

Do Data Breaches Matter?

A Review of Breach Data and What to Do Next

BREACH REPORTS:
COMPARE/CONTRAST

Table of Contents

DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

Feature

22.....Do Data Breaches Matter? A Review of Breach Data and What to Do Next

By Kristopher Dane – ISSA member, Puget Sound Chapter

This article discusses the threat of cybercrime and data breaches to organizations. The author discusses the economics of data breach information and then reviews the existing public data on breaches to see how markets are responding. The article concludes with a call to action to normalize breach reporting to better inform consumers and enable future research.

Articles

30.....FedRAMP’s Database Scanning Requirement: The Letter and Spirit

By Matt Wilgus – ISSA member, Raleigh Chapter

Many cloud service providers are not fully addressing the database scanning requirements for FedRAMP and have questions related to database security and FedRAMP. This article details the issues associated with not meeting the database scanning requirement, the most common reasons why this occurs, what can be done to improve this, and what to consider with database security beyond scanning.

34.....Smart Practices in Managing an Identity-Auditing Project

By Kerry Anderson – ISSA member, New England Chapter

Implementing an identity-management audit solution can be a milestone in the maturation of an information security program. This article discusses best practices to ensure the development and delivery of a successful access-audit program.

39.....On the Costs of Bitcoin Connectivity

By Ashish Gehani

Highly connected information technology systems typically have substantial economic value, making them attractive to resource-rich adversaries. Bitcoin is an example of such a system. The effect of high connectivity manifests in a number of orthogonal dimensions, each of which creates a different kind of security concern. We discuss each of them and possible mitigations.

Also in this Issue

3.....From the President

4.....editor@issa.org

5.....Sabbett’s Brief

Does Anybody Remember the Phone Book?

6.....Herding Cats

The SDN IS the Computer

7.....Perspective: Women in Security SIG

Cybersecurity Analysis – Where “Life Experience Application” Counts Most

8.....Security in the News

9.....Open Forum

Linking Information Security to Other Key Organizational Initiatives

10.....Crypto Corner

The First Levchin Prize

11.....Association News

14.....2016 International Election Candidate Profiles



©2016 Information Systems Security Association, Inc. (ISSA)

The ISSA Journal (1949-0550) is published monthly by
Information Systems Security Association

12100 Sunset Hills Road, Suite 130, Reston, Virginia 20190
703-234-4082 (direct) • +1 866 349 5818 (USA toll-free)
+1 206 388 4584 (International)



International Board Officers

President

Andrea C. Hoy, CISM, CISSP, MBA,
Distinguished Fellow

Vice President

Justin White

Secretary/Director of Operations

Anne M. Rogers
CISSP, Fellow

Treasurer/Chief Financial Officer

Pamela Fusco
Distinguished Fellow

Board of Directors

Frances “Candy” Alexander, CISSP,
CISM, Distinguished Fellow

Debbie Christofferson, CISM, CISSP,
CIPP/IT, Distinguished Fellow

Mary Ann Davidson
Distinguished Fellow

Rhonda Farrell, Fellow

Garrett D. Felix, M.S., CISSP, Fellow

Geoff Harris, CISSP, ITPC, BSc, DipEE,
CEng, CLAS, Fellow

Alex Wood, Senior Member

Keyaan Williams

Stefano Zanero, PhD, Fellow

The Information Systems Security Association, Inc. (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.

Greetings ISSA Members and Journal Readers!

Andrea Hoy, International President



In 2014, we experienced the “Year of the Data Breach,” and since then, while data breaches continue, the cases hitting the court rooms do not really seem reflective of the increased number of breaches reported. Take this further and the percentage of actual data breach cases that go to trial is quite small in comparison. So when our esteemed volunteers on the Editorial Advisory Board came up with this month’s topic—Data Breaches – Compare/Contrast—one of our authors rose to the challenge to provide us an interesting analysis of breach reporting and stock prices, asking “Do Data Breaches Matter?” Depends who you ask, but I’ll leave that to you to discover.

I overheard an interesting conversation on a plane flight last week. A company’s privacy officer was trying to explain to key management that information security, while related, was not what privacy did; it was not the privacy officer’s job to put security controls in place. The individuals in the conversation knew the person was doing a good job but were still unsure they understood the difference, that is, what they needed to capture and act upon to ensure the security of their customer data.

It led me to think about the challenges we as information security practitioners face on a day-to-day basis in our strategic planning and controls implementation, trying to keep data breaches at bay. As we look at them, we are finding that it is not just technology issues, but rather the processes and procedures or the administrative controls that are the underlying issue. We see privileged accounts being compromised and used as well as processes or procedures that were never documented (you may want to check out the article on developing an access-auditing program). We see poorly documented processes and procedures that were not followed are more prevalent with why breaches are successful...none of us has ever experienced the repercussions of an unpatched system or an undocumented, high-risk exception, right?

From an ISSA perspective, as we have become more strategic in moving our association forward, we have been working on identifying areas where we need to increase efficiency and improve documenting our processes and procedures so that we have consistency in what we do and how we do it. We are also finding opportunities for our members through building strategic alliances with other organizations that in the past we may not have even considered the benefits we could afford to each other. Some of these changes we are working on require modifications to our bylaws. I ask that you take the time to review and approve these updates during our upcoming elections in June, as a minimum of 10 percent of the membership is required to vote in order to make these improvements happen.

Thanks in advance for helping make ISSA—your association—better!!!

Moving forward,



Breach Reports – Compare/Contrast

Thom Barrie – Editor, the ISSA Journal

The Editorial Advisory Board is announcing a scholarship for best student article. If you know a student who might be inter-

ested, please let him or her know. Information is on [page 11](#).

The international election is coming up with President and five Director positions on the slate. Candidates have outlined their qualifications and goals in “Candidate Profiles,” [page 14](#) and following. Starting June 4, “let your voice be heard” by voting for the candidates best representing the direction you believe ISSA should be heading.

Do data breaches matter? Kristopher Dane describes research he conducted on the effect of data breaches on company stock prices in “Do Data Breaches Matter?” Does the market punish companies that suffer breaches? You’ll have to read it, but one interesting point is that there is “some evidence to suggest that consumers are tiring of breach announcements and not changing their behavior after a breach as they accept them as a cost of doing business.”

Next up is Matt Wilgus’s “FedRAMP’s Database Scanning Requirement: The Letter and Spirit,” in which he describes some of the reasons cloud service providers have difficulties with database scanning to meet FedRAMP compli-

ance requirements. He identifies five reasons for the difficulties, one of which is determining just what constitutes a database, which may not be as clear cut as you might think.

Frequent Journal contributor Kerry Anderson tackles the arduous task of developing an enterprise access-auditing program in “Smart Practices in Managing an Identity Auditing Project.” She provides great help and insights for getting the program off the ground and stakeholders on board. While a major project in itself, Kerry suggests that a successful implementation can prime the next step towards role-based access control and automated provisioning.

Ashish Gehani describes security concerns and vulnerabilities in Bitcoin technology in “On the Costs of Bitcoin Connectivity.” It’s a pretty good read. However, if you, like me, are still trying to get your head around blockchain technology, Accredited Standards Committee X9—with whom the *Journal* has a reciprocal relationship: if we publish an article of interest to their membership, we make it available on a special page on ISSA.org; if they produce something of interest to ISSA members, they share it with us—has a couple presentations that do a good job of explaining the technology: “[Making Blockchain Real for Business](#)” and “Demystifying Blockchain Mechanics,” which should be available soon. Demystifying is especially instructional.

Enjoy—Thom

ISSA JOURNAL

Editor: Thom Barrie
editor@issa.org

Advertising: vendor@issa.org
866 349 5818 +1 206 388 4584

Editorial Advisory Board

- Phillip Griffin, Fellow
- Michael Grimaila, Fellow
- John Jordan, Senior Member
- Mollie Krehnke, Fellow
- Joe Malec, Fellow
- Donn Parker, Distinguished Fellow
- Kris Tanaka
- Joel Weise – Chairman, Distinguished Fellow
- Branden Williams, Distinguished Fellow

Services Directory

Website

webmaster@issa.org
866 349 5818 +1 206 388 4584

Chapter Relations

chapter@issa.org
866 349 5818 +1 206 388 4584

Member Relations

member@issa.org
866 349 5818 +1 206 388 4584

Executive Director

exccdir@issa.org
866 349 5818 +1 206 388 4584

Vendor Relations

vendor@issa.org
866 349 5818 +1 206 388 4584

The information and articles in this magazine have not been subjected to any formal testing by Information Systems Security Association, Inc. The implementation, use and/or selection of software, hardware, or procedures presented within this publication and the results obtained from such selection or implementation, is the responsibility of the reader.

Articles and information will be presented as technically correct as possible, to

the best knowledge of the author and editors. If the reader intends to make use of any of the information presented in this publication, please verify and test any and all procedures selected. Technical inaccuracies may arise from printing errors, new developments in the industry, and/or changes/enhancements to hardware or software components.

The opinions expressed by the authors who contribute to the ISSA Journal are their own and do not necessarily reflect

the official policy of ISSA. Articles may be submitted by members of ISSA. The articles should be within the scope of information systems security, and should be a subject of interest to the members and based on the author’s experience. Please call or write for more information. Upon publication, all letters, stories, and articles become the property of ISSA and may be distributed to, and used by, all of its members.

ISSA is a not-for-profit, independent cor-

poration and is not owned in whole or in part by any manufacturer of software or hardware. All corporate information security professionals are welcome to join ISSA. For information on joining ISSA and for membership rates, see www.issa.org.

All product names and visual representations published in this magazine are the trademarks/registered trademarks of their respective manufacturers.

Does Anybody Remember the Phone Book?

By Randy V. Sabett – ISSA Senior Member, Northern Virginia Chapter



To quote Steve Martin in the movie *The Jerk*, “The new phone book is here!!” In this case, though, his line would be “The new DBIR is here!!” Yes, the ninth annual [Data Breach Investigations Report](#) (DBIR) from Verizon was released on April 26. While there is a wide variety of breach reports, Verizon’s tend to be among the most comprehensive—note that the 2016 DBIR report analyzed over 64,000 security incidents and 2,260 instances data breaches with confirmed data exfiltration. These occurred last year across a range of organizations in 82 different countries.

In 2015, more than 90 percent of incidents and data breaches fell into one of nine categories. Most commonly, security incidents were caused by miscellaneous errors, such as sending emails or paper documents to the wrong recipients (11,347 incidents); insider and privilege misuse, such as an employee using unapproved hardware like a USB drive to store sensitive information (10,490 incidents); and physical theft or loss of laptops and paper documents (9,701 incidents). The most serious incidents—those resulting in the most confirmed data breaches—however, were web app attacks, including hacking using stolen credentials and installing malware (908 confirmed breaches) and point of sale or POS attacks against environments where debit and credit card retail transactions are conducted (525 confirmed breaches).

As far as comparing and contrasting, the DBIR analyzed several million results of phishing tests. Their findings show that recognition of phishing messages is getting worse. Test phishing messages that were opened rose by seven percent, from

23 percent in 2014 to 30 percent last year. About 12 percent of those who opened the message went further and clicked on the malicious attachment. The median time between sending a phishing message and the first click on its attachment? Under four minutes. The DBIR noted, however, that the main perpetrators of phishing attacks are sophisticated, with significant time and resources to craft believable “bait”: in 2015, 89 percent of phishing attacks were perpetrated by organized crime syndicates and nine percent were perpetrated by state-affiliated actors.

Insider and privilege misuse was also common, with insiders most frequently motivated by financial gain, followed closely by espionage. The 2016 DBIR looked at how insiders’ motivations have changed since 2009, and while incidents motivated by espionage have risen, incidents motivated by the prospect of financial gain have fallen. Other inside actors are motivated by grudges, ideology, and even just plain fun. Even more concerning, actions by insiders are some of the hardest for organizations and law enforcement to detect. As evidence of this, consider that 70 percent of insider incidents take months or even years to discover.

The 2016 DBIR also shows that payment card data remains a popular target for attackers. POS intrusions accounted for 534 security incidents last year, almost all of which resulted in confirmed data breaches. Businesses in the accommodation, food service, and retail industries experienced most of these attacks, oftentimes after the attackers first compromised their POS vendors’ security. Almost all (97 percent) of data breaches involving stolen credentials leveraged

legitimate partner access to get to customer data.

Attackers also used physical devices to steal payment card information. Skimming devices physically implanted in magnetic payment card readers—for example, a pinhole camera installed on an ATM to surveil individuals entering debit card PINs—caused 102 security incidents in 2015. Of those, 86 resulted in confirmed data breaches. The vast majority (94 percent) of breaches involving payment card skimmers were related to ATMs, but attackers also targeted gas pump terminals (five percent of breaches) and PIN entry devices (one percent). In 2015, 70 percent of payment card skimming incidents were the work of criminal organizations.

Well, reciting the last of those dismal statistics means I’m done with the DBIR. So I’m headed off now to finish reading the phone book. Once I find my name I’ll know that “Things are going to start happening to me now.” Don’t bother looking that one up...it’s Steve Martin’s next line in the movie. See you next month!

About the Author

Randy V. Sabett, JD, CISSP, is Vice Chair of the Privacy & Data Protection practice group at Cooley LLP, and a member of the Boards of Directors of ISSA NOVA, MissionLink, and the Georgetown Cybersecurity Law Institute. He was named the ISSA Professional of the Year for 2013, and chosen as a Best Cybersecurity Lawyer by Washingtonian Magazine for 2015-2016. He can be reached at rsabett@cooley.com and he thanks Colleen Hannigan for her help with this month’s column.



The SDN IS the Computer

By Branden R. Williams – ISSA Distinguished Fellow, North Texas Chapter

This issue's theme is *Breach Reports*, of which there are plenty. If you have not downloaded Trustwave's most recent offering that dropped in the last two weeks, head over to their site to get it. There are a ton of great stats in there, and it's important for practitioners to understand how attacks shifted last year. While the past is not always an indicator of what is coming next, understanding how the trends progress is a good exercise for us all to go through. If for nothing else, the report is a reminder to look for items we may have missed in previous runs through our network.

As an example, Wordpress (and more specifically, one of its plugins) is quite heavily featured in this report. If you have any Wordpress installations in your environment, you should ensure they are patched. If you don't have any Wordpress in your environment, you should validate that assumption. It always cracked me up as a consultant when I was told definitively that "there are absolutely no Wi-Fi networks at our firm."

Why did I laugh? Because there usually was one.

I want to dive into one specific recommendation from the Trustwave report that struck me as odd, given how IT is deployed in this day and age. In a section entitled "Stopping Data Compromise, Now and in the Future," the first part of the last bullet under Firewall Configuration instructs firms to use hardware firewalls only. I had to reread that bullet a couple of times to really see if I was reading that properly.

I was.

When I was doing CISP/SDP consulting in 2004, I would expect this kind of recommendation. At the time, software-defined networking (SDN) existed, but in extremely basic forms. If you were a *NIX junkie like me, you used it as the epicenter to your home or lab. It worked great in those setups, and with a sophisticated automation system it could be used in the enterprise. Few enterprises had this in anything other than a lab.

But today, SDN is everywhere. It doesn't seem to matter if you are running a small firm or a big one; you are affected by SDN. It's revolutionized how we deploy IT resources, how we extend our networks beyond one building's four walls, and how we defend against bad guys. It might be one of the greatest assets we have on both the IT and security sides of our respective houses. Recommending that firewalls be hardware based is like telling retailers that they should only accept credit cards in person through a terminal. With the exception of terminal manufacturers and retailers who are only brick-and-mortar, nobody wants to give up the magic of electronic commerce. It's not just about the magic of ordering dinner from your laptop, we've also scaled our infrastructure in a way that hardware-only firewalls are not only impractical—they are ineffective.

I was recently chatting with my buddy Matt Springfield (www.12feet.com) and he was describing how hardware-only firewalls just don't cut it anymore when it comes to the scale of today's IT deployments—mostly due to limitations in Layer 2 networking at scale. What's interesting about this is that even though we have some of the coolest stuff in our data centers, it's still running on the foundation of connecting systems through networks—something originally published as part of the OSI model

in 1984. High-density computing to the level we have today didn't exist. As we grew our networks, we needed better capacity to sling those packets around them.

As Matt described the issue, I finally came to realize that hardware-only firewalls were simply too far away from the interconnected systems, and due to latency, capacity, and management issues, wouldn't be getting any closer. We will have to look to software to solve our security issues in these systems.

The business reality that we security people must understand is that players such as Amazon and Microsoft will continue to drive down the cost of computing. If firms want to compete in the market, they will have to drive down their IT costs as well. Transaction-cost theory will come into play and force our firms to match or beat compute costs. This means that we will continue to get farther away from hardware and just live in its abstractions. In order to protect these systems, we will have to embrace software-based firewalls and network controls.

So don't go and throw out those hardware firewalls yet. Think about what SDN can do for you!

About the Author

Branden R. Williams, DBA, CISSP, CISM, is the CTO, Cyber Security Solutions at First Data, a seasoned security executive, and regularly assists top global firms with their information security and technology initiatives. Read his blog, buy his book, or reach him directly at <http://www.brandenwilliams.com/>.

Cybersecurity Analysis – Where “Life Experience Application” Counts Most

By Rhonda Farrell – ISSA Fellow, Northern Virginia Chapter



When I examined the criteria relating to this month’s ISSA Journal topic, I was struck with the open-ended analytic opportunity for authors to respond to, given their experiential learnings to date within their applicable cybersecurity realm. Secondly, I was encouraged by the fact that they reinforced the concepts of ongoing cybersecurity continuous improvement, based on existing intelligence and lessons learned. Lastly, I was WOWED by the fact that they asked that the writer examine contextual analysis (applicability to the situation at hand) and the oft-sticky subject of information-sharing across the greater whole.

There are very strong parallels here with the recruitment and utilization of women from many diverse educational and professional backgrounds into the cybersecurity field, due to their innate curiosity and strong opportunity seizing and innovation skills, as well as their strong analysis, integration, and information sharing propensities.¹

Applicable experiential learning – Fitness for purpose

According to the recent (ISC)² study entitled “Women In Security: Wisely Positioned for the Future of InfoSec,” women are focusing on roles where those identified strengths will pay off in big dividends, primarily within the governance, risk, and compliance and security consulting arenas (per figure 1)—offering

plenty of breadth, depth, and operating scope to find their unique niche.²

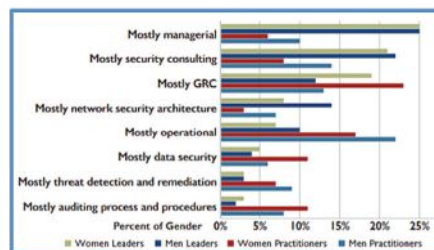


Figure 1 – (ISC)² 2015 – Primary functional responsibilities areas (per gender)

Additionally, the authors found that the average age of women leader respondents was mid-forties, with over 43 percent fifty or over, thus allowing them ample time to educate themselves, grow their pedigrees, and find a solid challenge space to grow within (per figure 2).

Distribution of Gender in Age and InfoSec Tenure	Women Leaders		Men Leaders		Women Practitioners		Men Practitioners	
	2013	2015	2013	2015	2013	2015	2013	2015
Age								
% less than 30 years	4%	4%	3%	2%	6%	5%	4%	6%
% 50 years or older	36%	43%	26%	39%	35%	34%	25%	26%
Average Age	45.7	46.7	43.7	44.6	44.4	44.7	43.8	43.0
Tenure in InfoSec								
% with 3 years or less	3%	3%	3%	2%	6%	6%	5%	7%
% with 16 years or more	31%	35%	30%	36%	27%	27%	26%	26%
Average InfoSec Tenure	13.4	14.4	13.7	14.5	12.4	12.5	12.5	12.7

Figure 2 – (ISC)² 2015 – Infosec age and tenure distribution (per gender)

What does that portend for our younger women ranks, either in the entry-level or practitioner roles, you might want to know, as well as how can we better utilize the wealth of knowledge, skills, and abilities of our seasoned professionals—think better fit! According to a recent RAND study that examined the state of the cybersecurity labor market, more firms are focusing on examining

what personality characteristics most strongly tie to the cybersecurity domains (innate curiosity as to how things work and can be manipulated to fail), both to satisfy currently available positions as well as to develop ongoing generations of cyber practitioners with solid hacker-oriented skills and expertise. Additionally, they identified special curricula focusing on programs for industrial control systems, applications at scale, cybersecurity management, and cybersecurity public policy.³

Utilization of existing intelligence and situational contexts to inform

The (ISC)² sponsored report also brought to light that cybersecurity women leaders and practitioners brought to the table a wealth of educational expertise, with nearly 60 percent of women leaders holding doctorate and master’s degrees, as well nearly 50 percent of our practitioners (per figure 3).

