajax developer's journal

LIVE SIMULCAST! AROUND THE WORLD ON SYS-CON.TV

PRODUCED BY SYS-CON EVENTS

American smart card microcontroller shipments through 2010. It predicted even stronger growth in Latin America, where it says compound annual growth rates will reach 59.1% over the same period.

Government and Enterprise Adoption

In 2004, the White House issued Homeland Security Presidential Directive 12 (HSPD-12) with the goal of establishing a single government-wide standard for identification credentials issued by the United States government to all federal employees and contractors. The implementation of HSPD-12 began on February 25, 2005 when the Secretary of Commerce approved FIPS 201, a document titled "Personal Identity Verification for Federal Employees and Contractors" issued by the National Institute of Standards and Technology (NIST) as part of its Federal Information Processing Standards (FIPS) publication series.

Through HSPD-12, federal employees and contractors will soon be required to carry a smart card – called a Personal Identity Verification (PIV) card – to access both physical and logical resources. These smart cards, when used with appropriate data collection systems, will identify their bearers in several standard ways — photographic images printed on the card, biometric data (fingerprints) stored on the card, personal information numbers (PIN) stored on the card, as well as other electronic credentials stored on the card, such as digital certificates.

Of course, government agencies have responded, investigating technology solutions that will enable them to meet HSPD-12 requirements. This is similar to what happened in the commercial market when Sarbanes-Oxley was passed several years ago – recognizing the need to comply, organizations sought out technical solutions that offered a "quick fix" to meet a regulatory deadline. While this approach achieved compliance, what many commercial organizations missed was the opportunity to leverage compliance-driven investments in technology more broadly.

Luckily, those commercial organizations aren't making the same mistake twice. A growing number of companies in a wide variety of vertical markets are executing smart card and smart chip deployments that pave the way for advanced security applications. The Burton Group surveyed global enterprises in oil and gas, healthcare, aerospace, pharmaceutical, hardware, software, and financial services – some with as many as 100,000 employees worldwide – as well as U.S. federal government agencies and organizations to understand the nature of their plans. Most of those organizations were attempting organization-wide rollouts rather than limited rollouts to specific groups.

Management and Advanced Applications

The scale of these deployments demands that smart chip-enabled devices be managed effectively to enable advanced applications. Without a card management system (CMS) in place to enroll users easily and securely, deploy smart cards and manage the lifecycle of these credentials, even small smart card deployments can be complex.

Card management systems let enterprises implement card-based identities, provisioning, authentication devices, and policy enforcement — increasing their overall security posture, improving the end-user's experience, and addressing regulatory requirements. They address the entire smart card credential lifecycle, from card and credential issuance to replacement and cancellation, as well as managing smart badging and applets. Correctly deployed, card management system technology provides unparalleled security for trusted distributed credential issuance and post-issuance management.

One advanced application that organizations are pursuing is enterprise single sign-on (ESSO). They're rolling out ESSO software so users can log in once and that login is automatically passed through to other applications, lessening the organizations' password management burden. Because this essentially creates one master "key," there's obviously a need to protect that key with strong authentication. Today, that often means a digital certificate embedded on a smart card. ESSO reduces human error, a major factor in systems failure, and is therefore highly desirable – but it was difficult to implement before the advent of smart chips.

A Look to the Future

Enterprises need to embrace a variety of authentication solutions that map to users around the globe, requiring a move beyond the traditional smart card model. The ever-growing power of microprocessors is freeing "smart" technology from its card container, enabling embedded chip smart devices that can be leveraged across many form factors to power a wide variety of applications. Today, many chips that were once embedded in plastic cards now find themselves in more versatile USB containers. Smart chips can literally go anywhere, and the future will find many other form factors to house them.

At the same time, new market drivers – such as the need for secure e-commerce transactions or validation of participation in government programs – will create new applications that smart chips will power. So long as these technologies are efficiently managed, security professionals will be able to harness their power for productive deployments.

"Smart chips are now freeing "smart" **technology from its card container"**

About the Author

Toffer Winslow is vice-president of product management and product marketing at RSA Security.

twinslow@rsasecurity.com

Visit the *New* www.SYS-CON.com Website Today!

