The ISSA Journal

October 2009
Volume 7 Issue 10

ISSA Founders
Nancy King
and Sandra Lambert

CELEBRATING 25 YEARS

The Shift Toward Enterprise 2.0

WEB 2.0 TECHNOLOGIES BRING BENEFITS AND CHALLENGES TO THE ENTERPRISE, AND CSOs MUST MANAGE THIS TRANSFORMATION IN A SECURE AND EFFICIENT WAY.

CSOs are both eager and cautious about bringing Web 2.0 tools into the enterprise and transitioning to an Enterprise 2.0 environment.

On the positive side, community-building networking applications and services can effectively link customers, suppliers, partners, and employees for fast and easy collaboration, which can quickly lead to greater productivity, effective data sharing, visibility into business processes, and ideally, improved profitability.

But on the flip side, Web 2.0 technologies come with myriad risks: business-inappropriate content or applications finding their way on to company computers, the increased possibility of viruses, worms, and malware, and accidental or malicious data loss.

Enterprises are still exploring the best uses of Web 2.0. **Corporate sales and marketing departments have taken the lead, using social applications to enhance customer relationships, attract new audiences, and heighten brand awareness.** For example, Dell offers a community network that provides communication forums, idea centers, blogs, and feeds that keep visitors informed, as well as provides opportunities to learn, participate, and collaborate.

Other organizational departments are taking advantage of Web 2.0 as well. For example, IT departments have created internal wikis and blogs to keep employees up-to-date with company information and allow for easy communication.

ENTERPRISE 2.0 CHALLENGES

Even though Web 2.0 has many advantages, it still poses significant risks. The network perimeter is no longer a building with walls and network cables, and securing it is becoming as difficult as defining it. Users now demand anytime access from anywhere, using laptops, remote kiosks, and PDAs to access corporate information. So if you're sitting at a coffee shop accessing webmail, communicating with friends, and updating your blog, are you inside or outside the company network?

Although most organizations have established standard protections such as email filters, firewalls, and virus signatures, **the ingenuity of hackers means that viruses, worms, and malware take on new shapes and infiltrate in new ways.**

Since many Web pages and sites can no longer be classified as simply "good" or "bad," reputation is unreliable as an indicator of threat potential. For example, Google may be trustworthy in and of itself, but users who build their own iGoogle portals with content coming from non-Google sites are beyond the hosting site's control.

These challenges may lead some people to believe that Web 2.0 should be banned in the workplace. Realistically, this is nearly impossible. Due to the increasing use of mobile devices, cloud computing, software-as-a-service models, and customer portals, Enterprise 2.0 is inevitable.

The new approach is to say "Yes" to Web 2.0 as a way of empowering employees to be more technologically efficient, and encouraging the Employee 2.0 mentality. The trick is to combine Web 2.0 technologies with the appropriate security measures, including a secure Web gateway for visibility and control of Web traffic.

Experts agree that a secure Web gateway can help you gain visibility and control of inbound and outbound Web traffic. Learn what to look for in a secure Web gateway by downloading A Competitive Guide to Selecting Secure Web Gateways now at www.websense.com/issa-swg

websense®
ESSENTIAL INFORMATION PROTECTION™

Table of Contents

Feature

Articles

Also in this issue

Cover photo and photos on pages 10-12: Rafael Guajardo of Rafael Photography.

The ISSA Journal (1949-0550) is published monthly by the Information Systems Security Association, 9220 SW Barbur Blvd. #119-333, Portland, Oregon 97219. **Postmaster**: Send address changes to ISSA Journal, 9220 SW Barbur Blvd., #119-333, Portland, Oregon 97219.

Welcome to the October Journal

Thom Barrie – Editor, the ISSA Journal

The big news around here is that starting in November the *ISSA Journal* will be going to all-electronic delivery. The format will remain exactly the same – 48-page, interactive, online magazine – and will be integrated into the ISSA website through ISSA Connect, available the first day of the month. You can read it online or download the full issue or individual articles to read on the go. The articles will also be available in text-only format through eNews and ISSA Connect. In Connect you will be able to start or join discussions on articles with members throughout the association. Think letter to the editor but in real time, not an issue or two later. Or start a discussion with the author if he or she is an ISSA member, and most are! What's more, you will be able to search the online *Journal* and archives for the information you want, when you want it.

While the monthly print version will no longer be produced, the plan is to twice a year come out with a printed *Best of the ISSA Journal*, which as its name implies would feature the best articles from the previous half a year. And you can let us know which articles they would be! (Authors, you only get one vote!) In the Journal community of ISSA Connect, you can communicate directly with the Editorial Advisory Board, letting us know which articles were the best (or worst - keep us accountable). You can also submit article and topic ideas, letting us know what things you want to read about.

It's been a great 25 years, ISSA. And I think you'll agree, it looks like the years ahead will be even better!

– *Thom*

CELEBRATING 25 YEARS ISSA®
Information Systems Security Association
CONNECT. LEARN. ADVANCE.

Headquarters ISSA Inc.
9220 SW Barbur Blvd. #119-333, Portland, OR 97219
Toll-free: 866 349 5818 (USA only)
Seattle local : +1 206 388 4584 • Fax: +1 206 299 3366 • www.issa.org

ISSA – THE PREEMINENT TRUSTED GLOBAL INFORMATION SECURITY COMMUNITY

The Information Systems Security Association (ISSA)® is a not-for-profit, international organization of information security professionals and practitioners. It provides educational forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.

With active participation from individuals and chapters all over the world, the ISSA is the largest international, not-for-profit association specifically for security professionals. Members include practitioners at all levels of the security field in a broad range of industries, such as communications, education, healthcare, manufacturing, financial and government.

The ISSA international board consists of some of the most influential people in the security industry. With an international communications network developed throughout the industry, the ISSA is focused on maintaining its position as the preeminent trusted global information security community.

The primary goal of the ISSA is to promote management practices that will ensure the confidentiality, integrity and availability of information resources. The ISSA facilitates interaction and education to create a more successful environment for global information systems security and for the professionals involved.

Hello ISSA members

Howard A. Schmidt, ISSA International President

Our 25th Anniversary Gala celebration was a grand event. We looked back over all the years, sharing stories of the early days, and we looked forward to what is in store as we position ourselves for the road ahead.

Starting with a handful of folks in California, ISSA has grown to nearly 10,000 members strong throughout 70 countries across the globe. It started with an idea that Sandra Lambert and Nancy King determined to bring to fruition. Could they have even imagined the scope and impact of that vision as it has spread across the globe! It was a great pleasure to honor these two founding members during our celebration.

I would like to acknowledge and welcome our new and returning International Board members who will be leading our association's next steps: Candy Alexander, Debbie Christofferson, Frederick Curry, Pamela Fusco, Andrea Hoy, Pete Lindstrom, Owen O'Connor, Kevin Richards, Brian Schultz, Scott Williams, Ira Winkler, and Stefano Zanero.

And with every new board installation, there are those retiring members whose passion and dedication were amply felt and will be greatly missed: Dave Cullinane, Bill Danigelis, Vernon Williams, and Ernest Zernial. Thank you for your excellent service to the association.

These years have seen tremendous growth and development in our organization and the profession we serve. You could say the information security profession has arrived. No longer an afterthought, our industry stands at the forefront, protecting the open flow of information while securing enterprise systems, government systems, and the global Internet marketplace from those that would do us harm.

We must ensure security professionals have the tools and access to the information necessary to protect these systems from increasingly sophisticated criminal attack, and we believe the best way is through collaboration with other professionals. We are now standing on the brink of a new ISSA in which our members – where ever they are – will have interconnectivity and association with each other on an unprecedented level.

ISSA Connect, rolled out during our anniversary celebration, will do just that: interactive communication with ISSA members, anywhere, any time. Now the great interaction you enjoy at the local chapter level will be expanded throughout the association. Just go to the ISSA website and get started. (See ISSA Connect on page 15)

We also announced the creation of the ISSA Fellowship Program, which will provide the information security profession progressive markers of significant professional achievement. The Fellowship categories consist of Senior Member, Fellow, and Distinguished Fellow. See page 12 for the inaugural group of Senior Members and Distinguished Fellows. Thank you to Vern Williams and Pam Fusco for their leadership in this program.

If you ask me about the benefits of ISSA membership, and there are numerous, first and foremost would be the connections I have made throughout the years, the great folks I have worked with at the international board level, at the local chapter level, and across the association. ISSA members are my colleagues, and they are my friends, as they are with you as well. We are resources to draw upon when problems need solving, and ISSA Connect will help solve even more.

Until next month…safe computing,

Howard A. Schmidt
ISSA International President

Using the Popular Press

By Branden R. Williams – ISSA member, North Texas, USA Chapter

The popular press is kind of like a squirrel – always searching for nuggets yet lacking attention span. If you saw *Up* this summer, think of Dug. Find the biggest story to one up my competition and get the exclusive to – SQUIRREL!

Longtime professionals know that security is a long-term process. There is no security light switch to toggle – it cannot be done overnight. In fact, unless a major overhaul in the culture and attitude toward information security occurs, companies tend to revert back to their pre-breach lifestyle. I've witnessed a laser focus on security blur to a beam you might find emanating from that flashlight you keep for emergencies, but never seem to remember to change the batteries: weak, unfocused, and not painful to shine directly in – SQUIRREL!

The popular press[1] needs negativity. They need it so badly that good news stories are derided and called *fluff* pieces. Real news must have a bad guy or bad event behind it. The treatment of information security in the popular press mimics this same attitude. Don't expect Brian Williams to talk about how great we're doing securing data because we've been breach-free for many months.

The press has been involved in security for a long time, but not always reporting breaches. If you were alive during World War II (or if you paid attention during history class), you might remember phrases like "Loose Lips Might Sink Ships," "Defense On The Sea Begins On The Shore," and "Defense In The Field Begins In The Factory." If this was not the first time that the country organized an information security movement on a large scale, it certainly was one of the most significant. These slogans were designed to remind people that any information about troop movement can give the enemy valuable information to mount an attack. While these slogans were created by the U.S. government, they were widely reported in the media.

The media reports mostly on breaches or big security violations or scandals today. Usually for the popular press to get involved, something bad either has already happened (like when dealing with a breach), or is about to happen (like when dealing with a virus or trojan horse). In either case, the popular press can be quite useful!

The popular press aims to incite action in individuals when discussing events that are about to happen. Confickr created quite a stir this year, and the media helped get the word out. Larger businesses generally have staff to assist with impending threats, and in most cases they do a really good job at preventing major impact to the business. Small businesses typically do not.

Imagine yourself finally quitting the rat race to start a photography business. You have a $20,000 investment to make in your business, and you know at least one computer is going to be part of that. Modern photographers use computers to edit their work, create value added offerings like DVDs, enable online ordering systems, and manage finances. What they don't typically do is add extra security to their networks, encrypt their sensitive files, and monitor the overall security posture of these systems. Users without constant support will suffer the most from security events on the horizon. The media helps to get the word out, inciting them to act.

When the media reports on events that have already happened, it provides useful information about the breach, legal and financial ramifications of the breach, what consumers can do to get assistance if their information is stolen, and makes examples out of the breached and the attackers (if they are caught).[2] Information security is a relatively young science, and has only dealt with mass adoption in the private sector after companies connect themselves to the Internet (again, in many cases). This information is tremendously useful to small and large businesses alike when reviewing their risk management process and to learn vicariously though another company's mistakes.

The challenge with the media is dealing with the – SQUIRREL – problem and discovering and managing the influx of information in a reliable manner. Remember, not all experts are ACTUALLY experts, and in this business people are quick to offer their opinions on the facts, especially if they don't know the facts (because the ones that do are typically bound by confidentiality agreements).

Use the popular press as one of the many tools in your arsenal to defend against hackers.

About the Author

Branden R. Williams, CISSP, CISM, is the Director of the PCI Consulting Practice at VeriSign and regularly assists top global retailers, financial institutions, and multinationals with their information security initiatives. Read his blog or reach him directly at http://www.brandenwilliams.com.

1 For the purposes of this article, the term "popular press" does not include information security related publications.

2 The TJX Companies breach is a fantastic example of this. There is almost too much information to digest on their breach.

A Key Player in the History of Information Security: Lt. Gen. Minihan

By Randy V. Sabett – ISSA member, Northern Virginia, USA Chapter

Breaking from my usual format, I thought I would get the perspective of an information security veteran. Gen. Ken Minihan is the former director of the NSA. Following his tour as DIRNSA, he moved into the venture capital arena as managing director at Paladin Capital Group. Gen. Minihan focuses on investing in companies that fit the profile of Paladin's Homeland Security Fund. I asked him recently what people in the ISSA community should be thinking about.

You have been involved in cybersecurity for almost 30 years. What changes do you think have been most significant during this time?

The changing nature of both the Internet and the threat vectors have caused a significant shift in the focus of cybersecurity. Previously, only the U.S. government needed to worry about protection of its systems. With over 85% of U.S. critical infrastructure in the hands of the private sector, the threats being posed by a multitude of actors have altered the landscape. Ultimately, three changes are quite significant. First, the intelligence community is beginning to recognize the structured nature of emerging threats, rather than the unstructured nature of past threats. Second, shared opportunities potentially exist amongst stakeholders resulting from the recognition of shared threats. Finally, there is a realization of the broad, strategic nature of current and future cyberthreats, rather than the more tactical, niche types of previous cyberthreats. All of these changes must guide our country's response.

The President has declared cybersecurity a national priority. Will things change significantly in the near term?

With the release of the Cyberspace Policy Review and the attention being paid to cybersecurity by Congress, enough momentum hopefully has been generated to bring our country to a point where there will be appropriate follow through. Unfortunately, not everything related to cybersecurity has worked well. A well-integrated team needs to be built that will allow an orchestrated response to cybersecurity threats. In effect, the government needs to get all four wheels on the ground and going at the same speed.

From an investment perspective, where should companies that provide cybersecurity products and services concentrate their efforts?

At Paladin, we focus on dual-use technologies. Specifically, we don't look at what I would call "gadgets." We look to fund companies that have technology solutions that can show success in both federal and commercial markets. Government requirements may drive the process, but companies need to provide solutions that will address government requirements and offer commercial opportunities. For both us and the company, this type of strategy mitigates risk over the long term.

The difference between "gadgets" and "solutions" seems to indicate that point solutions are not necessarily doomed. Would you agree and how would you advise companies to do that?

In addition to making sure that a technology solution has commercial and governmental applicability, companies should figure out very early on with what other companies they should partner. Having a long-term plan that contemplates strategic relationships with other, bigger players can go a long way to making sure a cybersecurity company has viability, particularly since the technologies are constantly changing.

Switching gears, what advice would you give to cybersecurity professionals?

Two thoughts. First, people need to recognize that this is a tough, complex, technical business. You can't simply go through a training course. Instead, it should be viewed as a process of ongoing education where it is important to keep up with changes in the industry (including the national dialog on policy issues). Second, the broader technology industry needs to create trusting relationships between citizens and the technologies that those companies create. People should trust that the software they install on their computer will work properly and be secure. They cannot do that today. Once they can, it will significantly improve overall security.

In wrapping up our chat, Gen. Minihan mentioned one other thought: the changes brought on by the cyberthreat have led to an environment where we will "never be at peace." From a glass half empty perspective, this is scary… but as a glass-half-full kind of guy, I view this as an opportunity for our industry to shine.

About the Author

Randy V. Sabett, J.D., CISSP, is a Partner in the Internet, Communications, and Data Protection (ICDP) practice group at Sonnenschein Nath & Rosenthal LLP, an adjunct professor at George Washington University, and a commissioner for the Commission on Cyber Security for the 44th Presidency. He may be reached at rsabett@sonnenschein.com.

The views expressed herein are those of the author and do not necessarily reflect the positions of any current or former clients of Sonnenschein or Mr. Sabett.

Cloud Computing Security Concerns

By Joyce Brocaglia – ISSA member, New Jersey, USA Chapter

Cloud computing is one of the most intriguing issues on the minds of security executives today. Your company is most likely either doing business in the cloud currently or is evaluating the risks and benefits inherent with the technology. Lynn Terwoerds was a speaker on cloud computing architecture at the recent Executive Women's Forum[1] national conference held in September. She is former Head of Security Architecture and Standards at Barclays PLC and spent eight and a half years at Microsoft. Currently she is a member of the Cloud Security Alliance. I've asked Lynn to share a few top-of-mind challenges she sees with cloud computing.

If you had to name just a few top-of-mind security concerns for cloud computing, what would they be? Can you go into some level of detail for each area?

I want to make sure companies are moving to cloud computing for the right business reasons, and not just riding a wave of marketing hype. In the end, cloud computing should be a means to advance your business. For example, by leveraging the cloud, your business may be able to introduce a new product or service rapidly with considerably lower cost of entry. In order to make that possible, I would expect you to have deconstructed your solution and mapped it against security and operational controls and a risk management framework that is in line with your business needs. You should have established a common terminology and taxonomy which would allow you to report on controls in a way that shows management that they got value for the money spent and that they are internally and publicly compliant.

My second concern has to do with managing internal cross-group interdependencies and vendor management. Your company is looking at cloud computing for business reasons and not marketing hype or pure love of new cool technology. Because you will trade a lot of control for cost savings and agility, not only should you have a cross-functional team of business stakeholders helping you drive the right solutions, but you also need to have a healthy relationship with your cloud vendors. It is critical to establish well-defined roles and responsibilities to ensure this cross-functional team actually functions and delivers the right solutions to your business. With vendors, the truth is that a contract cannot cover everything. That means you must have a detailed list of the assurances you need from the vendor and be able to both leverage contracts as well as ongoing due diligence to ensure your requirements are being met. Your vendor should be able to provide third-party risk assessments and make them available to you in as much detail as reasonable. Our industry will also have to modify common third-party risk assessments so they reflect new control areas for cloud computing and highly virtualized environments. There is a lot of hard work and devil-in-the-details in this area.

Thirdly, trust relationships in the cloud require a lot of consideration because there are trust issues at multiple levels. We have already briefly covered vendor management. Because the cloud is such a leveraged model, consumers of cloud services do not know the trust boundaries between their data and other customers' data. In multi-tenant situations, how do you know your data is secure when there is no hardware separation between you and another company's data? What if the other company is your competitor? Application trust boundaries also change in the cloud and the considerations depend on whether you're using IaaS, PaaS or SaaS. For example, your applications may not have been designed to work in a shared infrastructure and do not have explicit controls to prevent the disclosure of data between hosts (because in your private network they did not traverse an untrusted network). Now the application must take on securing communications because it lives in a shared infrastructure.

While this is far from an exhaustive list, I hope to show some of the considerations needed to leverage cloud computing. If you are looking for a high level but more comprehensive security guidance, please see Security Guidance for Critical Areas of Focus in Cloud Computing published by the Cloud Security Alliance.[2]

About the Author

Joyce Brocaglia is the CEO of Alta Associates, the industry's trusted advisors specializing in information security recruiting, and the founder of the Executive Women's Forum. Joyce may be reached at www.altaassociates.com and Joyce@alta-associates.com.

1 Executive Women's Forum – www.ewf-usa.com,

2 Cloud Security Alliance – http://www.cloudsecurityalliance.org.

INSERT Ethics INTO Public Web App Testing

By Michael Starks – ISSA member, Fort Worth, USA Chapter

The ISSA Code of Ethics charges us to obey the law, promote best practices, and avoid conflicts of interest. It was designed to keep us out of trouble. It is simple to read and seems pretty straight-forward, but understanding and practicing the code on a daily basis can be another story altogether. Subtle nuances work their way into our professional lives as we weigh options, consider consequences, and look to our peers in an ongoing process of careful consideration.

It is with such consideration that I have been observing an interesting trend lately: the testing of public web application security. Security professionals test these applications for vulnerabilities and talk about what they found, usually after going through some form of disclosure process. It is clear that the tests are in most cases unauthorized and may even be illegal in some jurisdictions.

There is a long history of testing the security of applications. Nary a day goes by that we do not read about some application security issue. No one wants to be seen as a liability, so when a company is put in the spotlight for security issues, bugs tend to get fixed. Smart companies have embraced this process and even provide security contacts within their company. They then work with the researchers to make the product more robust and to keep their customers safe.

Whereas finding security bugs in an application that you download and install yourself is seen as generally acceptable, testing that same application when installed on a remote system can be seen as offensive. The basic rule of thumb has been that the good guys only test the security of systems they own or manage.