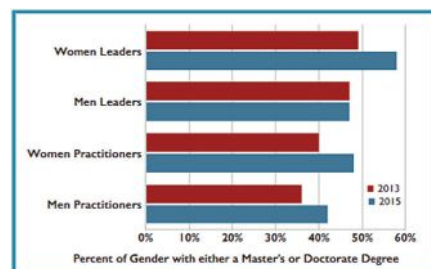


Figure 3 – (ISC)² 2015 – Academic achievement (per gender)

Additional study findings also support the case for diverse backgrounds, showing a blend of undergraduate degree focus areas including computer and in-

Continued on page 44

1 Glenn Llopis, “4 Skills That Give Women a Sustainable Advantage over Men,” Forbes Leadership (Aug 22, 2011) – <http://www.forbes.com/sites/glennllopis/2011/08/22/4-skills-that-give-women-a-sustainable-advantage-over-men/> - 2177f5dac973.

2 Women In Security: Wisely Positioned for the Future of InfoSec, a Frost and Sullivan market study in partnership with (ISC)² (2015) – <https://www.isc2cares.org/uploadedFiles/wwwisc2cares.org/Content/GISWS/2015-Women-In-Security-Study.pdf>.

3 H4CKER5 Wanted – An Examination of the Cybersecurity Labor Market, RAND National Security Division (2014) – http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf.

News That You Can Use...

Compiled by Joel Weise – ISSA Distinguished Fellow, Vancouver, BC, Chapter and
Kris Tanaka – ISSA member, Portland Chapter

Anti-Encryption Bill Released, Would Kill Your Privacy and Security

<http://thehackernews.com/2016/04/anti-encryption-bill.html>

This seems awfully familiar, doesn't it? The ISSA was at the forefront of the Clipper chip and LEAF debate years ago (the Law Enforcement Access Field, or LEAF, was essentially a backdoor). If the new anti-encryption bill makes any progress, we may find history repeating itself.

Burr and Feinstein Officially Release Anti-Encryption Bill, As Wyden Promises to Filibuster It

<https://www.techdirt.com/articles/20160413/15143434173/burr-feinstein-officially-release-anti-encryption-bill-as-wyden-promises-to-filibuster-it.shtml>

Yes, the battle over encryption is just beginning. It won't be an easy task to create guidelines that safeguard our information and our liberties, while at the same time, giving law enforcement the necessary tools and access to bring the "bad guys" to justice. Although we need these guidelines sooner rather than later, we must take the time to do it right. The proposed bill, as it is currently written, is unclear and full of holes. Like Wyden said, we should send this dangerous proposal back to the drawing board.

Cryptography Is Harder Than It Looks

<http://ieeexplore.ieee.org/stamp/stamp.jsp?reload=true&arnumber=7397719>

Bruce Schneier can always be relied upon to respond to legislation that may result in a cryptographic backdoor. I certainly agree that mandating backdoors is just not a good idea. Here Schneier makes it simple to understand: 1. Cryptography is harder than it looks. 2. Complexity is the worst enemy of security. Essentially, if a backdoor is implemented not only will the good guys gain access but more than likely, so will any attacker.

2016 Data Breach Litigation Report

<http://www.jdsupra.com/legalnews/2016-data-breach-litigation-report-61138/>

Bryan Cave LLP began its survey of data breach class action litigation four years ago in order to provide the public with a clearer picture of this growing industry, without the sensationalism and fear mongering often found in media reports. When it comes to mitigating risk, information is critical. Remember, a data breach is not just about the attack itself—you also need to know what happens after the incident.

So, FBI Director also Puts Tape over His Webcam

<http://thehackernews.com/2016/04/tape-webcam.html>

Sometimes the best solution is the easiest one. Apparently, FBI Director James Comey tapes over the webcam on his laptop. How ironic. Comey argues that companies should not make devices that are unhackable to law enforcement. However, that is exactly what he has done with his "webcam security device." The last thing we need in the security vs. privacy debate is another double standard.

Verizon Enterprise Suffers Its Own Data Breach, 1.5 Million Customers' Info Offered Up for Sale

<https://www.grahamcluley.com/2016/03/verizon-enterprise-suffers-data-breach-1-5-million-customers-info-offered-sale/>

The irony continues. Verizon Enterprise, well known for its annual report that highlights the latest trends in data breaches, was itself the victim of a data breach. It just proves that data breaches can happen to anyone—novice or expert. Next year's report should be quite interesting.

PCI Guru – PCI DSS v3.2 Draft Released

<https://pciguru.wordpress.com/>

For those interested in all things PCI, the PCI Guru can keep you abreast of the latest industry news. There is a lot of good information on the most recent release of PCI DSS in the current post. You will also find a wealth of information and analysis in past posts.

US Universities Failing in Cybersecurity Education

<http://www.securitymagazine.com/articles/87062-us-universities-failing-in-cybersecurity-education>

The article references a *U.S. News & World Report* survey from 2015 that states "not one of the top 10 US computer science programs...requires a single cybersecurity course for graduation." Now, I wouldn't take that at face value as I know there are a lot of good cybersecurity courses available at different universities. But, when it comes to the future of cybersecurity education, is this the "canary in the coal mine?"

A.I. + Humans = Serious Cybersecurity

<http://www.computerworld.com/article/3057590/security/ai-humans-serious-cybersecurity.html>

Using A.I. as a cybersecurity tool is one of my favorite subjects. Unfortunately, there's not enough information in this article to judge the new platform called A.I.², but the paper referenced may provide additional insight—http://people.csail.mit.edu/kalyan/AI2_Paper.pdf.

RAND Survey Shows Breaches Have Little Impact on Customer Loyalty

<http://www.darkreading.com/attacks-breaches/rand-survey-shows-breaches-have-little-impact-on-customer-loyalty/d/d-id/1325125?>

We are on the right track. Data breaches are quickly becoming a fact of life; however, only 11 percent of consumers in the study reported that they would take their business to another company if they were hacked. Most people appear to be satisfied with how companies handle their cyberattacks.

Linking Information Security to Other Key Organizational Initiatives

By Eric M. Harper – ISSA member, North Texas Chapter

Alex L. Nehlebaeff – ISSA member, North Texas Chapter

A company's information security leader, HR leader, and CEO walk into a bar.

"What'll y'all have?" asks the bartender.

"I'll have a shot of security awareness; the company is under another cyber attack," says the information security leader.

"I have a shot of employee engagement; the company is suffering from low employee morale," says the HR leader.

"I'll have a shot of everything else; clearly we have a lot to talk about," says the CEO.

In organizational life, there is no shortage of concerns. Think about some of the different companies you've been a part of and think of the different initiatives you've seen to eliminate waste, boost morale, drive fitness, or fill in the blank with any other organizational priority. Though these efforts are all well-intentioned and typically tied to strategy, they inadvertently compete for employees' attention. As a result, employees grow numb to the various messages and emails bombarding their in-boxes. And behind these well-intentioned and neglected messages, departmental leaders devise new avenues and ways to make their initiatives and priority more compelling. Though there is no silver bullet, we have a suggestion that just may help the next time you ramp up a security awareness effort.

Think about ways to combine seemingly unrelated initiatives in a way where the respective messages are reinforced by one another. Take for example informa-

tion security (IS) efforts and employee engagement efforts. It is, of course, natural for the IS leader to spend time emphasizing best practices in safeguarding company information; likewise, HR leaders often drive ways to boost employee engagement while addressing team dynamics. However, these undertakings are not mutually exclusive. In fact, as leaders in the organization we can work to support one another's efforts and draw connections between important organizational efforts.

It is no secret that information security is top-of-mind for executive leaders. A 2014 report from Gartner estimates that the 2015 global spend on security will exceed \$76 billion. Employee engagement also continues to be in the forefront of organizations as the global aggregate spend on employee engagement-related activities is expected to exceed \$1 billion in 2016. This investment in employee-engagement efforts is driven in part by research that illustrates how companies with high engagement levels typically outperform their competitors in key metrics.

Here is where magic ensues. As leaders, we can make explicit connections between highly engaged teams and the ability to safeguard systems as evidenced through departmental metrics. While there are countless studies that examine how highly engaged teams outperform lesser engaged teams, it is these local, company-specific examples that will resonate with employees. These powerful examples of organizational storytelling reinforce the important initiatives we drive. In fact, in our work together we talk to organizational leaders to

show the evidence-based safeguarding prowess of highly engaged teams. One example we often share is that highly engaged teams are more likely to report suspicious activities and behaviors. This is powerful. If organizations can leverage front-line employees against cyber attacks, these companies will dramatically reduce the likelihood of a security breach. Simply put, highly engaged employees make better stewards of company systems and data. Moreover, this message can be that much more compelling when it is underscored from different leaders across an organization.

When ordering up that next initiative, think creatively beyond the same old drink order. Sometimes a shot of information security with a dash of employee engagement can be a winning recipe for everyone.

About the Authors

Eric M. Harper, EdD, is a talent-management leader for a financial services company. His doctoral research focuses on the variables impacting employee engagement. He may be reached at eharper@gse.upenn.edu.



Alex L. Nehlebaeff, CIS-SP, is a retired US Navy Chief Petty Officer who has worked in the information security field since 1990. He currently serves as the senior information security leader at a financial services company. He may be reached at nehlebaeff@gmail.com.





The First Levchin Prize

By Luther Martin – ISSA member, Silicon Valley Chapter

On January 6, 2016, at the Real World Cryptography Conference 2016, Dr. Phil Rogaway was recognized for his contributions to practical applications of cryptography when he was awarded the first annual Levchin Prize¹ for significant contributions to real-world cryptography. The fact that Dr. Rogaway was recognized by the prize committee in this way is very significant.

The website for the Levchin Prize tells us this: “Rogaway is considered a giant in the field of symmetric encryption. He was given the Levchin Prize for his work on authenticated encryption and format preserving encryption.”

Saying that Dr. Rogaway is considered a giant in the field of symmetric encryption makes him sound quite impressive, but saying that he is a giant in this field is a bit like saying that Einstein was a giant in the field of physics: both of them made significant contributions to the field that fundamentally changed the way the rest of the field think today.

Dr. Rogaway was one of the pioneers that turned cryptography from a poorly understood black art into a science with rigorous mathematical foundations. Instead of just hoping that a cryptographic scheme is secure because nobody has found a weakness in it yet, we can now rigorously prove that certain weaknesses can *never* be found in carefully designed cryptographic schemes, no matter how clever and determined a hacker might be. That’s very useful.

But in addition to pioneering advances in theoretical cryptography, Dr. Rogaway also pioneered cryptographic technolo-

gies that have very practical applications in the real world. Format-preserving encryption (FPE) is one of these.

Ciphertext from an encryption algorithm usually looks very different than the corresponding plaintext. If we encrypt the plaintext string “4111111111111111” using AES-ECB, for example, we might get a string like “MKSqwaywf4N8i9gEci4yTUTPalvn-QBlBi+Uz6j1Tjig=” for our (Base64 encoded) ciphertext.

If the original string represented a credit card number, the encrypted version will not look like a credit card number at all. It will contain characters other than the digits 0 through 9, and will be longer than a 16-character credit card number.

Changing the format of data can cause problems in many of today’s legacy IT environments because some applications can only handle data that has a particular format, and modifications that work around this issue can be very expensive.

An approach that works well in many cases adapts the data to the environment instead of adapting the environment to the data. One way to do this is to implement encryption in such a way that ciphertext has the same format as the corresponding plaintext. This may be easy to do, but it is not easy to do securely.

To get ciphertext that has the same format as the corresponding plaintext, researchers have proposed many versions of FPE. The technology dates back to at least 1981, when the original US government guideline for implementing the Data Encryption Standard (DES) (FIPS 74) included a description of how to use DES encryption in a way that preserved the format of data on a character-by-character basis, (e.g., mapping a decimal digit to another decimal digit).

Over the following years, researchers proposed various other ad hoc (and non-secure) approaches to FPE, but in 2002 Dr. Rogaway (along with Dr. John Black) described three approaches to FPE and proved that they were secure. The FFX modes of AES that are currently used to encrypt millions of credit card transactions each day represent the evolution of one of these approaches, and the dramatic success of FPE technology should clearly indicate that Dr. Rogaway’s contributions to the field of cryptography are indeed of more than a purely theoretical nature.

Dr. Rogaway’s work on authenticated encryption is also important. Authenticated encryption provides a way to provide confidentiality, integrity, and authentication through a single clever use of an encryption algorithm. The Galois/Counter Mode (GCM) of AES is probably the most significant example of this technology. And although GCM is not widely used today, it will almost certainly become widely used in the future.

The single cipher suite that is required for implementations of TLS 1.2 by NIST’s Special Publication 800-52, “Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations,” is TLS_RSA_WITH_AES_128_GCM_SHA256, a cipher suite that uses the GCM mode of AES. So as TLS 1.2 is gradually deployed, the use of authenticated encryption will eventually become very common, even if it is not widely used today.

So, congratulations, Dr. Rogaway. This is an award that is clearly justified.

About the Author

Luther Martin is a Distinguished Technologist with Hewlett Packard Security Voltage. You can reach him at luther.martin@hpc.com.

1 The Levchin Prize for Real-World Cryptography – <http://levchinprize.com/>.

ISSA/ESG Special Research Project to Call on Members

ISSA and Enterprise Security Group (ESG) have joined forces to level-set the progress of the cybersecurity profession in relation to the world's ever-escalating demand on the cybersecurity ecosystem. This first-of-its-kind survey is being designed for use by cybersecurity professionals, governments, nongovernmental organizations, educational institutions, and the spectrum of businesses around the world that are increasingly dependent upon a reasonably secure data environment for the safe conduct of operations.

ISSA will be issuing the survey sometime within the next 30 days. ISSA will be asking all 10,000 members around the world to join in having the voice of the profession heard and take this opportunity to participate and ensure your perspectives are earmarked for development. All responses will remain confidential. Members will have secure access to the completed study and an executive summary will be available to nonmembers.

ISSA Fellow PROGRAM

2016 Fellows Cycle Open

Do you qualify for Senior Member, Fellow, or Distinguished Fellow? [The Fellow Program](#) recognizes sustained membership and contributions to the profession. No more than one percent of members may hold Distinguished Fellow status at any given time. Fellow status will be limited to a maximum of two percent of the membership.

Nominations and applications are accepted on an annual cycle. Applications will be accepted until August 1, 2016, at 5:00pm Eastern Time. [Apply today!](#)

ISSA INTERNATIONAL AWARDS

ISSA International Awards: Nominate an Outstanding Security Professional

ISSA annually recognizes outstanding information security professionals, their companies, and chapters that are at the top of their respective games. Who would you like to see recognized? Nominations may be made by any member. Anyone interested in making a nomination should thoroughly review the [Awards Policies and Procedures](#). All nominations and supporting documents must be received by May 16, 2016, at 11:59 p.m. Eastern time. This year's awards will be presented at the ISSA International Conference in Dallas,

November 2-3. Any member in good standing is eligible to propose candidates for:

- **Hall of Fame:** pays homage to an individual's exceptional qualities of leadership as well as an exemplary commitment to the information security profession.
- **Honor Roll:** recognizes an individual's sustained contributions to the information security community, enhancement of the professionalism of ISSA members, and advancement of the association.
- **Security Professional of the Year:** honors the member who best exemplifies the most outstanding standards and achievement in information security in the preceding year.
- **Volunteer of the Year:** recognizes a member who has made a significant difference to his or her chapter and the association through dedicated and selfless service to ISSA.
- **Chapters of the Year:** rewards chapters that have done an exceptional job of supporting ISSA's mission, serving their member communities, and advancing the field.
- **Organization of the Year:** acknowledges an organization that has contributed to the overall good and professionalism of the association and its membership.
- **President's Award for Public Service:** honors an individual's contribution to the information security profession in the area of public service.

[Submit a nomination today.](#) For any questions, please contact Leah Lewis, llewis@issa.org.

ISSA JOURNAL

ISSA Journal Scholarship for Best Student Article

This year the *ISSA Journal* will be awarding a scholarship for the best article by a university student. Recipient must be attending an accredited college or university full time and actively pursuing a degree.

The submission period is now open and the ISSA Journal Editorial Advisory Board will accept articles until October 1, 2016. We encourage students to follow the published [editorial calendar](#) but will consider any submission that is focused on information security. The Board will select the best student article that meets our qualifications for publication in the December 2016 issue of the *ISSA Journal*.

Submissions, comments, and questions can be directed to editor@issa.org. If you are interested, please see the *Journal's* website for our [editorial guidelines](#) and [calendar](#).



Growing Your Career through Chapter Leadership

By Debbie Christofferson – ISSA International Director and Distinguished Fellow

Why join an ISSA chapter board?

“I wanted to meet people in the field, get familiar with companies, technology, jobs, and people, and expand my horizons beyond my daily job. It allows me to contribute to my field.” – Dee Ramon, Information Risk Manager, CSC/Freescale, ISSA Phoenix Chapter

When you lose a job, take a buy-out, or change homes and jobs, you may find yourself disconnected, isolated, and unsure of where to turn for help. You need a new network! You can achieve this immediately by serving on your ISSA chapter board and actively engage, rather than sitting in an audience. As a board leader, you grow an extended network of experts and friends quickly. Get started right here!

Learning and growing

Leadership roles in ISSA will teach you much and afford as many opportunities as you choose. During my chapter leadership, Phoenix Chapter grew from under a dozen attendees to a Chapter of the Year award. We recruited a strong board, increased our value to grow membership and attract sponsors, and launched an annual conference.

Through activities and engagement in our professional community, you can earn a fellowship, lead major programs, and develop new skills. At the international level I have worked on the CISO Advisory Council, our annual Chapter Leadership Summit, and the Request for Proposal process for the ISSA association management contract. Opportunities exist for any talent, interest, or time you want to give. You can learn any-

thing you want, while supporting your career, company, colleagues, and businesses.

Interacting with experts

Associations offer a perfect target market in the field where you operate for those wanting to connect with our members. In a leadership role, you talk to these organizations and industry experts daily. Companies contact association leaders when seeking expertise or talent. When eBay located PayPal offices in Arizona, a recruiting manager was in the ISSA Phoenix audience. Relocated individuals reach out to ISSA to plug-in quickly.

Peer-board members are often leaders and luminaries in our field. You will be gaining easy access and building relationships with a large circle of influence and expertise. Expedite your results by engaging on the board in an area you enjoy or want to develop. ISSA chapters are made up of industry leaders and service providers from across sectors and companies where they operate.

Growing your career, business, and life

Join a chapter board for a fun and rewarding opportunity. You will build relationships and lifetime friends, while creating value for our industry and the business you serve. Ask your chapter leaders today about gaps and opportunities.

BE A LEADER. CREATE THE SUCCESS YOU WANT.

ISSA CISO Virtual Mentoring Series

Learn from the experts! If you're seeking a career in cybersecurity and are on the path to becoming a CISO, check out the [schedule of upcoming presentations](#).

For information on sponsorship opportunities, click [here](#).

CSCL Pre-Professional Virtual Meet-Ups



So, you think you want to work in cybersecurity? Not sure which way to go? Not sure if you're doing all you need to do to be successful? Check out Pre-Professional Virtual Meet-Ups to help guide you through the maze of cybersecurity.

May 31: 1:00 pm - 2:30 pm EST. [Basic Security Methodologies](#).

ISSA CISO FORUM

The CISO Executive Forum is a peer-to-peer event. The unique strength of this event is that members can feel free to share concerns, successes, and feedback in a peer-only environment. Membership is by invitation only and subject to approval. Membership criteria will act as a guideline for approval. Save the date for our 2016 events:

Charlotte, NC: May 19-20, 2016

Theme: [Infosec and Legal Collaboration](#)

Las Vegas, NV: July 31-August 1, 2016

Theme: [Convergence: Securing the World around You](#)

Dallas, TX: November 3-4, 2016

Theme: [Big!](#)

For information on sponsorship opportunities, click [here](#).

