ISSA JOURNAL

January 2018
Volume 16 Issue 1

The Best Articles of 2017

Table of Contents

DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

2017 Article of the Year

Also in this Issue

©2018 Information Systems Security Association, Inc. (ISSA)

The ISSA Journal (1949-0550) is published monthly by
Information Systems Security Association
4008 Louetta Road #261, Spring, Texas 77388
+1 (703) 382-8205 (local/international)

Hello, ISSA Members and Friends

Keyaan Williams, International President

2018: Looking Back, Looking Ahead

It is my pleasure to wish a Happy New Year to all of our ISSA members and friends.

According to EarthSky, "Our modern celebration of New Year's Day stems from an ancient feast in honor of the Roman god Janus—god of doorways and beginnings. Janus was depicted as having two faces. One face of Janus looked back into the past, and the other peered forward to the future."[1] This month's *Journal* is similar to the Janus celebration in that we are reflecting upon the best of last year while we look forward and prepare for all that 2018 has to offer.

Headlines from last year demonstrate that 2017 was a year full of surprises. Many difficulties and challenges had to be overcome, not just in information security, but in all aspects of life. Wars continue in the Middle East, and the threat of a new war looms in Asia. Political upheavals occurred at all levels of government in many countries. We have yet to realize whether these upheavals will be beneficial or detrimental, but the changes are affecting political relationships on a local, national, and global scale. Some countries successfully began the process of secession from a union in 2017, while petitions for independence for other countries were denied.

Natural disasters captured headlines with widespread damage caused by earthquakes, floods, hurricanes, and drought. Cybercrime rose, and old threats like ransomware took on new life. Even for the ISSA, we saw numerous changes. We had an unexpected change in leadership and an end to the long relationship with our management company. We also said farewell to a few chapters who closed their doors in 2017.

With all that happened last year, the story is not all doom and gloom. Much of what to consider part of the best of 2017 is the response provided for all these challenges. Where wars persist, the commitment to liberty and the end of terror has not waned. Where politics has become a distraction, the truth has come to light, and political leaders are being held accountable for their actions. Where natural disasters have destroyed communities, people came together to support each other and begin to rebuild the affected areas. Where cybercrime was a menace to everyone, ongoing investment in people, processes, and technology responded to this growing threat. Where the ISSA has changed—often unexpectedly—the International Board of Directors, chapter leaders, and our membership continue to do all we can to support the successful execution of ISSA's mission to develop and connect cybersecurity leaders globally.

I rarely make predictions or forecasts for the future. However, I am optimistic that 2018 is going to be a great year, especially for the security profession. We learned a lot in 2017. We learned about the dangers of complacency and a failure to invest in fundamental security controls. Many compromises that occurred in 2017 were avoidable with the right controls and processes in place.

Now that people outside of the security profession have a newfound respect for the work that we do, it is more likely that they will heed the recommendations of security professionals and apply the controls and practices that are required.

In summary, I think 2018 is going to be a great year for the security profession. Happy New Year!

~Keyaan Williams

1 EarthSky, "Why Does the New Year Begin on January 1?" EarthSky (January 1, 2016) – http://earthsky.org/earth/why-does-the-new-year-begin-on-january-1.

DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

ISSA
Information Systems Security Association

International Board Officers

President
Keyaan Williams
Fellow

Vice President
Roy Wilkinson
Distinguished Fellow

Secretary/Director of Operations
Anne M. Rogers
CISSP, Fellow

Treasurer/Chief Financial Officer
Pamela Fusco
Distinguished Fellow

Board of Directors

Candy Alexander
Distinguished Fellow

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

Mary Ann Davidson
Distinguished Fellow

Rhonda Farrell, Dintinguished Fellow

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

Shawn Murray, C|CISO, CISSP, CRISC, FITSP-A, C|EI, Senior Member

Deborah Peinert

David Vaughn, Senior Member

Stefano Zanero, PhD, Fellow

Information Systems Security Association
4008 Louetta Road #261, Spring, Texas 77388
+1 (703) 382-8205 (local/international)

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 inte raction 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.

ISSA JOURNAL

Now Indexed with EBSCO

Editor: Thom Barrie
editor@issa.org

Advertising: vendor@issa.org

Editorial Advisory Board

James Adamson

Phillip Griffin, Fellow

Michael Grimaila, Fellow

Yvette Johnson

John Jordan, Senior Member

Steve Kirby

Mollie Krehnke, Fellow

Joe Malec, Fellow

Kris Tanaka

Joel Weise – Chairman, Distinguished Fellow

Branden Williams, Distinguished Fellow

Services Directory

Website
webmaster@issa.org

Chapter Relations
chapter@issa.org

Member Relations
member@issa.org

Executive Director
execdir@issa.org

Advertising and Sponsorships
vendor@issa.org

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 corporation 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.

2017 Infosec Law Year in Review

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

As we start 2018, I thought it would be fun(!) to look back on a few significant legal events from 2017 involving the data security landscape. While these may not necessarily be the most attention-grabbing events, they represent some of the more interesting legal developments that occurred last year.

January

To kick off the year, amendments to Illinois' data breach notification law went into effect on January 1 that significantly expanded the Personal Information Protection Act. Changes included expanding the definition of personal information to include medical information, health insurance information, certain unique biometric data, and a username or email address in combination with a password or security question and answer. It also requires that the attorney general be notified of a breach in certain circumstances. Finally it scales back on the encryption safe harbor if an encryption key was or is reasonably believed to have been acquired in the data breach. These changes exemplify the direction being taken by many states in expanding their data breach notification laws. More to come in 2018.

May and June: WannaCry and Petya

In May, a ransomware attack that became known as WannaCry locked computer systems until payment was made to the attackers. Based on an exploit of a Microsoft vulnerability, the ransomware was reportedly developed from malware that had been developed by, and then stolen from, the US government. A patch from Microsoft had been released a few weeks before the attack, but companies that were affected hadn't reacted quickly enough. This led to almost a quarter of a million computers in over 150 countries getting hit by the ransomware. A variant called Petya emerged one month later that was based on the same Windows vulnerability as WannaCry.

WannaCry and Petya represented a change in the ransomware threat vector, since they weren't just finding success with small or medium-sized companies. The liability concerns associated with such attacks became significant for larger companies that had been hit. Concerns continue to escalate over other ransomware attacks.

September

Attackers took advantage of a web app vulnerability at credit reporting agency Equifax in September that led to the exposure of personal information on almost 150 million people (or, as many commentators like to point out, almost half the population of the United States). In addition to credit card information, some have speculated that other more obscure data collected by the company may also have been exposed and that only the class action lawsuits that have been filed will lead to understanding the full breadth of the breach. The FTC and state attorneys general have also gotten involved, launching investigations into the breach.

Also in September, the US Securities and Exchange Commission (SEC) announced that it had experienced a breach...in 2016. The SEC breach exposed securities information that could possibly have led to the theft of funds from companies through insider training. This attack showed, once again, that even government entities are not immune to cyberattacks.

December (and all year!)

Perhaps the biggest news from an infosec legal perspective in 2017 involved ongoing preparation for the General Data Protection Regulation (GDPR). A joke amongst infosec lawyers (yes, we do have a sense of humor) is that if companies were asking in December "Do I need to comply with the GDPR?," it's too late for them. For those of you who don't know, the GDPR will govern how companies (whether EU-based or not) process, store, transmit, and receive personal data. It replaces the existing EU law on use of personal data and goes into effect on May 25, 2018. Most notable about the GDPR are increased fines and extra obligations on both data controllers and data processors. GDPR compliance requires the implementation of appropriate technical and organizational security measures. What "appropriate" means depends largely on the business of each company. As many commentators have noted, there is no silver bullet. Compliance requires ongoing awareness and understanding of a company's processing of personal data.

What a year it was…and certainly there will be more in store as we start 2018. I'm off now to respond to a whole bunch of emails from current and prospective clients. One starts off "What's the GPDR?" (and no, that's not a typo…GDPR is misspelled throughout as GPDR). What a year it's going to be!

About the Author

Randy V. Sabett, J.D., CISSP, is an attorney with Cooley LLP (www.cooley.com/rsabett), a member of the advisory boards of MissionLink and the Georgetown Cybersecurity Law Institute, and is the former Senior VP of ISSA NOVA. He can be reached at rsabett@cooley.com.

De-Regulate

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

Happy New Year!

It's apparently going to be a cold one for many of us here in the States, so I hope those on the other side of the equator are enjoying those warm months.

This month, I'm going to pose a couple of ideas and thoughts around regulations. It's a sore subject for many of us, depending on if you are enacting regulations, complying with regulations, or trying to navigate the increasingly complex regulatory environment, globally.

Before we get too far into this, the goal here is to foster communication and the exchange of ideas, not politicize the concept.

Recent moves by the current US administration have suggested that federal regulations in some areas are too strict, too over arching, and need to be stricken or amended. A recent example is the FCC repealing the Title II rules of Net Neutrality, which caused interesting discussions (and sometimes dramatically uninformed vitriol) last month. In the wake of those movements, already one state has proposed enacting a state-centric version of net neutrality—essentially making it such that a state regulation could require a nationwide firm to operate differently across the country.

Whether you are for or against net neutrality, this move should signal to you that we are about to get back into the realm of states' rights vs federal rights, and that the regulatory and compliance play book in the US could potentially get at least fifty times more complex. We already see this with state data breach laws, where only two states in the union have yet to enact rules around data-breach notifications.[1]

If you are a company here in the US, you could literally face forty-eight different lawsuits (or one giant class action lawsuit) in the wake of an incident. Do any of you out there look over your annual income statement and think, "Gee, I feel like I underspent on legal and compliance services and head count this year."

Probably not, and no offense of course to lawyers and compliance professionals.

While I am not a fan of over-bearing regulation, there is a healthy balance that is worth striking with regulation that can work to reward entities that do "the right thing" by our citizens in such a way that the "impeding innovation" argument can be put to bed. The job of federal (or, I suppose in a utopian world, global) regulation should be to establish a baseline of good behavior that removes variance at the local level (be it a state, city, county, parish, or prefecture).

As security and compliance professionals, we should be ready for more and more wrinkles to show up in the regulatory landscape that will make our jobs much more complex. We're already seeing challenges with the Global Data Privacy Regulation (GDPR) in which components of this piece of legislation conflict directly with existing laws on the books in a number of different countries. It reminds me of that circular logic you sometimes get into when you try to diagnose a technical problem. If your Internet stops working you start by calling your service provider. Sometimes something like this happens: they blame the problem on your computer or router, so you call the next support team. The next support team of course blames it on the provider. Everyone is pointing fingers elsewhere and all you want to do is stream *Back Mirror* season four.

My advice to everyone is to simplify where you can. In all of my regulatory compliance work (especially GLBA and PCI DSS), the first question I typically ask is "Do you actually need that data?" The first response is always yes, but if you have the patience (and courage) to start to dig deeper, what I have found is the person on the other side of that conversation is answering questions in ways that limit or prevent changes to his or her work. People fight irrationally hard to preserve the status quo, even when it is not in the best interest of the firm and its stakeholders.

Keep asking the hard questions. Dig until you can find a real reason. Then challenge the reason on a business level to effectively show management what happens if you either remove that sensitive data, or protect it in a way that allows you to create a competitive advantage. Either way, both outcomes will improve the bottom line for the company. It allows you to leave an extremely positive mark on your firm, and demonstrates that you can work outside the confines of just security and compliance.

About the Author

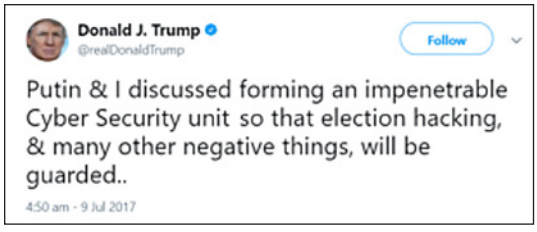
Branden R. Williams, DBA, CISSP, CISM is a seasoned infosec and payments executive, ISSA Distinguished Fellow, and regularly assists top global firms with their information security and technology initiatives. Read his blog, buy his books, or reach him directly at http://www.brandenwilliams.com/.

1 See the National Conference of State Legislatures website for details: http://brando.ws/2pZ2c0R.

The Craziest Information Security Stories of 2017

By Geordie Stewart – ISSA member, UK Chapter

What a year for cybersecurity in the news. It started with US president Trump appointing ex-New York Mayor Rudi Giuliani as US Cybersecurity Czar. While Giuliani is well known for his expertise in locker room talk, he's less well known for his cybersecurity leadership. Undeterred by his relative inexperience, Giuliani promised to "solve cybersecurity" as if it was a crossword puzzle or a game of Cluedo. Never mind securing the nation, it quickly emerged that he couldn't secure his own website. We haven't heard from him since. Perhaps the activation of a screen saver on his new work computer cut short a promising career in security leadership.



Phew, that's all sorted then

WE HAD THE WANNACRY RANSOMWARE. The NSA had lost control of a vulnerability that was weaponized and used against us. In fact, it was just like the horror film *28 Days Later* in which a virus escaped from a secret government lab. Large numbers of dead-eyed, slack-jawed, soul-less figures were seen staggering around. Not zombies, just network administrators and IT security staff working through the night to try to fix the damage. Especially hard hit were UK hospitals that had to cancel large numbers of operations. We'll probably never know how many people died as a result. It's almost enough to make you question the wisdom of stockpiling secret vulnerabilities in a cybersecurity arms race for mutually assured disclosure.

WE HAD THE EQUIFAX BREACH. Hundreds of millions of people had their Social Security numbers disclosed, putting them at risk of identity fraud. The good news was that for a monthly fee Equifax could monitor your credit score and let you know how badly it's been affected. The bad news was that the only way to fully eliminate your risk was to die. There's no escape from Death and Equifaxes.

FACEBOOK ADMITTED to the scale of activity on their platform aimed at influencing the US election outcome. MySpace tried to spread a rumor that they were behind it, but it failed to gain traction with their seven remaining users. Previously, Facebook CEO Mark Zuckerberg had said that it was a ridiculous idea that people were using his influencer platform to influence. Apparently, while millions of people look at Facebook every day, they don't take any notice of the content. Good news for democracy, bad news for all those cats who've learned how to play the piano and uploaded those videos for nothing.

WE HAD THE UBER BREACH. In the spirit of being the biggest and best at everything, Uber admitted to one of the largest security breaches ever. Then, it emerged that a ransom had been paid under the guise of a bug bounty program. It was a less convincing cover up than a Super Bowl wardrobe malfunction. Still, companies don't always make the best decisions in a crisis, and it's up to security professionals to guide them. Wait. What? It was the CISO's idea to pay a ransom and pretend it was a bug bounty? Please excuse the delay to your journey while your driver takes a detour to drop off some bags of cash.

IN DECEMBER UK MP DAMIAN GREEN RESIGNED after persistent rumors that a large collection of pornographic images had been found by police on his parliamentary computer. Fellow Conservative MP Nadine Dorries came to his defense by saying that she routinely shared her password with all her staff and that password sharing was rife in the UK parliament. She said it was "ridiculous" to assert that Green was responsible for the images on his computer. The practice of password sharing was also confirmed by Dorries' new intern, Vladimir. After an outcry, Dorries stated that she didn't have access to any government secrets, just highly sensitive correspondence with her constituents, which was all safely hidden under her password post-it notes.

Here's to a calmer 2018. No data leaks, no huge hacks, and for Facebook to deliver completely open, balanced, and fair coverage of our democratic systems. It's what next US president, Mark Zuckerberg, would want.