So what is one to do when wanting to perform research against applications which are only remotely-hosted? This results in a natural tension between previously established precedents. With the current trend of moving services online, we find ourselves at a juxtaposition where performing responsible[1] security research on remote systems may lead to an improvement of overall security in an increasingly connected world

Lofty intentions aside, a security analyst may see no distinction between a security professional performing a SQL injection attempt against a public web server and an attacker doing the same thing. Even if the professional has the intention of following up with an ethical disclosure process, the attempt in and of itself is unauthorized. Even the most innocent of attempts can have unintended consequences: services can crash, transactions can be corrupted, and sensitive data can be exposed.

"But wait!" say proponents of testing public web applications. If the bad guys are going to be attacking the site, how can a professional's testing with the intention of responsible disclosure be a bad thing? If it leads to improved security, does it ultimately benefit everyone? Furthermore, if an application is offered to the public, has the company abandoned an expectation of total control? In other words, should they not expect attacks and have secured the application appropriately?

Is it ethical to test the security of public web applications even if it is unauthorized? Does the intent to follow a disclosure process make it ethically palatable? Is it ethical not to test the security of an application accessible to the world, so as to keep raising the bar of protection from which we all benefit? How else can we hold those who are custodians of our information accountable? Should we take their word at face value while the bad guys attack?

As more services move online, the issue of testing public web applications will likely become more contentious. As ISSA members, we have agreed to abide by a standard of conduct, which is embodied in a code of ethics. If there is broad consensus that this is a practice not becoming of our profession, we should stand up and say so now. However, if there is a broader discussion to be had, the time to have this discussion is also now.

Regardless of the decision, one thing is clear: actions have consequences. Those involved in the practice of unauthorized web application testing may want to take a moment for reflection and consider the potential consequences, both professionally and legally.

What do you think? We want to hear from you. Please email ethics@issa.org with your thoughts.

About the Author

Michael Starks, CISSP, CISA, GSNA, is a security analyst working in Arlington, Texas. He is a founding member of the Rochester, NY chapter of ISSA and has served both ISSA and OWASP chapters in various capacities. His personal blog is at http://www.immutablesecurity.com, and he can be reached at issa-article@michaelstarks.com.

1 Responsible research usually implies that vulnerabilities are disclosed first to the software creator and only disclosed publicly after a patch has been issued or if the party declines to address them.

The ISSA International Ethics Committee is an active group of ISSA members missioned to maintain a framework for ethics relating to practices that support the ISSA Code of Ethics, provide guidance on ethical behavior for Information Systems Security professionals, and provide education and outreach that increase awareness and promote positive actions.

2009-2010 ISSA International Board

(seated, left-right) Debbie Christofferson, Andrea Hoy, President Howard A. Schmidt, Candy Alexander

(standing, left-right) Scott Williams, Secretary/Chief of Operations Pete Lindstrom, Brian Schultz, Chief Financial Officer Pamela Fusco, Stefano Zanero, Ira Winkler, Vice President Kevin Richards

(not pictured) Frederick Curry, Owen O'Connor

September 20, 2009 – Anaheim, California USA

ISSA 25th Anniversary Gala

ISSA International has reached a significant milestone as an association, reaching back to the earliest days of the information security profession. To celebrate that milestone, ISSA held its 25th Anniversary Gala in Anaheim, California on September 20th. With that many years comes a lot of history, and history begins with people, the men and women who have given of their time and talents to first give birth to the association, and then throughout the years to help it develop and grow into the global association of information security professionals it represents today. But the event was not just a time of looking back, resting on past laurels. The International Board looked forward to a vision of what's next: inauguration of ISSA Connect, transition to an all-electronic *ISSA Journal,* and the development of the ISSA Fellowship Program.

25th Anniversary Chair and International Director Debbie Christofferson (Phoenix Chapter) started the evening mentioning the "Security Star" moments that have been received from members and acknowledging the 25th Anniversary Committee comprised of Candy Alexander (New England and New Hampshire Chapters), Andrea Hoy (Orange County Chapter), Sandy Lambert (Los Angeles Chapter), Pat Myers, and Joan Rose (San Francisco Bay Area Chapter).

Introduction of the 2009-2010 International Board

International President Howard A. Schmidt introduced the 2009-2010 International Board: Kevin Richards, Vice President; Pete Lindstrom, Secretary/Chief of Operations; Pamela Fusco, Chief Financial Officer; and Directors Candy Alexander, Debbie Christofferson, Frederick Curry, Andrea Hoy, Owen O'Connor, Brian Schultz, Scott Williams, Ira Winkler, and Stefano Zanero.

Retiring board members Vernon Williams, Secretary/Chief Operating Officer; Dave Cullinane, Chief Financial Officer;

Orange County Chapter: Chapter President Al Brusewitz, International Director Andrea Hoy, and Powell Hamilton, Chapter VP.

Retiring board member Vernon Williams receiving thanks from President Howard A. Schmidt.

Debbie Christofferson, 25th Anniversary Chair and International Director; Howard A. Schmidt and Sandra Lambert.

Bill Danigelis and Ernest Zernial, Directors, were thanked for their for their excellent service to the association and were each presented with a personalized globe and pen desk set.

Schmidt gave a brief history of ISSA's beginnings with the efforts of Sandra Lambert and Nancy King in Southern California in the early 1980s and incorporation as a non-profit organization in 1984 (see *"The ISSA Story"* page 13). Since then many volunteers have continually committed themselves to the evolution of our profession by stepping forward to shape ISSA and keep us true to our mission. Each of them is a Security Star – both in professional achievements and in fostering the mission of ISSA.

Honoring Foundings and Past Presidents

Personalized "Security Stars," which were replicas of the Hollywood "Walk of Fame" Stars, were awarded to ISSA founding members and past international presidents, many of whom were present at the gala celebration:

Founders Nancy King and Sandra Lambert

International Board Presidents

1984-1985	Sandra Lambert, Los Angeles Chapter
1985-1987	Carl Jackson, South Texas Chapter
1987-1989	Harold Tipton, Los Angeles Chapter
1989-1990	Gerald Grindler, St Louis Chapter
1990-1992	Sally Meglathery, New York Metro Chapter
1992-1993	Vaune Carr
1993-1995	Genevieve Burns
1995-1996	Richard Owen, Jr., Phoenix Chapter
1996-1997	James Wade
1997-1999	Patricia Myers
1999-2002	Howard Schmidt, New England Chapter
2002	William Tompkins, Capitol of Texas Chapter
2002-2006	Dave Cullinane, Silicon Valley Chapter
2006-Present	Howard Schmidt, New England Chapter

ISSA Connect

Network. Collaborate. Learn. Excel!

Schmidt then switched gears to part of the new vision of ISSA starting with ISSA Connect: Network. Collaborate. Learn. Excel! Stepping beyond the vision of local chapters, even globally positioned local chapters, ISSA must position itself and its members to greater levels of collaboration across the association in order to address and counter the increased sophistication of the threats and challenges that face information security today – and those that do not yet exist.

ISSA Connect will utilize today's networking technology to leverage our collective experience, wisdom, and innovation through a members-only, online networking and collaboration community. ISSA members have a wide range of responsibilities and interests and need targeted networks and resources that go beyond geographic boundaries. ISSA Connect will expand the global association of local chapters to a

President Howard A. Schmidt with past presidents Sandra Lambert, Richard Owen, Sally Meglathery, Patricia Myers, Harold Tipton, and William Tompkins.

global community of interconnected and collaborative colleagues. This opportunity to interact with trusted peers and the wealth of knowledge and tangible resources that can be shared will grow exponentially. Owen O'Connor and Brian Schultz were acknowledged for their leadership in developing ISSA Connect. Go to www.issa.org and create your profile so your fellow members can tap into your unique expertise.

As part of integrating resources into ISSA Connect, the *ISSA Journal* is going all electronic – it will be instant, collaborative, and searchable (see *"ISSA Journal Goes All-Electronic Delivery"* on page 16). Bill Danigelis was acknowledged for his ongoing leadership in guiding the transition and integration of the *ISSA Journal* into ISSA Connect.

ISSA Fellowship Program

Schmidt also announced the creation of the ISSA Fellowship Program, which will provide the information security profession progressive markers of significant professional achievement. The program will encourage excellence in achievements, projects, and research and will encourage professional leadership and strategic collaboration among ISSA members.

The Fellowship categories consist of the following:

- **Senior Member** – minimum eight years in the field and six years ISSA membership
- **Fellow** – significant contributions to the profession and minimum 10 years ISSA membership
- **Distinguished Fellow** – exceptional service to the information security community and minimum 12 years ISSA membership

International Director Stefano Zanero, Italy Chapter; Dan LoPresto, Central Florida Chapter; Rene Lopez and Eric Cowperthwaite, Puget Sound Chapter; and Dan Pesserl, Motor City Chapter.

The inaugural group of Senior Members and Distinguished Fellows will be selected from the members of the ISSA Honor Roll and Hall of Fame. Six members who have accepted this call to an even higher level of service were introduced: Senior Members – Steve Haydostian, Pat Myers, and Rich Owen; Distinguished Fellows – Sandy Lambert, Harold Tipton, and William Tompkins. Vern Williams and Pam Fusco were acknowledged for their leadership in this program.

The evening wound up with anniversary keynotes by Martin Roesch, "10 Years of Security Breaches and How Security Has Changed," and Mischel Kwon, "Next Generation Security, Today's Challenge."

Congratulations, ISSA, for 25 great years.

The ISSA Story

Sandra (Mann) Lambert, ISSA President, Second Annual Conference 1985

By Sandra M. Lambert – ISSA Founding Member, Los Angeles, USA Chapter

In the beginning . . .

At the CSI annual conference in November 1980, around seven infosec professionals from the Los Angeles area became acquainted. While we had much the same work responsibilities, we represented different industries, including banking, aerospace, retail, energy, and insurance. We said that we ought to get together and talk about our infosec issues once back in Los Angeles. We were all busy and a year went by before we saw each other again at CSI in November 1981. We reiterated that, though from various business sectors, we had the same issues and problems, and we believed that we could all gain a tremendous knowledge base if we shared our hard-earned experiences and solutions. But time marched on.

Finally, I said to my friend Nancy Woolsey, the Infosec Manager at Lockheed, "If we don't put together a first meeting, we'll be talking about this forever." She concurred. I volunteered to get a meeting room at Security Pacific Bank (my employer); she picked a date, and we invited everyone that any of us knew who was doing infosec work in the Los Angeles area.

In January 1982 that first meeting was convened, co-chaired by Nancy and myself. The 25 or so people who attended all quickly saw the potential benefit to our companies in sharing our professional knowledge. That is how and when this organization was founded. Nancy and I believed that we could make a difference and we were willing to put our time and resources to bear.

Past President Sandra Lambert passes president's gavel to newly elected President Carl Jackson.

In deciding to invite people to future meetings, Nancy and I knew that we needed to have a name for these gatherings – a name descriptive of our goals. We had heard about a group in the San Francisco area called the Bay Area Computer Security Interest Group, so we initially called ourselves the Southern California Computer Security Interest Group. The interest and enthusiasm displayed at future organizational meetings convinced us that our vision of helping everyone to enhance his or her knowledge and professional skills, with the end result of providing for more rewarding individual careers and increased value to employers, was a valid starting point. It was so obvious, and the models were right there in front of us: the physical security folks had ASIS, the internal auditors had IIA, and the IT auditors had EDPAA (now ISACA). I had been an officer at the chapter and international board levels in EDPAA, so I left the ranks of that organization in order to form this new organization and to bring recognition and support to our emerging profession, which had different needs than the auditors.

At the February '82 meeting, a few more people showed up and we started an educational program as well as developing an administrative structure for the meetings. Realizing that in order to make a difference, this concept had to eventually be bigger than any one part of any one state, we determined that we needed to eliminate geography from our name. Aware of the Data Processing Management Association and accepting its descriptive name, we changed our name to the Data Processing Security Association. The educational program which we started then, and which lasted for a couple years, consisted of one of the attendees volunteering to pick one specific topic, talk about the pertinent issues that topic created within his company, and share how those issues were addressed and what solutions were applied. Then everyone would participate as it turned into a roundtable discussion. Oftentimes the speakers had no solutions to their issues and the group discussions helped them formulate options. It was simple. We had no money for speakers, so we were the speakers. We were the hands-on experts of the day in a fast evolving specialty.

In March '82, Nancy and I enlisted the help of three other regular attendees – Cole Emerson, Carl Jackson, and K.C.

Keffer. The five of us became the original operating committee and I was appointed president of our growing organization. During the next few months we continually discussed our name. We decided that "data processing" would soon be an outdated term. Many suggested names came to the forefront as we found that the acronym DPSA was already being used by other entities (and the "Department of Public Service & Administration" of South Africa we were not!). So, in May '82 we agreed on the name Information Systems Security Association, believing that it would be timeless and global. If you think we had a hard time deciding on the name, imagine the trials we went through in designing a logo that would be descriptive, not quickly outdated by industry dynamics, and not merely "physically oriented" (e.g., chains, locks, keys in all combinations)! Finally, it was decided that a stylized version of our acronym, ISSA, would be the logo.

Bob Courtney, Keynote Speaker at 2nd Annual Conference

ISSA™
INFORMATION SYSTEMS SECURITY ASSOCIATION, INC.

Throughout 1983 we sharpened ISSA's vision, set its mission, and determined that we would seek non-profit incorporation status, much the same as the other professional associations had done.

On March 8, 1984 we held our First Annual Working Conference in Los Angeles. We specifically called it a *working conference* because we wanted to ensure that our employers did not think we were off for a one-day boondoggle. In our effort to be cost-effective, the charge for ISSA members was $10 to cover lunch and refreshments, and $50 for non-members. I called in a couple well-known colleagues of mine from back east who somehow got their companies to pay their expenses to be our keynote speakers. I remember it like it was yesterday – the turnout was great (almost all of the 60 seats were filled) and we confidently knew that we were on the right track.

2nd Annual Conference Speakers

On March 28, 1984 we incorporated as a non-profit organization in the State of California, and this year we are celebrating the 25th anniversary of that event. At the initial formal elections I was chosen to be the Founding President of ISSA, Inc., a non-profit corporation. Cheryl Helsing (San Francisco) was VP, Carl Jackson (L.A.) was Treasurer, Denny Steinauer (Maryland) was Recording Secretary, and Russ Leone (L.A.) was Corresponding Secretary. In June, Nancy flew off to England to marry Colin King, left the infosec profession, and returned to federal government employment with the IRS in the London Tax Attaché office, addressing international income tax treaty and expatriate tax issues.

1989 ISSA Board

On March 28-29, 1985, we held our Second Annual Working Conference in Los Angeles. We had about 100 participants from all over the U.S., and we announced that the Bay Area was officially the second ISSA chapter. In the next few months, New York Metro became our third chapter, followed by Baltimore and Houston, and ISSA continued to develop local chapters. ISSA now has 140 chapters in 35 countries and we believe that we have only begun ISSA's international growth as we look forward to best meeting the needs of our global membership.

In summary, I'd say that we have stayed true to our original mission. It is very gratifying to know that after 25 years, ISSA's professional vision is accepted as your professional vision. Over the years, I had made life-long friends in the profession, learned new skills, and got better jobs – in large part due to squishing volunteerism into my "free time." In this profession, networking is the key word in building careers. I dare to guarantee you that the rewards of ISSA volunteer works are immense and most gratifying!

I wish to thank the long list of dedicated individuals who have made ISSA what it is today, many of whom I personally know and many that I have yet to meet. Collectively you supported ISSA's originating vision and mission for which many individuals and companies greatly benefit. It is due to your willingness to share your experience and knowledge that we are all made better in our profession. The whole is indeed far greater than the sum of the parts. ISSA is the world's largest, international non-profit association specifically dedicated to the ideals of information security professionals. YOU are ISSA.

Happy 25th Anniversary!

About the Author

Sandra M. Lambert is the managing partner of Lambert & Associates, LLC, where she specializes in information security and business continuity consulting with clients worldwide (http://www.lambert-associates.com). She may be reached at Sanlambert@aol.com.

ISSA Connect Network. Collaborate. Learn. Excel!

ISSA Connect offers you an exciting new communication tool to grow your worldwide network and better tackle the challenges of today and future threats of tomorrow. Log on at www.issa.org.

ISSA's 25th Anniversary Celebration looked back over the past 25 years of building a world-class professional organization and looked forward to the next stage of development. For 25 years the association focused on developing individual chapters, first in the U.S., then across the globe. Now with 140 chapters and nearly 10,000 members in 70 nations around the world, the focus is on enabling members to interact and collaborate with each other. ISSA Connect – our new professional networking and collaboration site – will expand the relationships members currently enjoy through their local chapters to the entire ISSA global community.

www.issa.org – Login to ISSA Connect and Join the Discussions!

We live in an era in which the need for information security is growing exponentially and often times the information is not readily available. We must rededicate ourselves and collaborate to address the threats and challenges that face us – and those that do not yet exist. We need to utilize the technology of today to leverage our collective experience, wisdom, and innovation. When asked the importance of interacting with other professionals, ISSA member Michael Versace explained, "That's where the knowledge is, the quality information I know I can trust." That's the idea behind ISSA Connect: interaction and collaboration with information security professionals throughout our association. Professionals are facing the same problems, searching for the same solutions, globally. With ISSA Connect, members can suggest solutions and our global community can join in the discussion.

What can you do with ISSA Connect?

Log on the ISSA website and update your user profile to join the global database and begin connecting with peers and colleagues who face similar industry threats and challenges:

- Access the information and resources you want, when you need them
- Interact with trusted peers, participating in and contributing to a wealth of knowledge and resources not limited by geographical boundaries
- Exchange information and learn from each other in one collaborative location
- Participate in discussion groups and communities, wherever your interests and expertise lie
- And, of course, develop friendships and relationships with like-minded professionals

Members access ISSA Connect via their normal member login. Set aside some time to explore the site, getting familiar with the structure and workings. Then, get down to the business of connecting, collaborating, learning, and excelling! ISSA Connect offers you an exciting new communication tool to grow your worldwide network and better tackle the challenges of today and future threats of tomorrow.

In Memory of Ed Hetsko

Founding President
ISSA Northern Virginia Chapter

Ed Hetsko passed away August 15th. Always a stalwart champion for ISSA, he will be deeply missed by his fellow colleagues.

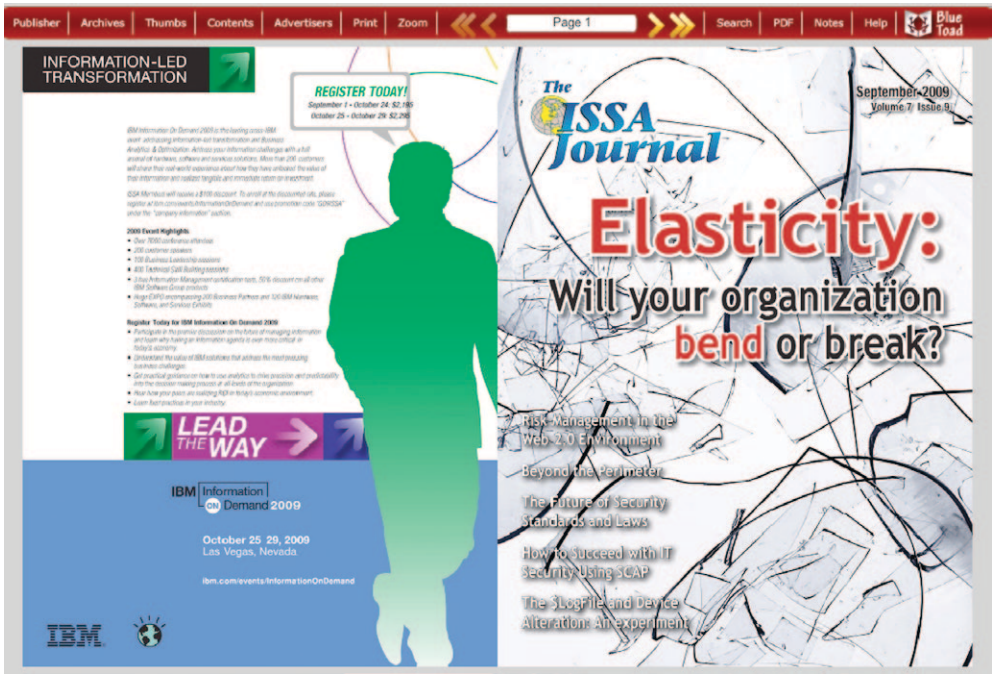
Ed was involved with the Colorado Springs Chapter for many years before moving to the Washington, DC area. He then embarked on establishing the Northern Virginia (NOVA) chapter in 2002, leading as the chapter's first president.