 **ISSA**
SPECIAL INTEREST GROUPS

Save the Date! Special Interest Group Webinars

Want to hear more from ISSA's Special Interest Groups? [Join free here!](#)

Women in Security SIG

May 9: 4:00 pm - 5:00 pm EST. [Overcoming the Real Barriers to Women in Security.](#)

Security, Education, and Awareness SIG

June 15: 9:00 am - 10:00 am EST. [10 Things Disney Can Teach Us About Running a Security Awareness Program.](#)

Healthcare SIG

June 23: 12:00 pm - 1:00 pm EST. [3rd Party Risk Assessment for Healthcare Organizations.](#)

Financial SIG

April 29: 1:00 pm - 3:00 pm EST. [Vendor Security Management for Financial Institutions.](#)

 **ISSA International Web CONFERENCE**

Breach Report Analysis: SWOT or SWAT?

2-Hour live event Tuesday, May 24, 2016

9 a.m. US-Pacific/ 12 p.m. US-Eastern/ 5 p.m. London

[Click here for more information or to register!](#)

View the calendar of web conferences [here](#). To sponsor an International Web Conference click [here](#).

Generously sponsored by  **Symantec**

 **ISSA**
JOURNAL

Elevate Your Career with Writing Experience

As a security professional, you have unique and valuable experiences, insights, and information that could positively impact infosec practitioners around the world. Exchanging that wealth of knowledge in our ever-evolving field is vital in helping us all do our jobs better and achieve our individual career goals. Effective writing is an essential skill for achieving your career goals. Do you have an article in mind? Would you find it helpful to bounce your ideas off of other members and get their feedback?

The Journal's Editorial Advisory Board will match you with an experienced author as a resource to help you practice and refine your skills, communicate your knowledge, and raise your visibility and stature. Join [Friends of Authors](#) today, and let us know your interests and goals.



Strategic Partners

ISSA International has entered into strategic partnerships with a number of organizations that include cross-promotion of our mutual activities. Welcome The Security Awareness Company.



the security awareness
C O M P A N Y

Why the Security Awareness Company and ISSA Partnered

All too often the little guys—the millions of small, innovative companies that drive the global economic engine—get ignored. This is true with information security, too; vendors want to sell to the “whales” because selling to the little guys is not always cost-effective. Makes sense.

Plus...the little guys don't always have the internal expertise, skills, available staff, or budgets to be aware of the need for—or have the ability to implement—proper security, security training, and awareness to their workforce.

Except...the Security Awareness Company, in partnership with the ISSA, believes that the little guys need a fair shot of getting their employees up to snuff, aware of and know how best to interact with technology in their personal, professional and mobile lives, even if they don't have a budget.

How many 3-20 person offices need security awareness? Doctors, dentists, and chiropractors. Bookkeepers, accountants, and insurance companies. Lawyers. Auto-repair shops +++

How many 25-250 person companies “...aren't worth the price of the phone call...” according to some sales cultures? We believe that these critical underpinnings of the global supply chain should be involved in their own security awareness, just like the Big Guys.

Ergo...

ISSA is the perfect example of our ideal partner: A strong, decentralized model, heavy localized involvement, and the ability to involve stakeholders of all sizes, from all industries.

We at the Security Awareness Company just want to do our part. Everything we provide to ISSA and its members of any size from 1 to 1,000,000 is Free! under [Creative Commons 3.0](#).

Enjoy...and Be Safe Out There!

Winn Schwartau, CEO and Founder
the [Security Awareness Company](#).

2016 International Election Candidate Profiles

The election of the International Board of Directors will take place online June 6–24. From the following slate of candidates, you will select the following positions:

International President
Five International Directors

Eligible voters include General, CISO Executive, Lifetime, and assigned Corporate and Government Organizational members as of June 6. Voting information will be sent to your primary email address on file. Please update your member profile to ensure you receive your credentials. If you have questions regarding your membership status, contact elections@issa.org.

President

Candy Alexander
Andrea Hoy

Five Director Positions

Mary Ann Davidson
Rhonda Farrell
Garrett D. Felix
Alex Grohmann
Robert Martin

DJ McArthur
Shawn Murray
Stefano Zanero
Daniel Ziesmer

Profiles of each candidate can be found on the pages that follow.

Your Vote Will Make a Difference

Did you know that on average, among professional associations, from five to seven percent of the membership actually make the effort to vote? That's right! Less than 10 percent of the membership is deciding who will lead your association into the future. Voting only takes a few minutes. Make your voice heard this year—and make a difference.

The ISSA elections open at 8 AM Eastern Time on June 6, 2016 and will close 11:59 PM Eastern Time, June 24, 2016.

You should have received an email from elections@issa.org. The email contains your unique voter login URL and your unique login credentials. The email was sent to the primary email address we have on file for you. If you do not see this email in your in-box, please check your junk folder and/or spam filter for your login credentials. If you do not receive your credentials or need assistance, please contact Leah Lewis at llewis@issa.org or call +1 866 349 5818 ext. 4082.

**President Candidate
Candy Alexander**

CISSP, CISM

As a recognized cybersecurity expert, I have 25+ years of experience in the field. In order to keep this focused on the ISSA, I ask that you visit my LinkedIn profile to learn about my professional background. (<https://www.linkedin.com/in/candyalexander>).



My commitment to ISSA is demonstrated by lifelong membership, service on the ISSA International Board (overseeing Communications, the *Journal*, Marketing/Branding, and PR), and as the Chief Architect for the Cyber Security Career Lifecycle®. I was also the first President of the ISSA Education Foundation and continue to serve on the board. I'm a member of the New England and New Hampshire Chapters. I have received numerous awards: Professional of the Year, ISSA Honor Roll, Distinguished Fellow, and ISSA Hall of Fame.

Statement of Goals

During my tenure, I have earned a reputation for my passion and for getting things done through leading and working with teams. It is now time to take on the role of International President. Based on what I am seeing in the world around us, it is crucial for ISSA to increase its relevance. This needs to be accomplished through developing and implementing new innovative programs. It is time for ISSA to take a fresh approach:

- **Demonstrate ISSA's leadership and value by highlighting our neutrality.** We must remain neutral to all certification and educational organizations in order to provide our members the best experience. Partnering with all—exclusivity to none.
- **Focus on ISSA's core strength—professional support system.** ISSA's strength is in providing networking and knowledge-sharing opportunities that are unique to each individual. It is important to continue building services using the Cyber Security Career Lifecycle® and deliver through chapters.
- **Develop innovative solutions.** It may sound like a cliché, but we are a profession based on technology. I will reach out to chapters and members to understand their needs, and then implement innovative solutions to meet those needs. It is important to identify cutting-edge solutions to deliver knowledge-sharing opportunities for our members.
- **Foster the community spirit.** ISSA is *the* security profession; we need to foster our community and celebrate it. We need to recognize our chapters and members who continue to give, while encouraging others to grow.

I urge you to make your voice and the voice of the profession heard by voting. I ask for your vote. Together we can make wonderful and exciting things happen.

(This information provided by the candidate who is solely responsible for the content.)

**President Candidate
Andrea C. Hoy**

CISSP, CISM, MBA

Andrea Hoy is arguably one of the leading women in her profession. A former advisor to the Pentagon, receiving the Security Education Manager's Award in 1991, she has worked on numerous committees in Washington, DC. Internationally she has assisted Fortune 20 corporations with establishing policies and procedures that comply with the European Union Privacy Directive, the Data Protection Act, and the Dutch Personal Data Protection Act.



Since 1998, Andrea has served ISSA: International Board as Director, Vice President, and current President. She has diligently served at the chapter level: Orange County Chapter Program Director, Vice President, and eight terms as President; and founding member of Ventura County Chapter. She initiated and founded the Financial SIG.

In recognition for Andrea's endless contributions and dedication to the industry and profession, she has been awarded the ISSA's Distinguished Fellow and is on the Honor Roll, as well as the YWCA Women in Leadership award.

While on the International Board, she has spoken with many members across our truly global constituency. She understands that various geographic locations have unique necessities and supported funding the EU Chapter Leaders' Summit, which is a good model for other regions.

Statement of Goals

- Expand ISSA's international presence initially by targeting underserved geographic regions
- Membership recruitment initiatives for new cyber professionals
 - Establish and expand student chapters on campuses
 - Create and provide continued support to Cyber Challenges and incorporate additional practice "cyber ranges" (K-12, high school, and collegiate)
- Ensure that our Special Interest Groups (SIGs) reflect topics that serve to educate our international communities
- Expand and increase industry discounts for ISSA members for global industry conferences and information security training (i.e., RSA, Black Hat, CEIC)
- Continue to drive the formalization of our Strategic Alliances with additional professional organizations, broadening the cyber scope to include governance, privacy, and other elements.

As a past Presidential Advisor, as well as a CISO Executive Forum Task Force and Financial SIG founder, ISSA Orange County Chapter President for over eight years, and founding member of Ventura County, our 151st chapter, I hope you find it in your heart to allow me to continue to represent you and expand our association across the globe.

(This information provided by the candidate who is solely responsible for the content.)

Director Candidate
Mary Ann Davidson

Mary Ann Davidson is the Chief Security Officer at Oracle Corporation, responsible for Oracle Software Security Assurance. She represents Oracle on the Board of Directors of the Information Technology Information Sharing and Analysis Center (IT-ISAC), and serves on the international board of the ISSA.



Statement of Goals

I have several goals I would like to pursue as a Director of ISSA International, one of which is in the area of regulatory impact. Many of us work in regulated industries; the rest of us soon may be as “cybersecurity legislation” becomes front and center in multiple countries. The degree to which we can leverage other’s experiences and knowledge in these areas helps us be smarter, faster. Without becoming lobbyists, we must nonetheless weigh in on public policy issues that affect us. Many regulators do not always understand the cost of mandated measures vs. tangible benefits of those measures. ISSA needs to “speak for the troops in the trenches” at the front lines of information security.

We must also strengthen our pipeline by targeting universities to recruit the next generation of practitioners for the “ISSA community of tomorrow.” We should also engage with universities to help instill in them the need for better security education in multiple disciplines such as computer science, computer engineering, and software engineering (and for that matter, business school curricula).

We are handicapped as professionals by the degree to which the underlying IT infrastructure actually is designed and built as infrastructure. If we do not change our collective mind-set (in part via educational change), there are not enough IT security professionals in the world to secure critical IT-based infrastructure any more than training more doctors will stem a plague. Further, cybersecurity is a function in support of larger business objectives, since business is about assuming risk and there is—alas—a paucity of understanding the systemic risk that the increase in IT-based systems can pose.

Ultimately, good public policy has to be implemented by the people doing the work. Improving the “inputs” to our professional lives—new recruits who can bring their educational experiences to us; better, more robust software and hardware engineered for today’s threats—will enable better “outputs”—defensible, robust cyber infrastructure.

(This information provided by the candidate who is solely responsible for the content.)

Director Candidate
Rhonda Farrell

Dr. Rhonda Farrell is an associate with Booz Allen Hamilton, primarily focusing on lifecycle activities as they relate to cybersecurity infrastructures within the IC, DoD, and federal civilian markets. Her prior career experience includes supporting operations, engineering, information security, and training initiatives within Fortune 500 companies throughout Silicon Valley, California, and the US Marine Corps at Quantico, Virginia.



Her educational background includes a BS in Business Administration (1999), an MBA in Strategic Management (2000), a JD (Technology focus – 2009), and a Doctorate of Science in Information Assurance (2015).

Her diverse professional memberships include decades of service to ISSA, the American Society for Quality (ASQ), Institute of Electrical and Electronic Engineers (IEEE), and the Women Marines Association.

She has served on the ISSA International Board of Directors since 2014, as a chapter officer since 2010, and as a chapter member, contributor, or committee member since 2003. She is currently a Fellow within the organization.

Over the last two years, as a member of the ISSA International Board of Directors, she has worked tirelessly to actively engage members and community participants from across the globe in special interest group (SIG) growth and centralization efforts; helped develop and pilot the mentoring working group for chapters, members, students, and faculty; promulgated planning and governance best practices at the board and chapter level; while seeking to create and instill a culture of performance excellence and service to one another and the profession. Lastly she continues to focus on automation and infrastructure activities that enable efficiencies across the Cyber Security Career Lifecycle (CSLC) program offerings, while expanding ISSA International strategic partner offerings and the Women in Security SIG internationally.

Statement of Goals

- Full centralization and growth of the core SIG offerings within industry and worldwide
- Expansion of the pilot Mentoring working group to include chapter and international participants
- Strengthened strategic partner offerings that expand professional development opportunities across the five population strata of the CSLC

Rhonda seeks your vote to continue working both domestically and internationally in the areas of performance excellence, holistic development of the security practitioner, industry partner integration, as well as continuance of all SIG-related growth initiatives, within a framework of heightened governance, strategic alignment, and service to the profession.

(This information provided by the candidate who is solely responsible for the content.)

**Director Candidate
Garrett D. Felix**
MS, CISSP



Garrett currently oversees the global privacy and information security strategy as Privacy Officer and Information Security Officer for EXOS|MediFit. Garrett has been a member of ISSA since 2005 and became a CISO Executive Member in 2007. He has served in various leadership capacities at the international, national, and local levels within the association. In December 2015, Garrett was appointed to fill a Director vacancy with the ISSA International Board, after serving four years on the ISSA CISO Advisory Council. Prior to that, he served three years as president of the Central PA Chapter. In 2014, Garrett was recognized as an ISSA Fellow. Additionally, he is currently a member of the Delaware Valley Chapter.

Garrett has further contributed to various ISSA projects, webcasts, presenting at the ISSA International Conference and via the Cyber Security Career Lifecycle™ Pre-Professional Meet Up. In addition to his involvement in other information security industry events, he has also been a frequent speaker on security and privacy issues impacting the Health, Fitness and Wellness Industry.

Statement of Goals

ISSA has provided me, as I am sure the majority of our membership, with access to a vast industry network of colleagues willing to share their experiences, successes, challenges, and expertise to help each other find ways to solve similar problems we face each day as cybersecurity professionals.

In December 2015, I stepped down from the ISSA CISO Advisory Council when I was asked and accepted an appointment to fill the remainder of a vacated Director term on the International Board. During this short time I have assisted ISSA in taking appropriate steps to protect ISSA Intellectual Property, as well as begin looking at ways in which we can expand the value of the organization as a true, international association. As such, I feel the work that I am just beginning will not be able to be truly accomplished and realized in the short period allotted from filling the vacancy.

In addition to the work that is underway, I will continue to support and drive international association objectives that will further develop and leverage cybersecurity resources in order to enhance the industry-leading value that ISSA can bring to our world-wide membership, the global information security community, and the next generation of information security professionals as a whole.

(This information provided by the candidate who is solely responsible for the content.)

**Director Candidate
Alex Grohmann**



Alex Grohmann has been a driving force in the information security community of Northern Virginia Chapter (NOVA) and would like to continue serving the members of ISSA at the international level.

Alex has been an active and contributing member of the local ISSA chapter board for over a decade and has held various roles including public relations, programs, president, and is currently the president emeritus of the chapter. During Alex's three years as president, the membership increased 11 percent to over 530 members, sponsorship quadrupled, and average meeting attendance regularly surpassed 120 attendees. He founded a Toastmasters chapter within the chapter to help promote public speaking for technology professionals. As a direct result of these efforts, NOVA was recognized as Chapter of the Year in 2014.

Mr. Grohmann's efforts also strengthened the local security academic community. For example, funding for NOVA's main scholarship, the Laurie McQuillen/Ed Hetsko memorial fund (\$25,000), was fully endowed. Additional yearly grants of \$5,000 were also distributed. Working with three local universities, he created a mentoring program. He also created a relationship with the Pete Conrad Foundation/Spirit of Innovation awards, positioning the chapter to be the exclusive Challenge Partner for all of the international high school teams competing in cybersecurity. Mr. Grohmann also served on the Washington, DC, InfraGard board for many years and is a graduate of the respected FBI Citizens' Academy. He is currently a member of the cybersecurity committee within the Northern Virginia Technology Council, as well as Northern Virginia Community College's Workforce Affinity Group.

As an independent security consultant with over 20 years of experience, Mr. Grohmann currently concentrates his efforts mainly in financial services but also recently in the energy sector. In 2014 he was awarded the Fellow status by ISSA and in 2015 he entered the Honor Roll.

Statement of Goals

1. Strengthen relationships between International and the individual chapters to provide guidance and consistently improve communications
2. Build upon the existing ISSA efforts in the workforce and education development areas, including the Cyber Security Career Lifecycle, to ensure they meet the needs of the next generation of security professionals.
3. Promote new and improved information sharing forums for security professionals, leveraging the ISSA organization.

Any consideration of Alex's interest to serve on the international ISSA board would be appreciated.

(This information provided by the candidate who is solely responsible for the content.)

**Director Candidate
Robert Martin**

CISSP

Robert Martin has over 12 years of experience working in the information security field. He is a Security Engineer for Cisco Systems, Inc. in RTP, NC.

Robert specializes in areas such as risk management, regulatory compliance, security solutions architecture, security audits, vulnerability assessments, and penetration testing.

From 2012-2015, Robert served as president of the Raleigh Chapter. During that time, the chapter membership grew at a rate of 125 percent. Currently, Robert serves on the Raleigh board as the Sponsorships Director. Robert is committed to serving the community through outreach by expanding the chapter's mission to students and military. He has held several other IT security advisory board positions over the years with a focus to bring about awareness of information security threats in an ever-changing global IT security economy.



Statement of Goals

1. Create greater synergy between the ISSA International Board and the local chapters.
2. Create an ISSA international information sharing platform so all ISSA chapters can share successful programs for membership growth/retention, annual conferences, and chapter events.
3. Create programs to attract new information security professionals from universities and technical colleges.
4. Create a speaking circuit of information security luminaries to present at local ISSA chapters and conferences to drive attendance and chapter growth.

(This information provided by the candidate who is solely responsible for the content.)

**Director Candidate
DJ McArthur**

CISSP, HiTrust CCSFP, EnCE, GCIH, CEH, CPT

DJ McArthur currently manages the data security department for one of Colorado's largest health-care providers, Centura Health. He served in the US Marines Corps, holds a degree in information systems security, is currently pursuing an MBA in IT administration in health care, and has served in previous roles as a data security architect and network security engineer.



Prior to the healthcare industry he has spent over 10 years in other verticals such as the Department of Defense, energy, construction, infrastructure, transportation, and architectural industries where he held various security roles and responsibilities. He has been an active member of the ISSA for over ten years, is currently the Director of Communications and has held various ISSA board positions for the local Denver Chapter over the last six years while helping plan and coordinate the Rocky Mountain Information Security Conference (RMISC).

Statement of Goals

1. Continue to promote education and awareness of information security-related issues and trends out to the community abroad.
2. Utilize the skills and lessons I have learned from serving at a local chapter level up to the International Board to better serve the chapters and help with the challenges they are facing today.
3. Ensure student members, mentors, and special interest groups have good support at the international level.
4. Continue to proudly represent myself as an ISSA member and any other duty, position, or honor bestowed upon me by the ISSA members and the community.

(This information provided by the candidate who is solely responsible for the content.)

**Director Candidate
Shawn P. Murray**

C|CISO, CISSP, CRISC, FITSP-A, C|E|

Shawn Murray is a Principal Scientist with the United States Missile Defense Agency currently assigned as a Senior Cyber Security Professional and is an officer in the US Civil Air Patrol. His previous assignments include work with the US Army Cyber Command in Europe, US Air Force, and with commercial industry in various roles in information assurance and cybersecurity. He has traveled the globe performing physical and cybersecurity assessments on critical national defense and coalition systems. Dr. Murray has worked with NSA, FBI, CIA, and the US Defense and State Departments on various cyber initiatives and has over 20 years of IT, communications, and cybersecurity experience.



He enjoys teaching and presenting as a guest lecturer on cybersecurity, business, and computer science courses for several universities. He has several industry recognized certifications to include the C|CISO, CISSP, and CRISC. He holds several degrees to include an Applied Doctorate in Computer Science with a concentration in Enterprise Information Systems. He is an ISSA Executive CISO member and chapter board member. He is also a professional member of IEEE, ACM, (ISC)², and is an FBI Infragard program partner. He enjoys spending time traveling with his family, researching and collaborating with other professionals in cybersecurity and cyber law, and volunteers in his community as a soccer coach.

Statement of Goals

As a practitioner and educator I am passionate about the current and future state of cybersecurity as well as collaborating with the people who lead the charge in this profession. As a Director on the international board, I would continue my service and represent the best interest of our international members and work with other international board members to steer ISSA into the future. I bring forth extensive experience applying information security concepts and educating future cybersecurity professionals expected to fill widening gaps in our career field.