About the Author

Geordie Stewart, MSc, CISSP, is the Principle Security Consultant at Risk Intelligence and is a regular speaker and writer on the topic of security awareness. His blog is available at www.risk-intelligence.co.uk/blog, and he may be reached at geordie@risk-intelligence.co.uk.

The Open Forum is a vehicle for individuals to provide opinions or commentaries on infosec ideas, technologies, strategies, legislation, standards, and other topics of interest to the ISSA community. The views expressed in this column are the author's and do not reflect the position of the ISSA, the ISSA Journal, or the Editorial Advisory Board.

Cybersecurity: A School Curriculum Necessity

By Craig Taylor – ISSA member, New England and New Hampshire Chapters

Do you think about cybersecurity training in your son or daughter's K-12 school? If not, you should be. From this cybersecurity veteran, we are not preparing our kids for the 21st century to spot and defend against online attacks, nor are we educating them on the best protective measures either.

Schools do a decent job teaching children about some cybersecurity topics including:

- The harm of cyber bullying
- Why you should never sext (send nude photos by text)
- Understand important privacy issues on Facebook and other social media platforms

But schools mostly fail to educate students on the fundamentals of 21st century online cybersecurity risks. Passwords, password management, and password tools are rarely, if ever discussed. Learning the fundamentals of a phishing or social engineering attack are woefully absent from our basic computer curriculum.

Why is it important to educate young students about these threats and to teach them necessary habits of online protection? Learning good online protective habits early matters a great deal. From a cybersecurity perspective, the Internet is the great equalizer for all nations, peoples, and groups. It is cheaper and easier than ever before in the history of the world to attack anyone, any business, located anywhere in the world from anywhere in the world with anonymity.

The risks we all face—from cybersecurity experts like myself to youngsters playing online games to their parents checking their bank accounts—come in many shapes and sizes. For all its conveniences and efficiencies, the Internet has no borders or boundaries. For criminals it has become a revival of the Wild West—a frontier where policing and the law are usually one or two steps behind emboldened and very smart hackers.

A recent Pew Center study on cybersecurity highlighted a troubling dichotomy among adults. The study found that while most Americans have directly experienced some form of data theft or fraud, many admit they "are failing to follow digital security best practices in their own personal lives, and a substantial majority expects that major cyberattacks will be a fact of life in the future."

While teaching our children as early as possible is imperative, the good news is we're not talking rocket science. The rules of cybersecurity are as easy to learn as it is to drive a car, and just as safe driving is tied to defensive driving, so too is the need to defensively operate our computers today.

Fortunately, schools and students are beginning to recognize this need. A series of investigative stories on the IT website fedscoop.com highlighted the challenges and opportunities of integrating cybersecurity literacy into school technology curriculums as early as possible. "Using technology is one of the three 'Rs' of the 21st century," said Michael Kaiser, executive director of the National Cyber Security Alliance, referring to the traditional subjects of reading, writing, and arithmetic. "If you don't graduate from high school knowing how to use technology, it's going to be a hindrance in the same way if you don't know how to read."

Making basic cybersecurity literacy a new "R" in school curriculums will expose students to lessons that can last a lifetime and teach them critical steps to protect themselves. The time to create good cybersecurity habits is when children first begin operating a computer. Rather than trying to "unlearn" bad habits (as identified in the Pew study) we should build a strong foundation of cybersecurity literacy skills in our students as early as possible.

We can do a better job of preparing our students to enter the workforce with a strong set of cybersecurity literacy skills. We can begin with a focus on the topics mentioned earlier: passwords, their management and tools, as well as understanding social engineering and phishing attacks. Engaged and enlightened students with a modicum of cybersecurity literacy will make a huge difference in creating a workforce prepared to defend against the daily cyberattacks in our homes and businesses of today and tomorrow.

This article first appeared in the New Hampshire Business Review, June-23 2017. Reprinted with permission.

About the Author

Craig Taylor is the Chief Security Officer for Neoscope Technology Solutions in Portsmouth. He can be reached at CTaylor@neoscopeit.com.

WIS SIG Mission: Connecting the World, One Cybersecurity Practitioner at a Time

Fueling Organizational Success via Global SIG-Enabled Engagement

By Rhonda Farrell – ISSA Distinguished Fellow, Central Maryland, National Capital, and Northern Virginia Chapters

They say that birds of a feather flock together, and our global SIGs are great examples of this in practice within the cybersecurity arena, including our two vertical (**Financial Industry** and **Health Care**) and two horizontal (**Security Education and Awareness** and **Women in Security**) Special Interest Groups. 2017 has been an outstanding growth year for our ISSA SIGs; a few of our more outstanding achievements are enumerated below:

- 138 percent increase in registered SIGs membership year to date
- 1000 percent+ growth for our friends of SIGs memberships
- 20 new Connect Event and SIG webinar partners
- 101 of 137 chapters being served
- 98 out of 195 countries represented
- SIG liaison personnel additions internationally and domestically
- Multi-Geography SIG stand ups and event offerings (Colorado taking the lead): FI SIG, HC SIG, Government, Oil & Gas, and Women in Security SIG meetings and events

As 2017 comes to a close, we need to recognize our leaders, speakers, volunteers, partners, advocates, and champions as we simply could not have achieved the growth we did without their help. To our fantastic global SIG leaders, advocates, and champions for 2017, a huge thank you for your service, commitment, and support. Your dedication to the ISSA International organization, members, and broader cybersecurity community is awe-inspiring.

- **Financial SIG:** Andrea Hoy, Mikhael Felker, Kathleen Doolittle
- **Health Care SIG:** DJ McArthur, Andy Reeder, Grant Johnson, Stephen Fitton, Gary Long
- **Security Education and Awareness SIG:** Kelley Archer, Jill Feagans
- **Women In Security SIG:** Domini Clark, Cassandra Dacus, our entire Denver WIS SIG Team (Sara Avery, Elizabeth van Ackeren, Mary Haynes, Debbi Blyth, Danielle Wilson, Danielle Wilson, Jen Wilson, Emily MacCormick, Nancy Philips)
- **Staff:** Monique dela Cruz, Leah Lewis, and Matt LoFiego
- **Global SIG Liaisons** across the globe

As we look to 2020 and focus on creating success coalitions and building international and chapter SIG collaboration to drive organizational and community growth, capacity building is going to be key to seeing those related strategy elements bear fruition. Two major aspects to be considered as we move forward programmatically are:

- The ability of ISSA and the chapters to *fulfill their missions* in an effective manner
- The ability to *enhance the overall quality of life* in the communities that organizations serve within (including advocacy, information sharing, relationship and social network building, and increased engagement, development, and personnel contribution increases) [1].

Continued on page 26

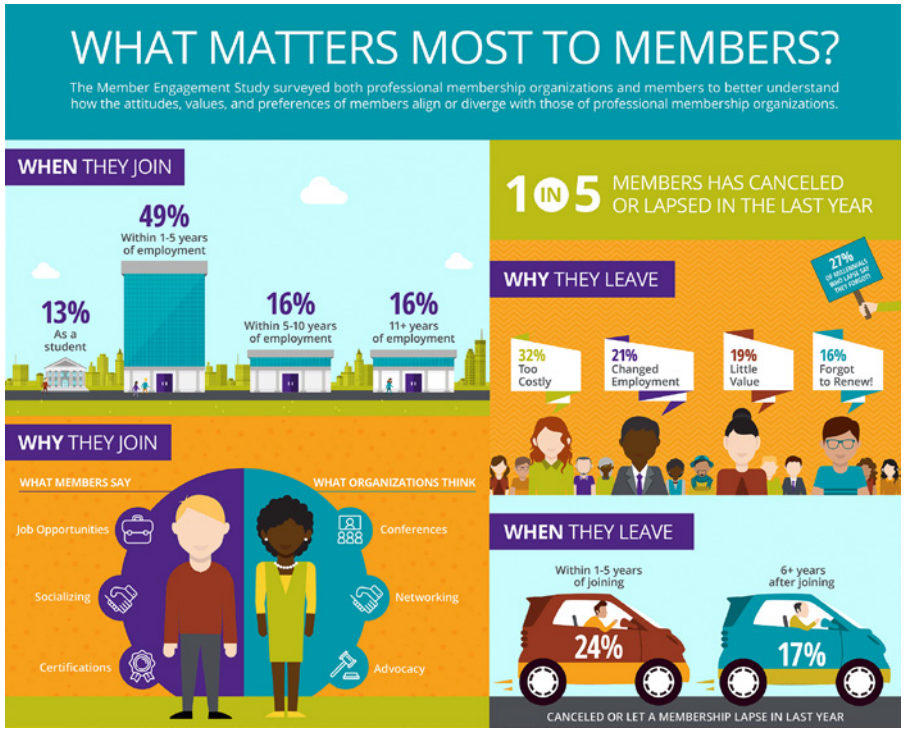


Figure 1: Member engagement – What matters most (1 of 3)

News That You Can Use…

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

FBI Tells Jo(e) Sixpack to Become an Expert in IoT Security

http://www.theregister.co.uk/2017/12/14/fbi_iot_security_advice/

Wouldn't it be great if everyone possessed a certification in "Home Cybersecurity?" As we continue to expand our cyber connections via the Internet of Things and increase the amount of data we share, we must remember that cybersecurity is everyone's responsibility.

How the Supreme Court Could Keep Police from Using Your Cellphone to Spy on You

https://www.washingtonpost.com/news/posteverything/wp/2017/11/27/how-the-supreme-court-could-keep-police-from-using-your-cellphone-to-spy-on-you/?utm_term=.e7197c121e39

Today's advancements in technology allow third parties to have access to a treasure trove of information that could directly impact our security and privacy. Therefore, it is high time that we look to the courts to update laws and guidelines that were created before the arrival of the world's most perfect surveillance device—the cellphone.

The 4 Top Security Concerns on the Minds of Millennials

https://www.forbes.com/sites/larryalton/2017/12/26/the-4-top-security-concerns-on-the-minds-of-millennials/#bc0134f7dc78

Thanks to the media, we all know millennials view things a little differently from other generations. But when it comes to cybersecurity, are their perspectives really that unique? Not really. According to this article, millennials are just as focused on keeping their data and devices secure by employing practical security efforts, as well as improving awareness and education.

FCC Just Killed Net Neutrality — What Does This Mean? What Next?

https://thehackernews.com/2017/12/fcc-net-neutrality-rules.html

The fight for net neutrality is far from over—even though the FCC voted to repeal the 2015 Open Internet Order, which required Internet service providers to treat all services and websites on the Internet equally. Get ready to take the battle to the next level as activists across the country turn to Congress and the courts to enlist their help in reversing the December decision.

Top 8 Cybersecurity Skills IT Pros Need in 2018

https://www.darkreading.com/careers-and-people/top-8-cybersecurity-skills-it-pros-need-in-2018/d/d-id/1330657

Are you looking to take the next step in your cybersecurity career? Do you mentor security professional hopefuls? If so, here are some of the top skills organizations are looking for in 2018. Plus, you won't want to miss quotes from Candy Alexander, ISSA International board member, who shared survey results from the recent ESG/ISSA report.

US Government Blames North Korea for WannaCry

https://threatpost.com/u-s-government-blames-north-korea-for-wannacry/129201/

It's official. The United States government has declared that North Korea was responsible for last May's WannaCry ransomware outbreak that impacted nearly a quarter of a million computers in over 150 countries. However, the bigger question is "Who will answer for the attacks?" Since you can't arrest a nation-state, who will be held accountable for the damages?

2017 Biggest Cybercrime Arrests

https://www.scmagazine.com/2017-biggest-cybercrime-arrests/article/720094/

As the number of breaches and cyber attacks continues to climb, you may be wondering if cyber criminals are ever brought to justice. Check out this list of notable arrests from 2017. Happily, sometimes the good guys are successful in the fight against cybercrime.

Online Fraud Dropped 33 Percent between Black Friday and Cyber Monday

https://www.esecurityplanet.com/network-security/online-fraud-dropped-33-percent-between-black-friday-and-cyber-monday.html

Good news! We are getting better at protecting ourselves from online fraud. But this doesn't mean we can rest on our laurels. We still need to keep moving the needle in the right direction, which includes increasing our vigilance when it comes to protecting our identities and our data.

ICS Cybersecurity Predictions for 2018 — The Bad, the Ugly, and the Good

http://www.securityweek.com/ics-cyber-security-predictions-2018-bad-ugly-and-good

As usual, it is time to dust off the crystal ball and see what is in store for cybersecurity in 2018. Will things be better, worse, or the same as last year? Here are a few more forecasts for your consideration:

https://www.csoonline.com/article/3242866/security/our-top-7-cyber-security-predictions-for-2018.html

http://www.govtech.com/blogs/lohrmann-on-cybersecurity/the-top-18-security-predictions-for-2018.html

http://www.informationsecuritybuzz.com/articles/2018-cybersecurity-predictions/

At the end of the year, revisit the predictions to see which ones came true. In the meantime, here's toa wonderful and cybersafe 2018! Happy New Year from the *Security in the News* team!

Solving the people problem in IT security

by Michael Howard, HP

As HP's Chief Security Advisor, I lead a global consultancy team that delivers industry-defining security and compliance solutions and services to a diverse customer base. All opinions are my own.

Despite the best advice of IT professionals, employees remain the largest security risk for organizations to contain. There's no quick fix for the so-called "people problem," where individual employees circumvent or flat-out ignore known security best practices. It's a costly way of doing business, but the situation is not entirely hopeless. I've found there are a few ways to get employees and security professionals on the same page. The answer to the people problem is, simply enough, people. An organization's security is everyone's responsibility. That means security professionals and employees must work together. Here are some tips both parties can follow.

For employees

1. **Be cautious with your email.** If messages look too good to be true, or if you don't know who they're coming from, don't click anything.

2. **Use the tools you have**. Follow the existing guidelines and corporate encryption policies to protect the data you're sharing around the organization.

3. **Take it seriously**. Don't take shortcuts. Corporate policies may seem like they're just adding extra work, but there's usually a reason to require the extra steps.

For security professionals

1. **Implement awareness campaigns**. Get the word out there constantly. Put posters on the walls and hold ongoing seminars. Security should be an open topic users feel empowered to ask questions about.

2. **Reward good behavior.** Incentive programs can be effective. Test employees by sending phishing emails and reward people who don't click.

3. **Share the losses**. Communicate what a breach could cost. Explain how supporting security can actually add to the bottom line of the company.

4. **Demystify IT.** Too often, employees don't even know who their security team is or what they really do. Create a dialogue between the security team and other employees; have them share stories and connect with the rest of the company.

Security professionals have additional undercover tools available to help them contain internal security risks. For example, IT can compartmentalize networks to make sure no one has full and complete access. Additionally, monitoring tools allow visibility into everything that touches the network. Teams can be reviewing websites as they're accessed, looking for signatures and valid security certificates. Security tools also provide ways of sharing information about websites visited and traffic coming back from those sites to look for signs of malware that may be coming in the door.

Assess and get started

Finally, security teams won't know how well they're doing without a baseline. Let's say there are 35,000 attempts on a company and 200 get through. Keep a record of that information. A proper benchmark should also track internal employee mistakes, including opening phishing emails, clicking on corrupt websites, or documents printed but never picked up, to determine how many breaches are occurring from those behaviors. By keeping a record of that data, security teams can track their progress over time. Security professionals have an army of employees capable of helping in the fight against cyber attacks. They just have to enlist them.

When you approach security as a business issue, and not just an IT issue, it reinforces the importance of security to all employees. Including security as part of the ongoing company conversation will keep it top of mind, making it part of everyday business operations.