In recognition of Ed's contributions to the information security community, the NOVA board has renamed the annual President's Award as the *Ed Hetsko President's Award* and the George Mason University scholarship fund to the *Ed Hetsko & Laurie McQuillan Scholarship Endowment*. You may contribute to the endowment fund at www.ISSA-NOVA.org.

While Ed is no longer with us, his legacy of information security excellence will live on through ISSA.

ISSA Journal Goes All-Electronic Delivery

Starting November first, the ISSA Journal will be delivered all electronically, through the online magazine, through biweekly eNews, and through ISSA Connect. While many may miss the paper version, our all-electronic delivery ushers unprecedented interaction and collaboration with the authors and their articles in real time. The familiar 48-page ISSA Journal format – the online version is exactly the same as the print version – will continue: the interactive, page-turning online version will be the primary format, and the full 48-page PDF will continue to be available for download for local viewing, as will individual articles.



Page one of the online ISSA Journal – just like the print version. Easy navigation across the top of the screen. Pages scale to fit your screen and zoom in for close-ups. Links take you to resources, advertisers, and authors.

For those who have not sampled the online version, the interactive magazine provides live hyperlinks to article resources and references as well as advertisers and conferences. Do you have a question or reaction to an article you are reading: with a click you can send an email to the author. Got a specific topic in mind? Each issue is searchable, and you may even search past issues. That's all great, but the big change is full integration with ISSA Connect!

With ISSA Connect your interaction with *Journal* readership is immediate, no waiting for the next issue or two with your letter to the editor – post your comments directly to ISSA Connect. Of course, you may still submit a letter to the editor for inclusion in the *Journal* – the choice is yours. If something you read gets you excited, comment directly in the *Journal* section, start a topic for general discussion, or contact the author if he or she is a member. The possibilities for discussion are limited only to our readers' interests and involvement, and we have nearly 10,000 members!

How to find the ISSA Journal

To read the current *ISSA Journal* each month, log on to ISSA Connect, and then click on "ISSA Journal" in the "Places/Communities" box. Here you may select the issue of interest to read. Here you may also read or post ongoing discussions relevant to each issue.

You may also find the current and past *ISSA Journal* issues on the ISSA website as usual. Just click on the Journal cover or select from the archives.

Summary of benefits

Rather than waiting on the vagaries of postal systems, the ISSA Journal will be available for instant access on the first business day of the month:

- Read remotely or download for local viewing
- Search for relevant topics of interest
- Start or contribute to discussions on *Journal* articles
- Provide immediate feedback to authors:
  - Engage authors who are ISSA members in ISSA Connect
  - Email authors who are not ISSA members
- Communicate directly the ISSA Journal Editorial Advisory Board, advising the subjects, focus, and authors that are most valuable and of greatest interest

Additionally, each eNews will feature an article from the current Journal.

Going Green

And if all the great features of our online *ISSA Journal* were not enough, all-digital delivery of the publication to nearly 10,000 members reduces our global footprint by 2500 lbs. (1134 kg.) per month and 30,000 lbs. (13,600 kg.) per year. ISSA Journal: fewer resources consumed – increased interaction with information and people: this is a good thing!

ISSA Journal – ISSA Connect – ISSA Collaboration

The Hole in the Cloud

By Richard Buttermore – ISSA member, Motor City (Detroit), USA Chapter

Cloud computing promises many benefits including better utilization of resources, capital expense savings, and on-demand scaling. However, underlying technologies, like virtualization, lack security measures that many may assume they have.

Abstract

Cloud computing promises many benefits, including better utilization of resources, capital expense savings, and on-demand scaling. However, underlying technologies, like virtualization, lack security measures that many may assume they have. Using even simple techniques, a hacker can obtain valuable information from an application which has been put on the cloud. Companies should understand what the true risks to cloud computing are and implement their plans (or not) accordingly.

Considering a cloud

Moving existing applications or deploying new applications to a cloud can reap many benefits, including scalability, better utilization of resources, and capital expense savings. From a security perspective, there are two choices for cloud computing:

- **Private** – hosting the application yourself, using your infrastructure and employing cloud technologies from companies like 3Tera or the open-source project EUCALYPTUS. In this case, it is still your data center and you just happen to be using cloud technologies.
- **Public** – contracting with a third party to host the cloud, either exclusively for you or as part of a shared infrastructure such as Amazon Web Services (AWS).

Since this article concerns cloud security, not cloud concepts or architecture, "hybrid" clouds (where there are both public and private providers) are not considered separately. From a security perspective, a hybrid cloud has the same risks as a public cloud in that at least some of it is outside an organization's direct control. Also not considered are distinctions between the *aaS ("<blank> as a Service") layers since the security implications of having something outside an organization's direct control is the issue, not at which layer that something resides.

Hacker + access + time = eventual compromise.

One of the foremost concerns of companies considering cloud computing for their enterprise is security.[1] [2] With this article, I will explain why security risks exist, demonstrate ways in which security can be compromised, and describe the implications of moving applications to a cloud.

Underneath the cloud: Virtualization

Portability is necessary to achieve the promise of cloud computing. That is, a cloud needs to move and copy whatever is using the cloud's resources from place to place in order to scale up and down on demand. In a cloud, this portability is enabled through virtualization, where computer resources (CPUs, storage, memory, and devices) are shared through various abstraction techniques. To scale on-demand, cloud management software does exactly that, copy and transfer something virtual. So, whether it is Google copying executable Python code from machine to machine within the App Engine environment or Amazon Web Services (AWS) copying an Amazon Machine Image (AMI) from server to server within its Elastic Compute Cloud (EC2) and booting ("spinning") it up, a cloud needs to have something virtual so it can be portable.

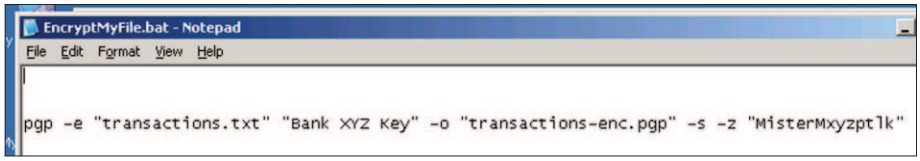
The problem

Virtualization was not invented to build clouds and was not designed with cloud security requirements in mind. It start-

1 Thomas Wailgum, "Cloud Hype Peaks, But IT Concerns Increase," *CIO* (August 26, 2009) – http://www.cio.com/article/500634/Cloud_Hype_Peaks_But_IT_Concerns_Increase (Accessed September 4, 2009).

2 Robert McMillan, "Cloud computing a 'security nightmare,' says Cisco CEO," *ComputerWorld* (April 22, 2009) – http://www.computerworld.com/s/article/9131998/Cloud_computing_a_security_nightmare_says_Cisco_CEO (Accessed September 4, 2009).

Figure 1 – Command in Batch File



ed in the 1960s with IBM[3] and the goal then was to support time sharing[4] to better utilize computer resources without disrupting other users of the same resources. Virtualization was built to run multiple logical machines, assuming that they all share the same physical security measures on a single server. It was not developed to make a virtual machine (VM) portable across organizational boundaries, although it does that quite well. The security risk is that a technology which was originally developed for one use and under one set of assumptions has been adopted for another use, allowing the potential for it to be exploited. It is actually quite common for security to be considered after the introduction of a new technology. Locks and alarms were added much later to cars, for example, once they became valuable enough to steal.

To understand the security implications of the cloud architecture, I will focus on the real-world use case of a medium or large company moving an existing application to a public cloud. Assuming the application for such a company would be complicated with lots of functionality, it would not make sense to rewrite it from scratch for a Google App Engine-like environment (if it even offered the capabilities needed). Re-hosting the application on a virtual machine, such as VMware or Xen, would be a cheaper and more stable way of moving it to the cloud by creating a virtualized version of what was originally on bare metal. Thus, moving to the cloud would be a re-hosting project (days or weeks) rather than a re-writing project (months or years).

To re-host an application, a company creates a virtual machine by installing the base operating system through the VM's management software, installing any application platforms needed on top of that, copying the application code there, and recompiling and testing it until they had a version that functioned as it had originally. To move the application to a cloud, this VM would then be given to a cloud provider to be run on their hardware and cloud software.

All computing environments involve some security risk. For cloud computing, the risk is that the VM image resides on someone else's machines, giving them physical access to the server. In a cloud, "physical access" means access to a copy of the virtual machine image. So, rather than allowing only badge-controlled access to the physical servers at their data centers, a company effectively gives a badge to anyone with access to the images at the cloud provider. Hacker + access + time = eventual compromise.

3 Various Authors, "Timeline of virtualization development," *Wikipedia* – http://en.wikipedia.org/wiki/Timeline_of_virtualization_development (Accessed September 4, 2009).

4 Amit Singh, "An Introduction to Virtualization", kernelthread.com (January 2004) – http://www.kernelthread.com/publications/virtualization (Accessed September 4, 2009).

The view from the cloud

Continuing the example, suppose one of those applications transmits a file containing financial data to another company each night. The application encrypts the file before transmission using Pretty Good Privacy (PGP). Running in batch mode, the script doing the encryption might look something like Figure 1 from within the virtual machine.

This is what the batch file looks like within the VM when logged in to both the physical machine and the virtual machine running on top of it. Note the embedded passphrase, "MisterMxyzptlk," used with the "-z" option, which allows the passphrase to be specified on the command line for unattended execution.

For simplicity, the script shown has just one line. But, this is not a purely "cooked" example. Using embedded passwords in scripts to perform automated tasks is a widespread practice, and PGP is quite common in corporate environments. Although the documentation for PGP and other PGP-like programs provides warnings about the *-z* option ("Use this feature with caution"), lots of companies use it anyway. It is too convenient not to use.

Hacking the cloud

Even though the batch file in the example is buried deep inside the virtual machine, it is easily accessible. When not running, an instance of a virtual machine is basically just one or more files found on the hard drive of the physical machine. For example, the following files were found on the physical machine on which these tests were run:

```
20 GB Hard Disk.vmdk
nvram
vmware.log
Windows Server 2003 Standard Edition.vmsd
Windows Server 2003 Standard Edition.vmx
```

The VMDK file (in bold, above) is a virtual disk file which stores the contents of the virtual machine's hard disk drive.[5] When the virtual machine is started (or "spun up"), the software which actually runs the VM, known as the *virtual machine monitor* or *hypervisor*, reads these files and maps them into the physical machine's memory and otherwise manages the resources of the physical machine so that they appear to be "real" to the virtual machine. On the physical machine, a virtual machine is just an array of bytes somewhere either on a disk, in memory, or both. And, like any array of bytes whether they are stored on a hard drive, resident in memory, or pulled out of the air as they pass by on a wireless network, they can be captured, examined, and hacked.

Although the hypervisor knows how these bytes are organized, it is not otherwise common knowledge. However, in-

5 Author Unknown, "What Files Make Up a Virtual Machine?" VMware, Inc. – http://www.vmware.com/support/ws5/doc/ws_learning_files_in_a_vm.html (Accessed September 4, 2009).

formation can still be extracted from them. Borrowing a digital forensic technique typically used to gain information about an unknown file, the "strings" program (by Mark Russinovich at Sysinternals[6]) can be used to extract all the ASCII characters from this hard drive file with a command such as the following:

```
strings "20 GB Hard Disk.vmdk" >
VMDKStringsOut.txt
```

Using simple tools like the DOS FIND command and a small script to break the file up so it can be loaded in to an editor, some interesting results can be seen even with this primitive hacking technique. As shown in Figure 2, without being logged in to the virtual machine, the contents of its hard drive can be viewed, including the PGP command with its embedded passphrase, highlighted in red. The name of the batch file is highlighted in blue.

```
ENCRYP~1.BATe.bO
EncryptMyFile.bat(
$\_
pgp -e "transactions.txt" "Bank XYZ Key"
o "transactions-enc.pgp"
s -z "MisterMxyzptlk"
FILEO
122943~1.ZIPun_O
```

Figure 2 – Passcode Found in VMDK

One common way of protecting batch scripts with embedded passwords is to restrict the file rights on the batch file so that only a user with the proper rights can read, write, and execute it. In a Unix-type environment, this might be done with a command similar to the following:

```
chmod 700 somefile
```

In Windows, the file permissions can be set or revoked through the Security tab of the Properties dialog which can be invoked by right-clicking the file name.

To test the effectiveness of using file rights to protect a batch file in a VM, a second batch file was created. This batch file contained the same command and an additional remark in it (to distinguish it from the first), as shown in Figure 3.

The file rights were then turned off for the administrator, generating an "Access is denied" message when attempting to open the file.

The "strings" file was generated after removing rights to the batch file. Sifting through this file from outside the VM, the second batch file with its PGP command and embedded password can easily be located as shown in Figure 4 where the PGP command and password are highlighted in red.

6 Sysinternals, www.sysinternals.com.

```
REM This file has access rights turned off even for the Administrator!
pgp -e "transactions.txt" "Bank XYZ Key" -o "transactions-enc.pgp" -s -z "MisterMxyzptlk"
```

Figure 3 – PGP Command in Batch file in VM

Figure 4 – Passcode Found in VMDK

```
AlE
REM This file has access rights turned off even for the Administrator!
pgp -e "transactions.txt" "Bank XYZ Key" -o "transactions-enc.pgp"
s -z "MisterMxyzptlk"
<param name="Interval" value=500>
<param name="SizerID" value="ActiveDesktopMover">
```

Unfortunately, restricting the rights to the batch file from within the VM does not affect the ability to see the contents of the file from outside the VM.

A brief aside: Astute readers will note that the example does not give the attacker everything. The passphrase in question would only unlock the local keystore which is inside the VM. An attacker could extract the keystore file from the VM image and use it and the passkey to falsify data (and sign it) before transmitting it to the counter party. The important lesson here is that compromising information like this is readily available once an attacker has access to the VM image.

Really digging in

The techniques shown here are trivial from a hacking standpoint. No self-respecting hacker, of any color hat, would consider these to be clever exploits. However, even these simple techniques can yield results once you have the virtual machine image (or a higher-level abstraction like source code). Applications running in an enterprise offer a trove of embedded information. Some examples, which could be seen in the data center of any organization with a reasonably complex information technology operation, include:

- web.config files for .NET applications which often contain passwords and other application configuration or security details.
- .properties files which are often used to store configurable parameters for a Java application.
- Text strings embedded in binary files.
- Header strings such as "orig-date" and "reply-to" to locate emails which may be stored in the clear on a cloud machine hosting an email server.
- Database connection strings, which often contain a password, of the form: Data Source=myServerAddress;Initial Catalog=myDataBase;User Id=myUsername;Password=myPassword.
- Source code containing sensitive security details (login credentials, FTP server IP addresses, commands used to send a file, etc.) such as in batch files or shell scripts, and Perl, PHP, and Ruby programs. These can be easily found by scanning for well-known commands used in securing or moving information around such as "FTP," "PGP," and "ssh" or commands used to escalate privileges such as "sudo" (superuser do), "su," and "runas."

- Any file signatures, metadata, or so-called "magic numbers" to locate sensitive documents that may be stored on a server as part of cloud-based office productivity or collaboration solution.

Embedding passwords and other sensitive details in source code and storing information in the clear in files can be an acceptable tradeoff when the physical machine is secured properly. These techniques may not be appropriate in a cloud environment, however.

Compression and encryption seem to help

In another test, two additional batch files were created. One was compressed and the other was encrypted. The compression and encryption were both done through the "Advanced Attributes" which can be set using the file "Properties" dialog through Windows Explorer. In this case, it does appear that either compressing or encrypting the batch file provides protection as the information in either batch file could not be located in the "strings" file. This makes sense since the VM's operating system would compress or encrypt the file before saving it to its disk and the hypervisor would simply store whatever was given to it.

Compression may not offer much protection, however, since there is no reason that someone with knowledge of the VM's internal structures could not simply extract the compressed file and decompress it outside of the VM. Encryption would offer better protection, one would assume, but could possibly degrade performance. In any event, the key to unlock it could still be in the VM somewhere which means that a determined and knowledgeable hacker could somehow dig it out. The technique in the following section provides some clues as to how this could be done.

Attacking the running VM

As mentioned previously, access to the VM in the first place is the problem, not the VM architecture itself. Having this access, there is no reason for a hacker to restrict himself to simply sifting through hard drive files. He can observe the virtual machine from the outside while it is running.

Using Windows' Task Manager, the process which is executing the virtual machine can be determined. Again borrowing a digital forensics technique, the *userdump tool* (available from Microsoft) can be used to dump the running process with a command similar to the following:

```
userdump -w 3964
```

Once the process dump has been obtained, it can be sifted through as easily as the earlier files. The passphrase can be seen in the process dump, highlighted in red (Figure 5).

It is not 100% clear why this shows up in the process dump. It may have just been a file that was recently opened and is still paged-in to memory, soon to be discarded. In any event, it is readily available for prying eyes.

Figure 5 – Passcode Found in Process Dump

```
ENCRYP~1.BAT e.bO
\&n
EncryptMyFile.bat
pgp -e "transactions.txt" "Bank XYZ Key" -o "transactions-enc.pgp"
s -z "MisterMxyzptlk"
FILEO
w03a2409.dll
```

Note that the process did not need to be stopped to dump it. The process continued to "live" during and after the dump. No security measure implemented inside the VM could prevent it or even know that it was done. In other words, the VM cannot protect itself.

This highlights another security issue: an attacker can examine anything the VM does while it is running. A sufficiently knowledgeable person could execute the hypervisor in an interactive debugger/disassembler and simply halt execution at specific points to examine the VM's state. An attacker could, for example, determine the entry point for a known function, say CryptEncrypt() from Microsoft's cryptography API (in advapi32.dll), and break execution at that point. After poking through memory a bit, an attacker could obtain the encryption key. This would require considerable technical expertise from an attacker. But it is within the realm of possibility, especially for a determined hacker when the payoff is high enough.

An open-source virtual machine solution like Xen may have a disadvantage over a closed-source solution. A hacker can read the Xen source code and learn about the internal structures of the VM image. He could, for example, figure out how the hypervisor stores the VM's virtual disk on the physical drive. With a better understanding and control of the structure of a VM image, a hacker can analyze binary data directly in the image rather than just looking for ASCII data, perhaps even developing a driver that mounts a VM like a hard drive and allows someone to poke around in its data as easily as they could a hard drive image. Once the structures are understood, moving the bytes around is trivial.

With an open-source virtual machine solution, a hacker would even be able to modify and recompile the hypervisor, adding code to make the hypervisor take action at specific points during execution (disk writes, network activity, etc.). The ability to modify and recompile source code is why open source network drivers are used by people hacking into networks: the driver can be changed to do things that are useful to a hacker like extracting specific packets, sending doctored packets, changing the network card to "promiscuous" mode, etc.

Yes, but…

The techniques described above were performed from an authorized state, with access to privileged modes of operation and files. Readers will note that this means the hacker needs access to the virtual machine image to do any harm. That is true. But with cloud computing, that is the point. The reality of cloud computing is that companies surrender physical control of the virtual machine (or any higher-level

abstraction like source code) in order for it to run somewhere in the cloud. One of the highly-touted advantages of cloud computing is automatic on-demand access to more resources – meaning that, not only will the buyers of cloud computing services not know where their VM is, they are not even expected to know or care as the cloud is designed (and marketed) to make knowing such details unnecessary. In this case "anytime, anywhere" translates to "all the time, you don't know where."

Where or how would one obtain a virtual machine image? Just about any way that security risks are traditionally caused through carelessness, poor policies, hacking, or nefarious intent. Some examples:

- VM images left on machines at the company where they were created or on hard drives discarded from the cloud provider
- Traditional hacking into the cloud provider such as Trojan horses, backdoors, social engineering, or hacking the password of the person who created the VM and uploaded it to the provider[7]
- Unscrupulous or careless operators at the cloud providers

The first example is the digital equivalent of leaving a server in the hall outside the server room or in the trash. It could happen anywhere there are sloppy policies or people doing things they really should not. The second is a risk for any data held on a server. Technically, there is little difference between stealing a credit card data file and stealing a virtual machine image file once a backdoor has been installed.

The third example is perhaps the most unsettling, implying that cloud providers might be careless with the virtual machine images (or code) with which they have been entrusted or that they have administrators who might sell a copy of a virtual machine for a fee. I have no information that cloud providers are insecure or that any particular provider might be a risk. A well thought out security architecture using a layered defense, cryptography, good policies, logging, and backup and recovery procedures should make a cloud implementation just as secure as any other environment. However, companies using public cloud providers might discover that the cheaper cloud provider did not have the same security measures as the more expensive provider down the (virtual) block.

