9 WAYS TO IMPROVE APP SECURITY | SOX FOR THE MIDMARKET

INFORMATION SECURITY®

OCTOBER 2009

guardian
honor-bound
resourceful
boundless
pioneer
communicator
visionary







2009 SECURITY AWARDS 7

TechTarget

INFOSECURITYMAG.COM

contents

OCTOBER 2009

VOLUME 11 NUMBER 9

FEATURES

ALSO

Teaching you security...one video at a time.

the academy

pro

www.theacademypro.com

home

www.theacademyhome.com

Traditional learning methods have always been about flooding students with as much information as possible within a given time frame -- often referred to as 'drinking from a fire hose'. The Academy Pro allows information security professionals to learn about today's most important technologies on demand and at their own pace.

The Academy has gone one step further by creating The Academy Home to show the average home user how to protect themselves from threats on the Internet by providing videos on today's best end user security products.

Check out The Academy websites at www.theacademypro.com and www.theacademyhome.com today. You'll be glad you did.

Sponsored by

CORE IMPACT
GIGAMON
PANDA SECURITY
SOURCEfire
McAfee
Network Critical
The Window to your Network™
ZSCALER
FORTINET
Nessus
SAINT
CISCO
exinda
Microsoft
TENABLE
Network Security
GFI
peer1
Fully scalable hosting solutions
Check Point
SOFTWARE TECHNOLOGIES LTD.
Shavlik

Security 7 Winners Chronicle Trends That Shape The Industry

BY MICHAEL S. MIMOSO

Looking back at five years of award winners provides a timeline of trends and events you need to absorb.

THIS IS THE FIFTH YEAR we've handed out the Security 7 Award, a milestone for sure. We've recognized some of the best minds in the security industry, be they pioneers such as Dorothy Denning or Gene Spafford, or folks such as Michael Daly, Stephen Bonner or Richard Jackson who don't have the same name recognition, but were held in such high regard by colleagues and contemporaries that they were nominated for our annual award and put on equal footing.

And while ultimately the award is for the people being recognized, it's really about the work they do and how they're adjusting to threats, managing risk and fitting in with the business. Looking back at the accomplishments of all the nominees from the past five years, it's a tidy, packaged look at how the security industry has matured. Some of the early winners were just starting to talk about the need to keep personally identifiable information safe and dabbling with bits and pieces of identity management, such as provisioning systems. Slowly, the conversations have turned toward risk management, and the integration and alignment of information security with the business.

This kind of movement is important to monitor and learn from; we're fortunate to have the Security 7 winners with us to chronicle their successes and struggles. A year ago, we turned the presentation of the awards in our publication over to the winners, inviting them to write first-person essays on a security issue they were passionate about. This year's collection of thoughts, insights and opinions begins on page 13, and much like last year, you'll be engrossed by the perspectives of these special people. This year, we've added to our Security 7 Award honor roll: Jerry Freese of American Electric Power; former Acting Director for Cyberspace Melissa Hathaway; Kodak's Bruce Jones; Humana Inc.'s Jon Moore; Adrian Perrig of Carnegie Mellon University; Bernie Rominski of Regis Corp.; and Tony Spinelli of Equifax. Seven winners from seven industries, each with a unique take on information security.

I urge you to absorb what they've written and look for new trends that may be landing on your plate in short order.

One is the issue of third-party security. Perimeters truly don't exist any more in the enterprise. Mobile devices extend and connect your employees outside the four walls of your office, and surely that's responsible for a fair share of grey hair. But an emerging and bigger risk stems from business partners who need access to your data, not to mention the emerging paradigm of risk presented by cloud computing.

Businesses need to find ways to address these risks without impeding the crucial business benefits presented by third-party relationships. You have to look into frameworks that will help you audit the security of your providers. You have to ensure that their policies closely align with

yours. You have to be satisfied, not only with their infrastructure protections but access controls, and hammer out liability issues in the event they are breached.

Some of our Security 7 winners recognize that sometimes bad things come in threes—or in this case, thirds. They've already instituted extensive programs that examine the security posture of those third parties they do business with. They understand risks and how quickly unchecked third-party relationships can take down a critical server or network segment; that kind of downtime does measurable harm to a company's bottom line. They're ahead of the curve and setting a standard for the next five years of information security. Learn from these people, for right now they represent the best of your profession. And remember that there's plenty of room on the Security 7 honor roll for the innovators of tomorrow's security initiatives.

Michael S. Mimoso is Editor of Information Security. *Send comments on this column to feedback@infosecuritymag.com.*

ARE YOUR NETWORK DEVICES HOLDING YOUR LOGS HOSTAGE?
WHAT YOU DON'T KNOW CAN HURT YOU.

OPTICS FOR SECURITY INFORMATION MANAGEMENT IS AN AFFORDABLE AUTOMATED LOG MANAGEMENT SERVICE THAT CENTRALIZES, ANALYZES AND RETAINS LOG DATA AND HELPS YOU USE IT TO SUPPORT BUSINESS FUNCTIONS. SCALABLE TO100% OF YOUR LOG DATA, SO YOU CAN REST EASY, GLASSHOUSE HAS GOT YOU COVERED.

FOR MORE INFORMATION CONTACT: SECURITY@GLASSHOUSE.COM

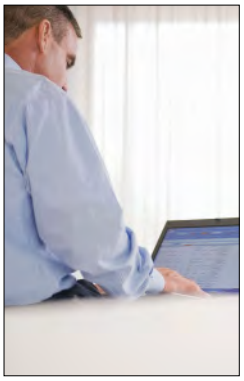
WWW.GLASSHOUSE.COM

GLASSHOUSE

VIEWPOINT

Readers respond to our commentary and articles. We welcome your comments at feedback@infosecuritymag.com.

Guest Services Includes Internet Security



Regarding Rick Lawhorn's column ("Security Best Practices in Hotels," Perspectives, September 2009 issue [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1365954_mem1,00.html]), the issue of who bears responsibility for the security of a hotel's guest-facing Internet service is one that, as a vendor of such services, iBAHN has been addressing for the past 10 years.

The list is often longer than just the hotel vs. the individual user; it also includes the user's corporate IT department as well as the hotel's broadband provider.

While agreeing with the points raised in your column, our experience indicates that guests at business-grade hotels expect high levels of service in all areas, including Internet access, and are quick to blame the hotel if they can't get connected to their corporate network or encounter a security breach from their Internet connection.

In theory it would be wonderful if users took the precautionary steps you recommend, but in reality this cannot be relied upon. It is for this reason that iBAHN invests in 24/7 network monitoring and our corporate VPN certification program to keep service levels high, identify potential threats to the network and manage these before any damage is done.

–CAROLYN SAIT, director of communications, iBAHN EMEA

COMING IN OCTOBER

Change and Control Management

Rarely does a week, or even a day, go by without requests to IT to provision new servers or users, upgrade or patch systems or change a firewall rule. Such changes enable business to function, but they must be managed otherwise serious exposures may result. Change management systems and procedures keep such updates in check and in line with IT security policies. Managing such a system requires a delicate balance of business savvy and security. Change and control management that's too rigid or poorly implemented can stand in the way of business. Properly done, however, change management can seamlessly integrate with an enterprise risk management program, keep approvals moving rapidly and efficiently and even reduce response times when incidents occur. This article covers change management best practices and enforcement procedures through a sample of experiences from companies well versed in change control.

Insider Risk vs. External Threats

Insider risk is touted as the greatest threat to sensitive enterprise assets, mostly because of privileged insiders, who often have unfettered access to customer data or intellectual property. Granted while this is a risk that must be monitored, is the insider threat an exaggerated risk? Are external attackers, often those financed by organized crime or enemy nation states a bigger risk? And just exactly who is an insider these days with all the access third-party service providers and suppliers have. This article will explore all of those angles through the opinion of security experts and observers in an attempt to get concrete answers to all of those questions.

Messaging Threats

Years after Bill Gates predicted spam would be eliminated as a security problem, email-based attacks continue to be a major concern to businesses. This feature examines the latest tactics and technologies attackers are using to keep one step ahead of email security tools and some of the things you should be doing to protect your business, your employees and your customers.

Beware of Internet Hazards

Enterprises face numerous potential liabilities online. Avoiding lawsuits requires a sound cyber risk management plan. BY JEANNE DEBUS

BUSINESSES ARE FACING NEW RISKS and increasing liabilities related to their Internet presence and use of the Internet. A decade ago the focus was on Internet privacy issues, but the spotlight has shifted to Internet liabilities and high-profile lawsuits are commonplace. Take Cecilia I. Barnes vs. Yahoo! Inc. [http://www.ca9.uscourts.gov/datastore/opinions/2009/05/07/05-36189.pdf]. In that case, a federal appeals court ruled in favor of the plaintiff, finding that the ISP failed to remove offensive material provided by a third party. Delta Airlines, eBay, iVillage and Ticketmaster are other prominent defendants in cyber lawsuits. Many lesser known organizations also have faced cyber lawsuits, or are vulnerable to one.

Understanding the risks associated with the Internet is no longer a necessity solely for ISPs, big business or e-commerce sites. All organizations must become knowledgeable about their cyber exposures and take steps to implement a sound cyber risk management plan. This is especially true now as many Internet liability lawsuits seek class-action status, raising the stakes even higher.

There are several categories of law governing Internet-related activities:

- Intellectual property (IP) law prohibiting copyright and trademark infringement such as the U.S. Copyright Act;
- Privacy legislation regulating the use and protection of personal information including the Fair Credit Reporting Act (107) and Privacy Act of 1974, HIPAA, and the Fair and Accurate Credit Transactions Act;
- Communications decency law regulating user-generated content and requiring ISPs and bloggers to make sure their content does not violate federal laws;
- Spam legislation requiring that unsolicited commercial e-mails be identified accordingly and recipients given the option to opt-out.

Each federal law and related state legislation demands a new level of responsibility regarding websites, email marketing, blogs and general use of the Internet. Financial institutions or retailers that lose personal financial data would violate the Privacy Act. An ISP or website operator that allowed a third party to post offensive material to a website they hosted or owned would violate the Communications Decency Act, as was the finding in *Cecilia I. Barnes vs. Yahoo! Inc.*

Cyber liabilities pose first- and third-party risks. Examples of first-party risks include failing to install the latest security patches, which then exposes IT systems to a virus resulting in business interruption and extra expenses; regulatory claims for

failure to notify in compliance with applicable law; and expenses related to privacy notifications, public relations, and cyber extortion. Third-party risks include an Internet advertising company tracking the behavior of a consumer on a retailer's website using "cookies," which many privacy advocates believe constitutes both deceptive practices and an invasion of privacy; a vendor posting an ad to an organization's website that contains slanderous content against one of its competitors; and privacy liability claims brought by others, caused by a hacker breaching your own system or using your system to access and breach a third party's network.

To control Internet exposures, businesses should take a three-pronged approach: educate, mitigate and insure. They should develop an Internet liability and risk management policy handbook that lists the potential risks and steps to prevent and/or reduce those risks. Minimum risk controls include enforcing an information security policy that must be followed by all employees, contractors or others with access to the network; ongoing monitoring of system security; automatic virus and threat notifications; a tested disaster recovery plan; and storing backup files in a protected location.

To control Internet exposures, businesses should take a three-pronged approach: educate, mitigate and insure.