Learn more at www.hp.com/go/printsecurityissa

© Copyright 2017 HP Development Company, L.P. The information contained herein is subject to change without notice.

b3773r p455w0rd5?

By Luther Martin – ISSA member, Silicon Valley Chapter

The fact that encryption provides protection that is essentially unbreakable can probably be accurately described as a "polite fiction." This is because there is always part of a system that lets you bypass encryption in a way that is much easier than putting implausibly powerful computers to work for implausibly long times to crack an encryption key. This principle was described by Adi Shamir in his third law of security: cryptography is typically bypassed, not broken. It is also why some people have been known to say that amateurs talk about encryption but professionals talk about key management.

In particular, access to keys is often controlled by a password, and those passwords are much weaker than the encryption that the password-protected keys provides. It might take a supercomputer until the heat-death of the universe to crack a cryptographic key, but common desktop computers can often crack many passwords in no more than a few days. And it turns out that many password policies have been making this worse instead of better. They might not be as bad as the password management seen in the 1932 Marx Brothers movie *Horse Feathers* ("You can't come in here unless you say 'Swordfish.' Now I'll give you one more guess."), but they are still not as good as they could be.

The basis for many of today's password management rules comes from the version of NIST's Special publication 800-63B, "Digital Identity Guidelines," that was published in 2003. This is the origin of requirements to rotate passwords every 90 days or to require the use of special characters in a password.

Many of the early ideas of how to make passwords more secure sounded perfectly plausible but did not work well in practice. In particular, rotating passwords every 90 days turned out to be a bad idea, as did requiring special characters in passwords. Both of these add little to no security to passwords. But they greatly reduce their usability, which means that it increases the cost of supporting users who are required to follow them. Requiring complex passwords can even reduce the security that passwords provide. Users who forget complex passwords will frequently fall back to their organization's password reset process, many of which are much weaker than the complex passwords that they help manage.

So it turns out that many of the requirements defined by NIST did not make sense. The *Wall Street Journal* recently ran an article about this,[1] in which they interviewed Bill Burr, the author of NIST's original password guidelines, as well as Paul Grassi, who led the process that led to their revision that was published in June 2017.

> The new guidelines, which are already filtering through to the wider world, drop the password-expiration advice and the requirement for special characters, Mr. Grassi said. Those rules did little for security – they "actually had a negative impact on usability," he said.

Instead of rotating passwords every 90 days, research suggests that a better approach is to only require users to change passwords if there is a sign that they have been compromised. And as once illustrated in the XKCD web comic,[2] using a sequence of four words is better than requiring complex passwords that use special characters.

NIST should be congratulated for recommending something that contradicts their previous guidance and basically admits that they were wrong. That probably was not easy for them to do.

But now that we know that the password policies required back in 2003 were bad, what are we going to do about it? Making sure that password policies agree with the most recent thinking on what makes a good password is a reasonable first step. But it seems that the older thinking on password management is deeply ingrained in the security policies of many businesses. Many of them may be unwilling to change their policies to ones that make more sense.

If you have one of these password policies where you work, why not try pointing out to your security department that these policies seem to do little more than increase costs while providing little additional security? Will they accept the new and improved best practices? Or will they insist on following the old ways? And if they insist on following the old ways, what will be their justification for doing this? Or if you are part of one of the organizations enforcing the older ways, why are you doing this? If you are just increasing costs while providing minimal additional security, why are you doing it?

About the Author

Luther Martin is a Distinguished Technologist at Micro Focus. You can reach him at luther.martin@microfocus.com.

1 McMillan, Robert. "About Those Online Password Rules… N3v$r M1#d!" The Wall Street Journal, August 8, 2017.

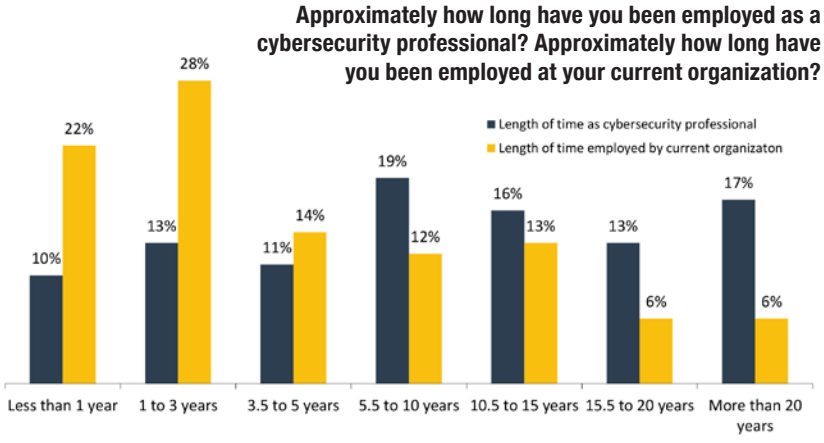
2 https://xkcd.com/936/.

Second Annual ESG/ ISSA Cybersecurity Survey

Cybesecurity Skills Crisis Causing Rapidly Widening Business Problem

The second annual ESG/ISSA Global Research project was released in October. ISSA has teamed up with ESG (Enterprise Strategy Group) to perform the research to better understand the cybersecurity profession. This research was performed using a global survey of ISSA members and has provided us with some interesting insights that I'd like to share.

To begin, it is important to understand that much like last year, the majority of the 343 respondents were from North America. Therefore, some of the responses may be considered US/North American centric; however, we believe that there is a common theme experienced across the globe. We also remain hopeful that next year we can increase participation from other regions of the globe so that all of our members can voice their opinions.



Length of time employed as a cybersecurity professional and at current organization/job

The professional

In looking at the responses to questions related to the individual professional, we found that much like our profession and membership most of the respondent were in the profession for seven-plus years. Although the ISSA has invested in growing the "next generation" of cybersecurity professionals with programs like the Pre-Professional Virtual Meetups, there is still a significant gap in those just starting out in this profession.

Security certifications

In order to provide a better understanding of the security certification industry, we asked our members which certifications they have achieved. The responses identified the top five, which are not a surprise and are listed in order: CISSP, CISM, CompTIA Security+, CISA, and CEH. What was surprising was the number of certifications that received a response: 71! To add a value perspective to this, we then asked which were the best certifications in helping to get a job. The same five were listed. Therefore, according to our research the security certification industry is robust. However, from a professional's point of view it is wise to focus on achieving and maintaining those in the top five.

The need for knowledge

As members of the ISSA know, it is important to stay on top of your game, as the saying goes. To that point we asked participants their thoughts on the statement, "Cybersecurity professionals must keep up with their skills or the organization is at a significant disadvantage against today's cyber adversaries" – with 96 percent of the respondents agreeing or strongly agreeing.

Ironically, in another question asked it was determined that realistically most respondents also agree that it is difficult to keep up with their skills due to the demands of the job. This is the challenge of today's professional.

How and where to gain the knowledge

Now that we have confirmed that maintaining and growing our KSAs (knowledge, skills, and abilities) are critical to our jobs and organizations, it is helpful to understand where our members experience the most value for their training budget and time.

In response to the question, "Which are the most effective methods for increasing your KSAs," the top three responses were (in order) attending specific training courses, participating in professional organizations, and attending industry trade shows and conferences. The important items to note are that our members appear to be utilizing the "Just in Time" or JIT learning model. The concept behind the JIT learning model is obtaining topical knowledge or training on a specific topic. As the research demonstrates, as professionals we don't always have time to attend a long-term class or course. Therefore, attending a local ISSA chapter meeting where a specific topic is presented is of value and interest. This could explain the popularity of online learning environments such as MindEdge and Cybrary.

Getting ahead in your career

Cybersecurity professionals are like any other professionals in that it is important to understand the progress of one's ca-

reer in order to prepare for the next step, and the steps there after. To better understand our member's view on career development, we asked "Which would be the most helpful in getting to the next level career wise?" The response was clear: the majority believe that a combination of having a globally accepted standardized career map and a mentor or career coach along with a training curriculum map would be the most helpful—with emphasis given to the first two.

Summary

As you can see by the few items reviewed here, the 2017 joint research project has a wealth of information that the ISSA can use to further our goals. From our association's perspective, we can use the information to define new services for you, our members. From a member's perspective, it provides you with insight as to the challenges that you and your peers may be experiencing. It also provides you information to use for budget justifications and strategic planning.

We invite you to download the full report. We also invite all of you to participate in the 2018 research project that will be announced in the spring of 2018.

Candy Alexander

ISSA International Director and Distinguished Fellow

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 25+ archived presentations.

Our CISO executives will help you envision the security enterprise leader of tomorrow and the path it takes to reach that pinnacle. This will guide CISO up-and-comers in what it takes to land this role, what the CISO of the future looks like, and steps you can take to build a CISO career.

CISO Mentoring Webinar Series Archive:

- How to Become the Next Security Leader or Information Security Officer
- The Top Five Life-Skills I Have Learned from Mentors in My Career As a CISO
- If a Small-Town Texas Lass Can Become an Information Security Officer, So Can You
- You've Been Acquired. Resistance is Futile
- A Day in the Life of a CISO
- And more…

ISSA.org => Learn => Web Events => CISO Mentoring Webinar Series

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.

Check out the 20+ archived meet-ups!

September 2017: A Day in the Life of an Ethical Hacker

June 2017: Hacking Games: New Ways of Getting Training

ISSA.org => Learn => Web Events => CSCL Meet-Ups

ISSA
SPECIAL INTEREST GROUPS

Special Interest Group Webinars

Want to hear more from ISSA's Special Interest Groups? Join free.

On-Demand Webinars

Each SIG event is designed to address the timely needs of our SIG members through a live, online event and a subsequent recorded version for on-demand viewing.

ISSA Women in Security SIG
Leading The State Of Colorado To Cybersecurity Success
Recorded Live: October 16th, 2017

ISSA Financial SIG
Preparing for Your Next Inspection
Recorded Live: September 15th, 2017

ISSA Healthcare SIG
Collaboration to Achieve Medical Device Security
Recorded Live: September 14, 2017

ISSA.org => Learn => Special Interest Groups=> SIG On-Demand Webinars

ISSA
JOURNAL

Elevate Your Career

As a security professional, you have unique and valuable experiences, insights, and information that could positively impact infosec practitioners around the world. 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 who have been published, and get their feedback on your drafts?

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.

ISSA INTERNATIONAL AWARDS

The 2017 international awards were presented at the international conference in San Diego. Recipients of the awards have been offered the opportunity to share their thoughts on the award, the ISSA, and the infosec industry.

Volunteer of the Year

Frank Gearhart

ISSA member, Colorado Springs Chapter

Thoughts on Being an ISSA Volunteer of the Year

I remain honored to be selected as one of ISSA's 2017 Volunteers of the Year. My chapter—Colorado Springs—is vibrant and deeply committed to the ideals of our profession. My voice is neither the most interesting nor the most vital, so I appreciate this opportunity from ISSA to present my thoughts on receiving this award.

My most significant professional accomplishment was earning CISSP certification. I took one of the last paper CISSP tests, and it was weeks before I learned that I'd passed. I wasn't even certain I was qualified to take the exam, but a colleague convinced me that my experience as a network architect and engineer would suffice. Cindy Thornburg, then the vice-president of our chapter, convinced me first to join the chapter and then the training team. Since then I've earned an M.S in Information Assurance, C|CISO certification, and I've presented at an ISSA conference. That CISSP started it all.

Our industry faces several challenges. The most critical is that we don't readily share information. We should borrow a page from the Federal Aviation Administration's Aviation Safety Reporting Program (ASRP), which encourages pilots, flight controllers, and other aviation professionals to report errors, mistakes, and problems in aviation operations or procedures. In exchange, the program provides confidentiality. The reports are used to identify and resolve problems in the system, not to investigate or punish individuals. After 37 years, that confidentiality remains unviolated.

If our profession had a similar program, organizations and individuals would be more inclined to report breaches, vulnerabilities, mistakes, and oversights. Sharing that information using a system such as the Open Vulnerability and Assessment Language (OVAL) would reduce the cost and impact of attacks and allow us to better harness the immense skills and knowledge of the hundreds of thousands of security experts around the planet.

My greatest professional challenge is getting security accepted as a necessary part of every system, every product, and every activity. While everyone gives at least lip service to the importance of security, some spend far too much time and energy looking for reasons to avoid implementing it. Our team works to find opportunities to know their missions and operations so we can help them understand the cost of security is worth it. Eradicating the "Department of No" reputation that IA has is difficult but necessary. Developing the critical soft skills necessary to do this isn't easy in a primarily technical profession, but we need to add these tools to our skill sets in order to be fully successful.

To my many talented, dedicated peers—those that I work with and learn from every day; those whose webcasts, blogs, and books I depend on the stay current; and those I listen to and learn from at conferences—I say "Thank you." From the brilliant researchers to the keyboard wizards to the inspirational teachers to the meeting jockeys, we work to keep data away from those that shouldn't have it and available to those that should. We protect from those with good intentions as well as bad. We sometimes even protect our clients from themselves.

We need to become quicker and more flexible. Just following procedures—even the best procedures—isn't enough. We also need to think of our profession differently. It's defensive by nature, but we can be more innovative and get ahead of our opponents. We also need to be more positive. A common saying in our profession is "We have to be right *every* time, while the attackers only have to be right once." We need to turn that around: Attackers have to get past all our defenses, while we only have to stop them at one.

Penetration testing and vulnerability assessments should play a larger role while "check the box" approaches should be eliminated. We should cautiously yet openly embrace new tools such as machine learning and deep automation, and adopt an information sharing approach that encourages near real-time cooperation among security players at all levels.

By vigorously and proactively testing our defenses we would encourage research into new defenses. By sharing that research, as well as detailed information about real attacks, we might even get ahead of the attackers— at least for a while.

I am proud to be part of this profession. This is my second career, so I'm a little late to the game compared to many of you. I learn from my colleagues every day—new techniques, new ideas, and new viewpoints. I plan to give back as much as I can—the same way many of you do.

~ Frank Gearhart

2017 Article of the Year

Lessons about Cloud Security from 1980s Horror Movies

By Kayne McGladrey – ISSA member, Puget Sound Chapter

This article discusses how businesses can apply three fundamental best practices for adapting current security programs to mitigate insider threats as applications and data migrate to the cloud.

Much to my parents' chagrin, I watched a lot of horror movies growing up. Many of these films had roughly the same plot—the protagonists would be safe, at home or at a party, and their phone would ring. Something went wrong, and they would get another suspenseful warning phone call. The third call was inevitably from inside the house, and the body count would rise as the protagonists tried to escape or defeat the villain. The bad guy was invariably a friend with a spare key and a dark secret, or he was demonically possessed. The message was clear: be careful of whom you associate with and whom you let into your house.

On-premise network security offerings and best practices might well have used the same play book as those slasher films. Administrators were led to believe that by configuring the firewall just right the heroes could stop the bad guys from getting in. Vendors told us that adjusting the anti-spam and virus-scanning policies would prevent the villain from getting into the office. Setting up a password-locking system after three failed attempts took the place of setting up an alarm on the front door. HR departments began participating in Identity and Access Management (IAM) initiatives and started handing out login credentials only to trusted individuals, often at the same time as they were providing badges to gain entry.

And like the cliché dramatic element, the villain already had a key to the building, and now we're all trapped inside with him. The cloud further upended the model of protecting everything behind the corporate firewall and inside the office walls. To survive, each company needs to understand what constitutes normal, so that they can identify the first warning sign. Survivors then need to be able to prioritize those warnings to avoid alert fatigue. Finally, survivors need to be thorough in deploying modern authentication and authorization systems, because what you miss is where the compromise will begin.