The sheer scale of the cloud might make it look more secure. With hundreds or even thousands of servers, finding a target VM might look like the needle in the haystack, and the physical server it is on would be secured with an administrative password anyway. If fact, both assertions are likely fallacies. If a VM contains sensitive information, a customer is likely to request that any servers it runs on be segmented off

7 On August 31, 2009, Amazon introduced multi-factor authentication which "provides an additional layer of security to the administration of your AWS account" – http://aws.amazon.com/about-aws/whats-new/2009/08/31/now-available---aws-multi-factor-authentication (accessed September 24, 2009). Presumably, Amazon has realized the risks of these administrative accounts being hacked and taken this step to prevent it.

from the others in a cloud. The ability to segment parts of a cloud for specific customers is increasingly being mentioned as a capability by cloud providers in marketing materials. To someone interested in attacking these machines, however, this shrinks the haystack considerably and even highlights which haystacks might provide the highest value. Regarding password protection on the physical server, with hundreds or thousands of machines to secure, it is more likely that they all have the same password, some pattern to the passwords, or a common security mechanism to make administration easier. Each machine may even have no password, relying instead on the physical and network security measures to provide protection. In security, this is sometimes referred to as the "keys to the kingdom" problem.

The exploits discussed here should not be considered breakdowns in virtual machine security. They are not the result of poor design, sloppy programming, lax policies, ignorance, or any other vice that typically compromises security. Virtualization technology needs to be highly optimized for speed and the fact that the hypervisor seems to store the contents of the VM in the clear on the base system's hard drive is not really surprising. The makers of hypervisors could encrypt or take other measures to obscure this information, but this may have a very negative impact on performance. Similarly, any process can be dumped and examined. This is not a failing of the process.

Conclusion

The bottom line is, cloud computing and virtualization give the equivalent of physical access to the machine and that is always a risk. Companies considering cloud computing should do the following at a minimum:

- Determine what information that could be damaging if leaked is contained in any applications being considered for cloud deployment
- Treat a cloud as though the physical server is being given to the cloud provider and assess the risks accordingly
- Vet cloud providers thoroughly and ask questions including how servers are protected, who has access to the servers, what the security policies are, and what recovery options are
- Take measures to secure confidential information to the extent it can be, including using encryption and realizing that absolute security may not be possible in the cloud
- Specify security requirements up-front in contract terms

Cloud providers' security measures are probably better than that of many of their customers. But as use of the cloud ramps up and more sensitive information and business functions move out there, cloud providers will inevitably become targets if they are not already.

References

—Keith J. Jones, Richard Bejtlich, Curtis W. Rose, October 2005, *Real Digital Forensics: Computer Security and Incident Response*, Addison-Wesley Professional.

About the Author

Richard Buttermore, CISSP-ISSAP, is a senior director in a technology practice specializing in strategic technologies such as cloud computing in CSC's Applications and Technology Services Group. He can be reached at rbutterm@gmail.com or followed on Twitter at http://twitter.com/rbuttermore.

Dysfunction Junction: Do standards function?

By Benjamin Tomhave – ISSA member, Phoenix, USA Chapter

The value of standards has seemingly fallen off in recent years while the organizations that author them fragment, grow distant, or simply fail to communicate and collaborate. Who will step in and provide the leadership needed to lead us to the next generation?

Abstract

The Internet as we know it is based on myriad standards. Without them we would not have the lives we lead. Yet the value of standards has seemingly fallen off in recent years while the organizations that author them fragment, grow distant, or simply fail to communicate and collaborate. The need for standards still exists, but the path forward seems murky at best. Who will step in and provide the leadership needed to lead us to the next generation?

Joining a standards committee can be a great way to round out a resume. It shows an interest in topics larger than today's problems or just focusing on one's career. It demonstrates an interest in helping the community at large. Or, so we would have you believe until you join a committee and begin to wonder what exactly you have gotten yourself into. After all, nobody tells you before signing up that you also need a graduate degree in *Robert's Rules of Order* or that you will have to become savvy in the ways of politics and bureaucracy. Nor do the brochures for Club Standards talk about how easily one might put one's foot into one's own mouth, alienating friends, making enemies, and potentially limiting one's career.

Surely this description appears to be over-the-top and filled with drama, and to a degree that is a correct assumption. However, to underestimate what all goes on in standards committees – as well as between them – is the making of great folklore and stories for the ages. Where else outside of government can an idea be developed slowly over the course of years and watered down to the point that the resultant standard is already implicitly present in the technology the vendors conveniently pushed in parallel? Yes, that is a cynical perspective, but it is also sometimes accurate.

The real question one might ask is if standards are still a useful concept. Never mind that the Internet exists at the mercy of standards, thanks in large part to the combined, though disjointed, efforts of the IETF, IEEE, ANSI, ISO/IEC, NIST, ARPA/DARPA, and various other international, federal, and private sector interests. Of course, most of these standards are focused outside of security, and thus perhaps represent a more readily useful utility versus security standards. After all, it has been at least a couple years since the last major weakness was identified in TCP or DNS or X.509, right?[1]

The answer to the question of usefulness is that standards are obviously of use. To think otherwise would be beyond cynical and would fail to take into consideration all the good that has come from these disparate efforts. Where the argument on utility breaks down, however, is when there is not a good consensus about the "right" path forward. Security standards, in particular, seem to suffer from this problem, leading us to a situation where vendors compete to dominate a given technical committee in order to see their protocol or solution of choice adopted as a standard (look into the ODF vs. OOXML history as an example of this dysfunction[2]). One must then wonder how it is that we got to this point. Is it really as simple as a lack of consensus?

The truth is likely far less interesting or conspiratorial, but may surprise people nonetheless. The torrid reality is that the world in the modern digital age simply moves too fast for the standards process. Combine this fact with current economic realities and we see that standards are in fact very important, not only to customers trying to buy interoperable products, but also to vendors who are trying to position their products ahead of the competition. At the same time, standards provide a double-edged sword because they potentially eliminate

1 Except for talks at Black Hat USA 2009 and DEFCON 17 about defeating SSL/X.509. No big deal, right?

2 Groklaw has extensive coverage of ODF vs. OOXML on its website at http://www.groklaw.net/staticpages/index.php?page=20051216153153504.

The torrid reality is that the world in the modern digital age simply moves too fast for the standards process.

the case for vendor lock-in. Despite vendors being heavily invested in the standards process, there is also a certain danger to their adopting standards through reference implementations and eventual product releases. Standards have historically provided a mechanism for leveling the field of competition, which some would say is beneficial in a capitalist society.

It is then from these stresses that we see the current situation. Vendors want standards because they benefit their products, but they do not want the standards because they also reduce lock-in and increase competition. Customers want standards because they result in improved competition, but oftentimes at the cost of quality and value. More importantly, vendors can easily become absorbed in trying to conform to myriad disparate standards instead of focusing on customer requests and requirements. The resultant mess is a world out of sync with itself all in the name of a process so bureaucratic that it is literally timed with a calendar.

An example: key management standards

One of the best examples of just how insane the standards community has become is looking at standards and specification development initiatives for key management. These standards have been triggered as a direct result of the increased demand for cryptographic services, such as required by PCI DSS.[3] With the increased demand for encrypting data comes the increased importance of proper management of cryptographic keys. These needs oftentimes extend beyond simple public key infrastructure (PKI) to managing large numbers of symmetric keys, as well as providing mechanisms for performing encryption operations either transactionally, transparently, or in batch operations.

For an example of just how complex the key management standards landscape is today, take a look at the list of "Key Management Standards and Specification Development Initiatives" that is being maintained by Cover Pages[4]:

- ANSI X9 Financial Industry Standards
- DMTF Security Modeling Working Group
- GlobalPlatform Key Management System
- IEEE P1619.3 Security in Storage Working Group (SISWG), Key Management
- IETF Provisioning of Symmetric Keys (KEYPROV) Working Group
- ISO/IEC 11770: Key Management
- KeyGen2: Key Provisioning/Management Standards Proposal
- National Institute of Standards and Technology (NIST)
- OASIS Enterprise Key Management Infrastructure (EKMI) Technical Committee
- OASIS Key Management Interoperability Protocol (KMIP) Technical Committee
- Sun Crypto Key Management System (KMS)
- Trusted Computing Group: Infrastructure Work Group and Key Management Services Subgroup
- W3C XML Key Management (XKMS)

For those keeping track at home, that is a list of thirteen (13!) different standards and specifications addressing key management – and that list is not even complete! Notice that OASIS itself has two committees on the topic,[5] working at times to separate, yet related, yet occasionally overlapping, ends.

In light of the above list, where is the benefit to customers, vendors, government, and the public at large? More importantly, to whom do you listen and on what topic? Assuming all of the above standards reach final, released states, then which standard would you, as a customer, expect vendors to implement? How do customers even know which standards are important?

Unfortunately, as customers, we often rely on vendors to tell us what is and is not important from an interoperability standpoint. After all, one of the primary benefits to customers is using standards to ensure that two products from competing vendors can be used together (e.g., IPSEC and VPNs). Given the above slate of competing and/or complementary standards, it seems unlikely that either customers or vendors will stand a fighting chance in the short-term. Overall, it seems likely that certain standards will rise to prevalence, not the least of which thanks to multiple vendors adopting them.

Muddling through

As a potential customer, how do you decide what standards are important, what standards are not (as) important, and what to press vendors to support? The answer to this question is not trivial. The worst possible answer is to require customers to become expert in each standard, which simply is not reasonable. Alternatively, customers can try to help each other out, though this could also lead to conflicts of interest for companies that are themselves in competition.

Taking the example of the key management standards, let's go through a quick analysis to see if some clarity can be found. As a reminder, look above to the enumerated list of standards.

The first targets we can eliminate are vendor-specific standards and standards from organizations outside our sector. For the purposes of this example, let's assume a generic non-financial services sector that prefers vendor neutrality and that is interested in symmetric key management. As such, we can eliminate Sun (vendor-specific), GlobalPartner (specific to smart cards), DMTF (their angle is unclear), ANSI X9 (useful information, but it is specific to financial services),

3 See https://www.pcisecuritystandards.org/ for more information.

4 Cover Pages Topic Document, "Cryptographic Key Management," Cover Pages – http://xml.coverpages.org/keyManagement.html.

5 Full disclosure: the author sits on both the EKMI and KMIP technical committees.

KeyGen2 (seems specific to PKI), NIST (specific to federal sector – excellent resource, especially for writing security policies, but not pertinent here), W3C (working group charter expired in December 2005), Trusted Computing Group (standard appears to pertain to drive solutions), ISO (specific to 11770, there seems to be a lack of consensus), and IETF (KEYPROV just deals with key distribution). The original list can then be shortened to the following based on these criteria and observations:

- IEEE P1619.3 Security in Storage Working Group (SISWG), Key Management
- OASIS Enterprise Key Management Infrastructure (EKMI) Technical Committee
- OASIS Key Management Interoperability Protocol (KMIP) Technical Committee

In a matter of about fifteen (15) minutes of Internet searches and intuitive analysis the original list of potential standards has been cut by approximately 77%. Now the fun part begins. Or so you would like to think, except for one problem. If you look closely at the three remaining standards you will find that none of them is released yet. Fast-forward through the research process and you will find the following:

- EKMI has had a draft since January 2009, but it lacks adequate reference implementations. It lost key leadership coincidentally with the launch of the KMIP technical committee.
- KMIP has a draft, has strong vendor support, and is moving forward assertively.
- P1619.3 has encountered a few setbacks and is clearly not on track with the schedule asserted in June 2008.[6]

After all this research, most customers would be disheartened. From an initial list of thirteen potential standards, only three hold true potential for ensuring interoperability and cooperation among vendors, of which only one is on-track to be released in the near future.

Is there hope?

The good news, however, is that there is a clear leader in the key management standards race. Unfortunately, it may not be the standard you would choose based on technical merits. In fact, as is often the case, the trip to standardization is often one fraught with consensus and the watering-down of what were originally good ideas.

To top things off, despite filtering the list to a clear leader, we have also uncovered a couple interesting problems: relevance and performance. In the first case, many of the standards did not have immediate or apparent relevance to the project at hand. In fact, one could go so far as to say that very few standards were truly applicable to "symmetric key management" – particularly not from an enforcement standpoint. Certain standards, such as from NIST and ISO, provide good references for many aspects of cryptographic key management, but not to the degree of ensuring conformance. NIST Special Publication 800-57 provides a very thorough set of guidance for key management throughout the entire key life cycle, but you will be hard-pressed to find a certification process supporting it in the commercial sector.

Performance is the other problem that seems to plague standards committees. In this context, performance relates to the work being doing and the time frames assigned for completing that work. Standards are not generally run on strict

6 Luther Martin, "Key-Management Infrastructure for Protecting Stored Data," *IEEE Computer*, Volume 41, Issue 6 (2008) – http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=4548189&isnumber=4548155.

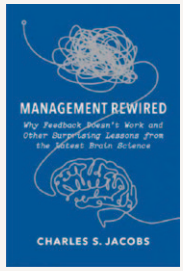
BOOK REVIEW

Reading Outside the Lines…

By Fred Scholl

Management Rewired

By Charles Jacobs



Good security requires the right state of mind within your organization. The security manager's role is to facilitate that state of mind within security team members, end users, and executive management. Along comes Charles Jacobs's new book, *Management Rewired*, which uses the results of modern MRI brain scanning techniques to provide security practitioners with guidelines on how to do that. Jacobs describes the failure, in business, of command and control management structures. But information security almost never has the "benefit" of such a structure. Jacobs's solution: "Rather than use force to get people to do our bidding, we'll be better served creating a mental environment that will select out what we need them to do." As such, the book is a gold mine of metaphors and stories that, with a little thought, can be employed to advance your security program. In fact, one of the key take-aways is the power of stories – as opposed to facts and numbers – to change the behavior of individuals and organizations. While this might be common knowledge, not many put it into practice in today's numbers-driven business. Jacobs's stories include slime molds foraging for food, Henry V defeating superior French forces in 1415, as well as the adventures of Odysseus and Agamemnon. If you don't have one, this book will help you develop a better security story for your organization. Let me know what you think.

About the Reviewer

Fred Scholl, PhD, CISSP, CISM, CHP, is a security consultant based in Nashville, Tennessee. A member of ISSA Middle Tennessee Chapter, he may be reached at freds@monarch-info.com.

schedules and are limited by the attentiveness of committee members. The OASIS EKMI and IEEE P1619.3 committees provide excellent reference cases for what happens when key leadership changes or when lead vendors modify their role in the process.

In contrast, the OASIS KMIP committee appears to be making excellent progress, but that is for a very specific reason. A handful of key vendors – many of whom were involved in P1619.3 and/or EKMI – got together on their own, drafted a standard, and then came to OASIS and asked to have a new technical committee launched. Thus, vendor support already existed to a high enough degree to nearly guarantee the swiftest process possible. That being said, it will still take the committee somewhere in the range of 18-24 months to take the standard to a final release state.

To top all of this off, consider the working groups that are developing standards, but without much visibility. The IEEE Key Management Summit held in September 2008 revealed this situation quite plainly. Many organizations wanted standards for key management, and yet many of the standards committees wanted their own standards to take precedence, despite the pre-existing work of other committees. Or, in other cases, certain committees had standards complete or in draft that, had they been known and recognized, could have provided a solid basis for cooperation. Unfortunately, some working groups simply had not been engaged by other standards organizations, or vice versa.

All of these observations paint a rather bleak picture of bureaucratic and dysfunctional practices and organizations plagued by in-fighting and painfully long development cycles. More importantly, customers are more-or-less at the mercy of the vendors, entrusting them with making decisions that will hopefully be in their best interest rather than their own self-interest. To top it all off, as in the case of KMIP, one is left to wonder if standards prevail because of the mandate of the most successful vendors rather than because of the virtues of the standard itself.[7]

A path forward?

Given the apparent dysfunction within most standards organizations, combined with the significant degree of overlap or competition, one is left to wonder if there might not be a better way to do things. Businesses operate under deadlines; why do standards committees not operate similarly? Many business decisions are made based on the apparent merits of the situation, so why do standards not benefit from a similar approach?

It would appear that the various standards organizations and processes could benefit from a degree of consolidation, collaboration, and some form of central leadership. The goal of such a central organization would be to globally coordinate development of standards, de-conflict standards that are on similar paths, bring participants together in a cooperative and collaborative manner, and work toward greatly improving communication, not only between vendors and committees, but also with customers. Too many announcements from too many organizations and vendors can actually serve to muddy the waters rather than provide a clear picture of the best way forward.

Unfortunately, this notion of having some central organization in charge is a naïve pipe dream. Given the competing interests of corporations and governments, it seems unlikely that all interests could be equally represented in an independent organization charged with coordinating all standards activity. As such, this leads to a counter-proposal: a single organization charged not with leadership but communication, cooperation, and collaboration. Specifically, such an organization could exist in order to monitor all standards activity, inform committees and organizations of activity, summarize the activity, and provide free and open analysis specifically targeted to customers.

If a tree falls in the woods...

In the end, one must wonder if there is enough interest in standards from the core constituency (customers) to justify creation of an organization that would be charged with monitoring standards organizations, encouraging collaboration and cooperation, and with providing expert analysis of current standards processes and drafts. More importantly, one must wonder just how this organization would be funded.

In general, it's unclear if the core constituency even cares. Do standards matter to the average enterprise? Interoperability is a frequent target for criticism of vendors, as is vendor lock-in, but to what end? Are deals being lost because of a failure to conform to standards? It seems logical that standards do serve a role once a tipping point is reach, but it's unclear how often these points are reached, or if it is frequent enough to be considered a pattern of good practice.

Yet imagine a world without standards. The Internet as we know it today…the digital age as we know it today…the entire computing age…none of it would exist without standards such as TCP/IP, Ethernet, 802.11, Peripheral Component Interconnect (PCI), Universal Serial Bus (USB), CAT5 and CAT6, RADIUS, Kerberos, LDAP, ATX, SCSI, IDE, PATA, SATA, and so on. Clearly the world has benefited from standards, whether or not the core constituency realizes.

Summary

Overall, standards are beneficial to society. However, the processes are plagued with bureaucracy, the development time lines are very long, and there is a general lack of interest from customers in the development process. There is demand for interoperability and cooperation, but no engagement beyond that point, leaving vendors to battle each other to achieve market superiority and prevalence. In many cases, standards are as much about de facto market position as they are about

7 Please note that this is not a criticism or observation of KMIP or the vendors supporting it. Rather, this is a general observation noting that KMIP is successful because of the drive of the large vendors that drafted it and are shepherding it through the OASIS process.

the development of meritorious and mutually beneficial frameworks.

The standards development process, vendors, and customers would benefit from an over-arching organization charged with monitoring standards processes, encouraging and coordinating collaboration and cooperation, and with providing expert analysis and recommendations. However, funding such an organization would likely be a daunting challenge, not the least of which being because it could serve to work against the self-interest of the vendors who would most benefit from the existence of the organization.

Unfortunately, the disparate and dysfunctional nature of the myriad standards bodies leads to excess market confusion. Too much competition amongst standards can lead to confusion that undercuts the standards process just as much as too little competition can create an unfair marketplace. Too many initiatives detract from those that have the most technical merit, creating confusion that eventually works against the interests of the vendors developing all the competing standards.

Leadership and consensus within the standards organizations themselves is also very important – particularly from the largest vendors. At the same time, this weight can be brought to bear unfairly on the process, and in some places can effectively undermine key initiatives. A standard committee that may be making good progress can suddenly find itself floundering if a key vendor pulls out of the process, even if the standard itself holds significant positive potential for the community at large.

Consensus is important, but at what cost? Standards epitomize the traditional academic approach to develop consensus around key topics. At the same time, they can also represent all that is wrong with using academic processes in corporate settings. Bureaucracy and long development cycles descend directly from the need to develop an adequate degree of consensus around all aspects of a standard, including the challenges in getting reference platforms implemented. Standards organizations would benefit from finding ways to dramatically lower time to market while maintaining process integrity.

Standards are too important to be allowed to continue in a dysfunctional and disengaged manner. It is time for customers and key organizations to step in and right the course, and perhaps help get the security and IT industries back on track in the process.

About the Author

Benjamin Tomhave, CISSP, is an independent consultant in Phoenix, AZ. He holds a MS in Information Security Management from George Washington University and is a member of committees within the American Bar Association and OASIS. He may be reached at tomhave@secureconsulting.net.

Speaking to their accomplishments and their views on information security.