Many insurance carriers offer Internet-specific liability policies, which vary greatly from carrier to carrier and are meant to be in addition to a company's commercial general liability and other policies. To provide the best coverage, many carriers will assess an organization's various cyber liabilities by reviewing its Internet marketing and/or e-commerce practices, its overall IT system security and the scope of its Internet reach. The policy will then be designed to cover both first and third-party risks.

When purchasing Internet liability coverage, it's important to inquire about the definitions and exclusions in the policy. Read a sample policy prior to purchasing the insurance. Require your vendors to sign a contract including a hold-harmless or indemnification agreement in your favor, require evidence of their professional liability insurance including contractual liability coverage in the form of a certificate of insurance, and follow up to make sure their insurance is maintained.

Taking these steps can help keep your company out of the courtroom or protect them in the event of a lawsuit.

Jeanne Debus is vice president at Cook, Hall & Hyde, Inc. [http://www.chhins.com/], a regional provider of commercial and personal insurance, employee benefits and risk management services. Send comments on this column to feedback@infosecuritymag.com.

Analysis | APPLICATION SECURITY

Developers Need Help with Security Errors

SQL injection attacks continue to plague Web applications. Companies need to invest in technology and education to hold off hackers.

BY ROBERT WESTERVELT

DEVELOPMENT ERRORS that leave a custom Web application prone to a SQL injection attack are still not being addressed, and that's a problem because of rampant attacks against Web-facing applications [http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1365263,00.html]. Custom Web apps are attractive because they're relatively simple to deploy. But coders often fail to address security, nor do they test apps for vulnerabilities prior to production.

A recent SANS Institute report on the top cyber security risks of 2009 [http://sans.org/top-cyber-security-risks/] was harsh on the continued problem of SQL injection flaws and called for a renewed focus on technology solutions to prevent SQL injection, and education of developers about the problem.

"It's going to be impossible to do security without some kind of augmentation to improve both our ability to see things as they happen and to figure out problems as they come along," says Jim Molini, a Microsoft security professional and an architect of the new Certified Secure Software Lifecycle Professional (CSSLP) certification. "The innovations that I expect to see at some point in the area of software security are going to involve that, whether it's some kind of automated cognition or automated intelligent response to these things."

By targeting SQL injection errors, attackers are going for the lowest hanging fruit. Automated scripts and free penetration tools have caused a set-it-and-forget-it mentality among attackers. And it's working. Web application vulnerability flaws in open source and custom-built applications account for more than 80% of the vulnerabilities being discovered, the SANS Institute report says. The report recommends IT organizations focus on patching Web-facing client-side applications, and detect and repair website vulnerabilities.

Rohit Dhamankar, director of security research at TippingPoint's DVLabs says awareness and education are important, but organizations also seem to be dropping

the ball when it comes to security testing of applications internally or through third parties before the application is deployed in production. By doing so, major flaws are slipping through because of inadvertently insecure programming practices. For example, some coders use SQL injection as a development shortcut by embedding arbitrary SQL queries in a URL, rather than coding them into the application on the back end. Attackers could manipulate the URL by injecting a malicious SQL query and reach backend databases, experts say.

"If the development organizations ensure that their employees have gone through secure programming practices and courses, it would lead to a decrease of such incidents," Dhamankar says. "From a security technology perspective, the companies could use intrusion prevention systems or Web application firewalls (WAFs) [http://searchsecurity.techtarget.com/magazineFeature/0,296894,sid14_gci1303838_mem1,00.html] to stop such attacks."

A large number of outsourced applications forced Chad Lorenc to take a look at the security of Web-facing and internal applications. Lorenc, information security and risk management specialist at scientific instruments and analysis equipment maker Agilent Technologies, uses a WAF from Imperva to boost security among internal developers and understand the basics of data flow within the company environment.

> "If the development organizations ensure that their employees have gone through secure programming practices and courses, it would lead to a decrease of such incidents."
>
> –ROHIT DHAMANKAR, director of security research, TippingPoint

Lorenc said the analysis provided by the WAF helped the company realize the different ways applications were being accessed by internal and remote employees, contractors, customers and partners. Programmers were happy to see peaks and calls of their applications, and were able to tweak them to improve performance. Penetration testers were able to identify weaknesses in applications and fix them without rebuilding the flawed application from scratch.

"As we monitored and allowed all these transactions to go, it allowed us to build profiles that helped us define the behavior of these applications," Lorenc said. "Very quickly without our interaction we found a consistent behavior of an application. We could find anomaly behaviors and red flags that signaled abuse."

Whether it is technology provided by a WAF or increased education and awareness provided to software coders and end users, the SANS Institute report makes it clear that once hackers find a hole, the risk of passing SQL instructions directly into a backend database rises precipitously, especially for financial institutions and retailers.

Digital investigations expert and SANS Institute instructor, Rob Lee of Mandiant, says attackers go in through the public facing websites in order to gain access to the credit card data on the backend side, he says.

"The attackers themselves, from the nation-state actors to the organized criminals who are involved here, are extremely organized in their methodology," Lee says. "They know what they're doing. There's a big payoff as a result of this and they're quite good." ›

Robert Westervelt is news editor of SearchSecurity.com. Send comments on this article to feedback@infosecuritymag.com

Scareware

MALWARE WRITERS are getting a leg up on users and enterprise security teams via scareware, or rogue antimalware. Hackers are finding success in tricking end users into thinking their machines are infected and promising them a fix, only to install malicious code instead. —*Information Security* staff

SOCIAL ENGINEERING Why does scareware work? Hackers prey on the fears of users, and in turn, walk off with scores of personal data that in turn sells for a profit. The SANS Institute Internet Storm Center says hackers lure users to a website, often taking advantage of some timely news story (one of the latest scams centered on Patrick Swayze's death). The site then serves up urgent pop-ups informing the user their machine is infected. The same pop-up offers an antivirus program that, for a fee, will clean up the problem–some even demand payment just to uninstall the program. In the meantime, the program is installing keyloggers, for example, that will steal sensitive data.

Q2 2009: 374,000

2008 scareware variants: 92,000

Expected Q3 2009: 637,000

UNDER THE HOOD SANS ISC found one example of a scareware notice that served a screen looking exactly like Windows Security Center. This is the kind of sophistication that reels in users. A SANS ISC analysis of the code found a high level of professionalism to the code. Popular JavaScript libraries were used to initiate a phony scan of the machine, pulling file names from the Windows directory to make it seem legitimate. The user is then informed they are infected and a pop-up offers them the option of installing the rogue antimalware, or to ignore it. However, no matter where you click, even if it's on the ignore button, the rogue program is installed.

Cost to victim: $34 million monthly worldwide

SCAREWARE NAMES

ANTIVIRUS 2009
MSAntiSpyware2009
System Guard2009
XPantivrus2008
WinPC Defender
XPAntiSpyware2009
SystemSecurity

SOURCE: Panda Security report– "The Business of Rogueware"

OVER-HEARD

"At this point, you would only see a serious cyberattack combined with a physical conflict. The Russians and Chinese are guys with capabilities and when the time comes, they will use them."

–JAMES LEWIS, Director, Technology Policy Program, Center for Strategic & International Studies (CSIS)

what drives *your* approach to IT security?

Balancing business priorities and risks is key to a solid approach.

SystemExperts helps you build a comprehensive and cost-effective information security plan that makes sense for your company. Right now, our **ISO 17799/27002 Compliance Program** helps you to focus resources on your most important business risks and comply with regulations such as **Sarbanes-Oxley, FFIEC, HIPAA, PCI,** and **Gramm-Leach-Bliley.** Best of all, our approach works equally well for "Main Street" businesses and the Fortune 500 clients we've proudly served for years.

If you want a practical IT security plan that addresses your real business risks, contact us today at 888.749.9800 or visit our web site at www.systemexperts.com/public.

- ISO 17799/27002 Compliance
- HIPAA and PCI DSS Compliance
- Application Vulnerability Testing
- Security Audits and Assessments
- Security Architecture and Design
- Identity Management
- Penetration Testing
- Security Best Practices and Policy
- Emergency Incident Response
- System Hardening
- Technology Strategy
- ASP Assessments

SystemEXPERTS
LEADERSHIP IN SECURITY & COMPLIANCE

guardian
honor-bound
resourcef
builde
pioneer
communicator
visionary

Critical Needs

Critical infrastructure protection must be addressed today to protect our country tomorrow. BY JERRY FREESE

THERE'S A MULTIDIMENSIONAL APPROACH to information security in the electric sector. On the business side, we have to protect the corporate networks and data. On the operational side, critical control system security is a mandate from industry groups and regulators. Given the reality of the financial and resource commitments these approaches require, it's often easy to forget that both exist in a larger security context of critical infrastructure protection (CIP).

In today's environment of competing financial requirements, CIP is understandably less a direct driver of security than it is an indirect beneficiary of whatever protection is deemed effective and affordable for business conduct or regulatory compliance. It's not the best situation given that CIP is key to the preservation of the social and economic fabric of our way of life. That would sound like pure melodrama if it weren't so true.

Even so, and in spite of the rhetoric from government and industry groups, the concept of critical infrastructure protection is little more than that…an understated and under-socialized concept, reserved for academics and government planners, lacking any tangible national-level threat to make it a real priority.

What's the reason that a compelling and imperative concept such as critical infrastructure protection hasn't been embraced for its own sake and hasn't prompted actions to ensure its implementation and long term viability? In some respects it comes down to perceived need.

Remember that prior to 2001, the electric sector and critical infrastructure in general enjoyed an essentially threat-free environment. Infrastructure assets and systems were isolated, and

Jerry Freese

TITLE Director IT security engineering

COMPANY American Electric Power

KUDOS

On the front lines of critical infrastructure protection

Defines, develops and executes all information security programs at AEP

Coordinator of AEP's compliance efforts around the North American Electric Reliability Corp.'s security eight standards, 41 requirements and 164 sub-requirements

AEP's primary data security architect

Contributes to NERC and FERC standards development and the energy industry as a whole

Member of the NERC Critical Infrastructure Protection Committee

Member of the FERC Order 706 Standards Drafting Team

Participated on the Infrastructure Working Group with the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency

Chairman of AEP's Executive Security Committee; committee facilitates major security initiatives company wide

Facilitates NERC CIP compliance efforts on both the technical and regulatory side; managing IT security implementations as well as relaying any new NERC and FERC orders and changes

Retired Naval cryptologic officer; experienced in information warfare

EDITOR'S PICK Critical infrastructure protection is finally and rightly being elevated as a priority, not only among the security industry, but by the White House. The recognition that critical infrastructure is a national strategic asset, in turn, elevates security pros such as Jerry Freese whose efforts go beyond data protection and identity management, and impact national security and our way of life.

even damage from natural disasters could be localized without fear of cascading outages. In other words someone would have to "be here" to conduct attacks against the U.S. infrastructure and the impact would probably be limited to specific assets and geographic areas.

Now the situation has changed. With the increased use of the Internet and multiple-system connectivity, the electric grid has become an interconnected and complex system of systems, with benefits of speed, efficiency and relatively low cost associated with its control and growth. From the industry perspective, the benefits were a boon for business and unprecedented growth in the use of advanced technology for grid management and communications.