IAM programs focused on granting access to legitimate users. This was based on the false assumption that no one else could impersonate those users, when in fact users often reuse passwords across multiple services, and companies lack the detail of typical user behavior patterns. In 2016, breaches at Yahoo!, LinkedIn, AdultFriendFinder, and other websites and services exposed over 3.2 billion users' passwords [1]. The risk is that dedicated bad actors can skip spear-phishing techniques and test for password reuse through credential stuffing [2].

In a credential stuffing attack, bad actors purchase password dumps (such as one of the Yahoo! dumps) on the dark web. The bad actors then configure an automated authentication tool to check common SaaS services, such as DropBox, Microsoft Online, SalesForce, as well as banks like Wells Fargo and payment services like Stripe and PayPal. Next, the bad guy rents a botnet and the computers in the botnet use the configuration files and password dump to check hundreds of thousands of username/password combinations across SaaS services and websites. Once the attack is complete, the bad guy can then choose to resell the valid username and pass-

word combinations or use them for his own purposes. The risk is that one or more of your users' passwords disclosed in a breach coincide with their password to one or more SaaS services in use by your organization. If the desired user's password is not in one of the many breaches, bad guys can still try 123456, which was the most common password out of ten million passwords aggregated in 2016 [3].

Businesses need to operate under the assumption that they have already been breached, and that one or more bad actors are actively impersonating their legitimate users. Organizations can take three fundamental steps to develop a security baseline, establish proactive monitoring and alerting, and deploy modern authorization technologies as they adapt their security programs to reduce the risks associated with the cloud.

Set a baseline for normal

Several years ago I led a project to deploy a centralized session-monitoring solution at an investment firm. They chose to use the solution initially for role mining rather than regulatory compliance. This firm had "cloned" user accounts for years rather than developing formal roles, and they believed that the initial effort would uncover users with too many privileges.

In a role mining project, analysts review the permissions that currently exist in the environment. This can be a case of reviewing Active Directory permissions, UNIX sudoers files, database GRANT statements, login privileges for known SaaS services, and permissions defined on SaaS services. As each potential source of permissions uses a different format for describing user permissions, human intelligence needs to be applied to find common elements. For example, a user may be able to edit an Excel spreadsheet containing financial data stored on a Windows file share, and they may also be able to view but not edit data stored in NetSuite. These permissions can be logically aggregated into a *role* if several individuals have similar permissions.

After six months, the project team consolidated and reported our findings. Although we did find the anticipated problems of too many users with too many privileges, the larger issue we uncovered was that a vast number of batch jobs used a standard set of shared credentials. This authentication scheme made it tough to deduce what privileged commands should be allowed by the batch jobs, particularly in cases where the first command observed in the session was to switch to the root account on UNIX systems. After much policy debate, the organization forced application owners to request distinct accounts for each application, and they set a drop-dead date for application compliance.

Each company needs to understand what constitutes normal.

> The CERT Insider Threat Center recommends organizations "carefully audit user access permissions when an employee changes roles within the organization to avoid privilege creep. In addition, routinely audit user access permissions at least annually. Remove permissions that are no longer needed." [4]

Businesses have been working for years to establish what users should be able to do and which apps they should be able to access. This includes access to SaaS apps, virtual machines hosted on IaaS, and machine-to-machine communications. Roles and rights obtained through role mining and audited as part of quarterly certification reports theoretically show what users can do.

ISSA
Information Systems Security Association International
www.issa.org

Members Join ISSA to:
- Earn CPEs through Conferences and Education
- Network with Industry Leaders
- Advance their Careers
- Attend Chapter Events to Meet Local Colleagues
- Become part of Special Interest Groups (SIGs) that focus on particular topics

Join Today: www.issa.org/join

Regular Membership **$95***
(+Chapter Dues: $0-$35)*

CISO Executive Membership **$995**
(Includes Quarterly Forums)

**US Dollars/Year*

What's less clear is what users do with those credentials. A CFO might stop at her local coffee shop in Chicago and log into NetSuite on the coffee shop's Wi-Fi. She could then drive to work and access Salesforce from her desk. This is a reasonable use case, whereas common sense would suggest that she should not be logging into NetSuite from London five minutes after she left the coffee shop.

Organizations should plan to deploy and integrate two or more monitoring technologies to understand typical use patterns.

Similarly, an IT administrator might be called in the middle of the night to work on a high-severity ticket on an IaaS server. It is reasonable that he would log in from home on the evening of the ticket. It would, however, be very unusual for him to log in the next evening from a different IP address and run privileged commands if there were no ticket.

Although these simple scenarios seem obvious, very few organizations have deployed the necessary technologies to detect this aberrant behavior, or even to understand what "normal" looks like during a work week. Consequently, organizations should plan to deploy and integrate two or more monitoring technologies to understand typical use patterns.

Privileged accounts on IaaS servers should be monitored. At the simplest level, this is a case of plugging the system log from the server into a security information and event management (SIEM) solution and hoping that an operator notices a red flag while manually reviewing the other log entries. More sophisticated solutions allow for monitoring of both privileged commands and privileged session monitoring and playback for later review. For example, rules can be set to send an alert to a security operations center. The security team can begin viewing a privileged session in real-time, and forcibly disconnect a session if it appears to be a breach. The most sophisticated solutions incorporate user and entity behavior analytics, and can quickly detect that a session is being run by an automated piece of attack software through automated analysis of keystroke patterns, or comparison of the active session against similar sessions.

Companies should also plan to monitor the use of SaaS servers by their users. At a minimum, this is again a case of plugging the firewall's network access logs into the SIEM solution. However, this will only detect use of SaaS services while users are in the office and behind the corporate firewall.

A more comprehensive solution is to deploy a cloud access security broker (CASB) and require mobile device enrollment via a mobile device management (MDM) solution. When a user attempts to access a SaaS service, the SaaS service provider validates that the user has been authorized via the CASB. This is easily accomplished at the office through configuration of a forward or reverse proxy (depending on the CASB). Mobile devices can be enrolled via an MDM solution to similarly use the CASB before accessing SaaS services. CASBs can define which groups of users can access specific SaaS services and some of the permissions within those SaaS services, such as screen sharing or data exports. Potential threats can be turned away if a bad actor with compromised credentials attempts to access a SaaS service without proxying through the CASB. Similarly, if the CASB rules define that users can view but not export data, bad actors can be thwarted in attempts to exfiltrate data in bulk.

Plan for alert automation

The security team at Target had deployed a sophisticated malware monitoring solution before the 2013 breach that exposed 40 million payment cards. The security team received alerts, and Target met the letter of PCI compliance at the time of the breach. Unfortunately, the security team either was understaffed and could not investigate all the alerts, or the system generated too many false positives to provide actionable intelligence [5]. Either way, it looked like they were asleep at the switch.

Today, organizations can investigate only 56 percent of the security alerts they receive on a given day [6]. Companies can anticipate a high number of false positives during the initial deployment phases of any IaaS or SaaS monitoring and alerting solution. Previously invisible batch jobs using shared accounts on IaaS servers will appear with unerring frequency in the logs. Employees accessing SaaS and IaaS solutions from home, coffee shops, and vacations will cause false alarms. CASB solutions will identify previously unknown shadow IT deployments of SaaS solutions that need to be incorporated into the corporate security program. Administrators running privileged commands without associated change control tickets will raise eyebrows.

If you are fortunate, the bad guys will leave your company alone while you configure your alerting solution. Your team will have the time to configure the alerting solution to filter out false positives. This will allow your security team to primarily investigate high-risk usage, and to proactively stop the next breach.

Regrettably, it's far more likely that the bad guys will attempt to overwhelm the monitoring and alerting solution while you're configuring it. In this increasingly common threat scenario, the bad actor will launch simultaneous attacks against an organization. These could include a distributed denial of service attack, an email malware campaign, or activating a previously-deployed but dormant piece of malware. These events will generate alert traffic from the monitoring solution, which provides a smokescreen for the real attack. The real attack will use compromised credentials and appear to be legitimate traffic and privileged command usage. The security team will be too busy investigating red herrings, and they are likely to miss the one atypical session. Research by Cisco has found that a just over a quarter of the investigated alerts (28 percent) are deemed legitimate, and less than half (46 percent) of legitimate alerts are remediated [6].

A company cannot hire their way out of this attack by bolstering the number of individual defenders who are manually reviewing logs and alerts. Consider that 44 percent of security operations managers see more than 5000 security alerts per day [6]. Although machine learning is a comparably new entrant to the security space, companies should plan to deploy some form of log aggregation and automated investigation software. At the core, these solutions should be able to identify attack patterns to assist investigators with a macro view of active threats. More sophisticated solutions should be able to identify peculiar behavior and actions by employees and subcontractors.

Deploy step-up authorization everywhere

In 2014, hackers breached JP Morgan Chase and exposed the names, addresses, phone numbers, and email addresses of 83 million account holders. This came as a shock, as JP Morgan Chase had enabled two-factor authentication across its computing estate. They just neglected to enable that feature on one server. Once the bad guys had established a beachhead with a compromised username and password on that neglected server, they compromised nearly one hundred additional servers on the network before the attack was detected. [7].

Companies should plan to implement some form of step-up authorization across all SaaS, IaaS, and on-premise computing resources in parallel with alert automation. The intent of step-up authorization is to increase friction and to mitigate the risk of a bad guy with a stolen password being able to use those credentials to complete an attack and establish an initial entry point for a breach. Step-up authentication can take the form of two-factor authentication or multi-factor authentication.

Two-factor authentication via SMS is often thought of as the first solution. Under this model, users are sent a secret code via SMS, which they must manually type to verify their identity. Regrettably, the bad guys know this and have built solutions to intercept SMS traffic before the legitimate recipient receives the text message [8].

Multi-factor authentication (MFA) can include SMS messages but can also include biometric, location-based, interactive voice response (IVR), or knowledge-based authorization (KBA) elements. For example, a user can swipe her thumb on her mobile phone if she is running a command with privilege on an IaaS server, but only if she is not at her office. Static KBA is the worst of these choices, as dedicated bad actors also have access to Facebook and can learn where targets went to elementary school, the names of their cats, and their favorite movies. Static KBA security questions and answers were also disclosed in numerous breaches in 2016.

At a minimum, companies should first plan to deploy step-up authorization for application and privileged-command usage for on-premise and IaaS servers. The next step is to integrate step-up authorization with all SaaS apps so that unusual traffic patterns require MFA. For example, the CFO who regularly stops for coffee at her local coffee shop might not need MFA to access NetSuite. There should, however, be a step-up

Want to annoy cyberattackers? Attend RSA Conference 2018.

If there's a cybersecurity development, you can be sure the world's largest infosec event will be there for you with strategies and solutions. And as an ISSA member, you can enjoy **$175 savings** on top of a **$700 discount** when you register for a Full Conference Pass by March 16 using discount code **18UISSAFDD**. Immerse yourself in five days of expert-led sessions, inspiring keynotes, in-depth trainings and innovative product demos. Rub shoulders with industry insiders and peers. Cyberattackers won't be happy. But your network will be thrilled.

Register today at **www.rsaconference.com/issa-us18**

Follow us on: #RSAC

authentication prompt when the villain attempts to use her stolen credentials to access NetSuite from London five minutes later.

Summary

We recommend that businesses work to establish a baseline of normal operations under the assumption that one or more bad actors will be identified during this phase. Next, companies should work to deploy meaningful alerts so that security managers can take action without being overwhelmed. Finally, organizations should create friction for bad actors by deploying modern step-up authorization technologies.

None of these solutions will guarantee that a company's defenses will not be not breached in the future. Deploying this combination of defenses, however, makes it financially more expensive and time consuming for the bad guys to maintain access to compromised credentials. It is more likely that the villains will move on to the company next door, which has all the security of a college house party in a horror movie. Your goal is to be around for the inevitable sequel.

References

1. Risk Based Security, 2016 Year End Data Breach QuickView Report, *Risk Based Security*, January 2017 - https://pages.riskbasedsecurity.com/2016-ye-breach-quickview.
2. Wang, Xinran, A Look at Sentry MBA - The Most Popular Cybercriminal Tool for Credential Stuffing Attacks, *Shape Security Blog*, March 9, 2016 - http://engineering.shapesecurity.com/2016/03/a-look-at-sentry-mba.html.
3. Guccione, Darren, What the Most Common Passwords of 2016 List Reveals, *Keeper Security Blog*, January 13, 2017 - https://blog.keepersecurity.com/2017/01/13/most-common-passwords-of-2016-research-study/.
4. The CERT Insider Threat Center, Common Sense Guide to Mitigating Insider Threats, Fifth Edition, *Software Engineering Institute of Carnegie Mellon University*, December 2016 - http://resources.sei.cmu.edu/asset_files/TechnicalReport/2016_005_001_484758.pdf.
5. Greenberg, Adam, Target Did Not Respond to FireEye Security Alerts Prior to Breach, according to Report, *SC Magazine US News*, March 13, 2014 - https://www.scmagazine.com/target-did-not-respond-to-fireeye-security-alerts-prior-to-breach-according-to-report/article/539263/.
6. Cisco, 2017 Annual Cybersecurity Report, Cisco, January 2017 - http://www.cisco.com/c/dam/m/digital/en_us/Cisco_Annual_Cybersecurity_Report_2017.pdf.
7. Bright, Peter, JPMorgan Chase Hack due to Missing 2-factor Authentication on One Server, *Ars Technica News*, December 23, 2014 - https://arstechnica.com/security/2014/12/jpmorgan-chase-hack-because-of-missing-2-factor-auth-on-one-server/.
8. Kessem, Limor, Android Malware about to Get Worse: GM Bot Source Code Leaked, *IBM X-Force Research Malware*, February 19, 2016 - https://securityintelligence.com/android-malware-about-to-get-worse-gm-bot-source-code-leaked/.

About the Author

Kayne McGladrey is a professional services director at Integral Partners with 20+ years of experience. Kayne has presented on cybersecurity to IEEE-USA and created the first industry-recognized online class about the fundamentals for professional services management. He may be reached at kmcgladrey@ipllc.co.

The ISSA Journal on the Go!

Have you explored the versions for phones and tablets?

Go to the Journal home page and choose "ePub" or "Mobi."

Mobile Device ePubs

- ePubs are scalable to any size device: iPad/tablet provide an excellent user experience
- You'll need an ePub reader such as iBooks for iOS devices

NOTE: choose ePub for Android & iOS; Mobi for Kindles

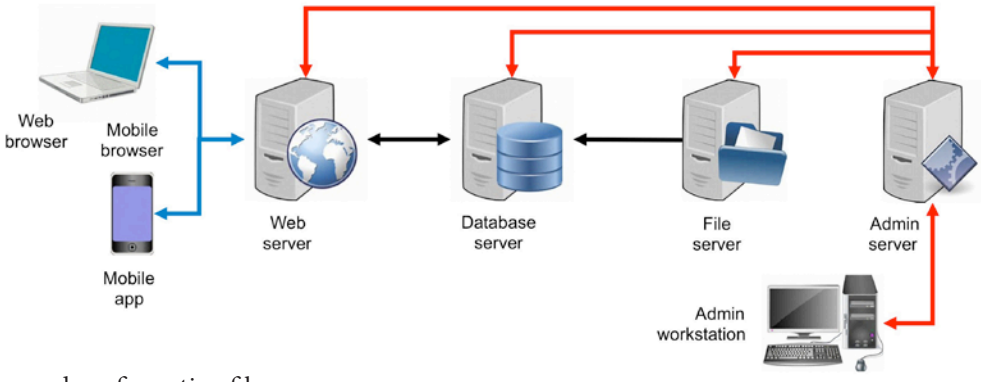
Take them with you and read anywhere, anytime…

Cryptographic Architectures: Missing in Action

By Jeff Stapleton – ISSA member, St. Louis Chapter

Documenting network topology, information technology, and system architectures are common development methods. However, cryptographic architectures are often ignored due to lack of knowledge or overlooked to avoid complexities. This article discusses the critical importance of identifying and understanding the cryptographic architectures.