Mary Ann Davidson

2008 Hall of Fame Award

Mary Ann Davidson is the CSO at Oracle, responsible for product security, as well as security evaluations, assessments, and incident handling. She is a member of the Global Chief Security Officer Council and was recently named one of *Information Security* magazine's top five "Women of Vision." She has served on the Defense Science Board and was recently named to the Center for Strategic and International Studies commission on cybersecurity. She has been involved in information security for the past 15 years and formerly served as a commissioned officer in the U.S. Navy Civil Engineer Corps, where she was awarded the Navy Achievement Medal.

Mary Ann Davidson receiving her award from International President Howard A. Schmidt.

What do you consider to be your most significant accomplishment as an information security professional?

I think my biggest accomplishment is building a great team, because you are only as good as the people willing to work for you and with you: any security improvements that I have made at Oracle were made by many people working in concert. In recent years, my team has been able to cope with an increasing number of products as a result of Oracle's acquisition strategy. They provide security subject matter expertise to a number of development organizations, and they are able to help newly acquired organizations to quickly jump on the Oracle Software Security Assurance bandwagon. Also, having a great team that executes so well has enabled me to work on "outside" projects like the Defense Science Board and the Center for Internet Security's Cybercommission for the 44th Presidency. What I have enjoyed the most has been testifying to Congress several times – an honor, a privilege, and a thrill.

What is the most important issue facing the industry and how would you like to see it addressed?

We have a national security problem because of poor cybersecurity. Fixing that requires radical change, starting with the mind sets of people who build software so they a) know they are building infrastructure, b) realize that infrastructure will be attacked, and c) design the infrastructure for resilience and self-defense. If every device (or piece of software) natively self-defended, we'd go a long way to improving everyone's cybersecurity. We need to apply the Marine Corps' ethos – *"every Marine a rifleman"* – to software. One of the ways to make that ethos part of what we do is to make security an integrated component of the IT and related curricula for all universities.

What is the biggest challenge currently consuming your time and energy?

Oracle makes a lot of acquisitions, and one of my big challenges is aligning the acquired entities with our secure development practices. To measure progress, we have developed a security scorecard in which – by group – we report how and where the group is in terms of compliance with our secure development practices. The scorecard goes to our security oversight committee and the CEO. Not surprisingly, we have found that when people know they are being "graded," they study harder – our compliance rates have accelerated since we started reporting progress to senior management. Also, sometimes we acquire entities that have not had a disciplined development practice (and of course, that affects security). We are identifying those groups that need "remedial help" and focusing the entirety of my teams' efforts on them (instead of being spread thinly across all groups).

What would you like to say to your peers?

Get involved in something bigger than yourselves: think about security in the larger picture of why what we do matters and how we can effect change. When I started in information security, it was like being the Maytag repairman: nobody called, nobody wrote, maybe a couple of customers (defense and intelligence) were interested in what Oracle was doing in security. Now, security is part of almost everyone's business because every business has an IT backbone. But it's bigger than that: our national security (in the economic and literal sense) rests on an IT backbone.

The last two wars have been "information-centric warfare" in which technology was a force multiplier. What happens to your ability to prosecute an information-centric war if the information flow dries up? Technology is only a force multiplier if you can use it; you are vulnerable if information use is denied you or turned against you by enemies. I always say that (officially) I have no favorite customers, but unofficially, anything I can do for the defense and intelligence communities to make their world better is a mitzvah – a good deed, indeed.

We live in what is the digital equivalent of the Wild West: we are traveling on heavily rutted roads and we face outlaws, predators, and ambushes. We want to move to nice, safe, clean interstates and not ever worry about being mauled by a grizzly bear. That digital world is worth building and none of us can build it alone.

Colorado Springs Chapter
2008 Chapter of the Year

More than 200 members

Mark Spencer

President ISSA Colorado Springs, USA Chapter

Mark Spencer is a senior systems security engineer with a major defense contractor. Currently president of the chapter, Mark served for seven years as vice president – on the elected board every year but one since 1999. He has been involved in information security full-time since 1993 and in some aspect of security throughout his military career.

What do you consider to be your chapter's most significant accomplishment in serving your members and your local information security community?

The Colorado Springs Chapter was among the first chapters chartered and has been around since the early '90s, but by the late '90s it had been foundering. We then decided, as a board, to focus on our membership and their professional growth. Since that time we have directed our every action to this end, including outreach to the community and non-members. This approach re-energized the chapter, and it has been growing – currently we have 360 active members – and we have helped to charter four other chapters. But it's not about the numbers…it's about service, to our members, to our community.

Colorado Springs Chapter President Mark Spencer and Chapter Board Member William "Wells" Fargo.

More than half our chapter members have professional certifications, and we encourage this professional growth through recognition programs such as recognition coins. We encourage and nurture those without certifications through a very active training and education committee. We do reviews for Security +, CISSP, and ISSEP. We reach out to other organizations like ISACA and SANS, promoting a range of professional certifications and obtaining discounts for our membership to make specialized training more affordable.

We maintain a yearly schedule which includes three conferences and 10-12 luncheons, all of which are no-cost to our membership. Our education program also includes helping to develop two masters programs and a doctoral program in Information Security at the Colorado Technical University. These education programs meet our needs and the university works with us to provide classroom space for our programs, including a wing of the university for our use during our one-day conferences (scheduled during their break) and thereby allowing us to minimize our overhead costs. Our relationship with Colorado Technical University includes the university providing ISSA memberships for all students enrolled in their information and digital security programs.

We focus on providing value to our membership. A one-day conference is typically $300 – ours are no charge – so our members save $600 for two one-day conferences. We search out and negotiate significant discounts and passes to other conferences in the region as well. The last time I checked, in 2006 we provided over $100,000 worth of services to our members and multiple scholarships to three local universities to support students studying information security.

We have sponsored an international outreach program for the past eight years. Whenever chapter members travel abroad, we provide a budget for them to hold informal discussions with local folks known as *Security Over Coffee and Donuts*. We helped the Santiago, Chile Chapter get started and will be working with folks in Bogota, Columbia to start a chapter.

What does it mean to you to be selected as Chapter of the Year?

It means that the hundreds of members who pitch in are being recognized for making the chapter what it is. It's not about the people who are the officers. It's about the people in the chapter who do all the work and help us make this chapter go. This is a very good chapter, and I am proud to be associated with it. The people work together well; they help one another. It is seldom, even in bad economic times, that we have very many chapter members out of work. At present we have five members looking – only five out of 360! Folks usually let us know before their contracts end; we pass the word around and somehow they get picked up. With 360 members looking for them, we'll find a place for everybody.

What is the most important issue facing the industry?

Our nation is trying to get its arms around cybersecurity. The government may make some decisions, like DoD did, to force people to be certified that will make it difficult to maintain employment. That's why we work so hard with our members to get the certifications that are appropriate. We've got to make sure we've got the proper people in terms of their skill sets to meet industry needs. That's what we try to do: provide a mixture of security management and security technical expertise, keeping the training programs available so we can all be well-rounded security professionals.

What would you like to say to your peers about your experience leading an ISSA chapter?

You must be committed to working for your membership; the more you are involved, the more return you get. Our chapters provide tremendous opportunities for our members to give back to our profession. Get involved!

Working with Standards – Special Section

In this section we will be presenting articles from information security professionals in the trenches and working with a wide variety of national and international standards.

How Much is an ISO/IEC 27000-Series Information Security Management System Actually Worth?

By Gary Hinson – ISSA member, UK Chapter

This paper identifies the benefits and costs arising from an Information Security Management System based on the ISO/IEC 27000 family of standards.

Summary

This paper identifies the benefits and costs arising from an Information Security Management System (ISMS) based on the ISO/IEC 27000 family of standards. It forms the basis for organizations both to develop better business cases justifying the initial investment in their ISMS implementation projects and to derive better metrics for optimizing the business value of their ISMSs in normal operation.

Organizations adopting the ISO/IEC 27000 family of standards (henceforth "ISO27k") to establish their Information Security Management Systems (ISMS) normally organize the associated work as implementation or organizational change projects requiring capital investments.[1] The amount of capital needed typically requires senior management approval, which is often the first explicit evidence of management support for the ISMS, itself widely acknowledged to be critical to the eventual success or failure of an ISMS.[2] A rational business model is therefore needed to estimate the costs and benefits of the ISMS, such that executive managers can reasonably assess the projected net value of the proposed investment, determine whether the proposed investment will generate worthwhile value, and make capital allocation decisions relative to competing capital demands.

Once operational, the ISMS becomes a regular management system, a set of internal activities funded through an annual budget like most other business functions. Tracking the costs and benefits due to the ISMS should help substantiate the projections and estimations in the original business case, and justify its continued funding.

This paper, expanding on two previous publications by the author,[3] [4] highlights the key business implications of implementing ISO27k by describing "typical" or representative benefits and costs, both financial and non-financial. The paper may thus be used to build business cases justifying ISMS implementation projects to senior management, and as a framework or template guiding the design of a system of ISMS metrics to measure and optimize the net value of their investment in information security management over the long term.

Business benefits of an ISMS

This section describes the financial and other business benefits an organization can expect to achieve by establishing and operating an ISMS based on the ISO27k standards.

Reducing information security incident costs

The primary purpose of an ISMS is to reduce the probability and/or impact of information security incidents, and hence

1 Laurence A. Gordon and Martin P. Loeb, *Managing Cyber-security Resources: a Cost-Benefit Analysis* (Mc Graw Hill, 2006).

2 For more on the ISO27k standards, please refer to ISO27001Security, an informational website about the ISO27k standards run by the author – http://www.ISO27001security.com.

3 Gary Hinson, "The Financial Implications of Implementing ISO/IEC 27001 & 27002: A Generic Cost-Benefit Model," (2008) – http://www.iso27001security.com/ISO27k_generic_business_case.rtf .

4 Gary Hinson, "Seven Myths About Information Security Metrics," *ISSA Journal* (July 2006). Also accessible online at http://www.noticebored.com/IsecT_paper_on_7_myths_of_infosec_metrics.pdf.

reduce the organization's security incident-related costs. However, the financial value of the savings is impossible to measure or calculate precisely. Given the sensitivity and hence reluctance for organizations to publicize details on security incidents they have suffered, the fact that few organizations systematically analyze the business impacts of information security incidents, and the variability of information security incidents, we lack the statistical or scientific basis for accurately predicting what would have happened without the ISMS in place. Nevertheless we can certainly estimate the value by projecting the anticipated reduction in probability of incidents occurring due to the range of preventive controls within the ISMS, and reduction of adverse impacts as a result of the detective and corrective security controls.

In effect, ISO27k organizations learn from others' mistakes.

An ISO27k ISMS emphasizes preventing or avoiding information security incidents wherever possible, rather than just minimizing and learning from incidents that do occur. The emphasis is a subtle but important benefit. Incidents that happen incur detection and resolution costs, as well as the business disruption, losses, and consequential costs, all of which are minimized if incidents are prevented or avoided. Furthermore, controls normally have to be improved after an incident anyway, whereas the best practice advice in ISO27k helps improve them beforehand. In effect, ISO27k organizations learn from others' mistakes.

For example, we might estimate that stronger preventive controls against malware would reduce the occurrence of malware incidents by, say, 50%, while improved detection and faster reaction to and recovery from malware incidents would cut the cost of malware incidents by around 25%. Estimating how many malware incidents we normally suffer and what they normally cost (e.g., in analysis and clean-up costs within IT, plus lost productivity and consequential losses in the business) provides the basis on which to estimate the anticipated savings from improving the malware controls. We would then move on to consider other forms of information security incidents in much the same way, ending up with an estimated value for the overall savings. Provided our estimations are sufficiently conservative and rational to survive management challenge, reduced incident costs alone will typically be more than sufficient to justify the cost of the ISMS – but we are far from finished yet.

Even if it is not already obliged to do so, the organization may eventually be forced into addressing its information security risks and controls by market, legal, or regulatory pressures, particularly if third parties demand ISO/IEC 27002 conformance or ISO/IEC 27001 compliance certificates as a prerequisite to inter-organizational business processes, information sharing, etc. By implementing the ISMS to its own time scales, management is able to choose the most cost-effective sequence and timing of activities, aligning them with other work and avoiding overlaps, gaps, or conflicts.

Bringing information security risks under explicit management control

In that it allows managers to direct and control the management of information security risks and controls more rationally and overtly than ever before, the ISMS creates further intangible/non-financial and tangible/financial benefits.

Compared to organizations that do not have an ISMS, those that do tend on the whole to appreciate and understand their information security risks better through having systematically analyzed them. They choose information security risk treatments more wisely and respond more effectively to changes in their information security risks.

An ISMS strengthens the existing information security control environment by emphasizing the organization's requirements and priorities for information security, focusing management's attention particularly on the greatest information security risks. It also allows management systematically to review and improve pre-existing information security controls, both initially at ISMS implementation time and periodically thereafter once the ISMS is operating normally.

The broad nature of the risks and controls used as examples within ISO27k reduces the chances of commonplace information security risks remaining unrecognized and perhaps untreated by the organization. The professional, standardized, and rational approach to managing information security risks promoted by ISO27k increases the consistency of information security risk assessment and treatments across multiple IT systems and business processes over time. Making vital information assets more readily accessible by employees who need them, and ensuring that the information is accurate, complete, and up-to-date, are just two examples of considering integrity and availability alongside confidentiality. The business benefits of information security are perhaps most easily demonstrated to management by considering the potential effects of security failures, e.g., drawing false conclusions from inaccurate or misleading information, or interrupting critical business processes because vital IT systems or data are offline.

ISO27k helps organizations mature their approach and processes for information security management. Through their direct involvement in the ISMS plus general security awareness activities, employees become increasingly familiar with information security concepts. The organization's capability and impetus to transfer certain information security risks rationally and selectively to insurers and other third parties, or to avoid certain risks by altering their IT systems and/or business processes (both of which are valid and worthwhile forms of risk treatment often neglected by organizations without an ISMS), increase.

ISO27k promotes an holistic, process view of information security, encouraging intra- and inter-organizational cooperation that improves the overall effectiveness and efficiency of information security management. Organizations that unduly restrict the scope of their ISMS lose out on this benefit. Organizations with discrete and relatively isolated "stovepipe" corporate functions for IT, software development, information security, risk, business continuity, compliance, internal auditing, etc., benefit from bringing them closer together through ISO27k. Collaboration on shared ISMS objectives can defuse the internal politics if any one function or business unit assumes the lead on its own account. Section 14 of ISO/IEC 27002, for instance, promotes the need for adequate contingency and disaster recovery planning to maintain critical business processes, supplementing the resilience, reliability, and other preventive measures recommended elsewhere in the standard. Organizations that already have a comprehensive approach to business continuity management may yet benefit from integrating those activities with their management of information security as a whole through the ISMS, avoiding duplication of effort and improving both effectiveness and efficiency (e.g., exploiting Business Impact Assessments performed for continuity planning purposes to identify critical business processes and the supporting IT systems needing strong information security controls). Similar savings are possible through alignments in other areas of the ISO27k standards such as Human Resources, IT and Physical/Site Security, and Facilities.

The benefits of standardization

The ISO27k standards describe a form of ISMS that is internationally recognized and highly regarded, yet at the same time flexible and adaptable. The core standards (ISO/IEC 27001 and 27002) have developed from BS 7799 during the past 14 years, while the family continues to expand and evolve to this day. By combining a risk-based approach with a management system, the ISO27k standards are widely applicable to most if not all types and sizes of organizations in a variety of markets and industries, albeit sometimes facing quite different information security situations. ISO/IEC 27002 recommends a suite of control measures that are generally accepted as best practice means of treating commonplace information security risks. Users are advised to consider their particular risks and determine whether the standard controls are both necessary and sufficient. Alternative or additional controls and other risk treatments can be implemented where necessary, but there is an implicit assumption that the stated controls are likely to suit most organizations, business units, departments, functions, etc. Any existing security controls which exceed the standards' requirements deserve a closer look and, if not justified, may perhaps be dropped or replaced. In short, using ISO27k avoids each organization "reinventing the wheel" on ISMS, saving the associated research and development costs. Organizations can simply implement the recommended controls knowing they are adopting a reasonable security baseline, and concentrate their finite resources on first identifying and satisfying any unique information security risk management and control requirements, and then improving over time.

Any existing security controls which exceed the standards' requirements deserve a closer look and, if not justified, may perhaps be dropped or replaced.

A further benefit is that ISO27k users share a common conceptual understanding and terminology for information security. They can, for example, discuss security requirements and controls more easily with business partners, consultants, auditors, and others who are familiar with ISO27k. Information security professionals who know ISO27k can get to work on the ISMS sooner with less effort to adjust to their new surroundings. Many of the technical tools supporting information security management are designed to support the implementation of ISO27k. ISO27k is the lingua franca of information security.

Government pressure to protect critical national infrastructures is yet another area that benefits from standardization. The developed nations are mutually and critically dependent on the security of the Internet and private networks. ISO27k offers the prospect of collaboration and cooperation to identify and address common information security risks at a global level.

The benefits of a structured, strategic approach towards information security

ISO27k comprises a logical framework for managing disparate information security controls and a rational basis for assessing and treating information security risks. It is internally and externally consistent, being reasonably comprehensive without being overly prescriptive. It is customizable and forms a solid basis on which to build organization- or industry-specific extensions as required.

In the absence of a comprehensive and holistic ISMS, organizations often address information security control investments as discrete point solutions. ISO27k encourages economies in areas such as physical protection for buildings or rooms housing critical equipment rather than protecting them individually (or leaving them exposed!). Security training of software architects, developers, and testers pays dividends across all development projects and, in time, all production systems and services, while pan-organizational awareness programs emphasize that information security is everyone's responsibility. Alignment and integration of information security into IT operations is another example where ISO27k extends the information security content and value of ITIL and ISO 20000.

ISO27k organizations almost invariably adopt information security policies and procedures that are better structured,

better written, more comprehensive, and more coherent than whatever they had beforehand. These are easier for staff and managers to follow consistently, especially as the associated awareness, compliance, and other management activities are themselves part of the ISMS.

The business impact analysis part of risk assessment provides the impetus for management to review the organization's business processes, IT systems, data and information flows, and external business relationships with the potential to reduce the overhead of duplicated and other unnecessary systems/data/processes (e.g., dispensing with inappropriate information security controls, rationalizing security processes, etc.), yet simultaneously improving the quality and dependability of information processing. The ISMS has an influence and relevance far beyond the IT department and may potentially be the trigger for business process re-engineering and similar profound organizational changes.

The emphasis is on management control and continuous improvement rather than proscribed compliance with specific requirements.

Business benefits of an ISMS accrue over the long term by management continually measuring the organization's performance and incrementally adapting the information security status in response to the perceived risks. An ISO27k ISMS encourages management to assess and react continuously to changes both within and without the organization regarding its information security risks and controls – for instance, identifying and responding to novel information security threats, newly identified vulnerabilities, and different potential impacts as a result of changes in the way the organization uses information. While all organizations could assess and respond to changing information security risks in theory, those with an ISO27k ISMS have the management system structure, policies, and processes to do so reliably in practice.

The benefits of certified compliance to ISO/IEC 27001

Certified compliance with ISO/IEC 27001 creates unique benefits for users of the ISO27k standards as opposed to other information security standards (such as NIST's *800-series Special Publications*[5] and the Information Security Forum's *Code of Practice for Information Security*[6]), valuable though such standards undoubtedly are. The most obvious advantage arises from the certificate itself, a formal statement by an accredited and hence trustworthy, competent, and independent body that the holder has properly implemented a compliant system to manage its information security. While having an ISO/IEC 27001 compliance certificate does not denote that the organization's information processes, systems, and networks are necessarily secure in an absolute sense, it does at least mean that the organization has brought information security firmly under management control and is proactively improving its information security. It assures stakeholders, auditors, business partners, industry regulators, etc., that the organization is actively addressing its information security risks, clearly demonstrating management's commitment to information security. There are obvious parallels here with other management systems such as those for quality (ISO 9000) and environmental protection (ISO 14000): the emphasis is on management control and continuous improvement rather than proscribed compliance with specific requirements.

ISO/IEC 27001 certificates are valuable both for the organizations named on them and for third parties who desire confidence in the certificate holders' ability to manage information security. There is more to this than mere marketing gloss, although ISMS certificates are legitimate differentiators for organizations that wish to be seen as secure. The certificates display competence and engender a level of trust that could otherwise only be achieved by third parties reviewing the holders' information security management themselves, a costly and awkward process (not least because of the inherently sensitive nature of information security and the practical difficulties of finding sufficient competent assessors/auditors). This is particularly valuable for large organizations dealing with multiple third parties, especially in information-centric industries, since their ISMS certificates significantly reduce the number and/or depth of third party security reviews they must entertain. There are emerging signs that ISO27k compliance certificates may eventually be de facto requirements for participation in certain industry segments. Meanwhile, ISO/IEC 27001 compliance certificates offer marketing advantage for early-adopters, being a "badge of honor" similar to ISO 9000 quality marks. Organizations that are reluctant to demonstrate their competence in information security management through certified ISO/IEC 27001 compliance may lose out to their certified peers who thereby gain competitive advantage.