My goals for my term include: Working to find solutions to address gaps in skill sets to address shortages while educating new professionals in ethical standards required to maintain credibility and trustworthiness; and working to find ways to bring additional value to our membership and to identify ways to bring in new members. Additional goals include working to identify resources for outreach programs and certifying new members in the profession internationally. I will be the voice of our members!

(This information provided by the candidate who is solely responsible for the content.)

**Director Candidate
Stefano Zanero**

I received a PhD degree in Computer Engineering from the Politecnico of Milano University. Currently, I am an Associate Professor at the Dipartimento di Elettronica, Informazione e Bioingegneria of the same university.



I have been a speaker at international scientific and technical conferences, including the Black Hat briefings, CanSecWest, DeepSec, and Hack in the Box. I have authored or co-authored over 60 peer-reviewed papers. I am a senior member of the IEEE (Institute of Electrical and Electronics Engineers) and the IEEE Computer Society, for which I am currently serving in the Board of Governors. I am also a lifetime senior member of the ACM (Association for Computing Machinery).

I am a founding member of the ISSA Italy Chapter and have served as an International Director over the past eight years. I have been named a Fellow of our association.

In 2004 I co-founded Secure Network, a high-profile information security training and consulting company based in Milan. In 2010 I co-founded 18months, a startup delivering in-the-cloud mobile, social-enabled ticketing solutions. In 2015 I co-founded a stealth-mode startup in the fintech sector.

Statement of Goals

Over the past years, I have dedicated most of my volunteer time to build and grow (with the help of countless great ISSA volunteers whom I cannot thank enough) our association's International Conference. If elected, I will continue devoting time to the development of the event.

I believe that ISSA can grow strongly outside of the United States, and if elected, I plan to devote my attention to membership development in the EU area. As the European Commission is currently funding the security area within the Horizon2020 plan, ISSA could and should be a trusted source and partner for security initiatives at the Commission level.

I am also a strong believer in partnerships, and I have helped the ISSA board to reach out to the IEEE and the Computer Society. We need improved cooperation with our (ISC)² colleagues to better serve our respective members..

I strongly believe that we are still under-exploiting the networking potential of ISSA, and we will need to figure out over the next two years how to evolve, connect, and integrate our chapters and members.

Finally, I think ISSA is still missing out on the younger members of the profession, in particular those starting from a technical approach. I think that ISSA can grow in its standing if it helps bridge the gap between seasoned professionals and managers and young, bright thinkers with potentially novel solutions in their minds. We need to be present in colleges and universities and to develop mentoring programs that allow student members to become better professionals.

(This information provided by the candidate who is solely responsible for the content.)

**Director Candidate
Daniel Ziesmer**

And last, but not least (assuming ISSA listed us alphabetically)...

In a year that is already replete with election campaigns and politics, I will spare you promises that cannot be kept, demands that cannot be fulfilled, and assurances that would surely ring hollow. Instead I will speak simply, and plainly.



Today I like to think of myself as an experienced risk management and cybersecurity professional, but I fully understand and know what it means to start at the bottom of a career ladder, working to build the knowledge, skills, and abilities to make that next step, and do so successfully. ISSA is an organization that provided me with opportunities to better interact with my peers and those who had advanced in their careers before me. It provided me a chance to transition my career, and at the same time reach out a hand and help those who were behind me. This organization is unique because we're not trying to sell something, and we're not asking for anything in return... that is a noble effort I want to continue.

My work as a former (and still part-time) educator and mentor perhaps most drives my desire to serve on the board: to carry forward a spirit of service and servant leadership. In fact, I chose to run this year because I heard from so many of you—whether unaffiliated professionals, new members, long-standing associates, or even vendors—that what you felt was most missing on the board was “a voice.” My purpose is to be a conduit that carries your ideas, needs, and goals into the board discussion, driving change that aligns with ISSA’s vision and mission, but also broadens the organization’s outreach and horizons as we look to the future.

As a former manager of a non-profit, as well as prior board director/president for other non-profit organizations, I have a unique appreciation of the complexities behind an operation that seems to go smoothly, and the challenges of satisfying a constituency. ISSA can appear as a deceptively simple organization, but it requires planning, organization, and careful management. My experiences provide me with the insights to make a distinctive contribution in this regard.

As we look to the future, the future of ISSA will be inextricably linked to the future of risk management and cybersecurity. For many, that future is described using words ranging from “exciting” and “challenging” to “difficult” and “terrifying.” But the future is not certain...we can shape that future, and we need strong organizations like ISSA that don’t just support our professional needs, but provide leadership and vision for businesses, government, and industry.

If you would like to learn more about me, visit my website at www.ziesmer.org, which includes a more detailed biography for your perusal. In addition, I encourage you to contact me directly at issaboard@ziesmer.org if you have any specific questions or inquiries. Thank you for your vote.

(This information provided by the candidate who is solely responsible for the content.)

**ISSA International
CONFERENCE**

2015 Chicago Keynotes & Sessions

Recorded sessions and presentation materials available at www.issa.org/?issacnf_home.



**CISO Panel Luncheon:
Advancing the Culture of Security**

[View the video.](#)



International Awards Luncheon

Shon Harris was awarded the Hall of Fame posthumously. She past away in late 2014. Her mother, Kathy Conion, accepted the award for her. The specialness of the moment increased with everyone in the room standing and applauding. Stephano Zanero, International Director, closed with, “Thank you to the audience for standing and recognizing a true luminary of our profession.”

[View the video.](#)

Tech Target Interview



**Reduce Information Security Costs with
Smart Strategy, Personnel**

Jeff Reich, chief security officer at Barricade.io.

[View the video.](#)



SURVIVAL STRATEGIES IN A CYBER WORLD

Hyatt Regency | **NOVEMBER 2-3** | Dallas, Texas

PREDICT **PREPARE** **PROTECT**

 **ISSA** International
CONFERENCE

2016

**REGISTER TODAY
EARLY BIRD RATES
UNTIL APRIL 30**

**NOVEMBER 2-3, 2016
HYATT REGENCY | DALLAS, TEXAS**

Do Data Breaches Matter?

A Review of Breach Data and What to Do Next

By Kristopher Dane – ISSA member, Puget Sound Chapter

This article discusses the threat of cybercrime and data breaches to organizations. The author discusses the economics of data breach information and then reviews the existing public data on breaches to see how markets are responding. The article concludes with a call to action to normalize breach reporting to better inform consumers and enable future research.



Cybercriminals pose a growing threat to corporate and personal information. Although governments have focused on the problem of information security for decades, rising dependence on digital data both for personal and corporate use has led to an increase in opportunities for cybercriminals to benefit from illegal access to that data. High-profile data-loss incidents at Honda, NASDAQ, Sony, Target, RSA Security, Lockheed Martin as well as warnings from several national governments about data security have heightened concerns in the private sector. An ongoing discussion in information security is the tension between the role of government to ensure the safety of its citizens versus the ability of the market to achieve efficient solutions on its own [4]. Recognizing that the risk posed by data loss is multifaceted, this study digs deeper into the relationship between data loss incidents and stock price impact by analyzing data breach announcements from the years 2000 to 2012 for publicly traded corporations listed on the New York stock and NASDAQ stock exchanges.

This article helps make sense of the appropriate role of government by checking to see if the markets are incentivizing good information security policies. This research builds on

other studies that have looked at the stock-price impact, but expands the data set used across market sectors, which will help confirm the validity of the previous research. In addition, this research looks for differences across various breach types to help provide guidance to decision makers on prioritizing information security investments.

Given corporate vulnerability to costly breaches, information security has moved “up the chain” with the establishment of C-level information security officer position in many firms. The creation of the CISO position reflects the reality that, in the words of a senior executive, “we are all IT companies” and there are significant risks associated with that reality [18].

Cybercriminals, attracted by low risk and high rewards, target information through a variety of means that range from taking advantage of software vulnerabilities to social engineering. Regardless of the attack vector, however, the outcome is the same: sensitive corporate and personal information end up in the hands of malicious actors. The recognition of cybercrime can be seen through the increasing popularity of insurance to transfer the risk [16] and the superior performance of information security stocks that have outperformed the market since 2011 [23].

A question of public policy: When should governments intervene?

The persistent threat of cybercrime and the various attack methods won't be new to the readers of this journal, but what might be new are the ways in which public policy can help address aspects of the data-breach problem. Before we dive into the analysis, let's first take a step back and consider the role of public policy. Jonathan Gruber's text, *Public Finance and Public Policy*, [10] outlines key questions that are relevant to the role of government in the economy:

1. When should government intervene in the economy?
2. How might the government intervene?

Generally, governments intervene in the economy for two reasons: to achieve efficiency (ensuring optimal production) or to achieve equity (ensuring a desired distribution of resources throughout the society). When markets are not achieving efficient outcomes, governments can step in to correct the failure. There are many potential causes of market failure, but here the focus is on one particular cause: imperfect information.

An important element of a competitive market is information flow. In order to have a truly competitive market, both the buyer and the seller must have information on anything that would impact their decision-making process. Researchers Roberds and Schreft describe the market for consumer information by describing a person's confidentiality as an economic good whose provision depends on two other goods:

1. The amount of personally identifiable information (PII) incorporated into that person's transactional identity

2. The level of security for this data or the degree of data integrity [20]

As more information about a consumer is included in his or her transactional identity, it becomes easier for payment processors to reduce account fraud. At the same time, however, increasing the amount of PII collected about consumers reduces their privacy and increases the impact if the data is misused. While consumers can be informed of the amount of PII incorporated into their transactional identity by reading the privacy statements, they cannot access information on security of their data.

How secure is my data?

While corporations in some sectors are required to outline anticipated uses for consumer data in privacy statements, there is no such requirement for disclosing the security measures that protect customer data. In 2003, California was the first to enact a data breach notification law. California Senate Bill 1386 requires notification if PII is "reasonably believed to have been acquired by an unauthorized person" [5]. Now almost every state has a similar law requiring consumer notification when PII has been lost or stolen. While this is a good start, the definition of what constitutes PII or what constitutes a breach vary widely from state to state and consumers don't know what is done to prevent future breaches. Whereas laws such as Sarbanes-Oxley require audits of financial records via third-party auditors and statements to the Securities and Exchange Commission, there is no consistent standard for information security.

The legislation and regulations defining information security standards have largely been sector specific:

 **ISSA** International

CONFERENCE SAVE THE DATE

FEATURING:*

800+ Attendees Expected
60 Sessions | 7 Tracks | CPEs
Up to 100 Exhibits
Career Counseling & Networking Center
Cyber Defense Center
International Awards
ISSA Party in the Sky
CISO Executive Forum

*Subject to change.



HYATT REGENCY | DALLAS, TEXAS **NOVEMBER 2-3, 2016**

Information Systems Security Association | www.issa.org | 866 349 5818 USA toll-free | +1 206 388 4584 International

- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires that certain healthcare-related information be secured.
- The 1999 Gramm-Leach-Bliley Act (GLBA) applies to the financial sector and requires financial institutions to develop an information security program.
- The 2002 Federal Trade Commission (FTC) Standards for Safeguarding Customer Information (Safeguards Rule) requires financial institutions under FTC jurisdiction to secure customer data.
- Federal Financial Institutions Examination Council (FFIEC) has a working group that monitors cybersecurity and provides tools to member organizations to assess their risk exposure [8].
- The 2002 Federal Information Security Management Act (FISMA) applies to government agencies and contractors and requires that an information security management strategy be set up consistent with NIST guidelines (NIST 800-53).
- Payment Card Industry Data Security Standard (PCI DSS) applies to organizations that handle credit cards by ensuring that merchants meet prescriptive security guidelines according to their transaction volume. Validation of compliance is performed annually, either by an external qualified security assessor or by self-assessment questionnaire.

A commonly cited market failure is that of information asymmetry, where one party to a transaction has much more information than the other. An information asymmetry currently exists between firms and between firms and consumers

regarding data breaches [13]. If a firm is breached but does not release the information to the public, the consumer is potentially damaged by identity theft. The piecemeal approach to regulating information security can leave certain sectors unregulated and, even for the regulated industries, consumers may not know what regulatory agency applies to a particular company without significant research. Furthermore, companies that are not covered by existing regulation may still hold corporate intellectual property or sensitive information on employees that should be secured to protect the company, the employee, and the competitiveness of our national economy. Enacting regulation that requires minimum standards with public notification of audits could raise awareness of information security and risk management across all sectors. In the words of Bruce Schneier, “Regulation—SOX, HIPAA, GLB, the credit-card industry’s PCI, the various disclosure laws, the European Data Protection Act, whatever—has been the best stick the industry has found to beat companies over the head with. And it works. Regulation forces companies to take security more seriously, and sells more products and services” [21].

The absence of publicly available security and breach information places investors at a disadvantage when it comes to assessing the risk position of a firm. Indeed, the absence of this information also affects anyone who is doing research into data breaches, including this author. Datalosddb.org, an organization affiliated with the Open Security Foundation that relied on volunteers to transcribe data breach announcements in order to maintain an open source database, stopped making their database available for download during the period this research was being conducted. Their website now refers to a private company called Risk Based Solutions that provides access to their data for a fee and provides some analysis of that data in periodic reports. If this information is not freely available for people who are looking for it, how can we expect consumers to make decisions based on it?

Does information matter?

In light of these potential challenges to the efficient functioning of the market, scholars from a variety of disciplines have begun to explore the impact of data on companies.

Subramani and Walden looked at the impact of e-commerce announcements on stock price [22]. Others have studied the impact of data-breach announcements on the stock price of corporations [9][2] and at the longer term financial performance of breached companies, finding negative impact in both cases [14]. Telang and Wattal found a 0.6% loss in the stock price of software vendors following a vulnerability report [24]. Including firm size along with the data-breach characteristics explains some of the cross-sectional variation in stock price [6]. Research has also taught us that the prevalence of cybercrime is based on an economic calculation of

ISSA International Web CONFERENCE


Don't Miss This Web Conference!

Breach Report Analysis SWOT or SWAT?

2-Hour Live Event: Tuesday, May 24, 2016

9 a.m. US-Pacific/ 12 p.m. US-Eastern/ 5 p.m. London

Once again, the new data breach reports are published. Are we, as security professionals, succeeding in protecting our assets? This session will review the latest breach reports, provide insight into current trends, and evaluate potential solutions.

Generously sponsored by  Symantec.

[REGISTER TODAY!](#)

For more information on this or other webinars:

[ISSA.org => Web Events => International Web Conferences](#)

¹ In the interest of full disclosure, I should say that I have not requested access to the data from Risk Based Solutions. It is entirely possible that they would provide the complete data set, but the point here is that the information should be public and easy to access.

availability of hacking skills relative to economic opportunity, and critically the attacker's selection of target is based on not only symbolic significance but also weakness in defense mechanisms [15]. Research has also shown that hackers are rational actors, and those who are more rational engage in preparation and reconnaissance, and their attacks are more successful than their more impulsive counterparts [3].

Now that we know that clear information is important in a market and that hackers are rational actors responding to the information available to them, we need to look to see if consumers and investors are responding to information on breaches. Previous research tells us that we should expect to see a small negative impact on stock price. This research significantly expands the sample size of data breaches and draws on a random sampling of data breaches for analysis rather than pre-selecting market sectors. Additionally, this study breaks up the data breaches into breach types, allowing us to examine if the market is punishing companies more or less depending on the nature of the breach.

Preparing for analysis

There are many ways in which a corporation can lose data and several classification schemata exist. Here we have adopted the classification schema developed by security experts Matthew Curtin and Lee Ayers [7], who split data breaches into three main categories:

- **Physical breaches:** There is a loss of physical control over the data. Physical losses are characterized by the loss of documents, computers, and media such as compact discs, tapes, and other drives.
- **Logical breaches:** There has been a failure of the information security management system. This is where the controls in place were exploited by employees (insider threat) or outsiders (hacker). These breaches occur due to “loop-

holes” in the security systems that are in place where the corporation's information security controls have failed.

- **Procedural breaches:** The corporation mishandled the data. These breaches are characterized by the loss of data through mailings, a.k.a. “snail mail,” publicly accessible information on the corporate website, or improper disposal of records.

We may expect investors to be more forgiving of a novel attack that causes a data breach over a breach caused by accidentally mailing PII out to customers.

Data breach incident data was downloaded from the data loss incident database at datalossdb.org.² The data included information on 5005 incidents that were narrowed down to 1023 incidents by eliminating incomplete records and those outside range of available stock-price information. The [datalossdb](http://datalossdb.org) data used a different breach classification schema than that used in this analysis, so the data was translated from the 25 category schema provided to the three breach category schema. Tables 1 and 2 show the final incident count in each category as well as the mapping between the [datalossdb](http://datalossdb.org) breach types and the types used in this analysis.

Data Breach Categories

Physical	388
Logical	499
Procedural	136

Table 1 – Re-Categorized incident counts

² [Datalossdb.org](http://datalossdb.org) previously provided a tool that allowed for the complete database to be downloaded as a csv file but this is no longer the case. The data for this study was downloaded without headers from <http://datalossdb.org/exports/dataloss.csv> on 2/26/2012. Similar data may be accessed through other sources such as Privacy Rights Clearing House.

When it comes to
cybersecurity,
being out of
the loop is a
dangerous
place.

Shared Knowledge.
Shared Security.



Your Membership
Will Provide You With:

- Peer-to-Peer Networking
- Continued Education & Training
- Career Development, Growth and Opportunities

Developing and Connecting Cybersecurity Leaders Globally



ISSA

Information Systems Security Association





www.issa.org

Breach Type Re-Categorization Key

datalossdb Breach Type	Curtin and Ayers Breach Type
Disposal Computer	Procedural
Disposal Document	Procedural
Disposal Drive	Procedural
Disposal Tape	Procedural
Lost Computer	Physical
Lost Document	Physical
Lost Drive	Physical
Lost Laptop	Physical
Lost Media	Physical
Lost Tape	Physical
Missing Laptop	Physical
Missing Media	Physical
Snail Mail	Physical
Stolen Computer	Physical
Stolen Document	Physical
Stolen Drive	Physical
Stolen Laptop	Physical
Stolen Media	Physical
Stolen Mobile	Physical
Stolen Tape	Physical
Virus	Logical
Web	Procedural
Email	Logical
Fraud/Social Engineering	Logical
Hack	Logical

Table 2 – Re-Categorization key

The stock-price and market-index data was collected from a commercial source called EODData.³ The end-of-day stock-price data was captured for all stocks traded on both the New York Stock Exchange (NYSE) and the NASDAQ exchange from January 1, 2000, through April 22, 2012. Table 3 summarizes the key variables used in this analysis along with their sources.

3 Due to licensing agreements, the author may not release the completed data used in this study as it includes pay-for-access data.

Critical Variables

Variable	Source
Incident Date	datalossdb
Breach Type	datalossdb
Number of Records Lost	datalossdb
Company	datalossdb
Ticker Symbol	EODData
Index	EODData
Stock Price Day 0	EODData
Stock Price Day -3	EODData
Stock Price Day +3	EODData
Index Price Day 0	EODData
Index Price Day -3	EODData
Index Price Day +3	EODData

Table 3 – Critical variables in the analysis

The analysis

This research looks for differences between the data-breach incidents as they are separated into different groupings. Several statistical tests were run to look for results with “statistical significance.” These tests look for differences in the data that are unlikely to be caused by chance.⁴ “Statistical significance” does not necessarily mean practical significance, which is why it is important to carefully consider the questions being asked to be sure the answers are actually useful. The data that we have allows us to ask several questions. In order to help inform the development of government regulation, we will assess the extent to which the market is self-regulating information security by asking the following questions:

- Do breached companies suffer a negative stock-price impact?
- Is the degree of the stock-price impact correlated with the number of records lost?
- Do more recent breaches show a greater stock-price impact?

Then we will try to guide information security investments by checking to see if there are differences across data-breach types by asking the following questions:

- Does the stock-price impact differ across breach types?
- Does the number of records lost differ across breach types?

4 This is quite a simplification and I recommend that those interested do some additional research, especially since data-driven decision making can be powerful and statistical tools are widely available (Microsoft Excel Analysis ToolPak, the open source R software). A free textbook can be found here: <https://www.openintro.org/stat/textbook.php> or the following courses can introduce you to the basics: <https://www.coursera.org/course/stats1>; <https://www.khanacademy.org/math/probability>.