Figure 1 – Application architecture



Every development project has various disciplines interwoven to achieve its goals. Project managers strive to keep schedules on target and within budget. Business analysts help define requirements and work with software developers to test solutions. Network engineers design and implement the hardware and relevant operating systems. Administrators install and maintain the associated software and configuration files. Information security professionals assist the project teams with ensuring compliance to the organization's and appropriate industry standards, reviewing security controls, and assessing the associated risks with fraud managers and business analysts. But cryptography and key management, a critical aspect, is often overlooked.

Regardless of the development methodologies used within the project, there are typical artifacts generated by the various teams. Documenting network topology, information technology, and system architectures are common project artifacts. For example, figure 1 illustrates a possible application architecture. While some network architects might call this "a cartoon" versus a more technical network diagram, nonetheless it provides an overview for team discussion purposes. The idea for this type of diagram is to avoid what some might call "getting lost in the weeds" and yet give a synopsis of the application flows, data storage, and user communities. For this scenario, users access an online application via a webserver, which is connected to a database server managed by a file server with system-wide administrative access via an admin server.

Application architectures

Figure 1 shows a logical information flow from left to right. Customers interface to an online webserver using a computer or mobile browser, or a mobile app. From a business perspective the web service is presumed to be agnostic with regards to the user experience; however, the information and protocols between the various client endpoints is often optimized and customized. Web and mobile browsers need formatting information (e.g., colors, fonts, images) in addition to the actual displayed data, while mobile apps are preformatted and only need the display data. An information security profession needs to keep those types of technology facts in mind when discussing these information flows. Mobile apps can be embedded with specific security credentials (e.g., cryptographic keys, digital certificates) and store other credentials (e.g., passwords) within a secure element. Conversely,

browsers can only rely on generic digital certificates and must download specific credentials or have users enter passwords. The webserver and user endpoints represent the application front-end process.

Figure 1 also depicts back-end processing consisting of the database server and the file server. The webserver interfaces to the database server. Client requests are received from the endpoints to the webserver, submitted to the database server by the webserver, information is returned from the database server to the webserver, and responses sent to the clients by the webserver. Further, data updates and configuration parameters are sent to the database server from the file server. All of the front-end and back-end servers are managed by various administrators. Servers often authenticate themselves to each other and sometimes communicate using security protocols such as Secure Socket Layer[1] (SSL), Transport Layer Security[2] (TLS), or Internet Protocol Security[3] (IPsec).

Figure 1 further shows administrative (admin) processing consisting of the admin server and admin workstation. The admin server communicates to the web, database, and file servers. The various application, database, and system administrators use the admin workstation. Administrators often authenticate to servers using Secure Shell[4] (SSH) with passwords or digital signatures. Notable the diagram only shows a single client endpoint for each type, a single server for each type, and a single admin workstation. However an information security professional needs to keep in mind that the actual implementation would include multiple servers likely deployed in multiple data centers. Further, there would be multiple endpoint types and multiple admin workstations.

While the application architecture shown in figure 1 might be a simplistic overview, it does provide an information security professional a basis for assessing risks. For example, the front-end security controls might include mutual authentication between the clients and the webserver. The browsers (or mobile app) must be able to accept the webserver certificate by sharing a common public key infrastructure[5] (PKI). Likewise, the webserver must be able to accept the client certificates by sharing a common PKI. However, the two PKI might not be the same; thus each PKI has a different trust anchor, also called a root certificate authority (CA). Likely, the webserver would use a publicly available PKI to enable as many browsers as possible to accept its certificate. Conversely, the webserver might use a private PKI for the mobile app since the mobile app is specific to the webserver. Similarly the mobile app might use the same private PKI in order for the webserver to accept its client certificate. However, browsers might use a public PKI or a private PKI depending on the application business requirements.

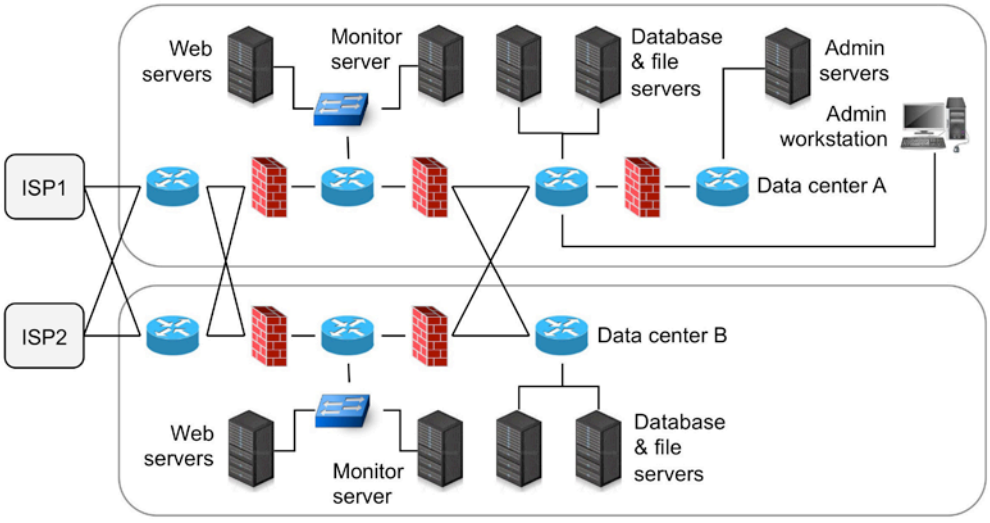


Figure 2 – Network architecture

As another example, the back-end controls might address network security between the webserver and the other servers, access controls for the database and file servers, and database encryption. Basically the security controls for confidentiality, authentication, and integrity[6] need to be considered. Secure connections such as TLS or IPsec between the various servers would likely use a private PKI but could employ a public PKI. However, servers running on an internal network behind firewalls and a demilitarize zone (DMZ) would have problems accessing a certificate revocation list[7] (CRL) or an online certificate status protocol[8] (OCSP) responder on the Internet. Database encryption is relatively new technology such that no industry standards yet exist with vendor proprietary solutions. Further, the admin security controls should cover separation of duties, administrator multi-factor authentication, authorization, and network security including SSH asymmetric keys. To address these issues, the information security professional needs a more detailed network architecture shown in figure 2.

1 RFC 6101 The Secure Sockets Layer (SSL) Protocol Version 3.0, August 2011 – https://www.rfc-editor.org/info/rfc6101.

2 RFC 5246 The Transport Layer Security (TLS) Protocol Version 1.2, August 2008 – https://www.rfc-editor.org/info/rfc5246.

3 RFC 4301 Security Architecture for the Internet Protocol, December 2005 –https://www.rfc-editor.org/info/rfc4301.

4 RFC 4252 The Secure Shell (SSH) Authentication Protocol, January 2006 – https://www.rfc-editor.org/info/rfc4252.

5 J. J. Stapleton and W. Clay Epstein, *Security without Obscurity: A Guide to PKI Operations*, CRC Press, Taylor & Francis Group, ISBN 9781498707473 - CAT# K24892, February 2016

6 J. J. Stapleton, *Security without Obscurity: A Guide to Confidentiality, Authentication, and Integrity*, CRC Press, Taylor & Francis Group, ISBN 9781466592148 - CAT# K20548, May 2014

7 RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, May 2008 – https://www.rfc-editor.org/info/rfc5280.

8 RFC 6960 X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, June 2013 – https://www.rfc-editor.org/info/rfc6960.

Network architectures

Figure 2 shows two Internet service providers (ISP1 and ISP2) connecting to a network deployed in two data centers (data center A and data center B) with multiple layers. Both data centers have an external router, which allows each ISP to cross connect to each other. The first and second firewalls represent a DMZ which protects the internal network from external connections. Another router within the DMZ routes network traffic to the web service but is also connected to a switch which replicates the network traffic to a monitoring server. Note that the monitoring servers were not included in the previous application architecture. It is a common situation that often one team or another is unaware of the overall design such that some information is lacking in the documentation. This knowledge gap is demonstrated by the presence of the switch acting as a data tap for the monitoring servers.

Figure 2 also depicts the internal network consisting of the database and file servers duplicated in both data centers. The internal networks have another cross connection allowing the database servers and the file servers to synchronize information. Note that data center A also shows an admin server behind an internal firewall. This type of network architecture is often called a secure zone; it is essentially a means to isolate a critical system such as the admin server. However, also note that the admin workstation connects to the internal network and so must connect to the admin server through the internal firewall. This is another example of a knowledge gap that is undocumented in the application architecture.

While the network architecture shown in figure 2 provides a more realistic viewpoint, it also offers an information security professional with more information for further assessing risks. For example, the network traffic on the webservers is transitory, but the monitoring servers represent a previously unknown permanent data store that retains copies of the network traffic. The current design shows the monitor server deployed in the DMZ and not on the internal network. Essentially the complete history of the webserver traffic is one firewall away from the Internet. Further, in order for the monitor server to access the encrypted webserver traffic, the webserver TLS keys are duplicated on the monitor server so the key negotiation can be replicated and the session keys can be determined. However, the security professional might consider running the monitor server inside the DMZ an unacceptable risk.

Conversely, the security professional would consider the admin server running in its own secure zone behind an internal firewall an acceptable lower risk. However, based on the network diagram the security professional has no information about admin access, separation of duties, approval procedures, or other management processes. Further, the network diagram does not provide any information about cryptography or key management so a cryptographic architecture is needed. But the nature of the cryptographic architecture might be adding cryptography and key management information to the existing application or network diagrams, or developing a new diagram specifically for the cryptographic architecture.

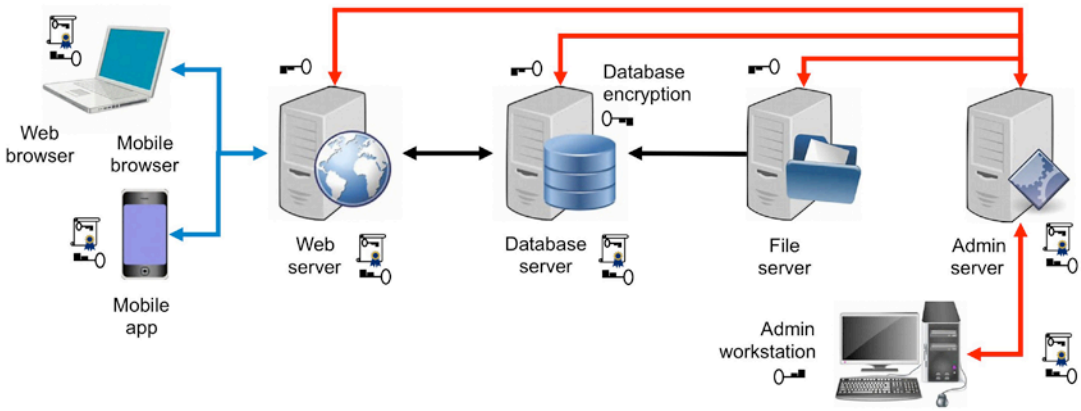


Figure 3 – Application with crypto architecture

Cryptographic architectures

Figure 3 is a duplicate of the application architecture from figure 1 with cryptographic information added to the diagram. The web browsers, mobile app, webserver, and database server are shown with a digital certificate and a private key. The certificates are used with the TLS protocol to establish session keys between the communicating parties. Thus, the web browser, the mobile browser, or the mobile app can establish a TLS connection to the webserver. Similarly, the webserver can establish a TLS connection to the database server and the admin server can establish a TLS connection to the various admin workstations. Further, each admin workstation has an SSH private key used for digital signature authentication, and the webservers, database servers, and file servers have the corresponding SSH public key to verify the digital signature. Also shown is a database encryption key. Thus, reusing the application architecture helps document some of the keys, but it does not provide network architecture or cryptographic protocol information.

Figure 4 is a duplicate of the network architecture from figure 2 with cryptographic information added to the diagram. The various TLS certificates and private keys are shown for the webservers, the monitoring servers, the database servers, the admin server, and the admin workstations. The SSH public keys are shown on the webservers, the monitoring servers, the database servers, and the file servers with the corresponding SSH private keys on the admin workstations. The IPsec private/public key pairs are also shown on the external routers for the cross connections between the two ISPs. However, what is not shown is the database encryption keys since

they are not part of the network topology and the TLS client certificates since the browsers and mobile devices are not included in the network diagram. Thus, reusing the network architecture helps document some of the keys, but it does not provide application architecture or cryptographic protocol information.

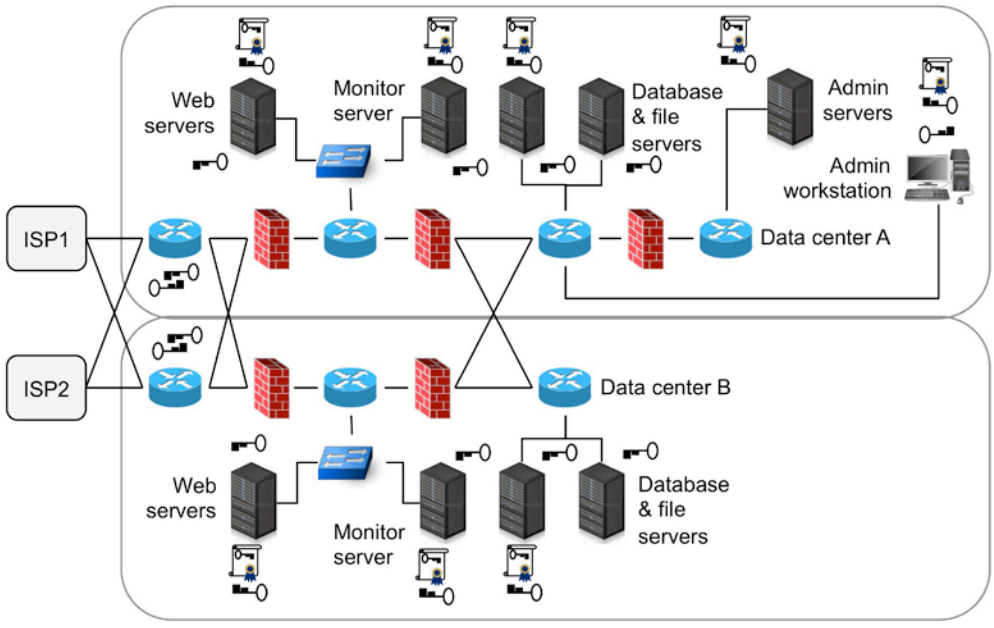


Figure 4 – Network with crypto architecture

Figure 5 is the cryptographic architecture, a separate diagram that borrows relevant data from the application and network architectures and provides cryptographic information including the various cryptographic protocols (IPsec, HTTPS, TLS, SSH), PKI, and database encryption. Database encryption solutions often use a database encryption key in memory but attempt to avoid storing the cleartext key using a variety of obfuscation and key management methods including cryptographic hardware security modules[9] (HSM). However, many implementations rely on password-based key derivation functions[10] (PBKDF) or misuse encrypted data as a cryptographic key. Thus, the security professional needs to assess the database encryption key management[11] methodology.