Security professionals are well aware that these changes come with a significant downside. Previously closed and remotely unreachable systems are suddenly vulnerable to a host of Internet-based malicious activities. It takes little imagination to understand that the critical electric infrastructure, so essential to American society, is suddenly at risk of becoming a prime target of hackers, social activists, nation-states and even terrorist organizations, with potentially society-altering consequences.

Government and industry are attempting to address this technology adoption with cybersecurity standards and proposed legislation mandating a more reliable bulk power system. It's a good start, but the first iterations of these standards only apply to a subset of the electric sector assets. Cybersecurity in the electric sector, which typically requires a comprehensive logical protection scheme across all networks and systems, has started to look a lot more like an exercise in specific, major asset compliance than it does an all-encompassing, risk-based, infrastructure protection strategy. Though this approach is more sensitive to financial requirements and considers the sheer scope of the infrastructure, it still suffers from the lack of true commitment to critical infrastructure protection.

Because we can't see the threat and haven't experienced any real digital warfare or its effects, we don't mobilize nationally across the public and private sectors and prepare our defenses against it.

What are the missing ingredients? First, it goes back again to perceived need. For most people, the idea of a potential major cyberattack on critical infrastructure, one that could provide the same net effect as actual physical destruction of assets and services across major geographic areas is difficult to grasp. Because we can't see the threat and haven't experienced any real digital warfare or its effects, we don't mobilize nationally across public and private sectors and prepare our defenses. Contrast that with a hypothetical situation where hostile forces are amassed at a U.S. border or a country has deployed a space-based offensive missile system. The national response would be immediate and decisive. The public would demand effective defensive measures be put in place, just in case the forces mobilized or missiles were fired. Protecting the people and the critical infrastructure would be the primary mission.

That brings us to the final missing ingredients; sufficient awareness of the threat and understanding of what we stand to lose in a major cyber incident. There are numerous individuals and groups throughout the world that are fully capable of launching cyberattacks against our infrastructure. The threat may not be imminent but it can manifest itself very quickly. If we're not actively going to pursue a national (private and public) information campaign and protection strategy, integrating strong security into our essential systems and services, the consequences to our critical infrastructure in the event of an attack could be severe. We need a "just-in-case" mentality for CIP. Our way of life may depend on it.

Public Servant

Securing the Internet means too much to the future of the U.S. economy and national security. BY MELISSA E. HATHAWAY

IN DECEMBER 2006, I received a phone call from one of my mentors and colleagues, Mike McConnell, who asked me to join him in serving our country to try to make a difference in a short period of time. As I contemplated leaving my private sector career, I was reminded of a quote from John Adams, "I am...under all obligations of interest and ambition, as well as honor, gratitude and duty, to exert the utmost of [my] abilities in this important cause." I accepted the challenge, and began my journey in serving our country.

During the course of my 30-month tenure, I had the privilege of serving two presidents and helped our government develop a cybersecurity strategy of unprecedented scope and scale that will facilitate revolutionary improvements in the United States' ability to secure and defend our critical national infrastructures. The strategy outlines an action plan to address the growing velocity and volume of threats to our information systems from attacks coming over the Internet, by insiders, and from the worldwide supply chain. Working across the executive branch, we developed and created a unified budget submission that gained bi-partisan approval from Congress and represents the initial down payment required to facilitate the actions outlined in the strategy. This was complemented by unprecedented engagement and openness with a wide variety of constituents during the review and publication of the Cyberspace Policy Review on May 29, and President Obama's detailed speech on cybersecurity that day, which marked the first time a global leader has spoken on the subject at length.

But I am worried that the government is not keeping pace to meet the challenges we identified in the Cyberspace Policy Review [http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf]. During the last decade and a half, the United

Melissa Hathaway

TITLE Former Acting Senior Director for Cyberspace

COMPANY National Security Council

KUDOS

Led the 60-day interagency review of cybersecurity policies and programs throughout the federal government

Oversaw the development of the Cyberspace Policy Review

Served under the Bush and Obama administrations

Under the Bush administration as Senior Advisor to the Director of National Intelligence, helped build the Comprehensive National Cybersecurity Initiative (CNCI)

Led development of a cross-agency budget submission to support CNCI

Established relationships in Congress to gain bipartisan support for cybersecurity initiatives

Testified and briefed with legislators more than 150 times

Former principal at Booz Allen Hamilton; consulted with DoD and the intelligence community.

honor-bound

EDITOR'S PICK Melissa Hathaway is an assertive, determined cybersecurity patriot, a person who devoted countless hours to bring cybersecurity to the forefront before Congress. Her work on the Obama 60-day review is landmark, and sets a high bar.

States has been seduced by phenomenal business and economic growth enabled by the effectiveness and efficiency of high performance global, networked environments. The United States has been one of the key global leaders on embedding technology into our day-to-day life, transforming the global economy and connecting people in ways never imagined. However, we have not invested in the resilience necessary to assure our businesses can operate in a degraded environment.

Our reliance on the conveniences of remote access, and the ability of our networked control systems to reduce costs and manpower needs, have led to weaknesses that are being exploited daily by our opponents. Our nation needs a safe Internet and we must take prompt actions to protect cyberspace for our current and future needs. I believe that our nation is at a strategic crossroad; that it is late in addressing this critical national need, and our response must be focused, aggressive, and well-resourced. We must work to understand the full extent of the vulnerabilities and interdependencies of this information and communications infrastructure, and work to increase its protections and resiliency across all of the sectors of government, military and commercial dependency that we have created.

As more of our nation's networks are compromised and more corporate, proprietary data is stolen, America will continue to lose market advantage and begin to be deliberately displaced by our opponents.

Our government must take bold steps to operationalize a partnership with industry. We need greater information sharing between the government and private sector on what is being targeted, and how, and why it is important to protect ourselves (personally, professionally, corporately, and nationally). As more of our nation's networks are compromised and more corporate, proprietary data is stolen, America will continue to lose market advantage and begin to be deliberately displaced by our opponents.

Our opponents are targeting our multinational and private corporations on at least three fronts: (1) through industrial espionage, they target corporate intellectual property and other proprietary data; (2) they attack other targets as mechanisms to reach yet other targets, sometimes through supply chains and sometimes to target relationships; and (3) they target corporate infrastructure, by infecting networks or otherwise creating a persistent presence, as a means to allow for future targeting on either, or both, of the first two fronts.

Our government cannot develop a strategy independent of private sector insight and cooperation. Our nation will need the private sector and its services and capabilities to find these attack profiles, inform the government of them and develop the solutions to resolve them. Our government needs to cultivate a public-private partnership and action plan that identifies the requirements for the future architecture, hardware, software and services that enable security and resilience. I believe that the private sector is ready to work with government on these efforts, and in order to take advantage of this opportunity, the government must actively engage the private sector and set aggressive milestones toward achieving common goals.

This is just one of the serious policy matters facing the United States in its continued dependence on information systems. As our country moves forward, it requires the strongest leadership in cybersecurity to navigate the jurisdictional ambiguities between individual departments and agencies, the laws that inhibit our ability to share information

and communicate the urgency of the situation. These efforts must be implemented in a manner that allows us to continue to foster innovation and enable our information and communications infrastructure to fuel the nation's economic growth. Cyberspace will not be secured overnight and on the basis of one good plan. The past 30 months represent the first steps toward making real and lasting progress, and are just the beginning of the beginning.

Cyberspace will not be secured overnight and on the basis of one good plan.

I am honored to be recognized with the Security 7 Award for the contributions made in the past 30 months. There are many leaders within the security profession who are deserving of this recognition. The distinguishing thing about being recognized by your peers is that you have to be nominated by someone who believes you are worthy of recognition, which, like most other opportunities, stems from a phone call or a request to take a different path—taking a chance that you can make a difference in another capacity.

Metric System

Security metrics must not only provide a view of security posture, but must support security budgeting and investment processes. BY BRUCE JONES

RISK METRICS were virtually non-existent three years ago when I took over as Kodak's global IT security and risk manager. The company's risk management process was cumbersome, time-consuming, inconsistent, and subjective; as a result, we were lacking a comprehensive picture of our security posture to the business.

I wanted a security metrics program that not only supported the budgeting and investment process for IT security but also provided an "at-a-glance" view of the overall risk posture. I researched different risk models from the National Infrastructure Advisory Council (NIAC), the National Institute of Standards and Technology (NIST), and Microsoft SFT, and came away with the opinion that their models would not fit our requirements relative to management and overhead.

I decided instead to rely on my previous business experience to develop our current metrics program: a tier-based approach to IT security risk management that uses a set of standard probability and business impact frameworks to provide a lean assessment process. One of the keys to our program's success is that reporting and presentation of security risk metrics is "business-user-friendly."

IT governance, risk and compliance (GRC) has emerged as a unifying theme in aligning risk and the business. The challenges of bringing each silo together are great rivers to cross. However, if approached correctly, such an alignment is achievable. IT GRC programs encompass the implementation of systems and

Bruce Jones

TITLE Chief information security officer/ Head of global IT security and risk

COMPANY Kodak

KUDOS

Member of internal IT risk council and information security advisory boards

Highest ranking security and risk management executive at Kodak

Runs a team of six responsible for the security of 27,000 internal users

Created Kodak's Global IT Security and Risk Management Program

Mandates that all risk decisions are made in alignment with business goals and risks explained in terms of impact to the business

Implemented an identity-based encrypted email system to communicate securely with third parties and partners

Developed an IT security architecture to drive standardization across IT security tools and infrastructure

Eliminated $2M in IT support expenses

Developed Web-based IT security training course that was deployed in 11 languages

To meet Sarbanes-Oxley segregation of duties mandates, managed team of 500 to remediate 100,000 segregation of duties conflicts and remediate 13,000 users with excessive system access

resourceful

EDITOR'S PICK Bruce Jones is a 27-year veteran of Kodak and his experience is gold in this industry. His efforts around risk management and compliance directly improve Kodak's bottom line, all while standardizing the way information security is managed and deployed company-wide.

processes to monitor current business activity. They should also determine, set and manage the risk tolerance level for the corporation, identify potential risks, prioritize and manage them. The IT GRC team, meanwhile, should determine what needs to be done to ensure continued compliance and provide a process for corrective action where necessary.

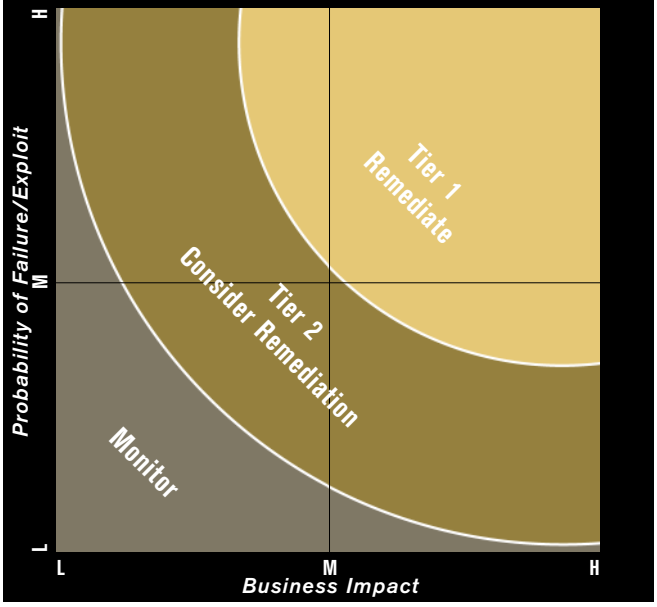
Having an agreed-upon risk management framework is a crucial element in this structure and provides a firm foundation for other discussion.