The World's Leading *i*-Technology News and Information Source

24/7

FREE NEWSLETTERS
Stay ahead of the i-Technology curve with
E-mail updates on what's happening in your industry

SYS-CON.TV
Watch video of breaking news, interviews with industry leaders, and how-to tutorials

BLOG-N-PLAY!
Read web logs from the movers and shakers or create your own blog to be read by millions

WEBCAST
Streaming video on today's i-Technology news, events, and webinars

EDUCATION
The world's leading online i-Technology university

RESEARCH
i-Technology data "and" analysis for business decision-makers

MAGAZINES
View the current issue and past archives of your favorite i-Technology journal

INTERNATIONAL SITES
Get all the news and information happening in other countries worldwide

JUMP TO THE LEADING i-TECHNOLOGY WEBSITES:

IT Solutions Guide
Information Storage+Security Journal
JDJ
Web Services Journal
.NET Developer's Journal
LinuxWorld Magazine
Linux Business News
Eclipse Developer's Journal
MX Developer's Journal
ColdFusion Developer's Journal
XML Journal
Wireless Business & Technology
Symbian Developer's Journal
WebSphere Journal
WLDJ
PowerBuilder Developer's Journal

Management Must Extend Culture of Security

RESPONSIBILITY TO CUSTOMERS

BY WINN SCHWARTAU

FOURTEEN YEARS AGO I warned MyBank (who is not one of my clients, I am one of theirs) about using social security numbers as solid identification. The Head of Security, three weeks retired from the Secret Service, said he would look into it. Nothing has changed except the security at MyBank has gotten worse.

I was recently met with the familiar telebanking voice, "Please enter your bank account and social security numbers." Whoah! Security alert! MyBank's new and improved system was using two pieces of publicly available information as proof positive remote identification. An embarrassed bank vice president had to duck for cover as the bellicose manager of telephone banking application development defended the security of his design.

If I had been a bad guy, I could have drained accounts and severely harmed the reputation of MyBank since it still took them 30 days to fix this gaping security hole. At least, with substantial goading on my part, management took some degree of responsibility even if the designers didn't.

Last month, my banker said that their online banking was *ready for prime time*. Login security was decent: a long secret account number generated by the bank, my federal EIN, a four-digit PIN, and no cookies.

I transferred $20K to pay my absurd American Express bill (which includes mortgage, airplanes, phones – everything that will earn me free trips) and a paycheck to "Greg" among others.

Several days later, Greg asked, "Where's my paycheck?" I had proof I sent it on the bank's "secure'" Web site. Amex was also not paid. I had proof I paid it, too. I called MyBank's Internet banking and was met with gross ignorance: they had no idea why the money had not reached its final destination nor did they care. "We pushed the <send> button," was all they could conjure up. Easy, I figured. I simply asked for proof of receipt of funds by Amex and Greg's bank – which is also MyBank, a few account digits away on the same routing table.

According to the managers at MyBank, they don't use acknowledgment receipts from online transfers. Silly me. I thought that was the law, which it is. But the clerks in Internet banking had never been taught the simple security procedure of non-repudiation and transfer authentication. Management didn't see fit to teach the customer service staff about basic security procedures that are the soul of integrity in financial circles.

It turns out, without telling its customers, MyBank immediately debits an account, and then holds onto the money for some undetermined amount of time. Silly me, I thought electronic transfers worked at the speed of electrons on wires and were reconciled around midnight in a batch transfer. The most disturbing security aspect is that no one at MyBank could tell me where my money was when it was not in my account and not in Amex's or Greg's. Silly me for asking MyBank to tell me where my money is.

Other banking friends tell me that this is the "secret" way MyBank finances its "free" online services. They hold the funds for a while, make some interest on it, and then push it along its merry way. The banks call it floating. If you or I do the same thing, it's a crime called kiting. Silly me. For the record, MyBank's media relations department never returned my calls.

Then security at MyBank plummeted to a new low.

I logged in and discovered MyBank had virtually eliminated its online security. The long private code was no longer required. Now, a publicly available account number and a mere four-digit PIN was the sole defense of any account at MyBank. The obvious attempt to simplify the user experience is a devastating blow to security. An ATM card only requires a four digit PIN, but it employs the "Something you own, something you know" identification mantra. Silly me for expecting better banking security on the Internet.

When I again attempted to pay my staff, Greg was again the victim. His money was snafu'd in the labyrinth of MyBank's infrastructure.

Believe it or not, an officer at MyBank then:

1. Cancelled my payment to Greg without my authorization.
2. Issued a payment from my account with something called a "Forced Check" to Greg without my authorization.
3. Withdrew a duplicate payment from my account without my authorization and deposited it in Greg's account
4. Cancelled one of the payments (still don't know which one) without my authorization.

I am pretty sure this is against the law, but I do know that this is absolutely terrible from a security standpoint: a

bank officer moving money in and out of my account without my authorization or notification.

Just to make things easier, or so I thought, I let the double payment to Greg stand, having no idea MyBank would only make matters worse by then removing the money from Greg's account without his authorization. This security-process transgression triggered a cascade of bad cheeks, overdrafts, and the freezing of his other accounts.