As a result of assessing the organization's information security risks and introducing or improving information security controls systematically through the ISMS, management may potentially negotiate reduced insurance premiums (or self-insure) and improved credit ratings. Along with the security improvements, the rational risk assessment and documentation of security controls contribute to this benefit, while certified compliance adds further assurance as to the quality of the organization's information security.

Other compliance benefits

Compliance has traditionally been a weak area in many organizations' management of information security. The recent

5 National Institute of Standards and Technology (NIST), Computer Security Division. Special Publications in the 800 series cover information security – http://csrc.nist.gov/publications/PubsSPs.html.

6 Information Security Forum, Standard of Good Practice for Information Security (2007) – https://www.isfsecuritystandard.com/SOGP07/index.htm.

Operating an ISMS in accordance with globally accepted good practice standards demonstrates due diligence towards information security.

upsurge of interest in governance is re-emphasizing the need for management to go the extra mile on compliance since organizations face an expanding range of external compliance obligations and senior managers are increasingly held accountable for information security and other incidents. As IBM puts it, "Business leaders can leverage security, risk, and compliance-related investments to competitively position their organization and satisfy complex regulatory guidelines."[7]

Some governments, industry regulators, business partners, or other stakeholders insist on ISO/IEC 27001 certification and/or ISO/IEC 27002 compliance, for example in connection with privacy laws or contracts and Service Level Agreements. An ISO27k ISMS therefore helps the organization avoid fines, commercial penalties, and other costs and impacts resulting from their non-compliance.

Section 15 of ISO/IEC 27002 specifically encourages organizations to evaluate their obligations to comply with applicable laws, regulations, license agreements, and contractual clauses relevant to information security. In risk terms, failing to comply with mandatory external obligations increases the possibility of adverse legal, regulatory, or commercial impacts that must be carefully managed alongside other information security risks. Once again, the systematic ISO27k approach forces management to face up to their responsibilities and provides a structured way for them to do so. Even when ISO27k compliance is not explicitly mandated, it may support or facilitate meeting other mandatory information security obligations (such as the Payment Card Industry Data Security Standard PCI-DSS) and invariably provides a broader context for information security than the individual regulations.

Certified compliance with ISO/IEC 27001 may narrow or negate third party claims for indemnity and compensation in case of information security incidents. It could certainly be argued that operating an ISMS in accordance with globally accepted good practice standards demonstrates due diligence towards information security on the part of management.

ISO/IEC 27002 section 15, plus sections 6 and 7 of ISO/IEC 27001, also recommend internal ISMS compliance activities such as management reviews and audits to ensure that employees follow the organization's own information security policies and procedures, etc. Many an information security policy or procedure sits quietly collecting dust on a cubicle shelf or languishing in some dark corner of the corporate intranet in organizations lacking a sound ISMS. Security awareness activities, management oversight, policy reviews, internal audits, and so forth all help drive up compliance, ideally to the point where information security becomes an integral part of the corporate culture – "the way we do things."

Reputational and branding benefits

Public and private sector organizations in industry sectors in which information security is a primary business objective (such as banking, government, and defense) clearly depend on establishing and maintaining information security as a core part of their brand value and image, and indeed an inherent part of their products and services. By the same token, if organizations in such sectors suffer information security incidents, their brands may be harmed and, in the worst cases, they may be put out of business. Recent high-profile incidents involving credit card processing companies, national intelligence agencies and so on ably demonstrate this.

While possessing an ISMS certainly does not guarantee that an organization will completely avoid information security incidents, it is a fair bet that they have better information security controls in place and hence will suffer fewer incidents than their peers without an ISMS, and furthermore that any incidents that do take place will probably be addressed and resolved more efficiently and effectively with less severe impacts. As awareness of this differential gradually spreads, some organizations are already starting to request if not demand ISO27k compliance of their business partners, and some are using their ISO/IEC 27001 certification as a marketing tool. Many IT outsourcing and offshore development companies based in India, for example, are actively adopting the ISO27k standards, offsetting the perception elsewhere in the world that India's data protection and other information security laws and practices are relatively weak. Information security could easily be the determining factor in deciding whether to use foreign call centers, back-office processing, etc., with ISO/IEC 27001 certified suppliers having a distinct commercial advantage (in other words, they are able to secure more business, increase turnover, and/or make higher margins).

An organization's reputation for strong or weak information security may conceivably affect its vulnerability to hacks, frauds, and similar concerted attacks, although this can work both ways. High-profile organizations effectively set themselves up as potential targets, even if they achieve that profile by promoting their security status. There is a lot to be said for the advice in a military training manual: "Try to look unimportant: the enemy may be low on ammo."

Costs involved in designing, implementing, and operating an ISMS

Whereas I have described the benefits of an ISMS at length to illustrate their rich variety, the costs of an ISMS are generally

7 IBM, "Introducing the IBM Security Framework and IBM Security Blueprint to Realize Business-Driven Security," (2009) – http://www.redbooks.ibm.com/redpapers/pdfs/redp4528.pdf.

more self-evident and specific to the organization; hence, this section is more superficial and brief.

ISMS specification, design, development, and implementation costs

The costs involved in establishing the management system part of an ISMS should ideally be considered separately from the costs associated with the information security controls themselves, particularly if expenditure on the controls would have been necessary even if the ISMS did not go ahead. This approach helps clarify the incremental costs involved in bringing all the information security controls together under a coherent management system. Activities such as reviewing information security risks and controls, updating existing or preparing new information security policies, guidelines, procedures, etc., should normally take place anyway. In practice, however, implementing an ISMS does imply additional activities and resource requirements, particularly if the organization does not already have reasonably strong and comprehensive information security controls. Simply preparing, reviewing, and approving the ISMS business case requires management time and effort.

Project management of the ISMS implementation project itself is a clear example of an ISMS-specific cost, as are the recruitment expenses relating to any additional information security managers or staff needed to run the ISMS and associated processes and systems thereafter.

Other one-off investments may be needed to bring specific elements of the organization's information security risk management and controls framework up to scratch, and these can usefully be identified as subprojects, perhaps separately cost-benefit justified and funded. Examples may include:

- Learning or content management systems to manage and disseminate security policies, procedures, etc.
- Identity/authentication and access management systems to control user IDs, access rights/permissions, etc., for application systems
- Vulnerability and change management systems to help keep up to date with security patches

ISMS certification costs

Pre-certification and certification assessment activities by an accredited ISO/IEC 27001 certification body are likely to cost a few thousand dollars, more if your organization is widespread and complex, less if you shop around. You also need to budget management and staff time to escort and assist the auditors on the day and deal with any significant non-conformances they identify that need to be resolved for certification. The quality of your ISMS and your readiness for the certification audit influence the time and hence costs involved. Stress levels are generally lower if you are well prepared.

You may be able to arrange combined audits of multiple management systems, reducing the overall cost but increasing the complexity and disruption caused. Ask the certification bodies about this.

The ISMS itself can be seen as a relatively minor overhead on top of the necessary expenditure on information security controls, compliance activities, security awareness, etc.

Annual surveillance and tri-annual re-certification assessments will also be needed but, in the grand scheme of things, these are relatively minor costs. Canny customers use them to drive home any outstanding security improvements, and as a source of good practice advice from the assessors.

Ongoing ISMS operational and maintenance costs

Once the ISMS is up and running, there will be various operational and maintenance costs, but they vary according to the nature and scope of the ISMS. It is probably worth differentiating the costs involved in running and maintaining the management system per se from those relating to the information security controls being managed, since the former are more likely to be discretionary while the latter tend to be required in any event to limit the organization's risks. Seen in this light, the ISMS itself is a relatively minor overhead on top of the necessary expenditure on information security controls, compliance activities, security awareness, etc., and should be entirely justified by the numerous benefits described in the first part of this paper.

Costs relating to organizational change

ISMS implementation requires a number of changes in the organization's information security activities, while the stability and structure the ISMS brings inevitably can make subsequent changes more difficult. Existing information security policies, procedures, practices, etc., will need to be documented, reviewed, and often adapted to suit the ISMS, and insecure working practices will (hopefully!) be eliminated. On the other hand, the continuous improvement cycles from ISO/IEC 27001 provide a mechanism to adapt more readily and efficiently to changes.

Employees, contractors, or business partners who consistently or flagrantly refuse to comply with the information security requirements, policies, procedures, etc., may have to be "let go," disciplined, sacked, and/or conceivably prosecuted. Changes of this nature are positive from an information security perspective and are anticipated to reduce the organization's information security impacts over time, but nevertheless cause disruption and short-term costs to the departments and teams immediately involved. The ISMS provides the context, information, and processes to deal with this in a structured manner, and I submit that it is far better to bring these

Please continue on page 39

Hacking the Kiosk

Managing the Risk of Public Information Systems

By Bradford Smith

Using the case of an interactive kiosk, this paper informs the reader how to identify threats and uncover common vulnerabilities.

Summary

Managing the security of information systems in today's interconnected world is a complex and challenging task. Maintaining an accurate perception of an enterprise's digital security posture is key to understanding what is at risk. Using the case of an interactive kiosk, this paper informs the reader how to identify threats and uncover common vulnerabilities from the perspective of people, process, and technology. It concludes with four timeless information security principles that are specifically applied to kiosks.

Interactive kiosks are prevalent in society – in the airport waiting area, the street corner phone booth, the business visitor lobby, and national hotel chains. They are often used for commercial purposes, such as the GPS tracking and advertising touch screen in the back seat of a taxi. Other times they provide a public service, such as those found at the Hall of Records at the community civic center.

One reason for this proliferation is the efficiency of paperless business processes. Companies can accept job applications or invoice customers without printing a single sheet of paper. As most companies already have web applications that perform these functions, the interactive kiosk is an efficient way to improve accessibility.

But this efficiency does not come without a price. Alarmingly, kiosks are beginning to appear in the news about computer intrusions. This is because kiosks provide temptation to both casual passersby who attempt to hack the device on impulse and malicious users who might launch sophisticated and targeted attacks against the kiosk infrastructure.

Kiosk data breaches

Listed below are some real incidents involving computer kiosks:

- **Automotive manufacturing** – Six distribution facilities were shut down for over seven hours after an ex-contractor used a kiosk in the visitor's lobby of one of the facilities to delete files and passwords on critical systems, causing more than $29,000 in damage and downtime.[1] This is just one example of a computer kiosk being used in an attack against a company.
- **Metropolitan transportation** – NYC taxi cabs outfitted with a kiosk in the back seat enable passengers to pay, track their travel via GPS, view advertisements, and watch news. An insecure touch screen gave passengers the ability to surf the internet and gain unauthorized access to the computer operating system itself. Potentially, malicious software could have been installed to steal the credit card numbers of future passengers. This story ran on WNBC-TV and prompted an investigation by the Taxi and Limousine Commission after a blogger published pictures that documented the compromised system. Although there were no reported cases of stolen credit card numbers, this is a good example of how a computer kiosk might potentially be used to attack others users of the kiosk.
- **Computer Security Vendor** – During a popular computer security conference in 2007, attendees demonstrated how to install adware and examine Google search histories of previous users of a public kiosk. The irony is that the kiosk was part of a display for a security vendor, causing some to assume it had been secured.[2] This is an example of an insecure information kiosk indirectly damaging a company's reputation.

Anticipating threats

Many of the threats can be identified by observing the unique aspects of information kiosks and how they are different from other technology. The distinguishing characteristics of the public kiosk are:

- **It is an unattended device** – Users operate it on their own, mostly without staff supervision or intervention.
- **It provides a specific service** – Only the features necessary to complete the task intended by the kiosk are enabled.

1 "Computer Contractor Pleads Guilty" – http://detroit.fbi.gov/dojpressrel/pressrel07/de060107.pdf.

2 "Conference Computers So Faux Secured," *Wired Magazine* – http://blog.wired.com/27bstroke6/2007/02/rsa_conference_.html.

Typically, users cannot install programs, tamper with kiosk software, access the underlying operating and file system, or view data entered by other users.

- **It is deployed in a variety of environments** – A kiosk could be set-up in the middle of a mall or even on an airplane. It could be set-up at a conference that changes locations every month or in a corporate lobby. Depending on the applications and data it requires, it is often connected to a network.
- **It accepts anonymous access** – Unlike a corporate network where users can be assigned different IT privileges according to groups and based on their identity, a kiosk generally allows all users to operate according to the same access restrictions. Therefore, it is not easy to distinguish between trustworthy and malicious users.

Simple threat classification

Based on the above characteristics, which are inherent to the kiosk environment, threats to the security of information kiosks can be classified into three categories: threats to the hardware, threats to the end users, and threats to the vendor.

Threats to the hardware

The biggest threats to the kiosk hardware are *vandals*. These people exploit vulnerabilities in the kiosk's physical access controls. This includes theft of hardware, for example from an unlocked cabinet, stealing accessories like the keyboard or mouse, or physical damage. Protecting against this threat is foundational, as stated in the common "law" of computer security that "if a bad guy has unrestricted physical access to your computer, then it's not your computer anymore."[3]

Threats to end users

The biggest threats to end users are *identity thieves and fraudsters*. These people exploit vulnerabilities in the kiosk's logical access controls. Their aim, in today's ecommerce-driven world, is to steal credit card numbers and personal information from others. A highly trafficked kiosk is a juicy target for their malicious software.

At the time of this writing an individual is currently awaiting jail sentencing for having installed malicious software that allowed him to intercept data from customers who used business kiosks. The stolen data was transferred to a website he controlled. The FBI discovered that he used this information to make over $30,000 of fraudulent charges to these accounts in three days.[4]

Threats to the vendor

The biggest threats to the vendor or owner of the kiosk are *competitors and cybercriminals*, broadly defined as anyone who can profit from the obtaining the company's confidential information. These people attempt to exploit vulnerabilities in the implementation of the kiosk. For example, due to the variety of environments in which kiosks are found, it can be difficult to deploy the kiosk on a dedicated network segment. So it is often connected to a shared network. This transforms the kiosk into a new attack vector for gaining access onto other systems on that network.

The author of this article encountered this situation while performing penetration testing at a government agency. Not only was the insecure kiosk connected to the internal network, but it had drives mapped to critical servers and unrestricted Internet access. Unfortunately, this is a common occurrence. A small vulnerability in the kiosk gives an attacker a large window into an organization's internal network.

The use of integrated networks in the airline industry has been frequently discussed. Recently, the U.S. Federal Aviation Administration cautioned that the computer networks onboard the new Boeing 787 Dreamliner may not properly isolate the passenger network from the plane's control network.[5] This is an important reminder of the consideration that needs to be given to the kiosk and how it relates to the system as a whole.

This brief survey of the threat landscape shows the potential impact that an insecure kiosk can have. The next section on common "low-hanging fruit" vulnerabilities further refines this understanding.

Exploiting Vulnerabilities

As mentioned earlier, the purpose of a kiosk is to provide a specific service. This is often enforced by special "kiosk software" that restricts a user from doing anything apart from the allowed function. If users can gain access to the underlying operating and file system, they can potentially bypass the kiosk access controls. Even the simplest application might have features that can give an attacker a foot-hold towards compromising the system. Therefore, the biggest challenge in securing a kiosk is limiting the features on an often feature-rich system. This is often implemented in kiosks by restricting the user to a logical "jail" or "sandbox."

The term used to describe this concept is *reference monitor*. The idea is that the part of the system that governs access control needs to be tamper-proof and impossible to circumvent. The most common ways to circumvent the kiosk access controls are listed below. These are all examples of *privilege escalation* vulnerabilities.

Word Processors

On the surface, a word processer seems like a straightforward application. But most enterprise word processors ship as part of a larger suite of products. One of the features included when installing Microsoft Word is a development environ-

3 "10 Immutable Laws of Security" – http://www.microsoft.com/technet/archive/community/columns/security/essays/10imlaws.mspx.

4 "Man Pleads Guilty to Hacking into Hotel Business Kiosks" – http://www.usdoj.gov/criminal/cybercrime/tandiwidjojoPlea.pdf.

5 "FAA: Boeing's New 787 May Be Vulnerable to Hacker Attack," Wired Magazine – http://www.wired.com/politics/security/news/2008/01/dreamliner_security.

ment called the VBA (Visual Basic for Applications) editor. This environment can be activated from a blank word document by pressing **ALT + F11** on the keyboard. Given access to this, a kiosk user could use the VBA editor to write a script that would give him access to computer functions that could be used to break out of the above-mentioned jail or sandbox environment.

Although not as likely to been seen today, the concept of privilege escalation can also be illustrated in *vi*, a de facto Unix text editor. In vi, users can insert text into the document and can also type commands that vi will execute for them. The "!" key refers to a shell escape and will execute a command *using the same privileges as the vi program!* If vi was allowed to execute with higher privileges than the user, access to previously restricted resources could be obtained through the shell escape. For example, executing *sudo vi* and entering the command *:!sh* would escape to the shell with root privileges. Other programs, including ftp, also use the ! key to invoke shell escapes.

Web browsers

Checking to see if a web browser is locked down is one of the first things a tester will do during a kiosk penetration test. It is not enough for the address bar to be disabled. Even if right-click is disabled, simply clicking on a hyperlink and pressing the **SHIFT** key at the same time will open up a new browser window, often with the entire address bar and menu enabled. Once the user has access to the address bar, he can usually access non-approved external websites as well as the file system and all mapped drives by browsing to C:\.

Calculator

All Microsoft Windows computers contain a hidden web browser. For this example Calc.exe is used, but the following works on any application that has a help screen. This can be accessed by selecting the help item (or press **F1**) from the menu bar of the application. There is a small icon on the program bar that when clicked gives the option to "Jump to URL." Websites and local files can be accessed using this method. This is illustrated in Figure 1.

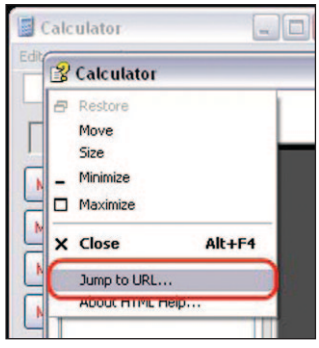


Figure 1: Accessing a hidden web browser in Microsoft Windows

Printer

Another easy way to exploit kiosks using Windows Internet Explorer is through the *Print* dialogue box. This can be accomplished by pressing **CTL + P** or **CTL + SHIFT + F12**. From within the print dialogue box, there are at least two ways to access the file system. One way is to select the "Print to File" check box and then click the "Print" button. This will open up a file browser. The second method is to right-click somewhere in the "Select Printer" area select "Add Printer" or

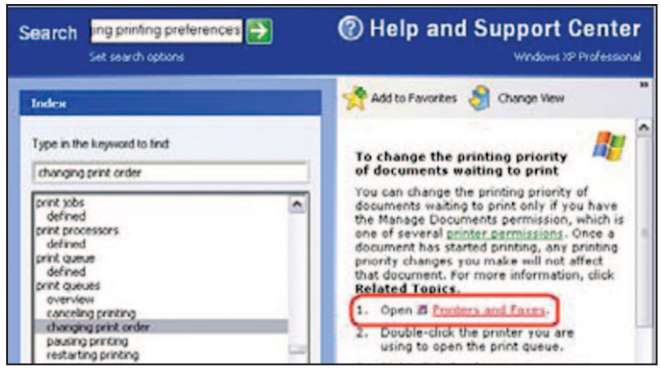


Figure 2: Using Help Center to launch the control panel

"Properties." Windows Explorer can then be accessed from the subsequent screens.

Help and support center

In addition to the hidden web browser technique described above, the Help Viewer can be used to launch the control panel. This can be accessed by pressing **WINDOWS KEY + F1**. Search for the help page on "Changing printing preferences." Click "Printers and Faxes." This is illustrated in Figure 2.

These four examples underscore the difficulty that kiosk administrators and software developers have with enforcing access restrictions. They also give an idea of how many, some seemingly esoteric, parameters and registry keys must be blocked by an admin who is trying to lock down a kiosk. Missing any one of these can let an attacker in.

Strategic recommendations

What does it mean for a kiosk to be secure? Often people pursue "security" without a clear idea of what that means. Usually, if the impact of a threat exploiting a vulnerability is negligible, then the kiosk can be called secure. It is important that the answer to that question take into account the context, threat environment, and potential vulnerabilities of the kiosk. Having done so, this paper presents four principles that can be incorporated into the process of securing the kiosk.