Most importantly, the overall IT GRC program provides a common framework for communication and collaboration. One prerequisite for meaningful and positive cooperation includes having a common set of controls. In addition, it is crucial to have a common risk management schema to ensure everyone ranks risk similarly. It is also important to have documented policies, procedures, and work instructions as well as a standard decision-making process. If the IT GRC program has these things in place, the groups involved will effectively speak the same language. It will be key to avoiding misunderstandings as well as eliminating future conflict between the various groups.

Having an agreed-upon risk management framework is a crucial element in this structure and provides a firm foundation for other discussion. First, it provides a simple basis for presenting complex risk data. It is also used to present a holistic risk-based view of the security posture for the entire organization. It also serves as an effective tool to translate operational and tactical risk data into meaningful business information, which is indispensible for communicating within the various levels of management. Having this common view of the risk posture helps drive data-based decisions and can be used for both short- and long-term budgeting decisions.

For Kodak, our tier-based approach does all this and more, including a formalized assessment and acceptance process that engages appropriate levels of management based on the tier level of the risk. In addition, a monthly dashboard is published that provides an "at-a-glance" view of the current risk posture.

FIGURE 1: IT Risk Assessment



Kodak's tier-based risk model is based on three levels of risk:

- Tier 1 is the highest risk level and represents threats that you never want to occur in your environment.
- Tier 2 risks represent a moderate level of risk; for these, it is important to understand what the threat is doing. For example, if it is growing and may soon become a top-tier risk, then quick action is needed in order to mitigate or eliminate it.
- Tier 3 risks represent the lowest level and in many cases are considered an acceptable level of risk. In order to calculate the risk tier, the probability is assessed against the business impact. *(see Figure 1, left.)*

Our probability and business impact frameworks, meanwhile, quickly assess the impact of risk. Each is organized into several topical areas, with their own set of statements that represent various risk levels from high to low. To assess probability or business impact, a user highlights which statements are true and makes a subjective determination based upon all factors presented. This results in a score from 0 to 10, which can then be plotted to determine tier level. The assessment process is not perfect; it's designed to get the risk into the appropriate bucket so that it can be dealt with appropriately. If the risk is borderline, it will typically be pushed into the higher tier level.

Taking a business-centric view in developing an IT GRC program is essential to gaining buy-in and support from the various levels of management.

Kodak's risk program approval/acceptance process is based on tier levels *(see Figure 2, below.)* For example, there is no reason for senior vice presidents to be involved in discussions regarding tier 3 risk, however only an officer of the company should be accepting the remediation plan for a tier 1 risk. Previous risk programs at Kodak required several senior managers to sign off on remediation, regardless of risk.

It is important to consider the entire range of risks holistically to determine if the aggregate represents a risk level that is above the tolerance of the corporation. Having a dashboard that shows collective risks is an important tool for communicating overall security posture to management.

Taking a business-centric view in developing an IT GRC program is essential to gaining buy-in and support from the various levels of management. Engage all parties that have a vested interest in the development of the IT GRC program; this team should include members from senior management and business management, the compliance officer, privacy officer, auditing group, application owners, and infrastructure owners. And be patient. Building a strong and comprehensive GRC program takes time and will be enhanced as you go forward as a living document and plan.›

FIGURE 2: Who Needs to Review and Approve Risks

Approver Tier Level	CIO	Chief Security and Privacy Officer	IT Director	Global IT Security and Risk Manager	Business Unit/Functional Unit Management	Business Unit/Functional Unit, Data Privacy Officer
Tier 1	Yes	Yes	Yes	Yes	Yes. President or delegate (must be a corporate VP)	Yes. Only if personally identifiable information is at risk.
Tier 2	No	No	Yes	Yes	Yes. President or delegate of their choice.	Yes. Only if personally identifiable information is at risk.
Tier 3	No	No	No	Yes	Yes. Anyone in the business unit/functional unit.	Yes. Only if personally identifiable information is at risk.

One to Many

Healthcare provider Humana Inc. has developed a security controls framework that addresses all of the industry and federal regulations it must comply with. BY JON MOORE

THE HEALTHCARE INDUSTRY'S increasing reliance on technology during this decade has been embraced by consumers, and this has created increased challenges for an already highly regulated sector. The need for superior information security is understandable; after all, consumers entrust us with their health and their wealth. By that, of course, I mean that Humana's subscribers and those of our peer companies are relying on us to help enable their quality of life securely and reliably.

Healthcare companies must comply with the myriad of state and federal regulations (HIPAA, Sarbanes-Oxley, PCI, and now HITECH) that have emerged since 2000; each is intended to result in healthcare companies safeguarding customer information. Achieving compliance can mean significant cost and regulation-related expenses for healthcare companies. But the cost of doing nothing can have profoundly negative consequences. In fact, the financial impact of data breaches is skyrocketing. Humana's challenge, like its competitors', is in achieving compliance with varying regulations cost-effectively and efficiently.

Complying with each security-focused regulation one-by-one is a natural compliance strategy, but it can easily push you into a never-ending chase of compliance aspiration. Just analyzing the multitude of control requirements from each regulation can be costly and eat into the quality time a company needs to actually implement and achieve meaningful information protection measures.

Humana has responded with an integrated compliance

Jon Moore

TITLE Chief information security officer

COMPANY Humana Inc.

KUDOS

Executive Council member Health Information Trust Alliance (HITRUST)

Humana's first CISO; runs the Enterprise Information Security Organization

Helps run Humana's global readiness and crisis management office

Counsels executives on information security

Oversees $6.92M budget and a team of 44

Developed policies and technology to secure Web-based customer-facing tools

HITRUST leader; helped develop a set of industry best practices around information protection and data integrity

Won HITRUST's Leadership Award for his work in developing the healthcare industry's Common Security Framework.

Established consortium of HITRUST IT, risk, physical security and privacy professionals to develop third-party audit program

builder

EDITOR'S PICK Healthcare is a national priority, and as it is elevated in our consciousness, security and information privacy will be paramount. Jon Moore's pioneering work at Humana and with HITRUST in establishing data protection and integrity standards is laying the foundation for future security professionals in the healthcare industry.

strategy. Instead of focusing on distinct compliance measures for each regulation, we concentrated on building an integrated security control framework across our enterprise. Its building blocks—common security controls, best practices and policies—are positioned to predictably lead to a state of compliance with a host of unique regulations. Our comprehensive, integrated approach has paid off significantly.

Instead of focusing on distinctive compliance measures for each regulation, we concentrated on building an integrated security control framework across our enterprise.

We initially created a security control framework with ISO 27002 as its foundation. Building on this internationally recognized standard for security enabled us to steadily mature our control framework. We have progressively adopted additional best practices, carefully aligning their common requirements to be responsive to multiple regulations. As a result, our framework provides clear guidelines we consistently follow in delivering an array of services across our enterprise, including consulting, control guidance, security assurance reviews and security-focused risk analyses. Our primary objective is achieving all our control framework standards, not simply conforming to individual regulations.

Our annual maturity assessment enables the continued viability of Humana's security control framework process. In 2004, we adopted the Capability Maturity Model Standard to assess the reliability of our program relative to the security framework. This domain-by-domain view of our maturity has been invaluable. It has enabled us to optimize our finite information protection resources by targeting them directly at areas with the greatest opportunities for improvement. As a result, we have consistently increased the overall maturity level of our program.

The progression of our framework maturity dovetailed with the formation of HITRUST, the Health Information Trust Alliance. Humana helped pioneer the healthcare industry's groundswell of support for HITRUST's development of a common security framework, a standard introduced earlier this year. As a HITRUST executive council member, I will continue to help oversee our industry's reliance on this unified and industry-driven set of security governance standards and controls offering valuable prescriptive implementation guidance. In addition, HITRUST's related services and certification initiatives are also enabling an unprecedented level of consumer, vendor and regulator confidence and trust of all healthcare entities. Healthcare needs this now more than ever.

Today, Humana's security control framework aligns with HITRUST's common security framework. We continually refresh it to ensure ongoing alignment and inclusion of the latest control objectives and prescriptive guidance from HITRUST. Of course, we also rely on technology's advantages to sustain our control framework's effectiveness. I recommend investing in governance, risk and compliance (GRC) technology that will enable and automate compliance maintenance, applications and evaluations with your control framework. GRC tools typically result in a positive return on investment and allow you to automate many of the manual risk and compliance processes that eat up valuable time that can be better spent implementing or improving your control environment.

Frameworks flanked by technology and people work. Achieving compliance is realistic if you develop and implement an integrated strategy. Build a security control framework that you believe in, and continually enhance, and, in time, compliance can be the expected result.›

Societal Security

Carnegie Mellon University's CyLab designs security to improve all aspects of society. BY ADRIAN PERRIG

DESPITE MUCH RECENT PROGRESS in the area of user-centric design of secure systems, user error continues to cause a large number of security vulnerabilities in current systems. Both user education and technology can help to improve this situation.

At CyLab at Carnegie Mellon University, our goal is to improve security in all aspects of society. First, we developed educational programs to train students in security. Second, CyLab researchers also engage in several efforts to design systems that continue to remain secure despite human errors, as well as develop technologies that provide improved situational awareness to the user.

Adrian Perrig

TITLE Professor electrical and computer engineering, computer science, and engineering and public policy; technical director, CyLab

SCHOOL Carnegie Mellon University

KUDOS

Research is on the cutting edge of network security and safe usability features

Developed Phoolproof Phishing Prevention, a software tool that relies on trusted individual devices to perform mutual authentication

Also helped build Seeing-Is-Believing, a version of PKI between mobile devices that eliminates the need for central key authorities through visual recognition of 2D barcodes

Oversees the development of Flicker, which leverages features in AMD and Intel hardware to limit execution of application-specific code to only isolated areas of a machine

Collaborated on Perspectives, a Firefox plug-in that cuts down the risk of users falling victim to man-in-the-middle browsing attacks.

Using the Secure Socket Layer (SSL) / Transport Layer Security (TLS) protocols for secure https Web connections as a case study, we will first describe how education has helped improve Web security, followed by a description of the Perspectives project, which provides additional information for users to make better security decisions. To provide some background for our discussion, we briefly revisit some SSL/TLS security-relevant fundamentals.

SSL/TLS is a protocol to provide communication secrecy and authenticity, and is invoked whenever we access an https-based Web page. Although SSL/TLS is a well-designed protocol, it still needs to face the complexities and realities of our computing environment, which result in numerous opportunities for user error and the following vulnerabilities.

Probably the most fundamental threat to SSL/TLS security is a so-called man-in-the-middle (MitM) attack, where an adversary interposes in a connection between a client and a server to eavesdrop on communication or inject malicious data. Such MitM

pioneer

EDITOR'S PICK Adrian Perrig's students and research teams aren't tasked with solving today's pressing security threats, instead, they're working on attacking tomorrow's threats by designing systems that cut down on user error. His invaluable work is the foundation for the security tools and practices of the next decade.

attacks can be mounted by any entity handling network packets, and is usually mounted in wireless networks in public environments, e.g., in coffee shops, airports, conferences, etc. The SSL/TLS protocol is designed to protect against man-in-the-middle attacks.