Figure 5 shows secured Hypertext Transfer Protocol (HTTPS) between public devices and the webserver. Thus the webserver has an asymmetric key pair consisting of a private key and a public key certificate. Because any public device can connect to the webserver, mutual authentication is not a realistic option as the device might not have a Transport Layer Security (TLS) certificate that the server can trust. Further, the webserver needs to share a TLS certificate that the public device can trust. Therefore, the webserver might get its TLS certificate from a publicly trusted certification authority (CA) for which the public device will have the CA certificates already installed. Alternatively the webserver might use a TLS certificate issued from a private CA but whose CA certificates would need to be installed on each of the public devices. Thus, the information security professional needs to assess the design of the public key infrastructure[12] (PKI) for the webserver.

Figure 5 also shows an Internet Protocol Security (IPsec) connection between the external routers. As discussed for figure 2 this allows a cross connection between the two data centers. IPsec allows the routers to authenticate each other over an encrypted tunnel. However, IPsec requires that both routers have asymmetric keys consisting of a private key and a public key, but depending on the key management schema used, a digital certificate might not be employed. The information security professional needs to understand the key management method supported by the routers.

9 Federal Information Processing Standard (FIPS) 140-2 Security Requirements for Cryptographic Modules, May 2001 – http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf.

10 RFC 2898 PKCS #5: Password-Based Cryptography Specification Version 2.0, September 2000 – https://www.rfc-editor.org/info/rfc2898.

11 X9.73 Cryptographic Message Syntax – ASN.1 and XML, 2017 – http://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+X9.73-2010+(R2017).

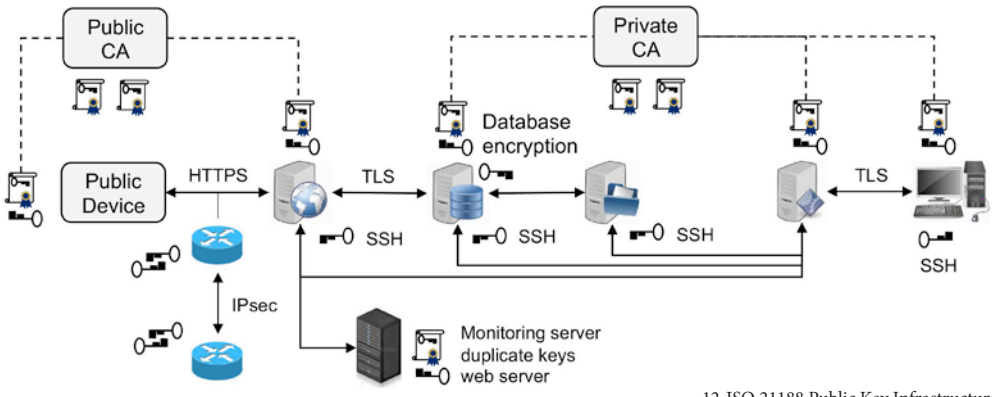


Figure 5 – Cryptographic architecture

Figure 5 shows the webserver keys duplicated on the monitoring server. As discussed for figure 2 the switch in the DMZ duplicates the network traffic. Because the monitor server shares the same TLS keys, it can renegotiate the same TLS session keys and decrypt the traffic. The monitoring servers can then data mine the network traffic for customer inter-

12 ISO 21188 Public Key Infrastructure for Financial Services — Practices and Policy Framework, 2006 – https://www.iso.org/obp/ui/ - iso:std:iso:21188:ed-1:v1:en.

actions, response times, and clicks. As further discussed for figure 2, the monitoring server retains copies of the network traffic. Thus, in addition to it having copies of the webserver keys, the monitoring server also has its own data encryption key. The information security professional needs to determine the data encryption and the key storage methods.

Figure 5 shows TLS between the webserver and the database server. Since this is an internal connection, mutual authentication is possible. The webserver might reuse its TLS certificate issued from the public CA and the monitoring server can use a TLS certificate issued from the organization's private CA. However, the monitoring server might not be able to validate the certificate status of the webserver's certificate because it might not be able to access the public CA certificate revocation list (CRL) or its online certificate status protocol (OCSP) responder. Alternatively the webserver might have another TLS key pair whose certificate is issued from the private CA. The information security professional needs to assess the design of the public key infrastructure (PKI) for the webserver and the monitoring server. Further, the information security professional needs to note that no TLS connection is shown between the database server and the file server.

For each of these scenarios the information security professional needs to understand the cryptographic architecture.

Figure 5 shows TLS between the admin server and the admin workstation. Again, since this is another internal connection, mutual authentication is possible. Further, since both machines reside within the internal network both can use TLS certificates issued from the private CA whose CRL or OCSP are accessible. Again, the information security professional needs to assess the design of the PKI for the webserver and the monitoring server.

Figure 5 shows Secure Shell (SSH) connections between the admin server and the web, database, and file servers. The admin server has an SSH key pair whose public key is stored on the web, database, and file servers for authentication. Administrators log onto the admin workstations, which establishes a TLS connection to the admin server, and then the admin server connects via SSH to the appropriate server for management and maintenance purposes. The information security professional needs to assess the design of the SSH key management scheme.

Another aspect the information security professional needs to consider is where the various TLS tunnels terminate. The IPsec tunnel endpoints terminate at the routers so no decrypted information is exposed outside the routers. However, the TLS tunnel endpoints might not terminate at the actual servers. For example, the HTTPS connection might terminate at the external DMZ firewall shown in figure 2 and not the actual webserver. If this were the case, then the network

ADVERTISE STRATEGICALLY

Surround our monthly themes with your organization's products and services...

FEBRUARY 2018
Legal, Regulations, Ethics

MARCH
Operational Security - Infosec Basics

APRIL
Internet of Things

MAY
Health Care & Security Management

JUNE
Practical Application and Use of Cryptography

JULY
Standards Affecting Infosec

AUGUST
Foundations of Blockchain Security

SEPTEMBER
Privacy

OCTOBER
Security Challenges in the Cloud

NOVEMBER
Impact of Malware

DECEMBER
The Next 10 Years

ISSA JOURNAL

Contact Sean Bakke
sean.bakke@issa.org

IT'S GOOD FOR BUSINESS

traffic would be unencrypted (cleartext) between the external firewall and the webserver within the DMZ. Likewise, the TLS tunnel between the webserver and the database server might terminate at the internal DMZ firewall. For this latter case the network traffic would be cleartext across the internal network. Similarly, the TLS tunnel between the admin workstation and the admin server might terminate at the secure zone firewall. For each of these scenarios the information security professional needs to understand the cryptographic architecture.

Conclusion

In summary, any development project produces artifacts such as an application architecture and a network architecture, but all too often the cryptographic architecture is overlooked. In the example architectures we considered several cryptographic protocols including HTTPS, TLS, IPsec, and SSH including symmetric keys, asymmetric keys and digital certificates. Modern day architectures have evolved with cryptography almost everywhere. Consequently, the critical nature of the cryptographic architecture needs to be included by information security professionals.

About the Author

Jeff Stapletonhas been involved in the development of ANSI and ISO standards for over 20 years, has chaired the X9F4 standards workgroup for over 15 years, and is the author of the Security without Obscurity *book series. He can be contacted via jjs78023@yahoo.com.*

Fueling Organizational Success via Global SIG-Enabled Engagement

Continued from page 9

We can best undertake future organizational success programs by focusing on member and volunteer engagement as aligned to the ISSA mission, vision, and goals. Recent research on non-profit member engagement, as depicted in the infographics in figures 1 through 3, show that we, as an organization, need to pay special attention to the generational needs of each population being served, and focus on the activity types that will keep our members and community partners highly engaged going forward [2].

Additionally, due to the decentralized hub-and-spoke organizational model that the ISSA Intl Global SIG program uses, volunteer engagement is also key to the organizational success model. Primarily this means charting a strong strategic vision and strategy that includes:

- Understanding volunteer motivations and trends [what drives them]
- Creating a vision for volunteer engagement [a strategy taking into account table 1 and table 2 data]
- Maximizing the investment in volunteers [personnel and management strategies and how to move from ideation to implementation]
- Minimizing challenges and embracing opportunities [leadership development that facilitates high levels of volunteer engagement]

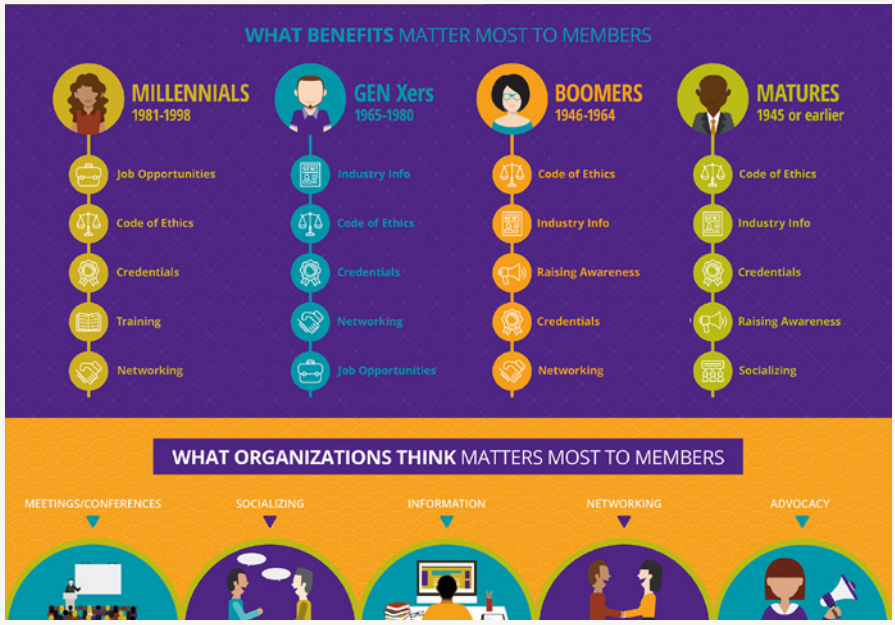


Figure 2: Member engagement – What matters most (2 of 3)

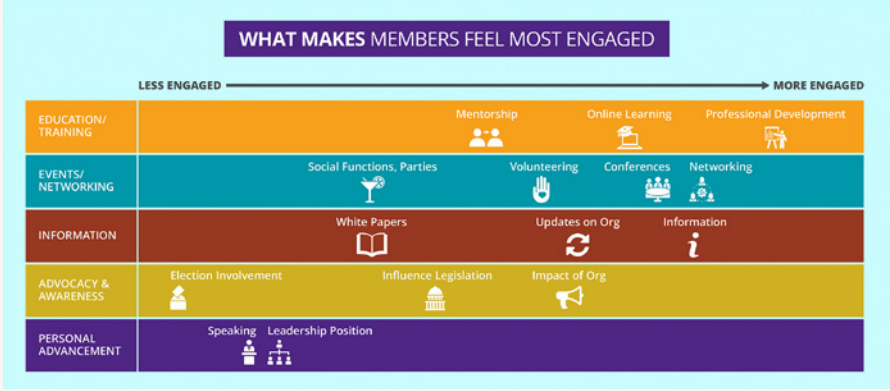


Figure 3: Member engagement – What matters most (3 of 3)

CONNECTION TO SERVICE			
		Affiliation Focus	**Skill Focus**
Time for Service	**Short-term (periodic)**	**Examples of Service:** • Corporate days of service with work teams • Weekend house-build by a local service club • Park clean-up event or trail maintenance • Walkers, bikers, runners for annual fundraiser **Traits of Volunteer:** • Strong sense of connection to the cause, work group, club, or organization • Generally expects a well-organized event (materials and instructions immediately available to perform task, etc.) • May be using the service opportunity to investigate a particular organization • May be part of a service group or meeting service requirements of a school, workplace, or club • May have unrealistic/naïve expectations about the ability to impact clients or long-term work of the organization • May prefer to identify with their service club or company rather than the organization being served	**Examples of Service:** • A one-time audit of an organization's finances by a professional accountant • A sports club teaching a youth group a particular skill and hosting youth for an event • A student completing a degree requirement • A chef preparing a meal for a fundraiser **Traits of Volunteer:** • Seeks a service opportunity tailored specifically to engage the volunteer's unique skill, talent, or resources • May be any age, although slightly more likely to be adults with higher levels of skills/education • Likely expects mutuality (i.e., a peer-to-peer relationship within the organization—accountant to treasurer; event host to ED; etc.) • May seek to negotiate timing of service • Appreciates recognition that is tailored to the unique demands of the position • May prefer to think of self not as a "volunteer" but an intern, pro bono consultant, etc., or other functional title
	Long-term (Ongoing)	**Examples of Service:** • Mentor • Leader • Teacher • Advocate • Special needs population visitor • Host or docent • Manager • Auxiliary member or trustee **Traits of Volunteer:** • Volunteers may become "over-invested" in work of organization and make demands • Effective implementation time-consuming • Ongoing oversight important; dedicated volunteer management staff recommended • Staff buy-in essential • Volunteers need to be given a voice in organization's operations that affect them, informed of important changes, and updated on progress on key objectives	**Examples of Service:** • Pro bono legal counsel • Volunteer/no-cost services by a functional practitioner • Loaned executive • Board member **Traits of Volunteers:** • Similar to the quadrant to the left in commitment • Generally prefers to contribute through specialized skills and training • May elect to contribute talents through specialized service or may contribute time through policy and leadership roles such as board governance, visioning, etc. • Often expects volunteer management that reflects the cultural norms of the given specialty or skill • Often combines talent with dedication to the cause, although the talent brought to the cause may supersede an allegiance to the mission • May have historical ties to the organization or cause and/or may have a family member (or self) who has benefited from the services of organization • Expects staff support, assistance with resources necessary to the job, and recognition appropriate to work performed

Table 1: Volunteer involvement framework – Types of volunteers

Table 1 depicts the volunteer involvement framework that differentiates volunteers by their affiliation (cause or mission alignment) or skills (type of volunteer work being done) service focus, and their service availability times (short, time-bound contributions versus ongoing, long-term service) [3]. Table 2 depicts the likely opportunities, challenges, and liabilities associated with each volunteer type. By better understanding our prospective and current volunteers' needs, we can ensure our leadership approach, style, and interactions enhance our leadership and volunteer development programs to maximize global organizational performance, thus leading to greater success for our global member populations, our stakeholders, and the broader cybersecurity communities we serve.

As the global SIG chair torch passes to DJ McArthur in 2018 and beyond, please offer your support, advocacy, and expertise. We know that with all of your efforts, the global SIGs can reach the 2020 goals of service to all chapters, across all countries of the world.