Timeless security principles

Although these principles were first published in 1970s,[6] their application remains relevant to computer systems today.

Fail-safe defaults

Because a kiosk serves a specific purpose, it is best to specify what actions a user can take, rather than what actions they cannot take. In other words, use a white list instead of a blacklist approach. Not only does this require less complexity, but it prevents failures from going unnoticed because an alert can be sent out when an intrusion is detected. The system can assume that anything not explicitly permitted is a security violation and commit the action to a log file.

6 Schroeder Saltzer, "The Protection of Information in Computer Systems." *Proceedings of the IEEE* 63, 1975.

Least privilege

Each component of the kiosk should operate using the least set of privileges necessary for its function. Avoid giving out any unnecessary capabilities. This also limits the damage that can result from accidents or errors.

Component	Example
Internet/network	Block outbound Internet access if the system's job is to provide access to a locally hosted website.
Network	Consider the kiosk an untrusted device and segregate the network it is connected to from the internal networks.
Operating system	Reduce the number of available features by running embedded operating systems or thin clients.
Hardware	Realize where hardware restrictions can be bypassed. The on-screen keyboard is often used to bypass restrictions from a limited or disabled physical keyboard.
Authentication	Access to administration areas should rely on proper credentials rather than obscure key combinations or mouse movements.

Least-common mechanism

One of the main features of a kiosk is that it is shared by many users. A certain amount of segregation and isolation is necessary. Potential information paths between kiosk users should be minimal. This might mean wiping the kiosk storage and memory after every session or at the end of the day.

Open design

It is strongly encourage that the kiosk implementation be subjected to threat modeling, code reviews, or penetration testing. Exposing and fixing the weaknesses of a system provides a high degree of confidence and assurance, rather than relying on ignorance of a system's vulnerabilities.

Summary

Many kiosks have faux security and are at risk of being exploited, potentially resulting in reputation damage, fraud, and identity theft, all of which can have a financial impact on an organization. By anticipating potential threats and uncovering common vulnerabilities, businesses can manage their public information systems with a high degree of confidence that the impact will be minimal should someone hack their kiosk.

About the Author

Bradford Smith is a consultant with Foundstone Professional Services, a division of McAfee, Inc. Brad offers trusted advice to professionals who need to advance their corporate information security strategy. His core expertise as a network and application security professional underpins the broader business objectives of his clients. He is based out of Foundstone's southern California office and may be reached at Bradford.smith@foundstone.com.

ISO 27000-Series ISMS continued from page 35

issues into the open than to pretend they do not exist, or even worse to remain blissfully ignorant of the risks.

Conclusion

Although the question posed in the title is challenging, the range of costs and benefits described here in generic terms has hopefully stimulated you to build your own business case for investment in a new ISMS or to get more value from an existing one. In particular, I have explained how the management system per se adds value to the information security controls.

Finally, I would like to emphasize the value of information security metrics. Most if not all of the costs and benefits identified in this paper can be measured using a combination of objective and subjective measures. A well-written ISMS business case explicitly identifies parameters that can be used as metrics to be tracked and reported once the project is approved and the ISMS is established. Even more importantly, metrics can help optimize the net value of an operational ISMS. ISACA's Val IT method[8] takes the line that a business case for, say, a software development project should project the anticipated costs and benefits, and that these in turn provide worthwhile metrics to help the organization get the most out of both the project and the delivered system. I recommend applying the same "total cost of ownership" and metrication concepts to your ISMS, using better information security for genuine long-term business advantage rather than mere survival. An ISMS that demonstrably generates net business value is an asset to the organization and thus self-sustaining.

Acknowledgement

I gratefully acknowledge the contribution of ideas to this article by Karsten M. Decker.

About the Author

Gary Hinson, PhD, MBA, CISSP, is an information security awareness specialist. Gary is a passionate supporter of the ISO/IEC 27000-series information security management standards through SC27, the ISO/IEC committee responsible for writing them, and www.ISO27001security.com. He may be contacted at Gary@isect.com.

8 ISACA "Val IT," (2006) – http://www.isaca.org/Template.cfm?Section=Val_IT3&Template=/TaggedPage/TaggedPageDisplay.cfm&TPLID=80&ContentID=51867.

OSSEC

By Russ McRee – ISSA member, Puget Sound (Seattle), USA Chapter

Prerequisites

Linux host for the OSSEC server/manager
OSSEC agents run on Linux, MacOS, Solaris, HP-UX, AIX and Windows

Similar Projects

OSSEC is included in OSSIM[1]

This month's *toolsmith* is the first that comes to you as the result of a contest I put forth on my blog challenging you, dear reader, to propose a topic. The contest promised that the reader whose topic I choose for a given month will receive an information security book of my choosing. Doug Burks of Security Onion[2] proposed OSSEC. Congratulations, Doug, I'm long overdue to cover OSSEC HIDS and am pleased to finally be doing so.

OSSEC HIDS, from Third Brigade (a Trend Micro acquisition), is an open source host-based intrusion detection system (HIDS) that performs log analysis, file integrity checking, policy monitoring, rootkit detection, real-time alerting, and active response. OSSEC runs on most operating systems, including Linux, MacOS, Solaris, HP-UX, AIX and Windows. Learn everything you need to know about OSSEC at the website.[3]

I asked Doug to tell me about his experience using OSSEC and he provided some excellent examples.

One of his favorite uses for OSSEC is on a webserver running the LAMP stack. With OSSEC installed and *file integrity checking* and *rootkit detection* enabled, OSSEC will immediately monitor `/var/log`. If an attacker tries to brute force his SSH or FTP daemons, OSSEC alerts Doug. If an attacker attempts HTTP reconnaissance, OSSEC will see the excessive HTTP error codes and alert Doug. If an attacker is able to circumvent defenses and gain access to the server, any file modifications or rootkit installations will be detected by OSSEC and Doug will be alerted. This makes Doug happy, but he's not done yet. He also configures *iptables logging* for OSSEC.[4] If an attacker port-scans the server, OSSEC notes that iptables dropped a large number of packets from a single source IP and will alert. Doug further increases his detective capabilities by installing Snort and configuring it for plain-text logging. OSSEC can monitor the Snort log and alert anytime Snort does (see more on Snort monitoring below). Yet another useful option on Apache webservers is the ModSecurity module that acts as a Web Application Firewall (WAF), includes signatures for many web attacks, and is customizable. OSSEC can monitor and alert on the ModSecurity logs as well. For WordPress defenders (that best be all of you WordPress users ;-)), there's the new WPSyslog2,[5] a WordPress plugin that sends WordPress events to syslog, which in turn is monitored by OSSEC. Every layer of Doug's system architecture is instrumented and all logging is aggregated into OSSEC.

Doug also suggests that OSSEC users consider *Active Response*. If enabled, OSSEC will not only alert but also configure TCP Wrappers and iptables to block traffic from the attacker's IP address. This translates to OSSEC moving from HIDS to HIPS (host intrusion prevention system).

NOTE: Like any use of intrusion prevention, proceed with caution. False positive detection with Active Response enable can lead to known good traffic being dropped. Yet, properly tuned, OSSEC running in Active Response mode can effectively protect your server from compromise.

Finally, Doug's also used or suggests using OSSEC as follows:

- User Account Auditing
  - Install OSSEC agent on all Windows Active Directory Domain Controllers
- PCI[6]
- DMZ under strict Change Control
  - File integrity checking
- Splunk as a Web Interface[7]

I think I know why Doug called his namespace Security Onion. The man knows his layers, also best known as defense in depth. Well done, Doug.

Install and configure OSSEC

There is an entire book[8] regarding OSSEC, and the installation chapter is freely available,[9] so I won't spend a great deal of time on what is already a well-established process.

1 http://www.alienvault.com/products.php?section=OpenSourceSIM.
2 http://securityonion.blogspot.com.
3 http://www.ossec.net/main/about.
4 http://www.ossec.net/wiki/index.php?title=Know_How:Iptables_Config.
5 http://www.ossec.net/wpsyslog2.
6 http://www.ossec.net/ossec-docs/ossec-PCI-Solution.pdf.
7 http://www.ossec.net/main/splunk-ossec-integration.
8 http://www.ossec.net/main/ossec-book.
9 http://www.ossec.net/main/manual/manual-installation.

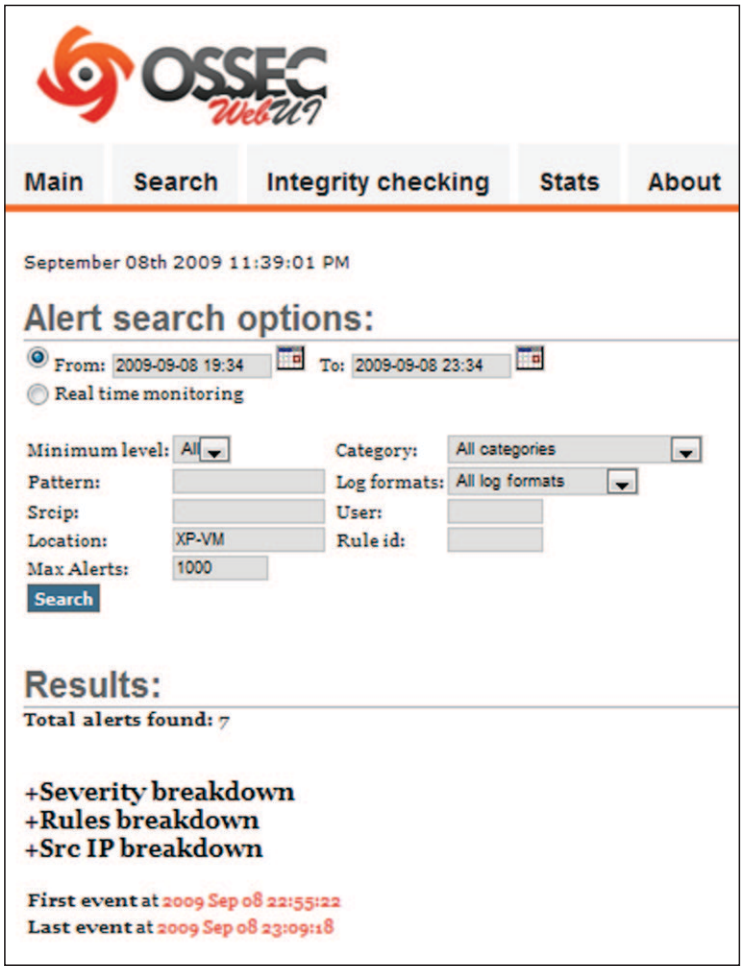


Figure 1 – OSSEC Web

On Ubuntu 9.04, setting up the server is as simple as downloading the latest OSSEC (version 2.2 is current as this is written) and executing the following:

1. `tar -zxvf ossec-hids-*.tar.gz`
2. `cd ossec-hids-*`
3. `sudo ./install.sh`

Be sure to allow port 1514 (UDP) if you're utilizing your server firewall so that agents can connect.

Execute `/var/ossec/bin/ossec-control start` to start OSSEC HIDS.

I followed all recommended conventions and installed the OSSEC server on my Ubuntu 9.04 servers. I further installed the OSSEC Windows agent of Windows XP and 2003 virtual machines.

Installing the agent is a point-and-click effort until you need to join the agent to the server. When prompted by the Windows agent, engage a terminal on the server and issue the following:

1. `sudo /var/ossec/bin/manage_agents`
2. Choose *A* to add an agent and provide the name, IP, and ID for the new agent.
3. Return to the menu and choose *E* to extract the key for the new agent, copy the key to a file or your clipboard, and make it available to the Windows host where you're installing the new agent.
4. On said Windows host, provide the OSSEC server IP and the agent key you extracted in step 3, save, and then start the agent.
5. You can confirm that the agent is running in the agent UI on the Windows host, and you can also choose *L* to lists agents on the server, from the manage_agents menu.

I also installed the OSSEC web interface (WI) on the server. As seen in Figure 1, the WI allows you to conveniently review and query events, modified files for all agents, and stats.

You certainly don't need the web UI, as you can configure email alerting to your preferences, and you can also grep or Splunk `/var/ossec/logs/alerts` for events of interest.

In `/var/ossec/etc/ossec.conf` on the server, and from *View => View Config* on the Windows OSSEC Agent Manager, you can tune the configurations to your liking. Decide what rules sets you'd like to make use of, what files and directories should be monitored for file integrity checks (think PCI compliance) as well as those you'd like ignored. You can also tune rootkit checks, log monitoring preferences, including syslog, Snort, and VMWare, as well as the active response option (again, set this carefully with lots of testing).

While I only tested OSSEC HIDS on Linux and Windows, it works quite capably on MacOS, Solaris, HP-UX, and AIX.

OSSEC HIDS: Defense in depth

OSSEC and Snort logs

I freaked myself out while writing this (neither uncommon nor difficult) when I fired OSSEC up for the first time on one of my stealth Ubuntu servers and the very first email alert it popped after the initial "ACK, I'm here" was as follows:

```
OSSEC HIDS Notification.
2009 Sep 10 10:55:08

Received From: flintstone01->/var/log/snort/alert
Rule: 20100 fired (level 8) -> "First time this
IDS alert is generated."
Portion of the log(s):

[**] [125:7:1] (ftp_telnet) FTP traffic encrypted
[**][Classification: Preprocessor] [Priority: 3]
92.243.8.139:21 -> none.of.your.business:37868

--END OF NOTIFICATION
```

Nice. Obviously I should have been watching `/var/log/snort`, and more obviously, had not been.

At first glance that alert looks really bad to someone who knows that there is absolutely no reason for an established

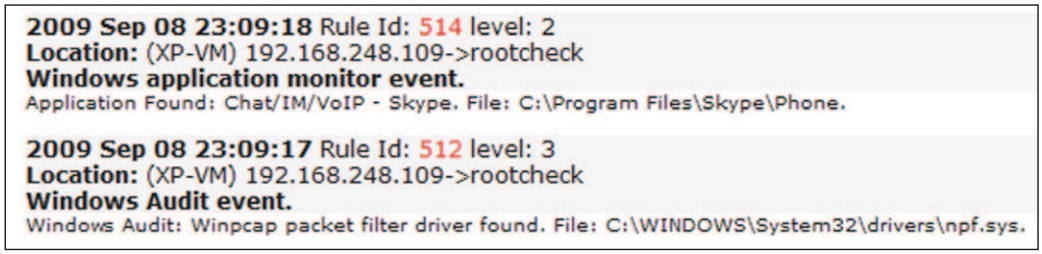


Figure 2 – OSSEC spots Skype and Wireshark

connection from the wild to his server, particularly traffic that has been interpreted as encrypted FTP traffic. "Breathe, son, breathe!" Either I've been rooted somehow (oh, the horror) or I'm running something weird and I've forgotten what the heck it…wait a minute, it's coming to me. Doh! I left Tor[10] running. A quick `netstat –ano` finds established connections to various hosts on 80, 9001, and 21, amongst others. Ok, color is returning to already uncommonly pale skin. I execute `sudo /etc/init.d/tor stop` and fire `netstat –ano` again. All established connections now show a time_wait state including the above mentioned 92.243.8.139. Thunk-thunk, thunk-thunk, my heartbeat returns to normal. Slap me for being stupid and careless, dear reader. OSSEC exhibits immediate value by helping keep my adult ADD in order.

OSSEC and PCI

PCI DSS 11.5 states that organizations must "deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly."

Note: For file-integrity monitoring purposes, critical files are usually those that do not regularly change, but the modification of which could indicate a system compromise or risk of compromise."

Now imagine that your organization is a PCI-beholden SaaS provider who manages numerous virtual nodes via VMWare. As an example, might we assume unauthorized changes to DHCP leases to be an optimal candidate for integrity monitoring, specifically the *dhcpd.leases* file? Would the following alert be useful in said endeavor?

```
OSSEC HIDS Notification.
2009 Sep 11 09:32:51

Received From: flintstone01->syscheck
Rule: 550 fired (level 7) -> "Integrity checksum
changed."
Portion of the log(s):

Integrity checksum changed for: '/etc/vmware/
vmnet8/dhcpd/dhcpd.leases'
Size changed from '599' to '1327'
Old md5sum was:'bc3c25d3cdab17f4b3e167d95b4ca988'
New md5sum is:'4ce2129e1c328aae35475096b59ede7c'
Old sha1sum was:'22fcb668c13ed27b133b2b46192637e32f2611b4'
New sha1sum is:'a9abc0dcdff71c8650ac9cc0beebd163f810c6ff'

--END OF NOTIFICATION
```

I think we can assume the above to be rhetorical questions.

OSSEC and application monitoring and audit events

Maybe you're working for one of those rare few organizations that actually does not let computer users do less than desirable things at work, such as use Skype or sniff network traffic. OSSEC can certainly help enforce those admirable tendencies as seen in Figure 2.

OSSEC and malware behavioral analysis

I run a Windows XP victim virtual machine to conduct malware analysis. As I'd begun to write this article I was noting the expected events that OSSEC should see, particularly changes to known good directories, files, and registry entries. But what I also spotted, making me further happy, was the following as seen in Figure 3.

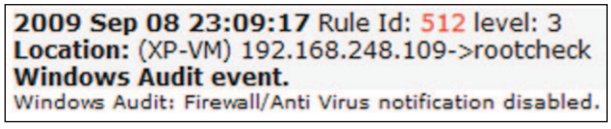


Figure 3 – OSSEC wonders why my AV is disabled

Spend any time playing with malware and you know that certain sample types will immediately disable any antivirus the victim host may be running. OSSEC alerted on that simple fact as well, lending credence to the fact that you should simply make use of OSSEC HIDS anywhere you can.

In conclusion

I challenge you to give me one good reason why you can't use OSSEC HIDS somewhere in your environment. Even if organizational policy or standard requires a different HIDS solution, OSSEC will serve you in labs or non-production environments. Daniel Cid, the OSSEC HIDS lead developer and project founder, and his hard working team have created a framework that I believe you can consider indispensible.

Cheers…until next month.

Acknowledgments

—Doug Burks, Security Onion

—Daniel Cid, OSSEC.net

About the Author

Russ McRee, GCIH, GCFA, GPEN, CISSP, is team leader and senior security analyst for Microsoft's Online Services Security Incident Management team. As an advocate of a holistic approach to information security, Russ' website is holisticinfosec.org. Contact him at russ@holisticinfosec.org.

10 http://www.torproject.org/torusers.html.en.

ISSA Events

7th Annual ISSA Louisville Metro InfoSec Conference: Riding the Security Lifecycle

ISSA EVENT

Kentuckiana Chapter of ISSA
October 8, 2009
Churchill Downs
Louisville, Kentucky, USA

Nationally and regionally known keynote speakers, technical and business/compliance breakout sessions, vendors displaying the latest in new technologies and services, 6-hour CPE certificates for all-day attendees, free breakfast and lunch.

Cost: $99 Discount to ISSA members: Save $20 (Cost = $79). For event details and registration go to: www.LouisvilleInfoSec.com.

Cornerstones of Trust 2009 Conference "Meeting Security Challenges in Changing Times"

ISSA EVENT

San Francisco Bay Chapter of ISSA
Silicon Valley Chapter of ISSA
October 14th 2009
The Crowne Plaza Hotel
Foster City, CA, USA

If you're in the San Francisco Bay Area or Silicon Valley security community, Cornerstones of Trust 2009 is the place to meet top security experts from the business and technology communities and learn about real world solutions. Hear from Mark Weatherford, CISO of the State of California; Pascal Levensohn, founder and managing partner of Levensohn Venture Partners; and 20 security professionals in a one-day, 4- track event.

Cost: $60 members, $90 associate members, $120 non-members if you register on-line; an extra $10 at the door. For event details and sponsorship opportunities go to: http://cornerstonesoftrust.com.

ISSA Hawaii 16th Annual Discover Security Conference

ISSA EVENT

Hawaii Chapter
October 14 – 15, 2009
Halekoa Hotel, 2055 Kalia Road, Honolulu, HI

Cost: $70. Discount to ISSA Members: $35, must be a current ISSA Member at time of registration. For event details and registrations: http://www.issahawaii.org/events.cfm?v=5&t=20090819&c=2159&lc=1.

2009 Triangle InfoSeCon

ISSA EVENT

Raleigh Chapter of ISSA
October 15, 2009
North Carolina St. Univ., McKimmon Conference Center
Raleigh, NC, USA

ISSA's Triangle InfoSeCon fifth annual security event draws hundreds of IT professionals from North Carolina and surrounding states and features three content tracks: Web Security & Web Application; Governance Risk Compliance; Information Security.

Cost: ISSA members - $30, standard registration - $85.