Unfortunately, many real-world issues still enable adversaries to mount attacks. For example, cryptographic vulnerabilities can enable attackers to mount MitM attacks, for example by exploiting the collision resistance of the MD5 hash function—researchers recently demonstrated a successful attack [http://searchsecurity.techtarget.com/news/article/0,289142,sid14_gci1343790,00.html] where they were able to obtain a bogus certificate that enabled creation of arbitrary additional certificates trusted by current browsers . Browser or OS vulnerabilities enable adversaries to inject bogus certificates into the trusted set of browser root certificates. Users can be tricked into visiting a bogus URL or to install bogus root certificates. CAs can be tricked into issuing certificates to the wrong entities. These are just a few examples that would enable an adversary to mount a successful man-in-the-middle attack. Given that we cannot redesign the current legacy computing environment in the near term, we need rely on education and technology to enhance the current state of SSL/TLS security.

Given that we cannot redesign the current legacy computing environment in the near term, we need rely on education and technology to enhance the current state of SSL/TLS security.

Over the past seven years, I have been teaching more than 100 students each year about the various issues with SSL/TLS. (The student composition was mostly Master's degree students enrolled in CMU's security MS programs.) In several instances, the lessons learned in class fell on fertile ground: the students immediately assessed the security of their banks' websites and informed their banks to report cases of inadequate security. In numerous instances, the banks listened to the students' feedback and promptly improved security. In some cases, it was as simple as fixing a typo by adding the critical "s" to complete the URL to "https" for the login page. In more difficult cases, students needed to convince the banks' security administrators that Javascript-based encryption loaded from a non-https page can be easily removed by a MitM attacker. In summary, by educating a critical mass of students that further disseminate security knowledge can result in real improved security for everyone.

Together with student education, technology that provides the user with additional information for improved security decision making can also enhance security. To improve security for https sites with self-signed certificates, as well as detect numerous attacks on https sites using bogus certificates, Dan Wendlandt, Dave Andersen and I designed and built Perspectives [http://www.cs.cmu.edu/~perspectives/] , a Firefox plug-in that connects to notary servers to assist in validating https credentials. Perspectives informs the user for how long an https credential has been observed for a given server [http://sparrow.ece.cmu.edu/group/pub/wendlandt-andersen-perrig-usenixatc08.pdf]. This simple user feedback enables users to make better security decisions, in fact, I gained more confidence in my personal Web browsing by knowing that the https credentials of the servers I visit had been in use for a while—which assures me of the absence of a variety of attacks.

In summary, by leveraging education and technology for improved user information, we can increase the security of our current systems in the short term. To achieve a stronger level of security in the long term, however, redesigning more robust systems seems to be necessary.

Talk Tough

Learn how to communicate with senior management about risk; it's your job. BY BERNIE ROMINSKI

I THINK I MIGHT be spending too much on information security.

I'll bet that's something you don't hear every day. It's an ice-breaker that I've been thinking of using at an upcoming meeting with senior management regarding information security risk. Of course, there's also a chance we're not spending enough; it's just the other side of the same coin, but I figure my executive leadership might be more intrigued with the former possibility. I know reducing operating expenses is a high-priority concern for them recently, so that might really get their attention.

The fact is that our security budget is right where it should be. If it's not, it's my fault. Why? Because my most important and challenging responsibility is making sure management understands what they're getting, and what they're not getting for their information security budget dollars. If they are making informed risk decisions that drive our security strategy, the budget will be there. Likewise, if the security staff attempts to make those decisions in a vacuum, we'll be apt to flounder trying to cover all the bases, spending more than we need while feeling that we are under-funded.

Senior management is ultimately responsible for addressing all business-related risk. They are accountable for all outcomes from our business activities, good or bad. They understand some risks very well; others they need to have a good sense of but depend on the counsel of experts in their various areas to feel adequately informed. Information security risk is something the typical executive might not understand as deeply as a security professional, nor should they. We don't pay our CEO to be an expert in the latest Web application firewall technology, and, thankfully, we don't pay our security manager to make decisions on buying, building and operating hair salons. We have our areas

Bernie Rominski

TITLE IT security officer

COMPANY Regis Corp.

KUDOS

Tasked with building an information security program and implementing controls to meeting PCI DSS and Sarbanes-Oxley requirements

Developed a security policy framework and conducted enterprise-wide risk assessment

Secures millions of transactions at Regis' 8,500 retail locations in the U.S.; manages a team of six

Must contend with constant merger and acquisition activity, requiring an agile security program

Implemented an encryption program to securely transport credit card numbers from the company's retail locations to its Minneapolis data repository

Deployed data loss prevention tools to analyze transactions for fraud and other card abuse

Member of ISACA, ISSA and CSI

communicator

EDITOR'S PICK Bernie Rominski is a security craftsmen, building a security and risk program in short order that examines the integrity of millions of relatively small transactions taking place in thousands of locations. His policy and process development sealed significant compliance gaps and guaranteed the security of his enterprise's transaction data.

of responsibility, but we're on the same team trying to carry out the same mission.

Early in my IT career, a CFO I worked for taught me some great lessons. I'll never forget one of the things he used to say regularly: "Bernie, explain it to me like I'm a 10-year-old." Of course, he didn't mean to suggest the average 10-year-old isn't smart. What he was saying in his very tactful way was that he wasn't interested in learning all of the techie ins-and-outs of the situation, that I shouldn't waste his time with fancy IT acronyms, and very importantly, that I shouldn't worry I'd offend him with my "dumbing down" of the subject matter. I was very appreciative of his method because though we did have very different duties, we both had a responsibility to find a way to communicate about the things we needed to in order to get our jobs done.

I was very appreciative of his method, because though we did have very different duties, we both had a responsibility to find a way to communicate about the things we needed to in order to get our jobs done.

I hesitate to make this comparison, but I'm reminded of certain public service announcements urging parents to talk to their kids about drugs. It might seem a bizarre parallel, and I wouldn't dream of suggesting we view our management as kids who might not know what's good for them, but one thing the announcements try to suggest is that as vast a communication gap as you might be facing, it's important to find a way to talk about topics that are important. These announcements aim to prepare you for an impatient audience that is far more likely to roll its eyes at you than to say "thanks for caring," The theme is that there's always another way to bring up the topic. If you're creative, and you know your audience, you can help make those connections. It just takes effort, and though it might seem sometimes like an uphill climb, we have to keep trying.

One effective way to build that connection is to make sure your security strategy is lined up with business objectives, and that you address security in the context of those objectives. If you speak with management about specific goals they're trying to reach, you're getting on the right page. Every business is different, but there should always be ways to build on the theme of alignment.

It's not an easy job, but we're the security experts, so the onus falls on us to help bridge the communication gap. We need to find a common language that works for us and our management. We should use whatever means are available to us to find that common ground—formal risk assessments, informal risk assessments, collaborative workshops, cave-drawings—the medium is less important than the goal; we need to keep talking, and we need to keep trying to talk better.

Compliance Second

Organizations need to prioritize security over compliance to ensure comprehensive risk mitigation. BY TONY SPINELLI

BUSINESS LEADERS and chief security officers take note: When it comes to risk mitigation, compliance alone is not enough to protect your enterprise. It takes a broader security strategy—of which compliance is a part of the whole—to hit the high-water mark. In fact, those organizations that focus on security first to become compliant are seeing greater business impact. Instead of focusing solely on meeting compliance benchmarks, these companies are changing the way they achieve a high-water mark for security performance.

Let's face it, we are entering an era of tighter statutory requirements and rapidly changing regulations. But focusing solely on statute requirements can lead to a disjointed strategy that is neither comprehensive nor aligned with business goals. While compliance mandates are often used to drive security investments, compliance by itself does not ensure a company's security posture.

And while compliance cannot be the sole focus of a security strategy, technology by itself cannot safeguard an enterprise. Increasingly sophisticated threats and growing concerns over data losses are just a few of the issues facing CSOs. For this reason, businesses simply cannot afford to think about security in purely technical terms.

Instead, businesses must look beyond their technology and compliance needs and understand the challenges of ensuring their company's security posture. Achieving this level of transparency requires the right mix of innovation, talent and technology underscored by a strategy that addresses risk at the broadest level. This is where relationships with business partners and vendors can play a valuable role. By joining forces with

Tony Spinelli

TITLE Chief security officer

COMPANY Equifax

KUDOS

Board member Information Assurance Board of the U.S. Dept. of Defense

Board member Georgia Tech Information Security Center

Board member Information Risk Executive Council

Has oversight for IT security and compliance; responsible for design, development, monitoring of IT and physical security

Manages team of 70 and multimillion dollar budget

Protects more than 6,500 employees in 15 countries

Instituted data loss prevention program to secure data of hundreds of millions of consumers and businesses worldwide

Oversaw enterprise-wide encryption and DLP programs

Tuned more than 1,000 production devices to sniff out bad traffic without impacting services

Instituted regular third-party risk assessments and reviews

visionary

EDITOR'S PICK Tony Spinelli has set a standard for data protection that is to be lauded. His institution of a worldwide data loss prevention program, partner assessment processes and participation in numerous and influential industry groups makes him a model security leader.

industry-leading third-party providers, companies gain access to new thinking and innovation to address key needs and challenges. With the right strategy and technology partnerships, businesses can drive a consistent and global set of security practices focused on risk reduction and information security.

At Equifax, we have implemented a strategy to minimize operational and information risk, which includes safeguarding data on hundreds of millions of consumers and businesses worldwide. Equifax tackled this complex undertaking by adopting a simple but powerful vision: that security must be treated as a business. Here's a snapshot of how it worked.

At Equifax, we have implemented a strategy to minimize operational and information risk, which includes safeguarding data on hundreds of millions of consumers and businesses worldwide.

Recognizing that compliance is not the only measure of security, Equifax set out to develop and implement a plan to consolidate all of its security functions into a centralized organization. Equifax chartered a process to assess the company's risks globally and then developed an integrated strategy that aligns its risk mitigation and information security needs with real-world business requirements.

In less than three years, Equifax made its vision a reality and not only transformed its security department into a global center of excellence but also enabled the company to drive greater synergies across its business units. Today, compliance is just one of the many benefits of Equifax's comprehensive security program and strong security position. Faster access to information, enhanced business intelligence and increased visibility of enterprise-wide IT services are among some additional business benefits Equifax has reaped by applying the right mix of innovation, business acumen and technology.

The ability to leverage this type of value from a security investment can go a long way in forging stronger ties with the businesses we protect. While it can be challenging to convince a business unit to dedicate significant capital to security initiatives, the process is well worth the return on investment. Applying security innovation to risk mitigation and data protection strategies can empower businesses to identify new growth opportunities and deliver better, customer-centric solutions.

Here's how we brought this approach to a few of our own business units:

- Equifax Personal Information Solutions, which provides consumer credit and identity theft protection products, has seen first-hand the impact of innovative security solutions at work. Partnering with Equifax's Security Engineering team, Personal Information Solutions enhanced the authentication process used by new customers to access their Equifax credit report online. As a result, customers were able to obtain their online credit report with greater ease and enhanced security functionality—resulting in increased revenue for the company's U.S. and U.K. operations.
- Another area gaining a competitive edge by working with our security team is Equifax Workforce Solutions, which provides employment and income verification as well as human resources business process outsourcing services. Workforce Solutions recently turned to Equifax Security to develop an authentication program for its commercial business portal. Benefits include increased security protection for business customers and a simpler and user configurable security interface.