Then it got worse. Greg says MyBank told him that the money was removed from his account (without authorization or notice) because my corporate account had insufficient funds to cover his paycheck. This security breach was in clear violation of any number of privacy and banking laws or compliancy governance besides being an absolute untruth.

If any one of these had been an isolated incident, I could write it off. But MyBank has created a pandemic of "no-security-culture" to the detriment of its customers and disregard of compliance guidelines. They chose to use the weakest identification possible. They violated all three basic security principles: confidentiality, integrity, and availability. Worse? MyBank, from what I can discern, does not train their staff on how to recognize that they are being manipulated by social engineering. Their development teams appear to have zero clue about security.

This derelict attitude, in any company, can only be sourced by top management and subsequently infused into the mid-management culture. I don't know of any other way that security can be so flagrantly disregarded.

Security and user experience (functionality) are inversely proportional, but it certainly appears that MyBank has taken the easy way out: listen to customers who complain about security barriers, remove or reduce their efficacy, and see what happens.

So have the telcos, phone companies in non-geek speak. For your consideration – for $100 or so, a Web site will provide you with the telephone records of anyone's cell phone. Don't know their cell number? No problem. Give them a name and you're good. The security implications are devastating: any and all cell and land-line phone records for sale on the Internet.

Law and Order lawyers (I mean fans…) know that phone records can only be released to the police with court authorization, aka warrant. We call that balance of power and judicial oversight.

A major telco representative and I appeared on a TV talk show to discuss the security and privacy aspects of this service, and what could be done about it. The telco supports the idea of legislation. It's the "Make a law against it mentality." What does a law do? Keeps the good guys honest. Think about that! Laws are only a local ordinance in cyberspace and management needs to recognize that laws are often completely meaningless when it comes to protecting data on a global scale. It is often up to senior management to establish the corporate security culture.

The telco guy then said, "Here's what consumers need to do to protect themselves further." He proceeded to discuss that his company uses great security and everyone is background checked as well as highly trained. But, even though the security of the telco is apparently being breached, somehow, by someone, he said, "Customers need to call customer service and set up a security pass code on their account." He seemed fine with this. I wasn't.

"Let me get this straight," I said. "My personal info, stored on your computers, is being illegally accessed by persons unknown who are selling it on the Internet and you want your customers to take responsibility?"

He hemmed. He hawwed. Didn't like the way I put it.

He further said that this security feature was already built into their application software. Translation: no cost to the company.

"If a pass code is all a customer needs to protect himself, why don't you just adapt a company-wide policy that says 'All customers shall have passwords'."? He didn't like that question either. I was striking at the heart of their lack of corporate security culture.

"Why don't you just spam your customers via e-mail and on their phones: 'We care about security and privacy. Please call ### to establish a password for your account. Thank you.' Automate it from the phone pad if you want."

Answer: security is a hassle for customers and we might lose some.

Tough.

Wrong corporate security culture.

I think back to the early '80s and remember the intense frustration of trying to get management to take security seriously. I think back to the early '90s and remember the intense frustration of trying to get management to take security seriously.

By then the Feds started to care. A little. In 1995, the seminal work of Bob Ayers, formerly of the Defense Information Systems Agency (www.DISA.mil), actually proved and measured the lack of security and weaknesses in military networks. It was bad news: the Department of Defense was accountable for their lack of security responsibility.

Then along came the March Commission and the Clinton Presidential Decision Directive (PDD-63), which validated much of our fears and research into cyber terrorism. The critical infrastructures of the United States represented the foundation of our newly accepted economic national security and was truly vulnerable. We were to blame for our lack of security responsibility.

But corporate management bemoaned with their classic apathy and arrogance: "What problem?" and "It can't happen to me."

At InfowarCon in 1997, we had one of the first intense public debates on who was supposed to protect the private sector (an economic national

security asset) from the bad guys, not just hacking, but international espionage and terrorism. There were two camps. One suggested that the government, perhaps led by the seemingly capable and well-funded military, should take the protective lead. The other camp said, "No, keep the Feds out of my company. We'll take care of ourselves." Differing views on responsibility.

Then 9/11.

The nation finally saw with too much visual clarity the interdependence between all of our infrastructures. We are all in this together. So, the Department of Homeland Security was formed to be the catchall of security, including cyber security, for America. And today, Congress searches for responsibility of failure or a scapegoat.

In December of 2003, Congressman Adam Putnam, chairman of the House Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, released the information security report card for the U.S. Government, with the Department of Homeland Security failing, and the Department of Treasury not even submitting a report (http://reform.house.gov/TIPRC/Hearings/EventSingle.aspx?EventID=652). The average score for the entire federal government was a dismal "D," indicating a total lack of assumption of security responsibility.

What is their corporate security culture? "Do as I say, maybe, not as I do."