Finally, considering the growing awareness of security and the enactment of legislation and corporate policies to address the problem, we will ask:

- Is the number of records lost dropping over time?

The data-breach incident data, combined with the stock-price data, was loaded into an SQL database. A random sample was taken from each breach type for analysis and the stock-price impact was calculated using the following equations:

$$\% \text{ Stock Price Change} = \left(\frac{\text{Stock Price } t_0}{\text{Stock Price } t_1} * 100 \right) - 100$$

$$\% \text{ Index Price Change} = \left(\frac{\text{Index Price } t_0}{\text{Index Price } t_1} * 100 \right) - 100$$

$$\text{Stock Price Impact} = \frac{\% \text{ Stock Price Change} - \% \text{ Index Price Change}}{|\% \text{ Index Price Change}|}$$

Negative stock-price impact but breach size doesn't matter?

Do breached companies suffer a negative stock-price impact?

Yes, a stock-price impact of -0.65% was found.

Is the degree of the stock-price impact correlated with the number of records lost?

No correlation was found.

Do more recent breaches show a greater stock-price impact?

Unclear, a statistically significant difference was detected between the time periods, but the trend is inconsistent.

This analysis shows that there is a statistically significant difference between the mean index-price change and the mean stock-price change in the data set. This difference is consistent with previous research; however, it is small at -0.65% and differs from the sometimes cataclysmic calls that a data breach will crash the stock of a company. To be sure, there are significant costs associated with a breach including notification and identity-protection provision, but the drastic stock-price drop isn't apparent in the data.

From the perspective of aligning market punishment with loss of public information, it is troubling that no correlation was found between stock-price impact and the number of records lost. This indicates that the market is not aware of or simply not responding to differing scales of information loss. Additionally, while the data is unclear, the stock-price impact shown over the three time periods (table 4) is trending in the wrong direction if you expect consumers to be punishing companies that suffer breaches. There is some evidence to suggest that consumers are tiring of breach announcements and not changing their behavior after a breach as they accept it as a cost of doing business [1]. This data may be a reflection of that trend.

Stock-Price Impact Over Time

Time Period	Mean Impact
July 5, 2001 - December 31, 2006	0.35%
January 1, 2007 - December 31, 2008	-1.88%
January 1, 2009 - January 26, 2012	0.22%

Table 4 – Mean stock-price impact over time

Breach types matter and lost records per incident may be down

Does the stock-price impact differ across breach types?

Yes, a statistically significant difference was found between the logical breach type and the procedural breach type with mean impacts of -2.32% and 0.728% respectively.

Does the number of records lost differs across breach types?

Yes, a statistically significant difference in the number of records lost was found between the physical and procedural breach categories. The complete results are shown in the tables.

Is the number of records lost per incident dropping over time?

No, the data was split into three date ranges, and the analysis did not show a statistically significant difference between the three ranges.

The significant stock-price impact found between the logical and procedural breach types with respective means of -2.32% and .728% remind us that there is noise in the data caused by other factors influencing stock price (since it would seem strange that a data breach of any type may result in a bump in stock price). The negative impact as a result of the logical breaches may be an indication that the market is becoming aware of the need for robust information security management systems and is punishing companies that implement those systems poorly.

This awareness of the logical breaches may be due to the significant number of records lost due to this type of breach. While the statistically significant difference was found between the physical and procedural breaches, the logical breaches show a mean loss of 6.4 million records per incident. As mentioned above, the lack of statistical significance between the logical and other breaches means that we can't rule out these results being chance, but applying professional judgment, we know major losses are possible.

Records Lost Across Breach Types

Breach Type	Mean Records Lost
Physical	449,294
Logical	6,411,905
Procedural	96,660

Table 5 – Records lost across breach types

When considering public and corporate investments to limit the amount of information being lost, this analysis provides direction. The logical breaches may be a good place to start to limit the magnitude of the loss. Secondly, this analysis shows that physical data breaches result in significantly more records being lost at a mean of 449,294 records per incident, whereas procedural breaches result in a mean of 96,660 records lost per incident.

This analysis has shown that the market does respond to data-breach announcements although the impact is small.

With an increasingly mobile workforce it may be difficult to legislate that companies stop losing physical assets to theft or loss, but there may be an opportunity to mitigate the risk of record loss by limiting the number of records kept on mobile hardware. Finally, the analysis of records lost over time shows that the controls put in place over the past decade to control information loss

may be having an impact. The mean number of records lost per incident has dropped from 2.4 million to 173,000 (table 6). If this drop makes you suspicious, it should. The difference isn't statistically significant, which may mean that the drop is a result of chance. Further analysis with updated information may result in a better understanding of the drop over time.

Records Lost Over Time

Time Period	Mean Records Lost
July 5, 2001 - December 31, 2006	2,427,383
January 1, 2007 - December 31, 2009	2,509,727
January 1, 2010 - January 26, 2012	172,938

Table 6 – Records lost over time

Conclusion and a call to action

Considering that the data-breach notification laws are now in place in almost every state and data-breach announcements are becoming daily events, this study might yield different results if repeated. Some reports indicate that the year 2015 set a record for the number of data-breach reports, which could be an indication that the notification laws are working to add information to the market [19].

We discussed the importance of clear and available information if the market is to self-regulate and the potential for the government to help fill the gaps if necessary. This analysis has shown that the market does respond to data breach announcements although the impact is small. Government efforts to enact data-breach notification legislation has taken a step toward leveling the information asymmetry between consumers and companies because some information on breaches is now available, but more needs to be done because we have seen that the market isn't responding to breaches based on the records lost. We have also seen that there would

be a benefit to repeating this type of research with updated information to measure the effectiveness of data-breach announcement laws or the impact of security-awareness efforts. The challenge, however, is that there is no publicly available, standardized database of data-breach incidents, nor do consumers have a measure of the security of their data.

As professionals who could benefit from impartial analyses and from the exchange of accurate information regarding data breaches, we should be pushing:

- Major industry players or government bodies to fund the creation of an accepted clearinghouse of breach information along the lines of the Common Vulnerabilities and Exposures database [17] that can be accessed by any interested party and is consistently available and free of charge. This would allow for consistent impartial analysis from a variety of fields that can continue to guide our internal investments in security. This data source should also be made readable for the general public so they can become informed about risks to their personal information [11].
- Normalization of state level data breach notification regulations so that companies can spend more time addressing the core security concerns and less time navigating the various compliance regimes that they face from state to state while maintaining a “high bar” for protection [12]. This normalization should include standardizing the definition of PII, notification triggers, notification time frames, and may also require notification when vectors for access to PII such as stolen online credentials are compromised. These credentials may be reused across accounts and compromise can “result in access to all, including banking and other supposedly secure accounts” [11].
- Development of a forum to discussion what security audits (along the lines of the financial audits required for publicly traded companies) might consist of. These audits would provide information to consumers and business partners on the maturity of the information security management strategies in place and would allow for companies to choose business partners who don't increase their risk exposure. Finally, these audits would allow investors to accurately place information security risk alongside other risks as they make their investment decisions.

All of these measures would help ensure consistent and available information is available in the marketplace, which will help regulators, investors, and information security professionals monitor the success and impact of information security investments.

Bibliography

1. Anand, P. (2016, April 14). *Market Watch*. Retrieved from “Are Americans over data breaches?” – <http://www.marketwatch.com/story/are-americans-over-data-breaches-2016-04-14>.
2. Arcuri, M. C., Brogi, M., and Gandolfi, G. (2014, April 08). “The Effect of Information Security Breaches on Stock Returns: Is the Cybercrime a Threat to Firms?”

- Retrieved from European Financial Management Association – http://www.efmaefm.org/0EFMAMEETINGS/EFMA ANNUAL MEETINGS/2014-Rome/papers/EFMA2014_0408_fullpaper.pdf.
3. Bachmann, M. (2010). “The Risk Propensity and Rationality of Computer Hackers,” *International Journal of Cyber Criminology*.
 4. Brennan, J. (2012, April 12). “Cybersecurity Bills Compete for Attention”. (T. Gjeltnan, Interviewer) National Public Radio. 88.5 KPLU, Seattle. Retrieved from <http://www.npr.org/2012/04/16/150745384/cybersecurity-bills-compete-for-attention>.
 5. California State Legislature. (2002, September 26). Senate Bill No. 1386. Retrieved from California State Legislature – http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf.
 6. Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004). “The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reactions for Breached Firms and Internet Security Developers,” *International Journal of Electronic Commerce*, 69-104.
 7. Curtin, M., and Ayers, L. T. (2009). “Using Science to Combat Data Loss: Analyzing Breaches by Type and Industry,” *A Journal of Law & Policy for the Information Society*. Retrieved from <http://web.interhack.com/publications/interhack-breach-taxonomy.pdf>.
 8. Federal Deposit Insurance Corporation. (2015, Winter). *Supervisory Insights*. Retrieved from Federal Deposit Insurance Corporation – https://www.fdic.gov/regulations/examinations/supervisory/insights/siwin15/SI_Winter2015.pdf.
 9. Goel, S., and Shawky, H. (2009). “Estimating the Market Impact of security Breach Announcements on Firm Values,” *Information and Management*.
 10. Gruber, J. (2011). *Public Finance and Public Policy*. New York: Worth Publishers.
 11. Harris, K. D. (2013, July 1). “Data Breach Report 2012.” Retrieved from State of California Department of Justice Office of the Attorney General – http://oag.ca.gov/system/files/attachments/press_releases/BREACH REPORT 2012.pdf?
 12. Harris, K. D. (2016, February). “California Data Breach Report.” Retrieved from State of California Department of Justice Office of the Attorney General – <https://oag.ca.gov/breachreport2016>.
 13. Kannan, K., Rees, J., and Sridhar, S. (2007). “Market Reactions to Information Security Breach Announcements: An Empirical Analysis,” *International Journal of Electronic Commerce*, 69-91.
 14. Ko, M., and Dorantes, C. (2006). “The Impact of Information Security Breaches on Financial Performance of the Breached Firms: An Empirical Investigation,” *Journal of Information Technology Management*, 17(2), 13-22. Retrieved from <http://jitm.ubalt.edu/XVII-2/article2.pdf>.
 15. Kshetri, N. (2005). “Pattern of Global Cyber War and Crime: A conceptual Framework,” *Journal of International Management*, 541-562.
 16. Mello Jr., J. P. (2016, April 21). “Insurance Industry Buzzes over Data Breach Ruling.” Retrieved from Tech News World – <http://www.technewsworld.com/story/83403.html>.
 17. MITRE. (2016, April 26). “CVE List Master Copy.” Retrieved from Common Vulnerabilities and Exposures – <https://cve.mitre.org/cve/cve.html>.
 18. Pierson, C. (2011). SecureWorld conference lunch keynote.
 19. Risk-Based Security. (2016, April). “2015 Reported Data Breaches Surpasses All Previous Years.” Retrieved from Risk-Based Security – <https://www.riskbasedsecurity.com/2016/02/2015-reported-data-breaches-surpasses-all-previous-years/>.
 20. Roberds, W., and Schreft, S. L. (2009). “Data Security, Privacy, and identity Theft: The Economics behind the Policy Debates,” *Economic Perspectives*, 33(1), page 26. Retrieved April 28, 2012, from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1341223.
 21. Schneier, B. (2008, January 15). “Bruce Schneier Reflects on a Decade of Security Trends.” Retrieved from Schneier on Security – https://www.schneier.com/news/archives/2008/01/bruce_schneier_refle.html.
 22. Subramani, M., and Walden, E. (2001). “The Impact of e-Commerce Announcements on the Market Value of Firms,” *Information System Research*, 135-154.
 23. Taylor, H. (2016, April 19). “Huge Data Breaches Have Been Good for security Stocks.” Retrieved from CNBC – <http://www.cnbc.com/2016/04/19/huge-data-breaches-have-been-good-for-security-stocks.html>.
 24. Telang, R., and Wattal, S. (n.d.). “Impact of Software Vulnerability Announcements on the Market Value of Software Vendors - an Empirical Investigation.” Retrieved from Information Security Economics Page – http://infosecnet.net/workshop/pdf/telang_wattal.pdf.

About the Author

Kristopher Dane, Associate at the international engineering firm Thornton Tomasetti, Inc., is a graduate of the University of Washington (UW) Master of Arts in Policy Studies program and a graduate of the Information Assurance and Risk Management Certificate Program at University of Washington. Kris holds certifications from the Department of Defense Committee on National Security Systems and is a member of the Evergreen State chapter of Infragard. He previously spent nine years as a Technical Program Manager before joining Thornton Tomasetti, where he brings his analytical, programming, and modeling skills to serve their Structural and Protective Design Practices. Kris may be reached at kristopherdane@gmail.com.



FedRAMP's Database Scanning Requirement: The Letter and Spirit

By Matt Wilgus – ISSA member, Raleigh Chapter



Many cloud service providers are not fully addressing the database scanning requirements for FedRAMP and have questions related to database security and FedRAMP. This article details the issues associated with not meeting the database scanning requirement, the most common reasons why this occurs, what can be done to improve this, and what to consider with database security beyond scanning.

In early 2011, the federal government published a cloud computing strategy, which has become known as the Cloud First policy due to a focus on evaluating cloud offerings before making new capital investments. The goal in this effort is to reduce inefficiencies in the government's use of information technology (IT).¹ This document was an initial catalyst for government adoption of cloud services, which although slow has been increasing. Cloud service providers (CSPs), which historically focused on private-sector clients, began tailoring services for government agencies. This document also mentions the involvement of the Federal Risk and Authorization Management Program (FedRAMP) to provide a standard, centralized approach to assessing and authorizing cloud computing services and products. While FedRAMP actually began in 2010, the Cloud First policy, along with subsequent memorandums, raised awareness of the program.

As FedRAMP has matured over the past five years, more CSPs and government agencies are participating. While changes have and continue to occur within FedRAMP, the first step in the FedRAMP process has remained a security assessment by a third-party assessment organization (3PAO) against a baseline set of requirements from the National Institute of Standards and Technology (NIST) 800-53 publication that covers security and privacy controls for federal information systems and organizations.²

During the planning phase of a FedRAMP assessment there are many security topics a CSP and 3PAO should explore. One of the questions a 3PAO will ask of the CSP is how vulnerability scanning is being conducted. Before beginning the assessment phase, a 3PAO may ask the CSP for the most recent scanning results or scanning results from the previous two months to understand remediation efforts. Most CSPs are able to generate some evidence and/or artifacts from a recent infrastructure or web application scan, albeit sometimes unauthenticated, but many do not have any evidence related to database scanning. This is problematic for the CSP from a compliance and a security perspective. The compliance impact is immediately identifiable as the CSP is missing a core FedRAMP requirement. However, the security implication of not assessing the repositories where the data is stored is also a concern.

The main difficulties with database scanning

The published FedRAMP guidance provides specific details relating to the types of scans to be conducted (infrastructure, web application, and database), the frequency (monthly) and style (authenticated)³; however, there is no guidance on acceptable tools, policies, or approaches. Much of the interpretation falls onto the CSP and 3PAO, and there are a variety of interpretations of the database scanning requirements by each of them. Unfortunately, many CSPs fall short of meeting

1 Vivek Kundra, Federal Cloud Computing Strategy, US Chief Information Officer, February 8, 2011 – https://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/federal-cloud-computing-strategy.pdf.

2 FedRAMP Program Overview, FedRAMP.org – <https://www.fedramp.gov/about-us/about/>.

3 FedRAMP JAB P-ATO Vulnerability Scan Requirements Guide, Version 1.0, May 27, 2015 – <https://www.fedramp.gov/files/2015/01/FedRAMP-JAB-P-ATO-Vulnerability-Scan-Requirements-Guide-v1-0.pdf>.

the requirements, either from not conducting the scans at all, or because the controls in place to meet the database scanning requirement are not adequate. Based on historical projects, questions received from CSPs, and discussions with joint authorization board (JAB) members and individual agencies, we have identified five primary reasons CSPs are struggling with database scanning.

Comprehending the need for database scanning

As simple as it seems, there is frequently a disconnect between what an agency (and the FedRAMP requirements) intend to see with database scanning and what a CSP performs. Frequently, CSPs consider scanning databases to be an easy task as the database server is a part of the existing infrastructure and should be covered in the infrastructure scans. The disconnect is in what the database scan is supposed to detect. The typical authenticated infrastructure scan will detect vulnerabilities in databases related to missing patches or releases. However, the credentials used in an infrastructure scan likely will not be able to assess security at the database level. Some examples include authentication settings, authorization and privileges management, and logging and monitoring settings. An infrastructure scan of a MongoDB may come back clean, particularly since there are only 11 Common Vulnerabilities and Exposures (CVE) Identifier Numbers in the NIST National Vulnerability Database (NVD).⁴ However, the infrastructure scan will likely not detect that a MongoDB instance does not require authentication, which was identified as a prevalent configuration within NoSQL databases on the Internet in July 2015 through various Shodan searches.⁵

A common complaint from CSPs is that this type of information relates to baseline configurations and should be categorized as policy compliance rather than vulnerability scanning. This is understandable since most vulnerability scanning vendors categorize these types of checks as compliance checks as opposed to vulnerabilities. However, information relating to database accounts, group membership, requiring authentication to access the database and other items, which is often identified in policy checks, is exactly what an agency wants to know from a database scan. In 2004, NIST started the Software Assurance Metrics and Tool Evaluation (SAMATE) project to establish a methodology for evaluating software assurance tools.⁶ While the site hasn't been updated much in recent years, the project is live and the site does provide a list of twenty or so typical checks expected in database scanners.

Understanding what is a database

Another concept that hasn't been as easy as it seems is explaining what defines a database, since a logical argument would

be if it isn't a database, it doesn't need a database scan. The question on what is a database came to the forefront when organizations started storing data in containers that would not typically be labeled as a database. Examples include Amazon Web Services (AWS) Simple Storage Service (S3), Microsoft Azure's Blob Storage, and folders at other cloud storage providers, such as Box. A CSP's application can read and write to these systems just like a traditional database. However, these systems don't fit the image of what a database has been historically considered. As such, the question that arises is what is a database? The semantics of the term *database* can vary and may bring about discussions about data models, implementations, etc. When asked "What is a Database?" most IT professionals will mention something related to a backend repository holding data. *Webster's Dictionary* has a simple non-technical definition that is "a collection of data that is organized especially to be used by a computer."⁷ The question of what needs to be scanned varies and during considerations on whether a system should be scanned; the question of how to scan it quickly arises.

Tools do not support database platforms in use

The tool sets for infrastructure scans are well known, as are web application scanners. Conversely, many CSPs do not know what tool to use for database scanning, and one frequent comment from CSPs is that there is no tool available that can scan the platform in use. The original database scanning tools only needed to support a few types of databases, typically relational databases such as Microsoft SQL (MSSQL), Oracle, or MySQL. However, in the past five years the rise of distributed storage (e.g., Hadoop) and the use of NoSQL databases, such as Cassandra, Dynamo, MongoDB and others, has greatly increased. Support for newer database types is growing, but it is slow. With the explosion of different database options, many of which have existed for only short time, it is very difficult for vendors to support all types. Occasionally, open source scripts may exist, but after the initial development support can quickly wane for open source solutions. For example, a script may be available for MongoDB 2.6, but not MongoDB 3.2.

One complaint heard from CSPs is that there are a few commercial-off-the-shelf tools specifically targeted at databases, but these tools typically support relational databases and are expensive. Licensing is often based on the number of database instances, which may easily get into the hundreds in a cloud environment.

Choosing the right policy

For databases that are supported by tools, there may be more than one policy available for use by the scanner. The Center for Internet Security (CIS) publishes benchmarks⁸ that are often used by CSPs, especially those using MySQL. However, many CSPs do not know the difference between the

4 National Vulnerability Database: search MongoDB - <https://web.nvd.nist.gov/view/vuln/search-results?query=MongoDB>.

5 John Matherly, "It's the Data, Stupid!" [blog.shodan.io -https://blog.shodan.io/its-the-data-stupid/](https://blog.shodan.io/its-the-data-stupid/).

6 NIST, Database Scanning Tools - https://samate.nist.gov/index.php/Database_Scanning_Tools.html; NIST, "About SAMATE" - https://samate.nist.gov/index.php/SAMATE_About.html.