References

1. Carol J. De Vita and Cory Fleming [editors]," Building Capacity in Nonprofit Organizations," The Urban Institute

CONNECTION TO SERVICE			
		Affiliation Focus	**Skill Focus**
Time for Service	**Short-term (periodic)**	**Opportunities:** • Can help promote organization, spread message, and build mailing list • Ideal for accomplishing short-term, intensive work to grounds or building • May use in database for advocacy, fund raising, or volunteer recruitment **Challenges:** • Not always possible to provide client-oriented service • Considerable advance planning required to assure that materials are available for large-scale service projects • Requires flexible schedule for staff leadership **Liability:** • Dependent on service project selected; best to notify insurance carrier of the date • May require an event rider on agency policy	**Opportunities:** • Great way to secure important assistance not otherwise available • Ideal training ground for more intensive service (e.g., committee, taskforce, or board work, as well as work in quadrant below) • Worthy addition to agency database • May use service opportunity to evaluate person for possible employment **Challenges:** • Poorly handled service opportunity may harm reputation of organization • Project preparation can be time consuming, may require considerable upfront support • If an internship, may require supervisor with same training background • May be a "cover" for a job search. If unemployed and finds a job, may leave volunteer assignment unfinished **Liability:** • Dependent on service project; investigate need for appropriate background check. • Long-term (Ongoing)
	Long-term (Ongoing)	**Opportunities:** • Strong mission-based, consequential outcomes likely • Worthy addition to agency database • Mechanisms for volunteer input strongly recommended • Capable, informed advocates for organization **Challenges:** • Volunteers may become "over-invested" in work of organization and make demands • Effective implementation time-consuming • Ongoing oversight important; dedicated volunteer management staff recommended **Staff buy-in essential** • Volunteers need to be given a voice in organization's operations that affect them, informed of important changes, and updated on progress on key objectives **Liability:** • Check requirements for appropriate background checks; Should be performed if volunteer works with vulnerable clients • Should carry some form of liability policy • May need to offer mileage or other forms of expense reimbursement	**Opportunities:** • High performer eager to further organization's work • Brings critical skill set to meet agency's needs • Strong representative in the community, likely to be an able advocate • May prove to be an able recruiter, "buddy," or orientation leader for new volunteers • May be an early retiree eager to be meaningfully involved • If not on the board, may be considered for board position **Challenges:** • Volunteer may need care and attention including dedicated workstation and computer and direct line to COO/ED • Other staff and volunteers must be knowledgeable about this person's role and open to engaging this person in deliberations that will affect the given area of work • Generally speaking, there are more volunteers eager for these types of assignments than there are non-profits ready to engage them • May perceive that he/she can "fix" the agency **Liability:** • If behaviors prove problematic, may require formal honor and retirement to move individual out of service • Should strongly consider directors and officers Insurance

Table 2: Volunteer involvement framework – Opportunities, challenges, and risks

(April 2001) – http://research.urban.org/UploadedPDF/building_capacity.pdf.

2. Abila, "Infographic: Member Engagement Study Overview," Abilia – http://www.abila.com/resource-library/infographic/what-drives-member-engagement/.
3. Sarah Jane Rehnborg et al, "Strategic Volunteer Engagement: A Guide for Nonprofit and Public Sector Leaders," The University of Texas at Austin (May, 2009) – https://www.volunteeralive.org/docs/Strategic Volunteer Engagement.pdf.

About the Author

Dr. Rhonda Farrell, D.Sc., J.D., CISSP, CSSLP, CCMP, CMQ/OE, CSQE is an Associate at Booz Allen Hamilton (BAH), a member of the Board of Directors at ISSA International, and an ISSA Distinguished Fellow. She is the Global SIG Co-Chair (Lead), the ISSA Intl Co-Founder of the Women in Security Special Interest Group (WIS SIG) and works cross-organizationally to actively enhance cybersecurity-oriented programs internationally. She can be reached at rhonda.farrell@issa.org.

Cyberwar and International Law

By Luther Martin – ISSA member, Silicon Valley Chapter and Cheryl He

There is a lot of discussion of cyberwar these days, though much is not based on a careful understanding of what might reasonably be called "cyberwar." The authors look at what existing international law tells us about cyber attacks and at what recent cyber incidents might reasonably be considered to be serious enough to be considered something more than annoying attacks by hackers.

Abstract

There is a lot of discussion of cyberwar these days. Much of this discussion has one thing in common: it is not based on a careful understanding of what might reasonably be called "cyberwar." Here, we look at what existing international law tells us about cyber attacks and look at what recent cyber incidents might reasonably be considered to be serious enough to be considered something more than annoying attacks by hackers. This point of view both explains the limited nature of the damage caused by most cyber attacks that have occurred to date and lets us speculate on what the future will bring.

Armed conflict is surprisingly common. The "Global Peace Index 2016"[1] report by the Institute for Economics & Peace suggests that only 10 of the 163 countries for which they collect data are not participating in some sort of conflict today. Peace is very uncommon. As more participants in today's conflicts develop the capability to attack the computer systems of their opponents, it seems likely that more conflicts will involve some type of cyber attack.

Many cyber attacks to date have targeted civilian infrastructure rather than government systems and have stayed below a threshold that we will explain below, while the relatively low costs to their perpetrators have resulted in such attacks becoming increasingly common. Because any business may find itself as a target of cyber attack, they are a threat that CISOs should think about, and perhaps even plan for.

The law of war

There may have been rules to warfare for as long as men have been fighting wars. Some of the world's oldest literature describes rules that warring parties should follow.

In the *Mahabharata* (c. 1000 BC), Book 12, the "Book of Peace,"[2] lists rules for warfare, some of which should still sound reasonable to us today. It limits what weapons allowed in war: "There should be no arrows smeared in poison, nor any barbed arrows—these are the weapons of evil people." It has rules for treating the wounded: "One wounded should be given medical treatment in your realm; or he may even be sent to his own home." And it has rules for humane treatment of prisoners of war: "If [you have] captured a man who has discarded his sword, whose armor is broken to pieces, who pleads with his hands folded in supplication, saying, 'I am yours,' then [you] should not harm that man."

Today, the law of war comprises two bodies of law: one defines when the use of force is justified (*jus ad bellum*, Latin for "right to war"); the other governs how belligerents need to conduct themselves during a conflict (*jus in bello*, Latin for "right in war"). Here, we are not really interested in justifying starting cyber conflicts. That is not something that most corporate IT departments think about doing, so understanding the application of *jus ad bellum* to cyber conflicts is probably not important. But since it turns out to be easy for businesses to become involved in cyber conflicts, particularly as targets, understanding how *jus in bello* may apply is more interesting.

The *jus in bello* aspect of the law of war is currently defined by the four Geneva Conventions and three additional Proto-

1 "Global Peace Index 2016," Institute for Economics & Peace – http://visionofhumanity.org/app/uploads/2017/02/GPI-2016-Report_2.pdf.

2 Fitzgerald, James L., ed. *The Mahabharata, Volume 7*. University of Chicago Press, 2003.

cols[3] that were added after the last Convention was ratified. The Geneva Conventions were first ratified in 1864. They were updated in 1906, 1929, and finally in 1949. Since 1949, three additional Protocols have been ratified. Two were added in 1977 and a third in 2005.

Signatories of the Conventions and the additional Protocols agree to only engage in warfare within what is allowed by the Conventions and the additional Protocols. If an opponent violates the rules of warfare, the injured party is allowed to conduct reprisals, but they must be appropriate to the injury received. The legal concept of *lex talionis*, the law of proportionality, needs to cover any such reprisals.

Note that limits for what actions are allowed by participants in a conflict do not have to be formal laws or treaties. In the Cold War, espionage was carried out within a set of guidelines that both sides informally agreed to and generally followed.

Treaties and the prisoners' dilemma

A situation called the "prisoners' dilemma"[4] may explain why this is true. A prisoners' dilemma[5] is a situation when two or more parties will all benefit from cooperating, but each will individually benefit more from non-cooperation at the expense of the others. When this happens, we should expect all parties to choose to not cooperate with the others. An example of this is when two or more parties decide whether to obey a treaty or to cheat on it.

If all parties agree to not develop nuclear weapons, for example, then all parties are safer. But if one party cheats, it gains an advantage over the others who have not developed their own nuclear weapons. In this situation, we should expect all parties to cheat on a treaty that bans nuclear weapons, or, perhaps even more likely, to not agree to such a treaty in the first place. Thus all parties need an incentive to not cheat in order for rules, either formal or informal, to be generally followed.

Cyber weapons may offer compelling advantages. They are generally relatively inexpensive to develop compared to the cost of conventional weapons like tanks, aircraft, submarines, or aircraft carriers. The US Government Accountability Office (GAO) estimates that the US government will spend over $54 billion on the F-35 Joint Strike Fighter program between the years 2015 and 2019[6] and that the program will probably end up costing about $1.5 trillion over its complete life cycle (research, development, procurement, operation, maintenance, etc.).[7]

An investment of the same $54 billion over a five-year period in cyber weapon research is likely to result in weapons that are capable of both crippling the economies of many nations and rendering many modern weapon systems ineffective—something that even the very capable F-35 alone probably cannot do. And an investment of $1.5 trillion over a few decades might even produce cyber weapons that are closer to science fiction than to those that we see today. So the significant capabilities that they may provide at a relatively low cost may make cyber weapons seem compelling to both state and non-state actors.

It may be relatively easy to use such weapons against adversaries while still maintaining a plausible level of deniability due to the largely anonymous nature of the Internet. Cyber attacks can be far more humane than the alternatives. Crippling a country's banking infrastructure may cause a very high level of economic damage, but without the level of death and destruction that accompanies the use of conventional weapons.

Because of these advantages, the prisoners' dilemma may lead to the universal development of cyber weapons, perhaps even to a cyber arms race. Controlling these weapons will be problematic until both governments and non-government entities have a strong incentive to agree to limits on developing or using them. But it is also likely that the use of cyber weapons will be limited by the existing law of war, so indiscriminate and all-out cyberwar is probably unlikely.

The law of cyberwar

It may be useful to think of all conflicts involving two types operations: conventional and cyber. At one end of the spectrum we have operations that only use traditional forms of force, while at the other end are operations carried out purely through the use of computers. Conflicts can also exist somewhere between the two extremes, involving some conventional operations and some cyber operations. It is clear how the law of war limits acceptable behavior in purely conventional operations, but it turns out that the existing law of war also can be interpreted in a way that applies to cyber operations. The most notable discussion of this is contained in the *Tallinn Manual*.[8]

The *Tallinn Manual* was written between 2009 and 2012 by a group of subject matter experts in a project organized by the NATO Cooperative Cyber Defence Centre of Excellence[9] (CDCoE) (based in Tallinn, Estonia). The output of this project reflects the views of the contributors as to how well the existing law of war can be applied to cyberwar. The consensus of the experts was that the existing law of war can easily be interpreted in a way that applies to actions in cyberwar.

Of particular interest is the way that the *Tallinn Manual* describes what qualifies as "armed attacks" in the cyber world. This is particularly relevant because the term "act of war"

3 ICRC, "Geneva Conventions of 1949 and Additional Protocols, and their Commentaries" International Committee of the Red Cross – https://ihl-databases.icrc.org/applic/ihl/ihl.nsf/vwTreaties1949.xsp.

4 Avinash Dixit and Barry Nalebuff, "Prisoners' Dilemma," Library of Economics and Liberty – http://www.econlib.org/library/Enc/PrisonersDilemma.html.

5 Tucker, Albert W. "The mathematics of Tucker: a sampler." *The Two-Year College Mathematics Journal* 14, no. 3 (1983): 228-232.

6 GOA, "F-35 Joint Strike Fighter: Assessment Needed to Address Affordability Challenges," US Government Accountability Office – http://www.gao.gov/products/GAO-15-364.

7 Joint Strike Fighter Program, "F-35 Lightning II Program Fact Sheet Selected Acquisition Report (SAR) 2015 Cost Data," US Department of Defense – http://www.jsf.mil/news/docs/20160324_Fact-Sheet.pdf.

8 Schmitt, Michael N., *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge University Press, 2013.

9 NATO Cooperative Cyber Defence Centre of Excellence – https://ccdcoe.org/.

is a political term with no precise meaning, while the term "armed attack" has a clear legal definition. Treaties and similar agreements define what actions will be taken or can be taken in the event of an armed attack; they do not specify what actions can be taken in response to an act of war.

In particular, the *Tallinn Manual* uses the effects of a cyber attack to judge whether or not it qualifies as an armed attack. Cyber attacks that cause effects that are similar to what kinetic weapons (guns, bombs, etc.) cause count as the equivalent of an armed attack. Guns and bombs do not temporarily shut down banks or temporarily take down websites. They cause more physical and permanent damage. Many, perhaps even almost all, cyber attacks fall short of the *Tallinn Manual's* definition of armed attacks. This limits the options that national governments have for responding to these attacks, at least if they want to stay within the limits imposed by international law.

Estonia (2007)

In 2007, the government of Estonia decided to relocate the Bronze Soldier, a memorial to the victory of the Soviet Army over Nazi Germany. The government moved the memorial from a central location in the capital city of Tallinn to the nearby Tallinn Military Cemetery. This provoked riots in the streets of Tallinn. Soon, cyber attacks against many Estonian government and commercial targets were underway. Hackers carried out denial of service and distributed denial of service attacks against government and private-sector websites, including the those of the Riigikogu (Parliament), as well as the Estonian prime minister and president. Many government ministries, e-banking organizations, and news outlets also suffered attacks.

The effects of these attacks are not the same as would have been caused by kinetic weapons. It seems very likely that the cyber attacks that occurred in this incident did not qualify as armed attacks, so the government of Estonia and its allies would have been somewhat limited in their options for retaliating. In particular, any military action would almost certainly not have been justified in this particular case.

Stuxnet (2009)

While there are many descriptions of the Stuxnet worm and its effects, there are very few facts available concerning this incident. What we do know for sure is that some time in 2009 a worm appeared on the Internet that seemed to target ranges of IP addresses in Iran, and that this worm seemed to target certain industrial control systems—the centrifuges that were being used in uranium enrichment operations by the government of Iran.

Once it infected the control systems for the centrifuges, Stuxnet seemed to increase the rate at which centrifuges would spin, possibly causing damage to them by making them spin faster than they were meant to operate. This could potentially cause an increase in the failure rate of the centrifuges that could be very difficult to troubleshoot.

ISSA Journal 2018 Calendar

Past Issues – digital versions: click the download link:

JANUARY
Best of 2017

FEBRUARY
Legal, Regulations, Ethics

MARCH
Operational Security — the Basics of Infosec
Editorial Deadline 1/15/18

APRIL
Internet of Things
Editorial Deadline 2/15/18

MAY
Health Care & Security Mangement
Editorial Deadline 3/15/18

JUNE
Practical Application & Use of Cryptography
Editorial Deadline 4/15/18

JULY
Standards Affecting Infosec
Editorial Deadline 5/15/18

AUGUST
Foundations of Blockchain Security
Editorial Deadline 6/15/18

SEPTEMBER
Privacy
Editorial Deadline 7/15/18

OCTOBER
Security Challenges in the Cloud
Editorial Deadline 8/15/18

NOVEMBER
Impact of Malware
Editorial Deadline 9/15/18

DECEMBER
The Next 10 Years
Editorial Deadline 10/15/18

If you have an infosec topic that does not align with the monthly themes, please submit. All articles will be considered. For theme descriptions, visit www.issa.org/?CallforArticles.

EDITOR@ISSA.ORG • WWW.ISSA.ORG

But essentially all that we know about Stuxnet is based on rumors. Many news stories have described in detail how the governments of the US, Israel, and Germany worked together to create and deploy Stuxnet. And many news stories and other reports have explained how the effects of Stuxnet delayed the Iranian nuclear program by degrading its ability to refine fissionable isotopes of uranium. But there are few, if any, facts to support these entirely plausible conclusions. A good summary of what is really known about Stuxnet and its effects is contained in the NATO CDCoE report "Stuxnet – Legal Considerations," by Katharina Ziolkowski.[10]

None of the governments of the US, Israel, or Germany has officially admitted to taking part in the development or deployment of Stuxnet. And the government of Iran has never officially admitted that any of the centrifuges used in their nuclear program were damaged by Stuxnet.

There is no hard evidence that Stuxnet had any significant effect at all.

There is no hard evidence that Stuxnet had any significant effect at all. The centrifuges used in the Iranian nuclear program were notoriously prone to failure,[11] and it is not clear that the number of centrifuges bought by the Iranian government increased after Stuxnet appeared on the Internet, suggesting that it might not have significantly affected the Iranian nuclear program at all.