History has shown that companies that treat security as a business enabler are much more effective in managing risk, protecting their data assets and ultimately sustaining an industry edge. If the current economic crisis has taught us anything, it is that risk is a constant in our marketplace. For this reason, we must be vigilant in our pursuit of security innovation and new solutions that can mitigate risk and still drive greater business value. Companies that understand this correlation between risk and innovation are the ones that will set the high-water mark for security—and business performance.›

honor roll

Information Security's list of past Security 7 Award winners:

2008

Bill Boni
Mark Burnette
Michael Mucha
Marc S. Sokol
Gene Spafford
Martin Valloud
Mark Weatherford

2007

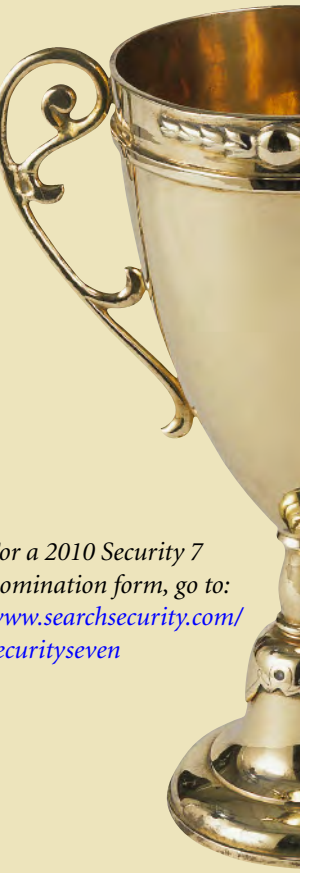
Michael Assante
Kirk Bailey
Michael Daly
Sasan Hamidi
Tim McKnight
Mark Olson
Simon Riggs

2006

Stephen Bonner
Larry Brock
Dorothy Denning
Robert Garigue
Andre Gold
Philip Heneghan
Craig Shumard

2005

Edward Amoroso
Hans-Ottmar Beckmann
Dave Dittrich
Patrick Heim
Christofer Hoff
Richard Jackson
Charles McGann



For a 2010 Security 7 nomination form, go to: www.searchsecurity.com/securityseven

Security Topics Tailored to Your Needs

You rely on *Information Security* magazine every month for original, in-depth information and analysis on the security of your enterprise. But as you know, to secure your data and network you need to be well informed every day. Stop scouring the web; become a member of SearchSecurity.com and receive tailored messaging delivered right to your inbox with the latest news, current threats, expert advice, white papers, webcasts, and much more on the security topics that YOU select including:

Network Security
Intrusion Defense
Identity and Access Management
Email Security
Web Security
Current Threats
Application Security
Compliance
Security Management
Platform Security

Stay informed 24/7. Activate your free SearchSecurity.com membership at www.SearchSecurity.com/join today.

SearchSecurity.com
The Web's best security-specific information resource for enterprise IT professionals

MOVING FORWARD

Truth is, application and information security teams work in silos and often meet only after an attack on a critical app. Here are nine tips you can use to prevent future costly incidents and improve application security.

BY CORY SCOTT

WHEN AN ENTERPRISE SUFFERS an application security incident, a whirlwind of activity takes place to triage the immediate problem. Application and security teams work side by side to identify the damage, implement a quick fix to prevent further losses, and perform a root-cause analysis to determine why the vulnerability existed in the first place.

Embarrassingly often, incident response is the first time application security is discussed in

earnest between information security and application teams. While policies may be in place and risk assessments have been performed, an attacker has opened an indisputable vulnerability that has slipped through the cracks. Even penetration testing results, with their inherent proof of exploitation, do not bring the same gravitas. Experienced testers have frequently seen findings explained away by a defensive application owner, remediation scheduled into the next release that never comes, or slapdash fixes that prevent the proof-of-concept, but not the underlying vulnerability.

When the root cause analysis is laid at the feet of management, the savvy information security officer will not only have an explanation for "what happened this time," but how to identify other cases of the same vulnerability in other applications in the enterprise. Even savvier information security teams can leverage the incident as a catalyst to enhance the assessment of applications and improve an inconsistent and underdeveloped application security program.

However, more often than not, these fledgling improvements can get crushed under the inertia of the organization. It can be difficult to shift people's attention from the "quick-fix" to "fix-the-root-cause" once the initial damage has been mitigated. The complexities of implementing an application security program can frustrate even experienced practitioners and the difficulty in establishing a business case can create stall-out, due to the large costs that many of these initiatives carry.

When attempting to improve application security after an incident, consider the following nine pieces of advice to forestall some of the challenges other organizations have faced.

1. IDENTIFY HIGH-RISK APPLICATIONS

(BUT DON'T SPEND TOO MUCH TIME ON THE INITIAL INVENTORY)

Most organizations already have a fairly good understanding of the applications that mean the most to the business. They're the applications that when performance or availability problems occur, everyone drops everything to fix. They're also the ones that require compliance and regulatory controls. However, many organizations also have third-party applications that provide a critical function to the business, but can be overlooked if the exercise is too introspective.

One inevitable thing that happens during an inventory exercise is that a rush of data is provided with varying levels of confidence and quality. Focus can shift away from the end result and toward the inventory practice, with elaborate schemes of identifying every last application. Limit the amount of effort on identifying applications and focus more on identifying which applications are in scope.

Determine what data or functionality is present in the applications that is worth protecting, and do some quick threat modeling to see if there is a clear path to an adverse event. In this threat model, assume that access control fails and the underlying application data and functionality is exposed to all. Critical Web application vulnerabilities often result in these outcomes, so those worst-case scenarios should be on the table.

Try to explain the risk in two sentences as if you were speaking to a layperson. A good example could be: "The PayThemNow application is used to transfer funds between the corporation and its payees. If an unauthorized transaction is entered into the system, it may be difficult or impossible to recover the funds." Another example: "The RebatePlease application collects significant amounts of customer information and makes it available to internal business units and an external check-processing provider. If the data is compromised, a breach disclosure may be necessary, and if the application logic can be subverted, customers can get rebates they are not entitled to receive."

On the other hand, when you end up stringing together a good number of "ifs", then you might consider moving the application down in your priority list. Applications where only reputational damage is on the line or where internal network access is required are two common areas where organizations spend too much time attempting to create a complete inventory.

Keeping the list small and doing a strong job on a subset of your application estate will yield positive benefits for application security in the longer term, and prevent stall-out and exhaustion.

2. DEVELOP A STRUCTURED, MEASURABLE AND REUSABLE APPROACH

(IT'S GOING TO TAKE MORE THAN A SPREADSHEET.)

The meaning, scope, and depth of an application security assessment, penetration test, or vulnerability scan can significantly vary based on the audience. The fact that we have at least three different process names with different approaches should be incontrovertible evidence of this issue.

Even within consulting firms with an established methodology and deliverables, there can be a surprising amount of variation in testing depth for a given function or sub-application. Use of tools is not a panacea to this problem either, as the underlying logic used to explore a given site and identify potentially vulnerable interfaces requires human guidance. An automated tool cannot determine whether the coverage is acceptable and whether or not the necessary tests are run.

By defining a shortlist of critical vulnerabilities to test, and a flexible approach on how to perform the assessment (tools, code review, or penetration testing), a skilled application security analyst can provide the appropriate level of coverage and demonstrate that the application has been tested sufficiently. While you may allow flexibility on which approach should be used, there should be a standard and reusable testing methodology for each approach.

Each test should include a standardized deliverable template, including a common approach to

INDICATORS

Application Assessment Metrics

THERE ARE TWO MAJOR classes of metrics used to measure security initiatives:

1. **Key Risk Indicators (KRI)** which measure the risks identified by the assessment program.

Examples of KRIs for this program would include: number of vulnerabilities still open for each application; applications within open vulnerabilities that have suffered a successful attack within the last year; and applications with open vulnerabilities with no clear path toward remediation or where the risk has been accepted by the business unit.

2. **Key Performance Indicators (KPI)** which measure the quality and coverage of the program's execution.

Examples of KPIs for this program would include: number of high-risk applications; number of assessments performed; code/component coverage for each assessment; assessment coverage per business unit; number of vulnerabilities opened for each application; number of vulnerabilities addressed with a plan; and number of vulnerabilities closed or remediated. ›

–CORY SCOTT

rating vulnerabilities, documenting each issue and its impact to the application. It should include steps to reproduce, and suggested remediation advice (perhaps supplied by central guidance) for development staff. The findings should also be in a portable format for reporting purposes.

Measuring the progress and risks identified by the assessment program is critical to maintain momentum and continue the dialogue with all stakeholders *(see "Application Assessment Metrics," p. 34)*.

3. CONSIDER TWO-PHASE ASSESSMENTS TO FIND DESIGN FLAWS

(DON'T JUST SCAN FOR YESTERDAY'S EXPLOIT.)

In application security, there are two primary types of vulnerabilities. Design vulnerabilities require changes to the underlying application design or architecture, while implementation vulnerabilities are typically fixed with additional code (such as an input validation library) or modification of code in a particular function of an application. Traditional application penetration testing is focused on implementation vulnerabilities, although a skillful tester can also identify the symptoms of some design flaws.

An application security design assessment is often used for high-value applications where there are aspects of the application that could result in security issues but do not lend themselves easily to implementation testing. Use of cryptography, logging, development practices, and other design review criteria are common examples of these aspects. The test is typically performed by an application security specialist in an interview format, and includes data flow diagramming around trust boundaries, threat modeling, review of development practices, limited source code review, and design documentation review.

While a design assessment may appear to be merely a paper-based exercise, a well-executed review can find systemic flaws that result in hundreds of implementation vulnerabilities which would have taken multiple man-months to identify in a traditional penetration test engagement.

As a result, it is recommended that some applications undergo a two-phase assessment that includes a design review in addition to a penetration test.

4. DEPLOY APPLICATION SECURITY SPECIALISTS WITH BUSINESS-SPECIFIC REMIT

(CONTEXT AND AVAILABILITY ARE CRUCIAL.)

Successful implementation of application security discipline requires significant alignment with application development practices of the organization and the application owners. If the enterprise has multiple development practices spread across multiple business units, it is important to deploy staff with close proximity to those teams. The application security specialist should represent the interests of the application security practice while becoming familiar with the underlying business that the application team supports.

A business-aligned application security specialist would maintain a critical watchlist of applications that require oversight and guidance, ensure that application development teams are aware of security guidelines and requirements, advocate security improvements in the application lifecycle, scope and schedule assessment activity, verify that third-parties used in the business follow application security guidelines, assist in incident response, and perform application security assessments and coordinate with other internal and external testing resources.

Where an organization cannot support a dedicated application security specialist, cross-

training information security and application development staff on the ground is an acceptable alternative. A developer with interest in security combined with a general information security specialist with some technical skill can make a strong combination when it comes to assessment and remediation.

At the enterprise level, there should be an application security head that will oversee the application security specialists, encourage reuse and economies of scale and scope of the application security teams, produce metrics and measure the success of the application security program, set standards and guidelines for application security assessment and development methodologies, and work with the larger information security community internal and external to the enterprise.

5. SCOPING IS CRITICAL, SO GET EVERYONE TO THE TABLE

(GET THIS WRONG, AND YOU'VE JUST WASTED THOUSANDS OF DOLLARS.)