7 Merriam-Webster - <http://www.merriam-webster.com/dictionary/database>.

8 Center for Internet Security - <http://benchmarks.cisecurity.org/downloads/benchmarks/index.cfm>.

audit levels. A Level 1 audit is not as stringent as a Level 2, but settings required in a Level 2 audit may impact performance. Additionally, when the benchmarks are used without any alteration, there are usually some false positives as the benchmarks do not take into considerations different implementations or environments. For example, a CSP may have very robust logging and monitoring in place, but fail a CIS benchmark check because the error log is in a different location from what is commonly expected.

Ensuring all databases are scanned

Even CSPs with a mature database scanning program may not be scanning all databases that are within the boundary. This differs from considering "What is a Database?" The backend repository for a software-as-a-service (SaaS) provider's flagship offering may be getting scanned with credentials on a monthly basis, but what about the databases in the ancillary and support systems? A compromise to one of these systems could jeopardize the security of the cloud environment. The aforementioned difficulties relating to tool selection, support, and policy selection arise when the database in use by the other systems is different than the database for the flagship offering.

Alternative considerations

The aforementioned challenges can be difficult to address, but typically they are not insurmountable. One strength CSPs often have in place is a knowledgeable development staff. If a tool or script doesn't exist, there is often a willingness to write one. Compensating controls may also exist that may provide a similar benefit to scanning, especially for databases that do not have available options. One example is a combination of a strong inventory management process and database monitoring tools. A CSP may be able to walk through the database

security configuration in a primary build, show how Puppet, Chef, or other inventory, configuration, or orchestration tools manage the image, and then use database monitoring tools to ensure unintended changes are not conducted. Database monitoring tools do not scan the database, but rather sit in front of the database and analyze the traffic being transmitted. If a modification to a user or logging table can be detected by the monitoring tools, the need to scan for that exact setting may not be needed. While FedRAMP calls out database scanning, a better description for the requirement may be a monthly comprehensive database reviews (which could be supported or conducted by scanning).

Holistically planning for database security

While the results of the database scan are one component of ensuring data is maintained securely, there are a number of other controls that will include the database environment. Having the following thoroughly documented in the system security plan (SSP), procedures, and other system documentation will help ensure the database environment is well understood and can save time during a FedRAMP assessment. The parentheses identify some FedRAMP controls where the database implementations can be addressed in the SSP.⁹

1. **Database Version** – What database platform is in use and what version? Document the current version and the road map for the future. (Inventory)
2. **Database Administrators** – Who should have access to all databases? This should be a short list of users. All other accounts should have a documented justification. (AC-2, AC-5)

⁹ FedRAMP System Security Plan (Template) – <https://www.fedramp.gov/files/2015/03/FedRAMP-System-Security-Plan-Template-v2.1.docx>.

ISSA International Web CONFERENCE

The Sky Is Falling... CVE-2016-9999^(mth)?

2-Hour Event Recorded Live: April 26, 2016

Security Software Supply Chain: Is What You See What You Get?

2-Hour Event Recorded Live: March 22, 2016

Mobile App Security (Angry Birds Hacked My Phone)

2-Hour Event Recorded Live: February 23, 2016

2015 Security Review & Predictions for 2016

2-Hour Event Recorded Live: January 26, 2016

Forensics: Tracking the Hacker

2-Hour Event Recorded Live: November 17, 2015

Big Data—Trust and Reputation, Privacy—Cyberthreat Intel

2-Hour Event Recorded Live: Tuesday, October 27, 2015

Click here for On-Demand Conferences

www.issa.org/?OnDemandWebConf

Security of IOT—One and One Makes Zero

2-Hour Event Recorded Live: Tuesday, September, 22, 2015

Biometrics & Identity Technology Status Review

2-Hour Event Recorded Live: Tuesday, August 25, 2015

Network Security Testing – Are There Really Different Types of Testing?

2-Hour Event Recorded Live: Tuesday, July 28, 2015

Cybersecurity Outlook: Legislative, Regulatory and Policy Landscapes

2-Hour Event Recorded Live: Tuesday, June 23, 2015

Breach Report: How Do You Utilize It?

2-Hour Event Recorded Live: Tuesday, May 26, 2015

Open Software and Trust—Better Than Free?

2-Hour Event Recorded Live: Tuesday, April 28, 2015

A Wealth of Resources for the Information Security Professional – www.ISSA.org

Database Platform	URL
Amazon DynamoDB	http://docs.aws.amazon.com/amazondynamodb/latest/developerguide/OtherServices.html
Amazon S3	https://aws.amazon.com/s3/faqs/#security
Apache Cassandra	http://docs.datastax.com/en/cassandra/3.0/cassandra/configuration/secureTOC.html
Apache Hadoop	https://hadoop.apache.org/docs/current/hadoop-project-dist/hadoop-common/SecureMode.html
Box	https://community.box.com/t5/For-Admins/Best-Practice-Choosing-Security-Settings/ta-p/3108
Microsoft Azure Blob Storage	https://azure.microsoft.com/en-us/documentation/articles/storage-manage-access-to-resources/
Microsoft SQL	https://msdn.microsoft.com/en-us/library/bb283235.aspx
MongoDB	https://docs.mongodb.org/manual/security/ https://docs.mongodb.org/manual/administration/security-checklist/
MySQL	http://dev.mysql.com/doc/mysql/en/security.html
Oracle	http://docs.oracle.com/database/121/ASOAG/toc.htm

Table 1 – Security pages for various database and storage platforms

3. **System Accounts** – What applications have system or machine accounts on the database? These applications should have a documented justification. (AC-2)
4. **Authentication** – How do users access the databases (e.g., two-factor, local authentication, etc.)? Ensure system accounts follow the same process of authentication. (IA-2)
5. **Authorization** – What privileges and/or roles are granted to database users? Ensure the implementation of role-based access control matches the design. (AC-2, AC-5)
6. **Periodic Review** – Are user accounts reviewed regularly for employees or applications that no longer require access? (AC-2)
7. **Encryption** – What is used to secure data in transport and at rest? The data should be encrypted using a module that is FIPS 140-2 validated. (SC-8, SC-13, SC-28)
8. **Virtual Local Area Networks (VLANs)** – What identifier is used to categorize databases? Note how databases are segmented from the other parts of the environment. (SC-7)
9. **Access Control Lists (ACLs)** – What rules are in place to protect the database environment? If there are specific ACLs supporting and securing the databases, have those extracted or know what strings to search for easy review. (AC-3, SC-7)
10. **Logging** – Are local settings used, or does logging occur via other means? Confirm that the logging enabled would support an investigation should a breach occur. (AU-2)
11. **Configuration Baseline and Settings** – How are the configuration baseline and settings reviewed and how often? There should be a documented process for the build and the periodic review. (CM-2, CM-6)

Beyond FedRAMP

While much of the content presented is directly related to FedRAMP, the challenges and concepts likely exist in many

organizations, regardless of compliance requirements. Databases are often thought of as relatively static pieces of the environment, but there can be a lot of moving pieces to secure them. With a general understanding of database security, some forethought on the potential compliance issues, and a willingness to consider the spirit of the requirement in addition to what has been written, an organization can improve the security around one of its most important assets, its customer's data.

Table 1 provides a list of the URLs for the security page of the platforms mentioned.

About the Author

Matt Wilgus is a Practice Director at Schellman & Company, Inc. Matt leads the security testing and assessment offerings. In this role he heads the delivery of Schellman's penetration testing services related to 3PAO and PCI assessments, as well as other regulatory and compliance programs. Matt has over 15 years of experience in information security, with a focus on identifying, exploiting, and remediating vulnerabilities, in addition to extensive experience enhancing client security programs while effectively meeting compliance requirements. He may be reached at matt.wilgus@schellmanco.com.



Easy and Convenient!

www.issa.org/store

Computer Bags • Short-Sleeve Shirt • Long-Sleeve Shirt • Padfolio • Travel Mug • Baseball Cap • Fleece Blanket • Proud Member Ribbon • Sticky Note Pads

Smart Practices in Managing an Identity-Auditing Project

By Kerry Anderson – ISSA member, New England Chapter



Implementing an identity-management audit solution can be a milestone in the maturation of an information security program. This article discusses best practices to ensure the development and delivery of a successful access-audit program.

Abstract

Implementing an identity-management audit solution can be a milestone in the maturation of an information security program because it signifies a move away from a *reactive* to a *proactive* posture. The project can be expensive, but its benefits are vast. This article discusses best practices to ensure the delivery of a successful access-audit program that can blaze a trail for other identity management projects, such as the implementation of RBAC (role-based access control) or automatic provisioning. These methods include how to corral the necessary cooperation and resources and develop a strategy to manage them effectively.

Periodic identity-management audits provide a mechanism for verifying individuals possess the appropriate access to computer systems, as well as physical locations. It is an essential component to starting and maintaining a role-based access control (RBAC) program.¹ Also, some compliance regulations compel recurring audits of access to computers and other logical assets. On the surface, the basics of conducting identity-management audits seem straightforward, but like many things the devil is in the details.

Why is identity-management auditing tough

The primary challenge in instituting an effective identity-management auditing program is the creation of a centralized repository of all access-related data.² This can be

especially true in IT infrastructures possessing any of the following attributes:

- Legacy applications and applications utilizing multiple operating platforms³
- Purchased third-party applications
- IT organizations that developed in silos with each development team using its access control methodologies
- Application portfolios that grew through numerous acquisitions or mergers of other enterprises over the years
- Decentralized access administration teams

Trying to coordinate appropriate and consistent data under any of these circumstances can be an experience analogous to herding cats. However, it is possible to overcome any impediments by identifying them in advance and developing a strategy to manage them effectively.

Engage a strong project leader

The selection of a project leader can make or break an identity-auditing project. The project leader needs to have sufficient experience managing large IT initiatives to overcome any obstacles and resistance encountered along the way. An internal candidate may be preferable because she is familiar with the organizational culture, political environment, and internal hierarchy. An external candidate will need time to gain this understanding. Also, an existing staff member might have an existing relationship with some stakeholders. A project leader might utilize several possible strategies for managing this initiative. The selection of a project-management strategy is

1 Ferraiolo, D.; Kuhn, R. (1992) "Role-Based Access Controls," 15th National Computer Security Conference (1992), Baltimore MD – <http://csrc.nist.gov/rbac/ferraiolo-kuhn-92.pdf>.

2 Thuraisingham, B.; Iyer, S. (2007) "Extended RBAC-Based Design and Implementation for a Secure Data Warehouse," Second International Conference on Availability, Reliability and Security (ARES'07)

3 Bradbury, D. (2007) "How to Implement Role-Based Access Control" – <http://www.computerweekly.com/news/2240083532/How-to-implement-role-based-access-control>.

situational, depending on the organization and its leaders. Some good qualities that the leader needs to possess include:

- Flexible and innovative
- Proficiency in project-management techniques
- Sufficient technical background to provide credibility with IT staff
- Capable of dealing with a variety of personality types
- Strong communication skills
- Resilient enough to handle frustration and stress

Understand the access inventory

It is essential to perform a survey of the different categories and sources of access data to get a basic estimation of the scope of the effort. The appropriate approach to take to gather this information will vary depending on the following⁴:

- Existing documentation of access-data stores
- Centralized or decentralized access-administration function
- Number of applications
- Integration of access management using standard mechanisms, such as Active Directory (AD) or Light Weight Directory Access Protocol (LDAP)

Mature organizations may have a centralized inventory of applications, databases, operating platforms, and other access repositories. If a central access repository does not exist, it may be necessary to develop one in conjunction with IT. This situation might require the infosec function to assume leadership in the creation or updating of this access inventory. Based on an analysis of the access inventory, the project team can develop tactical approaches for each category of access and an overall strategy for the project. This first is necessary regardless of the overall scope of any identity-management project and final goal of the project, including:

- Identity-management auditing
- Implementation of RBAC (role-based access control)
- Automatic provisioning (on-boarding/ termination/transfers)

Determine the minimum data requirements from access systems

Before approaching application owners and technical managers in regards to obtaining access extracts, it is essential to determine the minimum requirements regarding data attributes needed to provide end users with sufficient information for the performance of access audits. Frequently, identity-auditing solutions offer a wide variety of access attributes that applications can feed into the central access repository, such as last login date/time and date of last access update. However, many applications, especially legacy or vendor applications, may not have the ability to provide some data

attributes. Therefore, it is important to distinguish those important access attributes necessary to perform access audits and certifications.

Usually, these attributes are limited to access identifier (account/user id), system identifier/name, unique user identifier such as employee or customer number, and access right or privilege identifier. Access-administration systems might include data attributes in an extract not available, such as last login date/time, in all legacy applications.

Decide on an overall strategy

While a myriad of strategies may be applied to an access-audit management system, they are usually variations of two basic approaches⁵:

1. The big bang rollout
2. Phased rollout

The big bang approach delivers a system and associated repository capable of processing, managing, and storing all access data during its initial roll out. This strategy means a longer start-up and development before implementation, as well as greater resource requirements up front. Longer project cycles

5 Jorgenson, P. (2014) "Big Bang vs. Phased Rollout: Which ERP Implementation Strategy Is Best?" - <http://it.toolbox.com/blogs/inside-erp/big-bang-vs-phased-rollout-which-erp-implementation-strategy-is-best-62060>.



CAREER CENTER

Looking to Begin or Advance Your Career?

The [ISSA Career Center](#) offers a listing of current job openings in the infosec, assurance, privacy, and risk fields. Visit the [Career Center](#) to look for a new opportunity, post your resume, or post an opening. Among the current 1,037 job listings you will find the following:

- **Security Analyst (Penetration Tester)** – Digital Defense, Inc., San Antonio, TX
- **Junior IA/Cybersecurity Analyst** – Wyle, Pt. Mugu, CA
- **Information Security Specialist** – Amalgamated Bank of Chicago, Chicago, IL
- **Information Security Technical Risk Analyst** – University of Minnesota, Minneapolis, MN
- **Information Security Analyst I/II/III** – MSA, The Safety Company, Cranberry Township, PA

Visit our [Career Center](#) online for a full listing of job openings! Questions? Email Monique dela Cruz at mdelacruz@issa.org

4 Ibid. Bradbury, D. (2007)

can make it challenging to maintain momentum with stakeholders. The primary advantage of the big bang rollout is that when it is successful, it is done and the team scores a big success. There are numerous disadvantages to this approach:

- The system does not get a comprehensive testing until after complete implementation, which can lead to performance and production issues
- Delays in obtaining access data can create delays in the project’s critical path
- If the rollout experiences problems, the project may be viewed as less than successful and suffer a loss of support from key stakeholders

The phased rollout offers several advantages, such as showing initial successes, allowing early resolutions of any operational and performance issues, and potentially spreading capital costs across multiple years. The possible drawbacks to the phased approach are a loss of momentum over time and a longer period before the full benefits of the system are realized.

The selection of overall approach is dependent upon the particular circumstances and environment of the organization. Sometimes, a hybrid approach may prove beneficial, such as a proof of concept pilot with a high-profile area, for instance, Virtual Private Networks (VPN)/ Remote Access or privileged access audits, followed by a big bang rollout for the remaining access systems.

Don’t let a specific IDM solution determine the direction of the effort

It is important to determine what the specific requirements for an identity-management project are prior to reviewing potential vendor solutions and the functionality they provide. According to Gartner’s Roberta Witty, “Any product that forces you to change your business processes is not one that you want to pick.”⁶ By getting a clear vision of the identity-management objectives that the organization needs to address, it will be easier to review potential vendor solutions to obtain the best fit for the organization’s needs by allowing the alternatives to be filtered⁷ for specific functionality.

Be realistic about the challenges

Every IT project ever conceived has faced some number of challenges along the way. Before embarking on any project as potentially transformational as an identity-auditing initia-

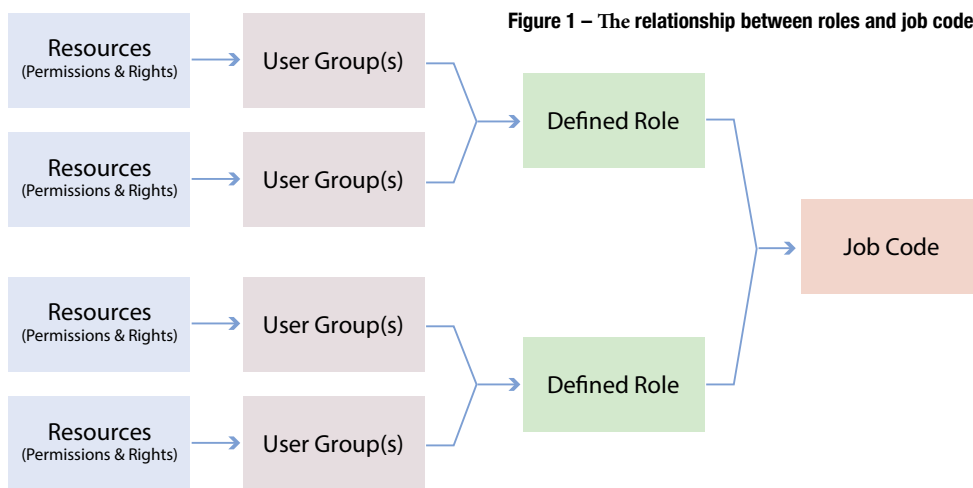


Figure 1 – The relationship between roles and job codes

tive, it is important to recognize possible obstacles to success and evasive tactics to circumvent the impact:

- The overall maturity of the organization and its infosec function
- Overall resistance to change
- Territorial behaviors in regards to sharing data
- Ability to associate a particular individual with an access account
- Overall state of the data
- Availability of budget and resources both for the project team and groups that will need to participate in the development and implementation

Get buy-in from stakeholders

A critical element in the ultimate success or failure of any business endeavor is acquiring the cooperation of stakeholders early in the process.⁸ Even if stakeholders give approval, it does not ensure their buy-in or rule out any potential indirect attempts to derail the project. Obtaining and maintaining stakeholder buy-in demands constant care and feeding throughout the life of the project. Care must be taken to incorporate activities that include active involvement such as solution design sessions that include representation from various stakeholder groups. This strategy will serve to build a sense of ownership in the final product by giving those using the solution a say in its architecture.

Be sure to include stakeholders in regular update meetings and celebrations of significant project milestones. Acknowledge the contributions of extended team members, such as end users and other development teams, in project communications vehicles like newsletters or briefings. Consider an internal social media site to keep all stakeholders informed of the various goings on of the project. The end goal of stakeholder-inclusion efforts is to make the final solution everyone’s “baby” rather than something forced on them.

6 Desmond, P. (2002) “Identity Management Tops” – <http://www.networkworld.com/article/2342277/access-control/identity-management-tips.html>.

7 “Top Identity Management Software Products (2016),” Capterra – <http://www.capterra.com/identity-management-software/>.

8 “9 Tips to Avoid Identity Management Implementation Pitfalls (2014),” Systems Alliance, Inc. – http://www.systemsalliance.com/who-we-are/insights/SAI_Blog/9-tips-to-avoid-identity-management-implementation-pitfalls.

Consider the needs of potential users

It is important to understand both uses and users for the identity-auditing function within the enterprise. Data presentation must enable users to perform their required tasks. Design decisions must incorporate the expected uses of the solution, as well as other potential value-added applications. This tactic means working with end users and managers to develop effective use cases that reflect the necessary tasks to be accomplished, as well as identifying ways to make them easier. One way to do this is soliciting involvement from a broad range of stakeholders in selecting a potential solution, such as representation from both IT and business organizations.⁹ One excellent way to do this is to shadow current end users performing critical identity-auditing activities to determine the work flow of the activities and capture any nuances in the performance of tasks.

Use job roles

Just dumping raw data from across the enterprise may not be an effective strategy for performing identity-access audits. There must be a clear distinction between data and usable information. Often the first step in identity-management audits is getting the necessary data into a centralized repository. Some access professionals think that merely having the data in a centralized repository is all that is needed to support identity auditing. However, the sheer volume and technical nature of raw data can make it difficult for users to interpret the data without extensive technical infrastructure knowledge. Raw data is often cryptic, using coding nomenclature developed for use by staff familiar with the use. To optimize the outcomes and make it easier for non-technical staff to utilize the data may require aggregating it into job codes that relate specific rights and privileges to a distinct task.¹⁰

Job codes (see figure 1) are an aggregation of the rights and privileges associated with specific job functions and user groups used to define these roles, such as customer service and help desk roles. A job code defines all the access required for a specific position in the organization. This activity is not trivial and requires the inclusion of subject matter experts from the security administration and business areas. However, the return on investment (ROI) in the long term is enormous. It is also a step toward role-based access (RBAC) for organizations planning a larger access-governance program. This effort can occur in parallel with activities required for the access-audit project.