For details and registration go to http://raleigh.issa.org/conference.html. Check us out...reserve your sponsorship slot or register now! http://raleigh.issa.org/confsponsor.html.

Application Security

ISSA EVENT

St. Louis Chapter of ISSA
October 20, 2009
Pujols 5 Restaurant, Westport Plaza
St. Louis, MO, USA

The Web is becoming more social. This presentation focuses on the dangers of increased functionality and gives you things to think about before increasing the attacking surface of your sites and applications.

Cost: free to ISSA members and guests. For event details and registration go to: http://stl.issa.org.

4th Annual Security Summit

ISSA EVENT

Rochester (NY) Chapter
October 28 – 29, 2009
Woodcliff Hotel and Spa Conference Center
Fairport, NY, USA

Cost: $120. Discount to ISSA Members: 10%, Early bird discounts also available. For details and registration: www.rochestersecurity.org.

The 24th Annual 2009 ISSA SoCal Security Symposium: Security in a Changing Environment

ISSA EVENT

Orange County Chapter of ISSA
October 29, 2009
Hyatt Regency Long Beach
Long Beach, CA, USA

Don't miss this fantastic opportunity to hear from an EXCEPTIONAL group of speakers! You'll also be treated to a first-class vendor exhibit, continental breakfast and buffet luncheon, exciting door prizes, and a happy-hour reception.

Cost: ISSA members, $75; non-members, $95. For details and registration go to: www.issa-oc.org/symposium.htm.

Magnify Your Security

ISSA EVENT

Metro Atlanta Chapter of ISSA
Wednesday, November 11, 2009
Loudermilk Convention Center
Atlanta, GA, USA

The goal of this conference is to give Information Security professionals the training, exposure and networking opportunities required to stay on top of current security issues and fulfill additional professional development needs.

Cost: ISSA members - $65; student ISSA members - $59; non-members - $100; student non-members - $75. Discount Code: 2009earlybirdspecialmember.

For registration go to http://www.issa.eventbrite.com. For details go to http://www.gaissa.org/conference/index.htm.

ISSA CISO Executive Forum

*CISO Forum dates and locations are subject to change.

Las Vegas, NV, November 12 - 13, 2009
Theme: Looking Forward: What CISO's will need to know in the next decade

ISSA EVENT

For details on the CISO Forum please visit http://ciso.issa.org. *CISO executive memberships are subject to approval; criteria is available at: http://ciso.issa.org/Membership/Membership-Criteria.html.

Industry Events

SecureWorld Expo

SecureWorld Expo is a security conference built for and by key decision makers, like you, from the largest enterprises, government and educational institutions across the nation.

ISSA members are offered a $100 discount off the $245 conference pass which includes access to the conference sessions, conference breakfast keynote, exhibits and open sessions (includes lunch) and 12 CPE credits. Register on-line using code ISSNWS9.

October 28 – 29, 2009
Seattle SecureWorld
Seattle, WA, USA

November 4 – 5, 2009
Dallas SecureWorld
Dallas, TX, USA

SecureWorld+ Extended Training 2009 includes 4+ hours of intense training worth 16 CPE credits and full access to the complete SecureWorld conference program. SecureWorld+ Pass is only $495 with special ISSA member discount, register using code ISSNWS9.

For event details and registration go to: http://www.secureworldexpo.com.

SC World Congress

October 13-14, 2009
Sheraton New York Hotel, New York, NY

The Congress features a comprehensive, two-day program presented in four tracks. Emphasizing quality content, innovative formats, global perspectives, ROI—and all taking place in the world's business capital—this is the one event you can't afford to miss.

ISSA members receive a $200 discount on conference fees, applied to the prevailing rate; by using the code ISSA in the box marked Promotional Code. Cost: $995+.

For event details and registration go to: www.scworldcongress.com.

SeACURE.IT Preview 2009

October 21 – 23, 2009
Milano Italy

SEaCURE.IT is the first international technical conference ever held in Italy on security releated topics, aimed at bringing together the leading experts from all over the world, to create a unique setting for networking and discussion among the speakers and the attendees.

Cost: €395 (conference), €1495 (trainings. Discount to ISSA Members: €95 on the conference, €295 on the trainings. Discount Code: mention ISSA membership in the notes.

For event details and registration go to: www.seacure.it.

OWASP AppSecDC

National Capital Chapter
November 10 -13, 2009
Walter E. Washington Convention Center
Washington, D.C., USA

AppSec DC 2009 will provide a venue for hundreds of IT professionals interested in securing web technologies to learn, interact, network, and attend presentations and training given by some of the world's top practitioners of web application security, suitable for everyone from federal decision makers and management to application security engineers and developers.

Cost: $345 until September 25th, then $395. Discount to ISSA Members: $50. Discount Code: ISSA09

For event details and registration go to: http://www.owasp.org/index.php/OWASP_AppSec_DC_2009#tab=Registration. http://guest.cvent.com/i.aspx?4W,M3,26bc4c77-e1ef-4bad-be46-eb7b0124276c.

DeepSec In-Depth Security Conference (IDSC)

November 17-20, 2009
The Imperial Riding School Vienna - A Renaissance Hotel
Ungargasse 60, Vienna 1030
Vienna, Austria

The DeepSec conference aims to bring together the world's most renowned security professionals from academics, government, industry, and the underground hacking community.

Cost: Conference Early Bird Booking €595, Regular Booking €645, On-Site Registration €695; Workshops Early Bird Booking €1295, Regular Booking €1495, On-Site Registration €1695; Conference + Workshops Early Bird Booking €1595, Regular Booking €1795, On-Site Registration €1995.

Discount to ISSA Members: 20%. Discount Code: issa-Xieph9.

For event details and registration go to: https://deepsec.net/register.

ISSA Membership Application

Information Systems Security Association
The Global Voice of Information Security

Return completed form with payment. * Required Entries

* Name _____ * Email _____

* Employer _____ * Daytime Phone _____

Certifications _____ Evening Phone _____

* Address 1 _____ Fax _____

Address 2 _____

* City _____ * Country _____

* State/Province _____ * Zip/Postal Code _____

* Account Verification: What is the last high school you attended? _____

Note: In order to obtain personal information and account access over the phone, ISSA Member services will ask for Account Verification.
Annual general membership dues of $95 per year include $28 for a one-year subscription to the ISSA Journal.

ISSA Privacy Statement:

The ISSA privacy statement is included in the Organization Manual, and is provided for your review at www.issa.org/privacy.htm.

To enable us to better serve your needs, please complete the following information:

Your Industry (Select only ONE number from below and enter here) _____

A. Advertising/Marketing	J. Engineering/Construction/Architecture	S. Manufacturing/Chemical
B. Aerospace	K. Financial/Banking/Accounting	T. Medicine/Healthcare/Pharm.
C. Communications	L. Government/Military	U. Real Estate
D. Computer Services	M. Hospitality/Entertainment/Travel	V. Retail/Wholesale/Distribution
E. Security	N. Information Technologies	W. Transportation/Automobiles
F. Consulting	O. Insurance	X. Energy/Utility/Gas/Electric/Water
G. Education	P. Internet/ISP/Web	Y. Other _____
H. Computer Tech-hard/software	Q. Media/Publishing	
I. Electronics	R. Legal	

Your Primary Job Title (Select only ONE number from below and enter here) _____

1. Corporate Manager/CIO/CSO/CISO	9. Operations Manager	17. Engineer
2. IS Manager/Director	10. Operations Specialist	18. Auditor
3. Database Manager, DBA	11. LAN/Network Manager	19. President/Owner/Partner
4. Database Specialist, Data Administrator	12. LAN/Network Specialist	21. Financial Manager
5. Application Manager	13. Security Specialist	22. Administrator
6. Applications Specialist	14. Contingency Planner	23. Educator
7. Systems/Tech Support Manager	15. Sales/Marketing Specialist	24. Other_____
8. Systems Programmer/Tech Support	16. Independent Consultant	

Your Areas of Expertise (Circle all that apply)

A. Security Mgmt Practices	E. Security Architecture	I. Operations Security
B. Business Continuity/Disaster Recovery	F. Applications/Systems Development	J. Physical Security
C Network Security	G. Law/Investigations/Ethics	K. Telecommunications Security
D. Access Control Systems/Methods	H. Encryption	L. Computer Forensics

I heard about ISSA from (circle one): Conference Poster ISSA Website Business Reply Card
An ISSA Member :_____ Other _____

Would you like to receive free product information and special promotional offers via mail from the industry's leading vendors? ☐ Yes ☐ No

Membership Fees

***Membership Category** _____
(list on reverse)

***Chapter(s)** _____
(Required within 50 miles of local chapter)

ISSA Member Dues *(on reverse)* $_____

Chapter Dues x **Years of Membership** $_____
(on reverse)

Additional Chapter Dues $_____
(if joining multiple chapters - optional)

Total Due $_____

Full payment must accompany this form.
Mail check/money order (payable to ISSA) to:

ISSA Headquarters
9220 SW Barbur Blvd #119-333
Portland, OR 97219

Phone +1 (206) 388-4584 • Fax +1 (206) 299-3366
www.issa.org

Or fax credit card information. Please see other side.

ISSA Code of Ethics

The primary goal of the Information Systems Security Association, Inc. (ISSA) is to promote practices that will ensure the confidentiality, integrity, and availability of organizational information resources. To achieve this goal, members of the Association must reflect the highest standards of ethical conduct. Therefore, ISSA has established the following Code of Ethics and requires its observance as a prerequisite for continued membership and affiliation with the Association. As an applicant for membership and as a member of ISSA, I have in the past and will in the future:

- Perform all professional activities and duties in accordance with all applicable laws and the highest ethical principles;
- Promote generally accepted information security current best practices and standards;
- Maintain appropriate confidentiality of proprietary or otherwise sensitive information encountered in the course of professional activities;
- Discharge professional responsibilities with diligence and honesty;
- Refrain from any activities which might constitute a conflict of interest or otherwise damage the reputation of employers, the information security profession, or the Association; and
- Not intentionally injure or impugn the professional reputation of practice of colleagues, clients, or employers.

Signature _____ Date _____

ISSA Membership Categories and Annual Dues

General Membership: $95 plus chapter dues

Professionals who have as their primary responsibility information systems security in the private or public sector, or professionals who supply information systems security consulting services to the private or public sector; or IS Auditors, or IS professionals who have as one of their primary responsibilities information systems security in the private or public sector; Educators, attorneys and law enforcement officers having a vested interest in information security; or Professionals with primary responsibility for marketing or supplying security equipment or products. Multi-year memberships for General Members, are as follows (plus chapter dues each year):

2-Year: $185; **3-Year:** $270; **5-Year:** $435

Organizational Membership: $115 plus chapter dues

Organizational memberships offer corporations, companies and government agencies the opportunity to purchase an ISSA membership for an employee. Unlike General and CISO Executive memberships, which belong to the employee, Organizational memberships belong to the employer and can be transferred as reassignments occur. When an employee is assigned to an Organizational membership, he or she has all of the rights and privileges of a General Member including the rights to vote and hold office.

With the purchase of 20 or more memberships, your organization will receive discounts of up to 20% and complimentary postings on ISSA's Career Services Center. You can also synchronize renewal dates for all of your employees to reduce administrative time and expense. All membership dues are non-refundable. Discounts and flat fee programs available with 20 or more memberships. *Please contact orgmember@issa.org for group rates.*

Student Membership: $30

Student members are full-time students in an accredited institution of higher learning. This membership class carries the same privileges as that of a General Member except that Student Members may not vote on Association matters or hold an office on the ISSA International Board. There is no restriction against students forming a student chapter.

CISO Executive Membership: $995

The role of information security executives continues to be defined and redefined as the integration of business and technology evolves. While these new positions gain more authority and responsibility, peers must form a collaborative environment to foster knowledge and influence that will help shape the profession. ISSA recognizes this need and has created the exclusive CISO Executive Membership program to give executives an environment to achieve mutual success. For more information about CISO Executive Membership and required membership criteria, please visit the CISO website – http://ciso.issa.org.

Credit Card Information

Choose one:

☐ Visa ☐ MasterCard ☐ American Express

Card # _____

Exp. Date _____

Signature _____

ISSA Chapters & Annual Dues

Changes/additions – visit our website – www.issa.org

At large 25

Central/South America

Argentina 0
Brasil - SP 5
Caracas - Venezuela 10
Chile - Santiago 30

Europe/Africa

Brussels European 40
Egypt 0
France 0
Irish 30
Italy 65
Netherlands 30
Nigeria 30
Nordic 40
Poland 0
Romania 0
Southern Germany 30
Spain 60
Sudan 25
Switzerland 80
UK 0

Asia/Middle East

Chennai 10
Hong Kong 30
Israeli 50
Pakistan Central 20
Philippines 20
Saudi Arabia 0
Seoul 80
Singapore 10
Tokyo 30

Oceania

Queensland 25
Sydney 0
Victorian, Australia 0

North America

Alamo (San Antonio) 20
Alberta (Canada) 25
Amarillo Area 25
ArkLaTex (Shreveport) 30
Baltimore 20
Baton Rouge 25
Blue Ridge 25
Bluegrass (Kentucky) 0
Boise 25
Buffalo Niagara 25
Capitol of Texas 35
Central Alabama 0
Central Florida 25
Central Indiana 25
Central New York 0
Central Ohio 20
Central Pennsylvania 20
Central Plains 30
Central Virginia 25
Charlotte Metro 30
Chicago 30
Colorado Springs 25
Connecticut 20
Dayton 25
Delaware Valley 20
Denver 25
Des Moines 0
East Tennessee 35
Eastern Idaho 20
Eastern Iowa 0
Florida Big Bend 0
Fort Worth 20
Grand Rapids 0
Greater Augusta 25
Greater Cincinnati 10
Greater Spokane 20
Hampton Roads 30
Hawaii 20
Heart of Texas 10
Inland Empire 20
Kansas City 20
Kentuckiana 35
Lansing 20
Las Vegas 30
Los Angeles 20
Madison 15
Mankato 20
Melbourne 25
Memphis 30
Metro Atlanta 30
Middle Tennessee 35
Milwaukee 30
Minnesota 20
Montgomery 35
Montreal 20
Motor City (Detroit) 25
National Capital (Washington DC) 25
North Plains/North Dakota 25
New England 20
New Hampshire 20
New Jersey 20
New Mexico 20
New York 55
North Alabama 15
North Texas 20
Northeast Indiana 10
Northeast Ohio 20
Northeast Wisconsin 25
Northern Indiana 10
Northern New Mexico 20
Northern Virginia (NOVA) .. 25
Northwest Arkansas 15
Northwest Ohio 25
Oklahoma 30
Oklahoma City 25
Omaha 25
Orange County 20
Ottawa 10
Palouse Area 30
Phoenix 30
Pittsburgh 30
Portland 30
Puerto Rico 35
Puget Sound (Seattle) 20
Quebec City (Canada) 0
Raleigh 25
Rochester (New York) 15
Sacramento Valley 20
San Diego 30
San Francisco 20
SC Midlands 25
Silicon Valley 30
South Florida 20
South Texas 30
Southeast Arizona 20
Southern Indiana 20
Southern Maine 20
Southwest Florida 25
St. Louis 20
Tampa Bay 20
Tech Valley of New York 35
Texas Gulf Coast 30
Tidewater, VA 30
Toronto 20
Triad of NC 25
Tri-Cities (Tennessee) 20
Upstate South Carolina 0
Utah 15
Vancouver 20
Western Oregon 20

The Changing Face of Emergent Threats

By Ken Dunham – ISSA member, Boise, USA Chapter

Does antivirus work anymore? Not so well if you plan on using it as a primary line of defense against emergent threats and certainly not alone. An aggressive cybercriminal effort leveraging malcode for massive fraud operations is well matured in 2009. The need to be both reactive and proactive is essential with strong security plans in 2009.

In some cases a reactive stance and aggressive software development efforts can win a notable battle in the war against malcode. Remember macro virus threats impacting Microsoft products, like Concept, that ran rampant for years? You don't hear about macro viruses anymore because of software changes that took place that effectively wiped them out as a threat for most users. Such examples are rare in this war, but they do happen. This notable victory naturally resulted in cybercriminals seeking counter actions to continue and to improve upon their fraud opportunities, focusing efforts on worms, bots, and similar threats.

Mebroot is an interesting example of changes in motives and means over the years and a lack of response by organizations. This code was developed, tested, and then released in the wild in December 2007. The code, bundled with Torpig for financial fraud, modifies the master boot record (MBR) of an infected disk and stores a kernel-level rootkit in slack space on the drive. It loads before Windows and is able to survive a wipe of the operating system. Twenty years ago that would have likely been an interesting POC. Today it is used for state-of-the-art stealth to support fraud operations. Even though this code has been in the wild for almost two years, many incident response teams still have no procedures in place to adequately address MBR-infecting malcode.

When performing an incident response, it is common in 2009 to find many malicious codes with very poor antivirus detection. When using multiscanners to scan newly captured samples, detection rates are commonly less than 50 percent, and sometimes below 10 percent, for dozens of updated scanners scanning a hostile file. With such poor odds it is clear that relying upon just one antivirus solution is inadequate in a multi-minor-variant temporary type malcode attach scene, where initial attack codes only need to survive without detection for a few hours or days. Using two different products on two different layers, such as at the gateway and host level, is a solid reactive best practice that helps to detect new threats, but it does not go far enough in light of today's threats.

Increasingly many large networks are focused on the network layer. Many ports are blocked and/or monitored automatically due to historical threats of worms and bots. As a result many of the threats and counter measures used in large enterprises today focus on TCP port 80 traffic. On a reactive side companies are working with IDS/IPS and similar solutions to identify known hostile and/or suspicious behavior. Even with heuristics, this reactive measure also falls short of protection against the constant knocking on the door of the network with new codes known to be undetectable at the time of attack.

Being proactive requires that you identify where the threats are migrating to and why and what one can do about that to lower the risk of attack. A few years ago bots and worms were the major threat. Today web-based attacks through third-party plug-ins and exploitation frameworks are clearly a massive force behind many of the top large scale attacks seen on the Internet. Social engineering and SEO poisoning is also another main vector for rogue security applications and malvertisements. As we reactively implement hostile URL checks, data coordination, new heuristic models and security solutions on the network layer, and advance antivirus to battle stealth, where will the threats migrate for the next generation of fraud?

Security must be identified as a priority. It takes true intelligence, not just information, to make informed decisions to lower global risk against an enterprise. This is partially enabled by industry collaboration. That and in-depth innovative solutions are required to continue to prioritize and empower organizations seeking to close the gap against emergent threats. Ask yourself this: Is your organization successfully reacting to current threats and proactively positioning against likely future threats?

About the Author

Ken Dunham has more than a decade of experience on the front lines of information security. As Director of Global Response for iSIGHT Partners, he oversees all global cyber-threat response and malcode research operations. He frequently briefs upper levels of federal and private-sector cybersecurity authorities on emerging threats, and regularly interfaces with vulnerability and geopolitical experts to assemble comprehensive malicious code intelligence and to inform the media of significant cyber threats. He can be reached at ken@kendunham.org.

INFORMATION-LED TRANSFORMATION

REGISTER TODAY!
September 1 - October 24: $2,195
October 25 - October 29: $2,295

IBM Information On Demand 2009 is the leading cross-IBM event addressing information-led transformation and Business Analytics & Optimization. Address your information challenges with a full arsenal of hardware, software and services solutions. More than 200 customers will share their real-world experience about how they have unlocked the value of their information and realized tangible and immediate return on investment.

ISSA Members will receive a $100 discount. To enroll at the discounted rate, please register at ibm.com/events/InformationOnDemand and use promotion code "GO9ISSA" under the "company information" section.

2009 Event Highlights

- *Over 7000 conference attendees*
- *200 customer speakers*
- *100 Business Leadership sessions*
- *400 Technical Skill Building sessions*
- *3 free Information Management certification tests, 50% discount on all other IBM Software Group products*
- *Huge EXPO encompassing 200 Business Partners and 120 IBM Hardware, Software, and Services Exhibits*

Register Today for IBM Information On Demand 2009

- *Participate in the premier discussion on the future of managing information and learn why having an information agenda is even more critical in today's economy.*
- *Understand the value of IBM solutions that address the most pressing business challenges.*
- *Get practical guidance on how to use analytics to drive precision and predictability into the decision making process at all levels of the organization.*
- *Hear how your peers are realizing ROI in today's economic environment.*
- *Learn best practices in your industry.*

LEAD THE WAY

IBM Information ON Demand 2009

October 25–29, 2009
Las Vegas, Nevada

ibm.com/events/InformationOnDemand

IBM