One of the most difficult phases of application security assessment is scoping. When you get this phase wrong, the results are at best meaningless and at worst provide a false sense of security. In order to get accurate and risk-aligned scoping for a given test, you need the application owner, a development representative, an information security representative, and an application security specialist to work together to define the test parameters.

- The application owner will be responsible for clearly stating the purpose of the application and how it is used. The owner is also responsible for engaging deployment and operations staff to assist the testing team.
- The development representative can answer detailed questions about how the application is architected and what the deployment environment looks like.
- The information security representative should give the testing team direction on what risks are relevant to the given application and what policies and guidelines the application is bound to.
- The application security specialist should delve into the nature of the application with the source material from the other three representatives and design a test plan that meets the assurance requirements.

Questions about the use of quality assurance or pre-production environments, number of test accounts, use cases, testing restrictions, access to source code, and other pertinent issues can be addressed at this point. At the end of the scoping phase, a document should be produced by the application security specialist that outlines the scope of the assessment, including what application functionality will be tested, the test approach, requirements to start the test, and what the deliverable will look like. If the application security specialist is not performing the test, he or she will confirm the scope with the testing team.

6. ENGAGE INTERNAL AND EXTERNAL APPLICATION SECURITY ASSESSMENT TEAMS

(BUT ENSURE THAT THE RESULTS FIT THE METHODOLOGY AND CAN BE MEASURED.)

After the approach has been defined, the first few engagements will set the precedent for the future of the assessment exercise. It is important to introduce a quality assurance checkpoint as the completed assessments start to come in to make sure the approach is being followed and where changes may need to be made in either the methodology or the assessment team.

As a result, it is recommended that the assessment program does not engage in too many

concurrent assessments at the beginning. Instead, attempt to collect assessments from a select group of well-established providers with different types of applications and deployment environments to determine how effective the methodology and metrics truly are. If you can find "security friendly" application teams in your organization, you might want to start with them first.

7. OBTAIN FUNDING

(NOT JUST FOR ASSESSMENT, BUT ALSO FOR REMEDIATION, IN THE SAME BITE.)

Security programs that only attempt to see how deep or wide the problem is without also attempting to correct the issue often find it difficult to gain acceptance among stakeholders outside of the security program. There is also an advantage of "striking while the iron is hot." If an incident has raised awareness about application security, interest may cool while you are waiting for assessment results.

A good rule of thumb is that remediation work will cost at least as much as the assessment work. By obtaining remediation funding up front, it may also be used as an incentive for application owners who fear yet another assessment without any means or budget to remediate issues that are found. Depending on the level of acceptance of uncertainty in the budgeting process, it may be advantageous to set a "not-to-exceed" remediation cost for each application. Where application fixes would exceed that amount, a separate funding case could be put forth.

Remediation funding can include short-term as well as longer-term solutions. Examples of short-term solutions include temporary deployments of Web application firewalls or other filters and development and documentation for input validation libraries. Longer-term solutions may include upgrades for legacy application frameworks and additional consulting or development resources to remediate issues.

8. REVIEW DEVELOPMENT LIFECYCLE AND VENDOR MANAGEMENT PROCESSES

(THIS BRINGS LASTING CHANGE.)

No one starts out building an application with the thought that it should lack sufficient security. Instead, the application builder uses the toolset and patterns that they are familiar with and are instructed to use by policy and process.

The problem is often that existing processes and controls do not sufficiently take security requirements into account or are flexible enough for application models with varying degrees of complexity or risk. By reviewing development practices and testing requirements, an application security specialist can look for opportunities to include security requirements during the design phase of the application and testing practices during the acceptance and implementation phases.

Two application security maturity models, OpenSAMM http://www.opensamm.org/ and BSIMM http://www.bsi-mm.com/, have been recently released to help perform an assessment of your existing development lifecycle and build a roadmap of where you need to go. OpenSAMM is particularly useful in determining levels of effort required for program improvements, and the BSIMM model is built from real application security program experiences which can be helpful in demonstrating that other companies are doing the same type of thing.

Also, if you looked at Microsoft's Secure Development Lifecycle (SDL) in the past and found it too detailed or focused on product development, look again at their SDL Optimization Model http://msdn.microsoft.com/en-us/security/dd221356.aspx, which is a streamlined version of the first revision with a useful self-assessment guide. Both SDL models are aimed at development

organizations and you may find discussion on risk management and assurance lacking.

In the case of third-party applications, alignment with vendor management and procurement practices can yield positive results. By performing a risk assessment prior to contract approval (or even during vendor selection), the application security team can provide the necessary security criteria and assurance requirements.

9. DON'T FORGET ABOUT DETECTION AND RESPONSE CAPABILITY

(BREACHES WILL HAPPEN AGAIN, AND THE COST WILL BE HIGHER IF YOU'RE UNPREPARED.)

Unfortunately, despite the best efforts made by application and security teams alike, breaches will continue to occur. However, the impact of any given breach can be reduced if there is an adequate audit trail of application activity and a skilled responder who can assist the application team in forensics and root-cause analysis.

Some institutions have implemented Web application firewalls in monitoring mode only or leveraged other types of monitoring technologies to keep track of external untrusted access to Web applications over the Internet. However, it is always best to have the application generate meaningful log entries that can be used to re-create an attacker's interaction with the application. There are frameworks available that outline security logging requirements that should be evaluated during application design.

Another role of the application security specialist can include assistance during an incident, including determining the original application flaw used during the breach, recommendations on immediate fixes to prevent further exploitation, and review of log and audit trail activity.

Application security is a tough problem to tackle during times of relative calm, but when an incident takes place, both opportunities and challenges arise. Establishing an assessment program, putting together appropriate metrics, addressing development lifecycle issues, and putting specialists in place can have a lasting impact on the enterprise and help reduce the frequency and cost of breaches in the future.

Cory Scott is a director at Matasano Security, an independent security research and development firm that works with vendors and enterprises to pinpoint and eradicate security flaws, using penetration testing, reverse engineering, and source code review. Prior to joining Matasano, he was the vice president of technical security assessment at ABN AMRO/Royal Bank of Scotland. He also has held technical management positions at @stake and Symantec. He has presented at Black Hat Briefings, USENIX, and SANS, and leads the local Chicago OWASP chapter. Send comments on this article to feedback@infosecuritymag.com.

Your One Stop Shop for All Things Security

Nowhere else will you find such a highly targeted combination of resources specifically dedicated to the success of today's IT-security professional. Free.

IT security pro's turn to the TechTarget Security Media Group for the information they require to keep their corporate data, systems and assets secure. We're the only information resource that provides immediate access to breaking industry news, virus alerts, new hacker threats and attacks, security standard compliance, videos, webcasts, white papers, podcasts, a selection of highly focused security newsletters and more — **all at no cost.**

Feature stories and analysis designed to meet the ever-changing need for information on security technologies and best practices.

INFORMATION SECURITY®

www.SearchSecurity.com

Breaking news, technical tips, security schools and more for enterprise IT professionals.

SearchSecurity.com

www.SearchSecurity.com

Learning materials geared towards ensuring security in high-risk financial environments.

SearchFinancialSecurity.com

www.SearchFinancialSecurity.com

UK-focused case studies and technical advice on the hottest topics in the UK Security industry.

SearchSecurity.co.UK

www.SearchSecurity.co.UK

Information Security strategies for the Midmarket IT professional.

SearchMidmarketSecurity.com

www.SearchMidmarketSecurity.com

Technical guidance AND business advice specialized for VARs, IT resellers and systems integrators.

SearchSecurityChannel.com

www.SearchSecurityChannel.com

TechTarget®
The IT Media ROI Experts

Smaller public companies bear significantly higher pain in terms of revenue and costs per employee complying with Sarbanes-Oxley.

DISPROPORTIONATE PAIN

BY NEIL ROITER

MENTION THE SARBANES-OXLEY ACT (SOX), and the conversation is likely to steer toward giant multinational corporations and the need for broad and deep governance, risk and compliance (GRC) programs, and the chilling image of CEOs and CFOs doing the Enron perp walk. SOX forced many of these companies to re-examine and overhaul their financial controls and accounting systems, file all sorts of new reports, and pay tons of cash to the Big Four audit firms.

But thousands of smaller public companies are the ones feeling most of the pain. The cost of SOX compliance is disproportionate for these companies, both in terms of percentage of revenue and cost per employee, in some cases running into the thousands of dollars per head, as opposed to the hundreds for large enterprises.

"Larger companies have been built to have audits going on frequently. They are complex, so they have compliance programs," says Ed Moyle, a manager with CTG's information security solutions practice and partner at SecurityCurve. "That's where the bigger costs come in. Smaller companies have been focused on growing revenue, not focused on a compliance program, and it's very costly to retrofit."

SOX put a real burden on smaller firms. There were anecdotal reports of some companies

delaying or even shelving plans to go public because of it. More strikingly, Kiplinger reported in 2006 that 100-200 companies—including some big names—were reverting to private ownership each year since SOX was enacted in 2002, mainly because of the cost of compliance.

Developing an efficient SOX compliance program is the key for midmarket companies. The right approach can help cut unnecessary costs and give your company the most benefit from improved financial controls and the insight gained from examining your practices and monitoring your systems.

But it's still going to cost you, and, if you are a smaller company, it will cost proportionately more than large enterprises. It's unavoidable.

"You still have to comply and there's a lot of bureaucracy in compliance and you can't spread the cost across as much of a base," says Michael Rasmussen, president of Corporate Integrity. "So, there's still all the overhead of a larger company. While it does scale down some, it doesn't scale down proportionately."

SEC GRANTS 'RELIEF'

The Security and Exchange Commission (SEC) took note of the basic inequity of holding smaller firms to the same requirements as mega-corporations, and issued new guidelines in 2007. The SEC delayed initial compliance for companies with less than $75 million in public equity and reduced some of the forms and reports required.

WHO IS IN CHARGE?

CFO at Top of SOX Org Chart

Expert say an organization's chief financial officer usually runs SOX compliance; audits erase the possibility of conflicts of interest.

YOUR CHIEF FINANCIAL OFFICER (CFO) is almost certain to be the person in charge of SOX compliance. Michael Rasmussen, president of Corporate Integrity, goes so far as to say it must be the CFO. In smaller companies, it's common for IT to report to the CFO; it's natural for finance and IT to come together under the CFO for SOX compliance. The CFO, he says, should "roll up his sleeves" and get involved in managing SOX compliance, because it's fundamental to his job.

Doesn't that raise the possibility of conflict?

"No," Rasmussen says. "That's why you have audit. Let the auditor be the independent validator."

SecurityCurve's Ed Moyle and Diana Kelley agree that SOX responsibility typically falls to the CFO, although conditions vary from firm to firm. The CFO understands the company's operations, the communications channels and can make sure the controls aren't interfering with the business.

"However, I'd caution small companies for collusion purposes," says Kelley. "If the CFO is the one doing anything funky with the books, that puts them in oversight of what's going on with IT checks and balances. So the COO–or the CEO if he serves operationally–should be observing." ›

–NEIL ROITER

These companies did not have to include a management assessment of their financial controls in their annual report until the fiscal year ending December 15, 2007 or later, and don't have to include an external auditor's attestation until the report on the fiscal year ending December 15, 2009 or later. What's more, companies going public don't have to begin compliance reporting until their second year as a public company.