Architect in extensibility and scalability

The number and types of access roles tend to expand over time. This situation is particularly true when you consider the inclusion of cloud-access identities and mobile apps.

9 Butler M (2011) "Extending Role Based Access Control," A SANS whitepaper - <https://www.sans.org/reading-room/whitepapers/analyst/extending-role-based-access-control-34975>.

10 Ferraiolo, D.; Kuhn, R. (1992) "Role-Based Access Controls," 15th National Computer Security Conference (1992), Baltimore MD - <http://csrc.nist.gov/rbac/ferraiolo-kuhn-92.pdf>.



ISSA Journal 2016 Calendar

Past Issues – click the download link: [↓](#)

JANUARY

↓ Securing the Cloud

FEBRUARY

↓ Big Data / Data Mining & Analytics

MARCH

↓ Mobile Apps

APRIL

↓ Malware Threat Evolution

MAY

Breach Reports – Compare/Contrast

JUNE

Legal, Privacy, Regulation

JULY

Social Media Impact

Editorial Deadline 5/22/16

AUGUST

Internet of Things

Editorial Deadline 6/22/16

SEPTEMBER

Payment Security

Editorial Deadline 7/22/16

OCTOBER

Cybersecurity Careers & Guidance

Editorial Deadline 8/22/16

NOVEMBER

Practical Application and Use of Cryptography

Editorial Deadline 9/22/16

DECEMBER

Security Architecture

Editorial Deadline 10/22/16

You are invited to share your expertise with the association and submit an article. Published authors are eligible for CPE credits.

For theme descriptions, visit www.issa.org/?CallforArticles.

EDITOR@ISSA.ORG • WWW.ISSA.ORG

When planning the architecture and infrastructure for any access-management system, the best advice is to “Think Big,” or at least build in a potential upgrade strategy. Two areas to take into account are storage capacity and performance. Access data tends to grow over time, sometimes exponentially, and the underlying database and storage architecture needs to be capable of supporting data growth. It is important to allocate sufficient processing capacity to handle feeds from the application systems. Additional data feeds may become difficult to process during the process cycle. This gating factor can be managed through capacity planning and architectural design.

Understand reporting requirements from the beginning

The importance of reporting may not get the appropriate amount of consideration during the initial design and development of the access-audit system. Provide a basic description of core reporting requirements, including full report descriptions. While it is often true that end users may not fully recognize every necessary report, they should be able to identify at least some categories of reporting and the necessary elements of those reports. Determining the types of reporting that will be required will allow the database architects to design a schema to support reporting requirements. There may also be a provision for a data warehouse.

Recruit an executive evangelist

Senior executive-level support can provide the project with visibility and communicate its significance to the organization. The power of this support should not be underestimated, especially when that backing comes from a C-level executive or the board of directors. Another strategy is to recruit an executive evangelist for the identity-auditing project. This individual can rally the troops when necessary, especially since identity-auditing project can dishearten the team and stakeholders due to long implementation cycles.

Be innovative and flexible in handling challenges

Every identity-auditing initiative follows its unique journey and encounters different challenges, such as legacy systems, inconsistent account-naming standards, or difficulties binding account access to specific individuals. The sheer quantity of access data can create issues around data loading, performance, and reporting. Resolving these concerns may require out-of-box thinking, flexibility, and innovative approaches. Encourage team learning that focuses on providing solutions through the development of an open approach to questioning. The team looks beyond the standard methods to work out innovative solutions by offering both ideas and solutions. While learning the team process may appear similar to brainstorming, it seeks to weed out unworkable strategies to avoid wasting resources on a dead end.

Be prepared for round two

The adage is “success breeds success.” A delivery of a successful access-audit program can heighten the appetite for the next logical follow on identity-management projects that build upon the foundation of the access-audit program, including¹¹:

- Implementation of RBAC (role-based access control)
- Automatic provisioning (on-boarding/termination/transfers)
- Single sign-on solutions

Conclusions – A pivotal step in the maturity process

Identity auditing or other identity-management projects are challenging, especially the earliest efforts in this area. First efforts often come upon a myriad of impediments that require resolution for the project to go forward, including:

- Discovery of all the potential access-data repositories
- Sheer volume of access data
- Incompatible and inconsistent account naming conventions
- Difficulties associating individuals with an access account
- Failure to remove dormant and terminated accounts

Resolving these thorny issues is necessary to assure the security of the organization in regards to identity-access management risks, and in many cases meeting access certification-compliance requirements. Identity-access management projects can be expensive and resource intensive to implement. However, the benefits are enormous in the diminishing of access-related risks, decreased security-administration costs, and overall effectiveness of the access-management function. Implementation of identity-management initiatives marks a pivotal milestone in the maturity progress of an information security organization because it signifies a movement away from a reactive to a proactive posture.

About the Author

Kerry A. Anderson, CISA, CISM, CRISC, CGEIT, CISSP, ISSMP, ISSAP, CSSLP, CFE, CCSK, MBA, MSCIS, MSIA, is an information security and records management professional with more than 18 years of experience in information security and IT across a variety of industries. Ms. Anderson has an MBA, MS in Computer Information Systems, and a Master’s in Information Assurance. Ms. Anderson is the author of The Frugal CISO: Using Innovation and Smart Approaches to Maximize Your Security Posture, published by CRC Press. She can be reached at kerry.ann.anderson@verizon.net.



¹¹ Musthaler, L. (2012) “Expert Advice on Implementing Role-Based Access Control (RBAC), Network World – <http://www.networkworld.com/article/2186904/infrastructure-management/expert-advice-on-implementing-role-based-access-control-rbac.html>.

On the Costs of Bitcoin Connectivity

By Ashish Gehani



Highly connected information technology systems typically have substantial economic value, making them attractive to resource-rich adversaries. Bitcoin is an example of such a system. The effect of high connectivity manifests in a number of orthogonal dimensions, each of which creates a different kind of security concern. We discuss each of them and possible mitigations.

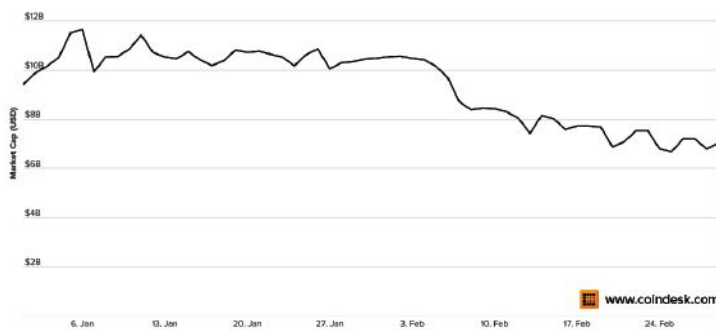


Figure 1 – Bitcoin market capitalization during the time frame when the largest exchange declared bankruptcy. Source: CoinDesk

Abstract

Highly connected information technology systems typically have substantial economic value. This makes them attractive to resource-rich adversaries, such as nation-states that may seek to exert an influence on particular participants or even the entire system. Bitcoin is an example of such a system. The effect of high connectivity manifests in a number of orthogonal dimensions, each of which creates a different kind of security concern. We discuss each of them and possible mitigations.

The cumulative value of existing Bitcoins crossed \$10 billion in November 2013 [3], as illustrated in figure 1. Bitcoin can be used at numerous vendors, ranging from 75,000 mainstream companies [14] to an online black market [22]. In February 2014, a Bitcoin exchange declared bankruptcy, claiming \$480 million in Bitcoin deposits had been stolen. While attacks by individuals have been studied both in academic literature and by software developers, the system's resilience to state-level adversaries has received less

scrutiny. We consider problems that can arise when significant resources are brought to bear on attacking the highly connected Bitcoin network.

Background

David Chaum proposed the idea of digital cash over three decades ago [6], back in 1982. It used novel cryptographic constructs to imbue electronic transactions with the anonymity of physical cash, to ensure that digital cash could only be created by banks [7], and to prevent individuals from spending the same digital cash more than once [8]. Over the years, thousands of academic papers have been written on the topic, and hundreds of startups have been created to translate the ideas into practice [13].

The use of digital cash remained limited to a small set of technology enthusiasts as recently as 2008. In October of that year, Satoshi Nakamoto proposed Bitcoin [18], the first digital-cash scheme that was completely decentralized. It supports anonymous users, has no central mint, and distributes the effort of preventing double spending. In the wake of the financial recession and uncertainty in global economies, Bitcoin has grown rapidly. The Bank of England estimates that over 40 million Bitcoin accounts have been created worldwide [14].

By early 2013, the size of the Bitcoin market had crossed \$1 billion [12]. Since late 2013, the size of the market has fluctuated in the range of \$3-14 billion [3]. Bitcoin is now an acceptable form of payment at more than 75,000 mainstream companies. It can be used to buy computers from Dell, book hotels through Expedia, and pay for service from Dish TV. The users are more mainstream as well, with only 22 percent professing to be anarchists in 2014, down from 42 percent in 2013 [14].

Goal

While financial transactions between banks are regulated and monitored, little oversight exists for pseudonymous digital-cash systems such as Bitcoin [16]. Academics and developers have studied the system's vulnerability in the face of malicious participants. However, the analyses typically assume that a majority of the participants are cooperative. Our study relaxes the assumption to examine risks that arise when significant adversaries are involved, such as large multi-national organizations or state-level actors. We consider attacks where adversaries are afforded large amounts of computation and storage, control over the significant portions of or locations in the communications networks, and enough funding to employ numerous skilled developers for extended periods.

Understanding the resilience and vulnerabilities of the highly connected Bitcoin system to large-scale attacks has at least three benefits:

- It enables us to understand what adversaries, ranging from criminals or terrorists to hostile nations, may be able to accomplish through extant Bitcoin infrastructure.
- It allows us to understand how government agencies can manage the system to enforce the law.
- It lets us prioritize the research needed to understand the complex dynamics that result from the interplay between the technical, economic, and legal aspects of the Bitcoin ecosystem.

Bitcoin basics

We now describe the essence of Bitcoin. This will allow us to explain the types of risks that result when adversaries are sufficiently powerful. Every participant is identified by a public key (and knowledge of the corresponding private key). When a participant wishes to make a payment, he signs and broadcasts a transaction. This points to past transactions through which the payer has received sufficient funds to make the payment, and lists the payer, the payment amount, one or more payees, and the amounts to be paid to each of them. The payment is only considered valid after it has been added to the public ledger, which is a chronological list of all the transactions that have occurred since the beginning of Bitcoin in early 2009.

Any participant can aggregate a number of transactions into a block, compute the hash of the catenation of the public ledger and the block, and then search for a hash preimage in a predefined range (which serves as a proof of work). The resulting block and proof are appended to the public ledger, which is referred to as a blockchain. This process is known as mining Bitcoins because the first participant to successfully add the block receives a fee, as well any differences between the payments made by payers and the total received by the payees.

Consequences of connectivity

We describe the implications of high connectivity for the Bitcoin network. These occur in multiple dimensions—communication, computational, privacy, and logical control—as we explain below.

Communication dependence

Bitcoin was designed to work in distributed environments, where network connectivity is not always reliable.

Consequently, when participants are disconnected from each other, they continue to operate with miners in each partition extending their blockchain. When connectivity is restored, the blockchain that took the most work to create is accepted by all participants. This introduces a vulnerability in the case that an adversary controls the network infrastructure.

The more obvious vulnerability occurs when data transmissions are interfered with. For example, the Chinese government's Golden Shield project (also known as the Great Firewall of China) supports IP blocking, DNS redirection, packet and URL filtering, and resetting connections [24]. This would allow it to selectively filter transactions from particular participants, preventing them from reaching miners who should incorporate them in the blockchain. The result would be that the victims would be unable to receive or send payments, effectively having their assets frozen.

The less apparent weakness manifests when control information in the network is manipulated. Bitcoin allows any host to join the network. In order to bootstrap its connectivity to the network, a new node connects to a seed set of hosts, asks them for lists of their neighbors, and can then recursively contact them to enlarge its set of lists. However, an adversary that controls the network infrastructure can manipulate the reachable set of hosts. This results in a less subtle weakness—the ability for the adversary to scope the set of neighbors of a victim, and thereby determine which transactions are forwarded.

The more subtle concern results from the ability of the adversary to shape the topology of the network. Bitcoin relies on random neighbor selection to yield a low-degree, low-diameter network for efficient propagation of information [10]. This is consistent with well-understood properties of expander graphs. By filtering bootstrapping messages, the adversary can alter the shape of the network connectivity graph, as illustrated in figure 2. While this has limited impact for small networks, this results in severe scaling challenges for large networks. In particular, it can result in high latency for information propagation [1], reducing the usability of the system. This is of particular concern to unstructured peer-to-peer networks, such as Bitcoin, which can only handle seven transactions per second on average. (In contrast, Visa typically processes 2,000 transactions per second [19].)

Trust aggregation

While highly connected systems contain many nodes that are online at any given point in time, they must accommo-

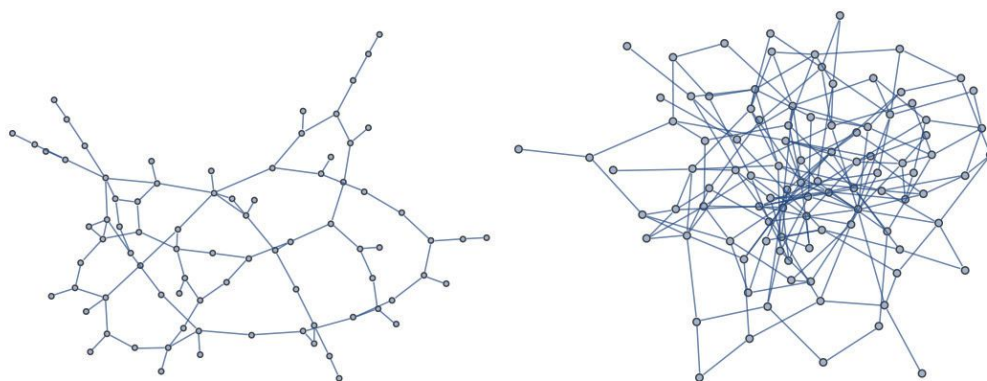


Figure 2 – Depictions of small Bitcoin networks, each constructed as a random graph. The second network contains about the same number of nodes as the first but with roughly double the number of links between neighbors. This results in lower susceptibility to node disconnection and shorter average diameter (and hence communication latency).

date nodes that may be temporarily unreachable. Often this results in trust being delegated to proxies that act on behalf of nodes, either in their absence or when the nodes themselves do not have sufficient resources (such as power, memory, or computation capability). However, over time trust starts to aggregate in a limited subset of the network, making the system vulnerable to targeted attacks.

In the context of Bitcoin this manifests in two forms. First, users may choose to use a wallet service where they authenticate to the service that then acts on their behalf. This is achieved via the user sharing his Bitcoin credentials with the wallet provider. Further aggregation of trust may occur if the wallet provider also serves as an exchange (for converting between bitcoin and national currencies). Users may opt for this arrangement due to its convenience. The bankruptcy of Mt. Gox [11] demonstrated the weakness of such pooling of trust.

Devices with resource constraints can utilize a light version of the Bitcoin software. This has the advantage that it limits its activity to checking transactions related to the user, rather than validating all activity in the system. For example, instead of retaining the entire blockchain (that is currently over 26 GB), it can maintain just the headers (that currently take a little over 23 MB) [19]. However, this has the effect of becoming a second avenue through which trust becomes more centralized. This is because users of light Bitcoin clients rely on others to validate the integrity of the rest of the blockchain.

If an adversary is able to command more computational power than the rest of the participants together, he can exert control over which variant of the blockchain is accepted by the Bitcoin network. In this case, the adversary can select a particular blockchain and extend it faster than others can extend what was previously the legitimate blockchain. The consequence is that all participants will accept the adversary's blockchain. To see that this is a real threat, note that the Bitcoin community recently objected to the pooling of resources by GHash.IO members due to this concern [5].

Privacy violations

The presumed anonymity of participants in the Bitcoin network is based on the fact that they are only identified by their

public keys. However, large amounts of data are collected by programs such as Upstream and PRISM [23]. This auxiliary information can be used to de-anonymize some public keys. Further, all transactions in the entire history of the Bitcoin network are recorded in a single public ledger that is necessarily available to every member. It has been shown that this can be leveraged to further de-anonymize other participants' public keys [17].

Metcalf's law [21] observes that the value of a network grows as the square of its size, measured in nodes. A corollary to this is that an adversary seeking to de-anonymize participants gets quadratically increasing opportunity to do so as the size of the network grows. More concretely, when the number of Bitcoin users increases by a factor of ϕ , the number of transactions between different users is expected to grow by a factor of $O(\phi^2)$. The chance that the adversary is able to subvert the privacy of any transaction grows commensurately.

In practice, the Bitcoin network consists of nodes that run the full protocol while others run the light version. We model the total number of nodes as N . The fraction of the nodes running the full protocol is denoted by f . Therefore, on average there are $(fN)^2$ edges between nodes running the full protocol. Since $(1-f)N$ must then be running the light protocol, the ratio of light nodes to full nodes is $\frac{(1-f)N}{fN} = \frac{1-f}{f}$. Thus, there will be $\frac{1-f}{f}(fN) = (1-f)N$ edges between nodes running the light and full versions. In the above model, we can consider the fraction of transactions whose privacy can be violated. This can be viewed as three cases: first, when the adversary subverts a fraction s of the light software—that is, $\frac{s(1-f)N}{(1-f)N+(fN)^2}$ of all transactions will be de-anonymized; second, when the adversary subverts the same fraction of the software running the full protocol, that is, $\frac{s(fN)^2}{(1-f)N+(fN)^2}$ of the transactions will be affected; and third, when the adversary subverts the same fraction of both types, that is $\frac{s(1-f)N}{(1-f)N+(fN)^2} = s$. Asymptotically, (as $N \rightarrow \infty$) the fraction of transactions with privacy violations goes to 0, $O(s)$, and $O(s)$. The cost of the third option is bounded below by the cost of the second option, while the benefits are comparable. We can therefore conclude that the nodes running the full protocol are most attractive as targets of a well-provisioned adversary.

Logical coupling

The reference code is developed jointly in open fora by members of the Bitcoin community. However, sufficiently motivated adversaries could infiltrate the group over time. The potential for damage can be gauged by studying past incidents resulting from software flaws. In August 2010, an integer overflow vulnerability was exploited to bypass a verification

check [9]. Failure to discover it would have allowed two accounts to fraudulently be credited with 184 billion Bitcoins.

The homogeneity in the deployed code base leaves the system brittle to attacks. Again, we can understand the risk by considering a case that occurred without malice. In March 2013, a new version of the Bitcoin software was released. The use of a new database inadvertently increased the number of transactions that could be reported at once [4]. The discrepancy resulted in older versions of the software rejecting transactions that the newer version accepted. The resulting operational disruption caused the value of Bitcoins to drop by 33 percent [15].

The frailty is the direct consequence of the interplay between high connectivity and tight logical coupling. The software engineering regime used for developing Bitcoin code does not support graceful operation in the face of discrepancies. For example, the ecosystem currently avoids fixing bugs that would disconnect older clients if the bug does not affect correctness.

Mitigation

Bitcoin is organized as an unstructured peer-to-peer overlay. At the end of the 1990s and in the early 2000s, significant research effort was invested in creating structured peer-to-peer systems. The lessons learned can be applied to use distributed hashables or alternate approaches to reduce the scaling problems. If node churn is low, such solutions are likely to improve its stability. Reducing the aggregation of trust requires users

to adopt wallets that maintain credentials on their devices rather than at proxies. Offline processing of transactions on their behalf can occur through third-party escrow. Bitcoin's scripting capability allows these to be enforced using its multi-signature primitive without trusting intermediaries. Further, as the storage and computational power of mobile devices grows, the need to run light versions of the protocol will decrease. This will reduce the dependence on external verifiers.

The current approach for de-anonymizing users of Bitcoin first clusters the large number of anonymous users based on idioms of use [17] and then connects clusters to real-world identities using associations determined out of band (by transacting with known entities, for example). Changing the patterns in which transactions are carried out, or using intermediaries that mix the inputs and outputs of many users into single transactions can add layers of privacy.

Finally, an increasing number of implementations of the Bitcoin protocol are being deployed. As the diversity in the running codebase grows, so will the resources needed to corrupt all versions of the software. Further, the chance that at least one implementation's other developers will notice grows exponentially.