Information security has only gotten worse in the last 20 years. In March 2004, the General Accounting Office (GAO) reported there were 1.5 million reported cyber-attacks against government facilities in 2003, a threefold increase over 2002 (*http://www.gao.gov/new.items/d04467.pdf*). In 2005, more than 55 million consumer records were lost or stolen, often en masse on data storage media.

The private sector continues to face an unenviable dichotomy of responsibility:

1. Provide security, indeed, force some degree of security, upon their customers, and reduce the security/privacy incidents and the support costs, or
2. Treat security as an intrusive evil that could lose some customers

Endless reports and studies cite what we have known for years: people will do more good to aid and abet security than technology – by taking responsibility for their own security, if we can seduce them into doing so. Left to their own devices, people will take the easy, lazy, and insecure path instead of taking personal responsibility. Ergo, a small percentage of customers will proactively add security to their profiles.

Corporate security culture starts at the top. How many managers understand the real security issues we face, much less are able to discuss the intricacies of their interdependence? How many managers follow the same advice and policy directives they expect their staff to follow? How many managers know their counterparts at competitive organizations who all face the same threats? How many managers look to outside solutions, like the U.S. government? How does this culture, or lack thereof, translate to customer service and security?

Congressman Putnam said in his report of Washington, D.C., "This is not a town of the 'can do.' It's often the town of the 'it can't be done, and let me tell you all the reasons why not.'" Security should not fall victim to this negative attitude, rather enforcing customer security and privacy should be a service enabler. MyBank now offers the online option of changing your password from your social security number. They don't force it. That's just dumb. You do it for your staff via policy, but not for your customers. Explain that one. (Oh yeah, someone might give up your cell service. Then why don't all of you guys do the same thing? Jeeez. Talk to each other.)

One answer lies in a rapprochement between competitors within the same industries, and a détente between government and the private sector, each of whom have almost diametrically opposed modi operandi. Impossible you say?

Not.

Look to the relentless work, achievements, and progress made by the FS-ISAC, the Financial Services Information Sharing and Analysis Center, born from Clinton's PDD-63 (www.fsisac.com). With the cyber-economy being "the economy," according to National Security Advisor Condaleezza Rice, what more compelling an arena to define the necessity of responsible cooperation than the financial infrastructure.

"Responsibility means working to improve **security beyond checkbox compliance**"

Cooperation means taking responsibility, not passing the buck. Responsibility means doing what is right, not merely what is convenient. Responsibility is the recognition that just as we teach children how to behave, we must often treat staff and customers in similar ways: enforce reasonable boundaries of behavior for their own good. Responsibility means working to improve security beyond checkbox compliance, and setting reasonable and effective defensive postures for the company as well as its customer base.

We know better. The customer often just doesn't care. It's taken 20+ years to affect some level of security awareness at the management level. Let's not take another 20 years to protect all of the endpoints of our networks: the customer.

About the Author

Winn Schwartau is president of Interpact, a security awareness consulting firm, and author of several books, including the recent Pearl Harbor Dot Com.

winn@thesecurityawarenesscompany.com

NetApp simplifies regulatory compliance.

The road to regulatory compliance starts with NetApp.
NetApp storage solutions simplify your environment and keep regulated data online, secure, and instantly available. One view of your data across a single architecture helps you manage your regulated data through the information lifecycle. So you minimize risk and maximize control with lower operational costs than ever before. Visit *www.netapp.com/go/roadmap* to get your free copy of the *NetApp Roadmap for Regulatory ompliance*, a new report showing how NetApp simplifies data storage. Don't let regulations like HIPAA and SE Rule 17a-4 throw you off course. Take a closer look at NetApp now.

NetApp®
The evolution of storage.™

SPEED
ESSENTIAL™
SECURITY
from SafeNet

Now you can have both speed and security.

SafeNet's SONET encryption.
The protection you want, with a lot more speed than you're used to.

When speed is essential, SafeNet is a necessity. We offer the only family of SONET encryption products with a throughput of up to 10Gbps – plus security at the physical, data link and network layers. We give you the highly secure AES algorithm with a 256-bit key length. And SafeNet solutions can secure OC48 and OC192 networks – but will also blend transparently into OC3/OC12, or OC3/OC12/OC48 systems. So if you need protection that runs fast and deep, call SafeNet today and ask about Speed Essential Security. It's where high speed meets high security.

For a free copy of the **Frost & Sullivan white paper**, "WAN Services and Encryption: Protecting Data Across Public and Private Networks," visit *www.safenet-inc.com/hse/0810*

Call 1-800-697-1316 to be SafeNet sure.
www.safenet-inc.com/hse/0810

SafeNet®
The Foundation of Information Security

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