The fresh SEC guidelines, [http://www.sec.gov/rules/interp/2007/33-8810.pdf] the "Interpretive Guide for Management," issued in May 2007, were designed to give smaller businesses clearer direction—there is no instruction manual for SOX 404—on how to implement and maintain a compliance program to cut cost and make the management assessment program more effective. The CliffsNotes version is available in a brochure, "Sarbanes Oxley Section 404: A Guide for Small Business" [http://www.sec.gov/info/smallbus/404guide.pdf] but after digesting that you'll need to get very familiar with the full document.

The guidelines stress that your management processes aren't bound by any one method or that of your external auditor. You should also take a risk-based approach that focuses on the areas of highest risk of "material misstatement" in your financial statements. This point actually goes a long way to reduce the scope of your program. Previously, companies were expected to address all areas of risk; now they can zero in on the ones that really count. Finally, your evaluation can be customized for your company's specific facts and circumstances—one size doesn't fit all, especially for small companies with their businesses processes, perhaps specialized markets or services and management structure.

> "With clarification comes some relief, but it's still a burden on the organizations. That's not going away."
>
> –MICHAEL RASMUSSEN, president, Corporate Integrity

The guide also provides better direction on appropriate supporting evidence and documentation, and for evaluating weaknesses in your controls. The guidelines do not replace internal control frameworks to be followed, particularly Committee of Sponsoring Organizations of the Treadway Commission (COSO), which is the generally accepted framework for SOX (COSO expanded its original 1992 framework in 2004, with "Enterprise Risk Management—Integrated Framework").

However, Corporate Integrity's Rasmussen sounds a note of caution, lest you expect too much from these guidelines.

"With clarification comes some relief, but it's still a burden on the organizations," he says. "That's not going away."

YOUR SOX AUDITOR

The Big Four—Deloitte Touche Tohmatsu, PricewaterhouseCoopers, Ernst & Young and KPMG—have created a whole industry around SOX compliance, hauling in most of the fees.

But if you're a smaller public company, that doesn't have to include you.

The upside of hiring one of these giants is their extensive expertise and vast resources in all matters SOX. If they're good enough for Humongous International, they must be good enough for you, right?

Not necessarily. The Big Four will, naturally, send their sharpest and most experienced

auditors to work with their biggest clients; it just makes good business sense to focus your best service on the clients paying the most bucks. Not to mention that if a company does have a rough audit, better it be a mom-and-pop shop than some high-profile, multibillion corporation.

For the same steep fee, your $25 million or $50 million company is more likely to get a bright, eager and very inexperienced auditor, perhaps a year or two out of college. That person may have graduated at the top of his or her class, and have a good grasp of the regulation and guidelines, but little or no understanding of the business you run, its operational and sales practices, and the market in which it is engaged.

If your company is new not just to SOX, but *any* regulatory requirements, you're going to want an auditor you can draw on for advice and guidance, not just to pass or fail on your controls.

"Where these auditors don't have the knowledge is on the operational side. So they may understanding the compliance process, but when it comes to understanding the business and how financial systems work and how they interrelate, there's a dearth of knowledge."

–ED MOYLE, manager information security solutions practice, CTG; partner, SecurityCurve

"Where these auditors don't have the knowledge is on the operational side," says Moyle. "So, they may understanding the compliance process, but when it comes to understanding the business and how financial systems work and how they interrelate, there's a dearth of knowledge."

One result can be a near-fanatic focus on every possible level of every control, rather than focus on evaluating the effectiveness of key controls over areas of greatest risk. Diana Kelley, co-founder and partner at SecurityCurve, tells of the security director at a brokerage house whose auditor was fixated on the fuel supply for the backup generators for her data center.

"The data center had propane to fuel their backup power, but no backup for the propane," she relates. "And the auditor dinged her on that for SOX. It's a case of running down every possible check box without understanding compensating controls and other methods for providing resiliency."

Part of the problem is that SOX 404 and the guidelines are sufficiently vague to give audit firms a lot of leeway, and the wider the scope of the engagement, the more money they can charge. That's why it's important to work in close collaboration with your auditor early on in the compliance process and reach some understanding of the focus points and scope of the engagement.

"Auditors must be held in check," says Rasmussen. "They want to work very broadly because it means more work for them. Work with them and say, 'what can we come to agreement on; let's scope this together and come to some understanding.'"

The aim, Rasmussen explains, is to understand what the auditor is looking for, and getting him to sign off on a control structure that's reasonable for your company, "that's not going to just bury it."

You should also involve the auditor early because of the "break" small companies get in not being required to have auditor attestation until year two of compliance. Your man-

agement assessment can easily go awry the first year without an understanding with your auditor, and you can get badly bloodied when the auditor comes in later on.

Auditors aren't the only ones responsible for runaway scope. Sometimes IT managers use SOX as a pretext for pushing through pet IT or security projects that the CFO has turned down based on previous arguments.

In addition to getting the auditor involved up front, hiring an outside consultant makes sense at the outset. If your management team lacks SOX expertise and experience, or if they simply have too much to do helping run the business, a consultant can help you make good choices—including the right audit firm—and avoid costly mistakes.

Rasmussen advises small public companies to steer clear of the Big Four, because they are likely to get relatively inexperienced people. He says small companies will get better

RESOURCES

Help Available

There are many online resources that can help midmarket companies with Sarbanes-Oxley compliance.

Unified Compliance Framework

http://www.unifiedcompliance.com/

Provides "toolkits" that help build a compliance program that maps to any number of regulations.

SOX-Online

http://www.sox-online.com/

Independent source of information on SOX, COSO, COBIT, the SEC and the Public Company Accounting Oversight Board (PACOB).

COSO

http://www.coso.org/

Independent source of information on SOX, COSO, COBIT, the SEC and the Public Company Accounting Oversight Board (PACOB).

COSO

http://www.coso.org/

A source of information and documentation on the generally accepted framework for SOX; includes useful, including a very useful SOX guidance document for small public companies http://www.coso.org/Publications/erm_sb/sb_executive_summary.pdf.

BIG FOUR AUDITORS

Audit companies offer white papers and other resources that help with SOX compliance. For example, Deloitte has a very useful document for small companies http://www.deloitte.com/dtt/cda/doc/content/us_sarbanes_NAF%20013108.pdf.

service and consistency with any number of the smaller, local audit companies that cater to SMEs and actually like doing business with smaller clients. He also suggests investigating mid-tier companies such as Jefferson Wells, Grant Thornton, BBO Seidman and Crowe Horwath, among others.

MORE THAN SOX?

Your company may be on the small side, but you still may have to deal with more than one regulation. For example, if you take credit cards, you also have to deal with PCI DSS. If you're a financial services company, you're probably subject to GLBA. And just about every company must be leery of the 40-plus state data breach disclosure laws. Even if you're only subject to SOX now, it's a good bet that a year, or two years or five years from now, there will be other regulations that you'll have to deal with.

> "There's a common infrastructure of controls that can be used for multiple compliance purposes."
>
> –MICHAEL RASMUSSEN, president, Corporate Integrity

Rasmussen says redundant multiple assessment programs are often "what's burying organizations, large and small." You'll have hundreds of spreadsheets and questionnaires, often covering the same data and asking the same questions. GLBA, for example, involves identity and access controls around personal information, while SOX is going to be dealing with identity and access controls and separation of duties.

"There's a common infrastructure of controls that can be used for multiple compliance purposes," he says.

Better to develop a compliance program from the start, with a broad base of meta controls that you can map to particular requirements as they come along. Then you can fill the gaps as a particular regulation requires.

"Be prepared for compliance, not just SOX," says Kelley. "It's going to be a painful investment if you haven't been compliance aware. Do you want to spend that money heavily every time there is a new mandate?"

Neil Roiter is senior technology editor for Information Security. *Send comments on this article to feedback@infosecuritymag.com.*

ADVERTISING INDEX

TECHTARGET SECURITY MEDIA GROUP

INFORMATION SECURITY®

EDITORIAL DIRECTOR Kelley Damore

EDITOR Michael S. Mimoso

SENIOR TECHNOLOGY EDITOR Neil Roiter

FEATURES EDITOR Marcia Savage

ART & DESIGN
CREATIVE DIRECTOR Maureen Joyce

COLUMNISTS
Jay G. Heiser, Marcus Ranum, Bruce Schneier

CONTRIBUTING EDITORS
Michael Cobb, Eric Cole, James C. Foster, Shon Harris, Richard Mackey Jr., Lisa Phifer, Ed Skoudis, Joel Snyder

TECHNICAL EDITORS
Greg Balaze, Brad Causey, Mike Chapple, Peter Giannacopoulos, Brent Huston, Phoram Mehta, Sandra Kay Miller, Gary Moser, David Strom, Steve Weil, Harris Weisman

USER ADVISORY BOARD
Edward Amoroso, AT&T
Anish Bhimani, JPMorgan Chase
Larry L. Brock, DuPont
Dave Dittrich
Ernie Hayden, Seattle City Light
Patrick Heim, Kaiser Permanente
Dan Houser, Cardinal Health
Patricia Myers, Williams-Sonoma
Ron Woerner, TD Ameritrade

SEARCHSECURITY.COM
SENIOR SITE EDITOR Eric Parizo

NEWS EDITOR Robert Westervelt

ASSOCIATE EDITOR William Hurley

ASSISTANT EDITOR Maggie Wright

ASSISTANT EDITOR Carolyn Gibney

INFORMATION SECURITY DECISIONS
GENERAL MANAGER OF EVENTS Amy Cleary

EDITORIAL EVENTS MANAGER Karen Bagley

VICE PRESIDENT AND GROUP PUBLISHER
Doug Olender

PUBLISHER Josh Garland

DIRECTOR OF PRODUCT MANAGEMENT
Susan Shaver

DIRECTOR OF MARKETING Kristin Hadley

SALES MANAGER, EAST Zemira DelVecchio

SALES MANAGER, WEST Dara Such

CIRCULATION MANAGER Kate Sullivan

ASSOCIATE PROJECT MANAGER
Suzanne Jackson

PRODUCT MANAGEMENT & MARKETING
Corey Strader, Jennifer Labelle, Andrew McHugh

SALES REPRESENTATIVES
Eric Belcher ebelcher@techtarget.com

Neil Dhanowa ndhanowa@techtarget.com

Patrick Eichmann peichmann@techtarget.com

Jason Olson jolson@techtarget.com

Jeff Tonello jtonello@techtarget.com

Nikki Wise nwise@techtarget.com

TECHTARGET INC.
CHIEF EXECUTIVE OFFICER Greg Strakosch

PRESIDENT Don Hawk

EXECUTIVE VICE PRESIDENT Kevin Beam

CHIEF FINANCIAL OFFICER Eric Sockol

EUROPEAN DISTRIBUTION
Parkway Gordon Phone 44-1491-875-386
www.parkway.co.uk

LIST RENTAL SERVICES
Kelly Weinhold
Phone 781-657-1691 Fax 781-657-1100

REPRINTS
FosteReprints Rhonda Brown
Phone 866-879-9144 x194
rbrown@fostereprints.com

TechTarget
The Technology Media ROI Experts

INFORMATION SECURITY (ISSN 1096-8903) is published monthly with a combined July/Aug., Dec./Jan. issue by TechTarget, 117 Kendrick St., Suite 800, Needham, MA 02494 U.S.A.; Phone 781-657-1000; Fax 781-657-1100.