Related work

Although Bitcoin is a relatively recent construct, by November 2013 the cumulative value of existing Bitcoins had crossed \$10 billion. This has motivated numerous analyses, both in academic literature [2] as well as in practice. They can be categorized into prospective studies consisting of theoretical attacks that have been proposed and retrospective ones, which have been undertaken after failures that manifested in practice.

The first group are typically attacks against the steps used for minting, transacting, and validating Bitcoins. The threat model usually assumes that an individual or small group of colluding entities aim to gain more Bitcoins than they are entitled to. Often the attacks attempt to exploit race conditions that result from the fact that Bitcoin is a distributed protocol. For example, a *Finney attack* occurs when an entity validates a transaction but delays reporting it to the network and colludes with the payer who double-spends the amount to another payee. After the payer has received goods or services from the second payee, the original validated transaction is released to the network, causing the second payee's payment to be rejected. In practice, the cryptographic protections, network dynamics, and economic incentives have sufficed to thwart these types of attacks.

In contrast to the first group, the retrospective analyses focus on software flaws discovered in the field. Even though the Bitcoin system itself is decentralized, over time some participants began to aggregate trust by depositing their Bitcoins in a few exchanges. In February 2014, the Mt. Gox Bitcoin exchange filed for bankruptcy after losing \$480 million [11] of customer deposits. It blamed the losses on theft made possible



ISSA Journal Back Issues – 2015

Past Issues – click the download link: [↓](#)

- [↓ Legal and Regulatory Issues](#)
- [↓ The State of Cybersecurity](#)
- [↓ Physical Security](#)
- [↓ Security Architecture / Security Management](#)
- [↓ Infosec Tools](#)
- [↓ The Internet of Things](#)
- [↓ Malware and How to Deal with It?](#)
- [↓ Privacy](#)
- [↓ Academia and Research](#)
- [↓ Infosec Career Path](#)
- [↓ Social Media and Security](#)

EDITOR@ISSA.ORG • WWW.ISSA.ORG

by the fact that multiple Bitcoin transaction identifiers could be derived from the same signature. (This property is known as *transaction malleability*. It resulted from OpenSSL treating signatures with a different number of leading zeros as equivalent [20].) However, such attacks can be guarded against by avoiding central points of failure—that is, participants maintain custody of their own digital cash.

Conclusion

We discussed four security concerns that arise from the high connectivity of the Bitcoin network and the weaknesses that result from each. First, we considered the consequence of relying heavily on communication network connectivity. Second, we covered the effect of connecting nodes with asymmetric (superior) computational power. Third, we reported on the fragility of privacy in the face of high connectivity. Fourth, we highlighted the concerns that come from tight logical connectivity (as occurs with homogeneity in the operational code base). Finally, we discussed possible mitigations.

Acknowledgment

This work was partially funded by the US National Science Foundation (NSF) under Grant IIS-1116414 and Department of Homeland Security (DHS) Science and Technology Directorate. The views and conclusions contained herein are the author's and should not be interpreted as representing the official views of DHS, NSF, or the US government.

References

- [1] William Acosta and Chandra, “Improving Search Using a Fault-tolerant Overlay in Unstructured Peer-to-Peer Systems,” *IEEE International Conference on Parallel Processing*, 2007.
- [2] Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua Kroll, and Edward Felten, “Research Perspectives and Challenges for Bitcoin and Cryptocurrencies,” *36th IEEE Symposium on Security and Privacy*, 2015.
- [3] “Bitcoin Market Capitalization,” *Blockchain Info* – <https://blockchain.info/charts/market-cap>.
- [4] Vitalik Buterin, “Bitcoin Network Shaken by Blockchain Fork,” *Bitcoin Magazine*, 12 March, 2013 – <http://bitcoin-magazine.com/3668/bitcoin-network-shaken-by-blockchain-fork/>.
- [5] Michael Casey and Paul Vigna, “BitBeat: Mining Pool Rejects Short-Term Fixes to Avert ‘51% attack,’ ” *The Wall Street Journal*, 16 June, 2014 – <http://blogs.wsj.com/money-beat/2014/06/16/bitbeat-a-51-attack-what-is-it-and-could-it-happen/>.
- [6] David Chaum, “Blind Signatures for Untraceable Payments,” *Advances in Cryptology*, Springer, 1983.
- [7] David Chaum, “Security without Identification: Transaction Systems to make Big Brother Obsolete,” *Communications of the ACM*, Vol. 28(10), 1985.
- [8] David Chaum, Amos Fiat, and Moni Naor, “Untraceable Electronic Cash,” *Advances in Cryptology, Lecture Notes in Computer Science*, Vol. 403, Springer, 1990.
- [9] CVE-2010-5139, National Vulnerability Database, National Institute of Standards and Technology, 6 August, 2012 – <https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2010-5139>.
- [10] Christian Decker and Roger Wattenhofer, “Information Propagation in the Bitcoin Network,” *13th IEEE International Conference on Peer-to-Peer Computing*, 2013.
- [11] Carter Dougherty and Grace Huang, “Mt. Gox Seeks Bankruptcy after \$480 Million Bitcoin Loss,” *Bloomberg*, 28th February, 2014 – <http://www.bloomberg.com/news/2014-02-28/mt-gox-exchange-files-for-bankruptcy.html>.
- [12] Rip Empson, “Bitcoin: How an Unregulated, Decentralized Virtual Currency Just Became a Billion Dollar Market,” *TechCrunch*, 28 March, 2013 – <http://techcrunch.com/2013/03/28/bitcoin-how-an-unregulated-decentralized-virtual-currency-just-became-a-billion-dollar-market/>.
- [13] Ian Grigg, “A Very Fast History of Cryptocurrencies BTC – Before Bitcoin,” *Financial Cryptography*, 8 April, 2014 – <https://financialcryptography.com/mt/archives/001491.html>.
- [14] Olga Kharif, “Bitcoin Economy Widens as Parents Pay Digital Allowance,” *Bloomberg*, 24th September, 2014 – <http://www.bloomberg.com/news/2014-09-25/bitcoin-economy-widens-as-parents-pay-digital-allowance.html>.
- [15] Timothy Lee, “An Illustrated History of Bitcoin Crashes,” *Forbes*, 11 April, 2013 – <http://www.forbes.com/sites/timothylee/2013/04/11/an-illustrated-history-of-bitcoin-crashes/>.
- [16] “Regulation of Bitcoin in Selected Jurisdictions,” *Law Library of Congress, Global Legal Research Center*, January, 2014 – <http://www.loc.gov/law/help/bitcoin-survey/regulation-of-bitcoin.pdf>.
- [17] Sarah Meiklejohn, Marjori Pomarole, Grant Jordan, Kirill Levchenko, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage, “A Fistful of Bitcoins: Characterizing Payments among Men with No Names,” *13th ACM Internet Measurement Conference*, 2013.
- [18] Satoshi Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” *Cryptography Mailing List*, 31 October, 2008 – <https://bitcoin.org/bitcoin.pdf>.
- [19] Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder, “Mechanics of Bitcoin,” *Bitcoin and Cryptocurrency Technologies*, 2015.
- [20] Anders Nilsson, “The Troublesome History of the Bitcoin Exchange MtGox,” 14 February, 2014 – <https://anders.io/the-troublesome-history-of-the-bitcoin-exchange-mt-gox/>.

- [21] Carl Shapiro and Hal Varian, *Information Rules*, Harvard Business Press, 1999.
- [22] "Silk Road," Wikipedia, retrieved on 1 October, 2014 – [https://en.wikipedia.org/wiki/Silk_Road_\(marketplace\)](https://en.wikipedia.org/wiki/Silk_Road_(marketplace)).
- [23] Craig Timberg and Ellen Nakashima, "Agreements with Private Companies Protect US Access to Cables' Data for Surveillance," *The Washington Post*, 6 July, 2013 – https://www.washingtonpost.com/business/technology/agreements-with-private-companies-protect-us-access-to-cables-data-for-surveillance/2013/07/06/aa5d017a-df77-11e2-b2d4-ea6d8f477a01_story.html.

- [24] Jonathan Zittrain and Benjamin Edelman, "Empirical Analysis of Internet Filtering in China," *OpenNet Initiative*, 20 March, 2003 – <http://cyber.law.harvard.edu/filtering/china/appendix-tech.html>.

About the Author

Dr. Ashish Gehani of SRI International holds a BS (Honors) in Mathematics from the University of Chicago and PhD in Computer Science from Duke University. His research focuses on data provenance and security. He may be reached at gehani@csl.sri.com.



WIS SIG: Cybersecurity Analysis – Where “Life Experience Application”

Continued from [page 7](#)

formation sciences, engineering and related technologies, as well as business entities (per figure 4), thus again bolstering the case for utilization of broad experience bases, different perspectives, and greater situational contexts from which to draw upon, to help move the cybersecurity field forward.

Percent of Gender in Top 3 Undergraduate Majors	Women Leaders		Men Leaders		Women Practitioners		Men Practitioners	
	2013	2015	2013	2015	2013	2015	2013	2015
Computer and information sciences	35%	43%	45%	46%	43%	42%	47%	49%
Engineering and engineering technologies	11%	14%	22%	23%	8%	14%	18%	20%
Business	21%	13%	13%	12%	18%	13%	11%	12%

Figure 4 –(ISC)² 2015 – Undergraduate major (top 3 per gender)

FUTURE predictions

While the (ISC)² and RAND studies show a gap both in the number of women within the profession, as well as a deficit of cybersecurity practitioners overall, respectively, they also offer solid information as to where the future of cybersecurity is moving towards.

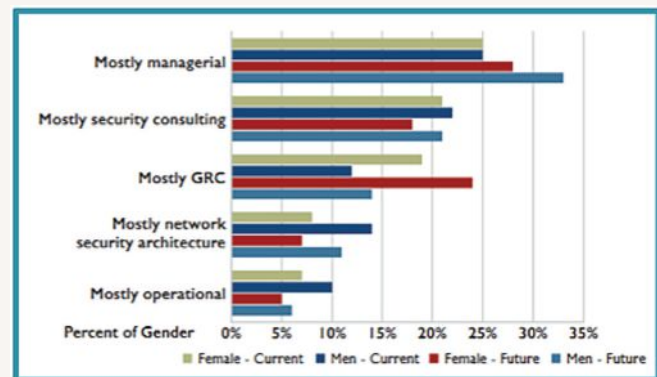


Figure 5 – (ISC)² 2015: Future practice area growth (per gender)

Figure 5 depicts the most highly forecast future practice area growth, and figure 6 highlights the most significant likely needed cybersecurity-related skills.

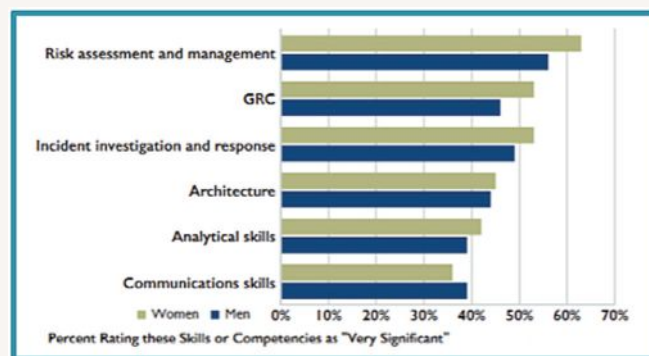


Figure 6 – (ISC)² 2015 – Significant skill ranking (per gender)

Bolstering these findings is a CSO magazine article advocating for an increased focus on government cybersecurity roles, both to promulgate ongoing public-private partnerships as well as to best prepare for future career opportunities, as there are vast opportunities to learn, grow, and innovate your way to success.⁴ The article also offers some great advice: “Think of long-term investing as the model ... Treat your career the same way as your wise investments.” Additional words of wisdom include reminding people to give back to their local cybersecurity communities in order to build skills and expertise as well network your way to success.

Here’s hoping you find your next GREAT niche soon!

Join the international conversation at #ISSAWISSIG, WIS-SIG@ISSA.ORG, and via LinkedIn.

Be BRAVE, Be BOLD, Own Your Future!

About the Author

Dr. Rhonda Farrell, J.D., CISSP, CSSLP, is an Associate at Booz Allen Hamilton (BAH) and a member of the Board of Directors at ISSA Intl and ISSA-NOVA. She is the Co-Founder of the WIS SIG and can be reached at rhondafarrell@aol.com.

4 [Dan Lohrmann](#), The Case for Taking a Government Cyber Job: 7 Recommendations to Consider, *CSO Online* (Aug 7, 2014) – <http://www.csoonline.com/article/2462428/infosec-careers/infosec-careers-the-case-for-taking-a-government-cyber-job-7-recommendations-to-consider.html>.



ISSA Membership Application

Return completed form with payment. * Required Entries

* Name _____ Certifications _____
 * Employer _____ * Email _____
 Job Title _____
 * Preferred address for receiving mailing (choose one): Home Professional
 Home Mobile Professional
 * Address 1 _____ * Phone _____
 Address 2 _____ Fax _____
 * City _____ State/Province _____ * Country _____ * Zip/Postal Code _____

In order to obtain personal information and account access over the phone, ISSA Member services will ask your provided security question.

* Security Question: _____ * Security Answer: _____
 * Only Online Journal: Yes No 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/?PrivacyNotice.

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 (List 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

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 _____

Membership Fees

Membership Categories (descriptions on back)

General Membership: \$95 (USD) plus chapter dues
 2-Year: \$185 (USD); 3-Year: \$275 (USD); 5-Year: \$440 (USD)
 Government Organizational: \$90 (USD) plus chapter dues
 Student Membership: \$30 (USD) plus chapter dues
 CISO Executive Membership: \$995 (USD) plus chapter dues

*Membership Category _____
 (See above)
 *Chapter(s) _____
 (Required within 50 miles of local chapter - list on reverse)
 Referring Member & Chapter _____
ISSA Member Dues (on reverse) \$ _____
Chapter Dues x Years of Membership \$ _____
 (on reverse)
Additional Chapter Dues \$ _____
 (if joining multiple chapters - optional)
Total Membership Dues \$ _____
ISSA Foundation Donation \$ _____
 A tax-deductible contribution, as allowed by US tax code, can be made in addition to your ISSA Membership Payment. For more information on the foundation and its programs, visit www.issaef.org.
Total (dues + ISSA Foundation) \$ _____

Print out and mail or fax form to:
ISSA Headquarters
 12100 Sunset Hills Road, Suite 130, Reston, VA 20190
 Fax +1 (703) 435-4390
 Phone +1 (866) 349-5818 • www.issa.org

You may fill out the form and submit it electronically as an email attachment. You will need an email account to send it.

Submit by EMAIL to: member@issa.org

Membership Categories and Annual Dues

General Membership: \$95 (USD) 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: \$275; 5-Year: \$440.

Government Organizational: \$90 (USD) plus chapter dues

This membership offers government agencies the opportunity to purchase membership for an employee. This membership category belongs to the employer and can be transferred as reassignments occur. When an employee is assigned to this membership, he or she has all of the rights and privileges of a General Member.

Student Membership: \$30 (USD) plus chapter dues

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 (USD) plus chapter dues

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 _____ CVV code _____

Please check the following:

Where would you place yourself in your career lifecycle?

- Executive:** CISO, senior scientist, principal or highest level in respective field
 Senior: department manager or 7+ years in respective field
 Mid-Career: 5-7 years with an identified field of security specialty
 Entry Level: 1-5 years, generalist
 Pre-Professional: Student or newcomer exploring the field

The most important aspects of my membership for the current membership term are:

- Build or maintain professional relationships with peers
 Keep up on developments and solutions in cybersecurity, risk or privacy
 Establish a professional development strategy to achieve my individual career goals
 Increase my personal visibility and stature within the profession
 Share my knowledge and expertise to advance the field
 Develop the next generation of cybersecurity professionals
 Earn CPEs/CPUs to maintain certifications or credentials
 Access to products, resources and learning opportunities to enhance job performance
 Problem solving or unbiased recommendations for products and services from peers
 Gain leadership experience
 All None

Most challenging information security issue?

- Governance, risk and compliance
 Securing the mobile workforce and addressing consumerization
 Data protection Application security
 Security and third party vendors Security awareness
 Threat updates Legal and regulatory trends
 Endpoint security Incident response
 Strategy and architecture
 All None

Which business skills would be most valuable for your professional growth?

- Presenting the business case for information security
 Psychology behind effective security awareness training
 Budgeting and financial management Business forecasting and planning
 Management and supervisory skills Legal knowledge
 Presentation skills Negotiation skills
 Written and verbal communications
 All None

ISSA Chapters & Annual Dues

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

At-Large..... 25	Switzerland..... 80	Central Florida..... 25	Inland Empire..... 20	North Oakland..... 25	Silicon Valley..... 30
Asia Pacific	Turkey..... 30	Central Indiana..... 25	Kansas City..... 20	North Texas..... 20	South Bend, IN (Michiana).. 25
Chennai..... 0	UK..... 0	Central New York..... 0	Kentuckiana..... 35	Northeast Florida..... 30	South Florida..... 20
Hong Kong..... 0	Latin America	Central Ohio..... 20	Kern County..... 25	Northeast Indiana..... 10	South Texas..... 30
Philippines..... 20	Argentina..... 0	Central Pennsylvania..... 20	Lansing..... 20	Northeast Ohio..... 20	Southeast Arizona..... 20
Singapore..... 10	Barbados..... 25	Central Plains..... 30	Las Vegas..... 30	Northern New Mexico..... 20	Southern Indiana..... 20
Sri Lanka..... 10	Brasil..... 5	Central Virginia..... 25	Los Angeles..... 20	Northern Virginia..... 25	Southern Maine..... 20
Sydney..... 0	Chile..... 30	Charleston..... 25	Madison..... 15	Northwest Arkansas..... 15	Southern Tier of NY..... 0
Tokyo..... 30	Colombia..... 5	Charlotte Metro..... 30	Mankato..... 20	Oklahoma..... 30	St. Louis..... 20
Victorian..... 0	Ecuador..... 0	Chicago..... 30	Melbourne, FL..... 25	Oklahoma City..... 25	Tampa Bay..... 20
Europe, Middle East & Africa	Lima, Perú..... 5	Colorado Springs..... 25	Memphis..... 30	Omaha..... 0	Tech Valley Of New York... 35
Brussels European..... 40	Puerto Rico..... 35	Connecticut..... 20	Metro Atlanta..... 30	Orange County..... 20	Texas Gulf Coast..... 30
Egypt..... 0	Uruguay..... 0	Dayton..... 25	Middle Tennessee..... 35	Ottawa..... 10	Toronto..... 20
France..... 00	North America	Delaware Valley..... 20	Milwaukee..... 30	Palouse Area..... 30	Tri-Cities..... 20
Irish..... 155	Alamo..... 20	Denver..... 25	Minnesota..... 20	Phoenix..... 30	Triad of NC..... 25
Israel..... 0	Alberta..... 25	Des Moines..... 30	Montana..... 25	Pittsburgh..... 30	Tucson, AZ..... 10
Italy..... 65	Amarillo..... 25	East Tennessee..... 15	Montreal..... 0	Portland..... 30	Upstate SC..... 0
Netherlands..... 30	ArkLaTex..... 0	Eastern Idaho..... 0	Motor City..... 25	Puget Sound..... 20	Utah..... 15
Nordic..... 0	Baltimore..... 20	Eastern Iowa..... 0	Mountaineer..... 25	Quebec City..... 0	Vancouver..... 20
Poland..... 0	Baton Rouge..... 25	Fort Worth..... 20	National Capital..... 25	Rainier..... 20	Ventura, CA..... 30
Romania..... 0	Blue Ridge..... 25	Grand Rapids..... 0	New England..... 20	Raleigh..... 25	West Texas..... 30
Saudi Arabia..... 0	Boise..... 25	Greater Augusta..... 25	New Hampshire..... 20	Rochester..... 15	Yorktown..... 30
Germany..... 30	Buffalo Niagara..... 25	Greater Cincinnati..... 10	New Jersey..... 20	Sacramento Valley..... 20	
Spain..... 60	Capitol Of Texas..... 35	Greater Spokane..... 20	New York Metro..... 55	San Diego..... 30	
	Central Alabama..... 0	Hampton Roads..... 30	North Alabama..... 15	San Francisco..... 20	
		Hawaii..... 20	North Dakota..... 25	SC Midlands..... 25	