In the absence of any reliable information, it is hard to judge whether or not Stuxnet was damaging enough to qualify as the equivalent of an armed attack, but Ziolkowski's legal analysis suggests that it was not just a clever bit of technology. Stuxnet was carefully tailored to keep its effects from violating international law, which could have justified any possible retaliation by Iran: "Under the supposition that the malicious software has been created, installed, and controlled by one or more States and indeed did not cause any damage of physical nature, it appears not to reach the threshold of illegality pursuant to public international law and thus to be a 'legal masterpiece.'"

So the best information available suggests that Stuxnet probably did not cause enough damage to qualify as an armed attack. This means that the government of Iran probably would not have been justified in using armed force to retaliate against one or more countries that it might have suspected carried out the Stuxnet attack.

German steel mill (2014)

In December 2014, the German government's Bundesamt für Sicherheit in der Informationstechnik (BSI) (Federal Office for Information Security) released their annual findings report "Die Lage der IT-Sicherheit in Deutschland 2014" ("The State of IT Security in Germany 2014").[12] This report describes a successful cyber attack on an unspecified German steel mill, although it provides few details. This attack apparently compromised the control systems for the steel mill and resulted in significant physical damage to at least one of the blast furnaces used in the mill.

Of all of the cyber attacks publicly known, this attack seems to come the closest to counting as an armed attack because there was significant physical damage caused by it. While the damage caused may not have been exactly like the damage that would have been caused by guns or bombs, it was probably very similar. It might have been similar enough to the effect of kinetic weapons to have counted as the equivalent of an armed attack.

Because there have been very few cyber attacks that cause significant physical damage, it may be the case that this particular cyber attack is the only attack to date that might reasonably be considered to be equivalent to an armed attack; it is also the only one that might reasonably be considered serious enough to justify a military response by the affected country.

Summary

There are compelling reasons why participants in twenty-first century conflicts would engage in cyberwarfare. Cyber weapons are almost certainly much less expensive to develop and use than conventional weapons, and the anonymity provided by the Internet can make it extremely hard to reliably identify exactly who carried out a cyber attack. Launching damaging cyber attacks against government or military targets will almost certainly be regarded as an act of war by politicians, so many participants in the cyber attacks have largely restricted their attacks to non-government and non-military targets. Cyber attacks have generally not caused the type of physical damage that might classify them to being equivalent to an armed attack, thus limiting the ways in which governments can respond. If this trend continues in the future, businesses may unwillingly become targets in cyber conflicts.

So it certainly looks like businesses are on the front lines of cyberwar, whether they want to be or not. A reasonable precaution is thus to hope for the best (not being the target of a cyber attack) but to be prepared for the worst (that you will end up being the target of a cyber attack).

About the Authors

Luther Martin is a Distinguished Technologist at Micro Focus. You can reach him at luther.martin@microfocus.com.

Cheryl He is a Software Engineer at Hewlett Packard Enterprise. You can reach her at cheryl.he@hpe.com.

10 Dr. iur. Katharina Ziolkowski, "Stuxnet–Legal Considerations," NATO CCDCoE (2012) - https://ccdcoe.org/sites/default/files/multimedia/pdf/Ziolkowski_Stuxnet2012-LegalConsiderations.pdf.

11 Greg Thielmann and Peter Crail, "Chief Obstacle to Iran's Nuclear Effort: Its Own Bad Technology," The Christian Science Monitor, Dec. 8, 2010 –http://www.csmonitor.com/Commentary/Opinion/2010/1208/Chief-obstacle-to-Iran-s-nuclear-effort-its-own-bad-technology.

12 "Die Lage der IT-Sicherheit in Deutschland 2014," Bundesamt für Sicherheit in der Informationstechnik – https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile.

Biometric Electronic Signatures

By Phillip Griffin – ISSA Fellow, Raleigh Chapter

This article discusses mutual and multi-factor authentication based on passwords combined with biometrics.

Abstract

Biometric sensor data is rich in information content. A microphone, camera, or touch-screen device can collect sensor data for matching a user's biometric sample against a previously enrolled biometric reference template. This user sample can serve as a *something-you-are* authentication factor.

That same sensor data can also contain something a user knows, user knowledge, a *something-you-know* authentication factor. Both biometric matching data and user knowledge can be extracted from the same sensor data to enable strong, two-factor identity authentication. When user knowledge is a shared "weak secret" known only to communicating parties, it can be input into an authenticated key exchange (AKE) protocol, such as the password AKE (PAKE).

By operating an AKE protocol, communicating parties can achieve mutual authentication and establish a secure communications channel. A PAKE protocol can be coupled with biometrics to form a biometric AKE (BAKE) protocol. BAKE can enable two-factor user authentication and mutual authentication. However, BAKE is not only useful for authentication of a user identity. BAKE can be extended to create a biometric electronic signature that is convenient for use in electronic commerce, government signing, and automated smart contract applications.

The *ISSA Journal* article, "Transport Layer Secured Password-Authenticated Key Exchange," describes using a password-authenticated key exchange (PAKE) protocol[1] "to achieve mutual authentication" [1]. PAKE has been proposed as a means of preventing phishing and man-in-the-middle attacks when embedded in the transport layer security (TLS),[2] and without "major changes to the TLS protocol" [1]. In their "Security Standardization Research" (SSR 2014)[3] conference paper [2] described in the *ISSA Journal* article, Manulis, Stebila, and Denham propose to augment the TLS protocol following a successful TLS handshake.

The addition of PAKE to TLS enables secure client-side authentication for the many users who lack digital certificates and who must rely instead on passwords to authenticate their identities. By inserting PAKE within the TLS protocol, client-side passwords are protected from exposure to attackers lurking on the line or impersonating the target server. The PAKE protocol provides mutual authentication so that password users can gain assurance they have connected to the intended server without exposing their credentials in the clear.

However, the use of PAKE for authentication and secure communications does not depend on the TLS protocol. PAKE can be used without TLS and to some advantage. PAKE "does not rely on trustworthy certificate authorities (CAs), a fully functional public key infrastructure (PKI), adequate browser certificate revocation checking, or changes to user behavior or in their understanding of certificate validation" [1]. When combined with biometrics, PAKE offers a strong two-factor authentication alternative to TLS, one "well suited for implementation in resource-constrained environments, those limited by processing speed, limited memory, and power availability" [3], such as the Internet of Things (IoT).

These systems can provide convenient, easy-to-use, cost-efficient authentication and secure communications solutions in constrained environments, those not able to support the

1 Wikipedia, "Password-Authenticated Key Agreement," https://en.wikipedia.org/wiki/Password-authenticated_key_agreement.

2 Douglas Stebila, "Secure Modular Password Authentication for the Web Using Channel Bindings," https://www.douglas.stebila.ca/research/papers/SSR-ManSteDen14/.

3 SSR 2014, "Security Standardisation Research," http://ssr2014.com/.

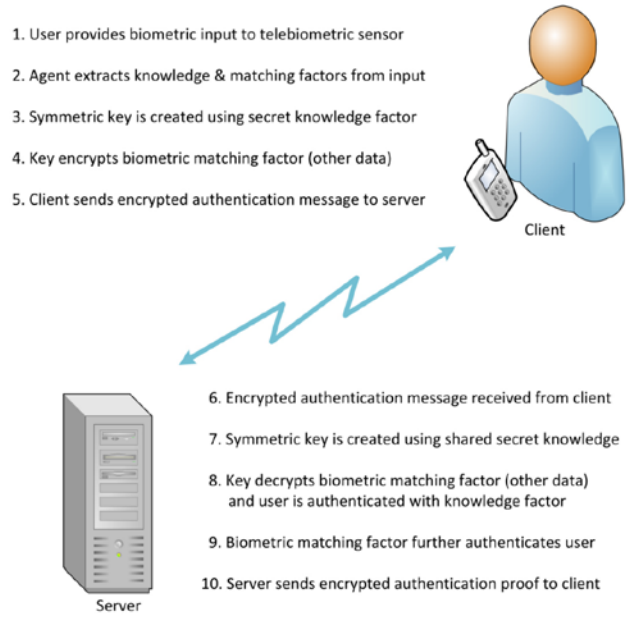


Figure 1 – Biometric authenticated key exchange (BAKE)

overhead of a PKI. Figure 1 provides a high-level depiction of the steps in a BAKE protocol.

The PAKE protocol, and by extension BAKE, are based on a Diffie-Hellman key agreement scheme for key establishment. Instead of relying on public-private key pairs, PAKE relies on a weak secret shared by communicating parties. A weak secret is something a user can easily recall. Several PAKE mechanisms have been standardized internationally in the ITU-T X.1035: "Password-Authenticated Key Exchange" (PAK) recommendation[4] and in the ISO/IEC 11770-4 Key management – mechanisms based on weak secrets standard.[5]

Knowledge extraction

Secret knowledge shared between a user and server can be collected from a user and "presented to the system in many ways and formats" [4]. These range from "a simple password entered through a keyboard device, to a PIN entered using a smartphone touch screen, to human speech recorded by a microphone" [4]. Once data that contains user knowledge is collected, it must be converted or mapped into a suitable string format before it can be input into a PAKE protocol.

User knowledge can be extracted from biometric sensor data,[6] the same data source that collects user biometric matching samples. Many biometric types contain user knowledge, but an easily understood example is the case of voice biometrics. Consider a user with an established server account associated with a passphrase that is registered in some format of the words "how now brown cow." By speaking this phrase into a microphone sensor, both biometric matching data and user knowledge can be presented by the user to an identity-authentication system.

The collected raw sensor data can be passed along to a biometric verification system for user matching. The same sensor data can also be processed using a speech recognition tool such as the Google Cloud Speech API[7] to convert the user's speech into text. These converted words can be processed to map them into the exact format expected by the server, perhaps a set of words concatenated to form the string "hownowbrowncow."

This string format is suitable for input into a PAKE protocol. When this secret is associated with a server account, the user can be authenticated by simply speaking this phrase. The speakers words are "extracted from a voice biometric sensor using speech recognition techniques and formed into a password string" [4]. This input string returns a key from the Diffie-Hellman process and that key can be established on the server based on the password associated with the user account. The user credentials are never transferred in the clear.

Other biometric technology types can also be used with BAKE. Besides voice, sensors that can collect fingerprints and hand and facial gestures are now widely available on many mobile devices. They are also making their way into assisted living and healthcare environments where observations of user gestures can be collected by "image-based biometric authentication system" [3] sensors.

Gesture biometrics

In 2013, Fong, Zhuang, and Fister [5] described using captured video images of the hand gestures of an individual as input to an image-based, biometric authentication system. The authors referred to the data in these gestures, a "sequence of hand signs," as a "biometric password" [5]. The collected hand sign images, which represented letters of the alphabet, provided a context from which biometric feature extraction could be performed on the "hand shape and the postures in doing those signs" [5].

When the gestures provided by an individual represent characters or character strings in a user password, the sensor data collected can provide two distinct authentication factors, *something-you-are* biometric matching data and *something-you-know* user knowledge data. This capability is illustrated in the American Sign Language (ASL) symbols shown in figure 2. The results of their research implementation demonstrated that it is possible to collect two authenticator factors from a single user authentication attempt. The results also demonstrated that two authentication factor types could be collected using a single sensor input.

Other more traditional biometric technology types could also be used with hand gestures instead of relying hand shapes and postures. User fingerprint matching data can be collected at distance from an individual's hand signs and extracted from

4 ITU, "X.1035 : Password-Authenticated Key Exchange (PAK) Protocol," http://www.itu.int/rec/T-REC-X.1035-200702-I/en - Freely available.

5 ISO, "ISO/IEC 11770-4:2006," https://www.iso.org/standard/39723.html.

6 Phillip H.Griffin, "Biometric Knowledge Extraction for Multi-Factor Authentication and Key Exchange," *Procedia Computer Science*, Volume 61, 2015, Elsevier, freely available at http://www.sciencedirect.com/science/article/pii/S1877050915029804.

7 Google, "Cloud Speech API," https://cloud.google.com/speech/.

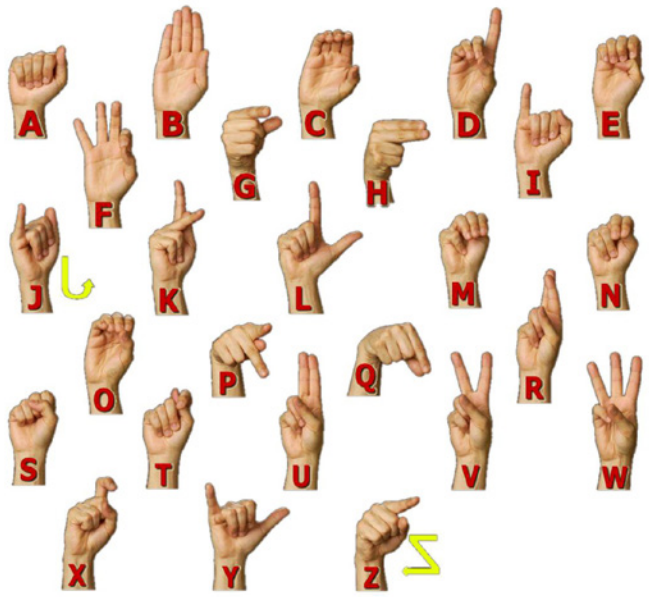


Figure 2 – American sign language (ASL) [7]

captured images. If more than one sensor is used, a voice or face biometric can be collected and coupled with gestures collected by a different sensor. The gestures could provide a password value and the voice or face a biometric. Biometric authentication coupled with strong confidentiality protection during data transfer by using PAKE makes it possible to provide services to users with diverse abilities, such as greater access to information , and opens the possibility of providing new services, such as trusted remote-document signing.

Biometric electronic signature

The definition of an electronic signature (e-signature) can vary by legal jurisdiction. In the United States, an e-signature is specified under the Uniform Electronic Transaction Act (UETA)[8] and the Electronic Signatures in Global and National Commerce (ESIGN) Act.[9] These acts define an electronic signature as any process, symbol, or electronic sound performed by an individual and associated with information that the individual agrees to accept and sign, and an indication of intention to conduct an electronic transaction.

The 2017 version of the X9.84 Biometric Information Management and Security standard[10] specifies three new biometric-based e-signature techniques. These techniques are the biometric electronic signature token (BEST), signcrypted BEST (SBEST), and biometric electronic-signature authenticated-key exchange (BESAKE). Two of these techniques, BEST and SBEST, rely on a functioning public key infrastructure (PKI). The BESAKE technique extends BAKE to create an e-signature protocol without the need for digital certificates.

These three techniques can be used to electronically sign agreements of any type or format. All three are intended for use in electronic commerce and other commercial or governmental signing events. These techniques provide multi-factor user authentication and mutual authentication, and protect the confidentiality of e-signer biometric data and other information. The X9.84 biometric e-signature techniques combine biometric authentication with cryptography and are suitable for use in cloud and distributed-ledger environments, including smart contract applications.

Figure 3 describes the BESAKE processing steps and illustrates how the BAKE protocol can be used for purposes other than user authentication, extending TLS, and establishing a secure communications channel.

Steps 1-6 in figure 3 describe how an encrypted BESAKE e-signature token is created. The token contains a proper e-signature agreement, including indications of acceptance of terms and intention to e-sign. The token also contains user biometric information, a server challenge, and any other data needed by a contract application. Steps 7-12 describe the processing required when validating the claimed identity of the e-signer. Processing of the actual agreement is left to the application.

BESAKE can be used to authorize a transfer of value in a smart contract. The encrypted results of steps 1-6 in figure 3 can be placed safely in a cloud, distributed ledger, or smart contract environment. In a smart contract context, chain code will cause steps 7-12 in figure 3 to be processed when a smart contract event signals that the contract has been performed. Step

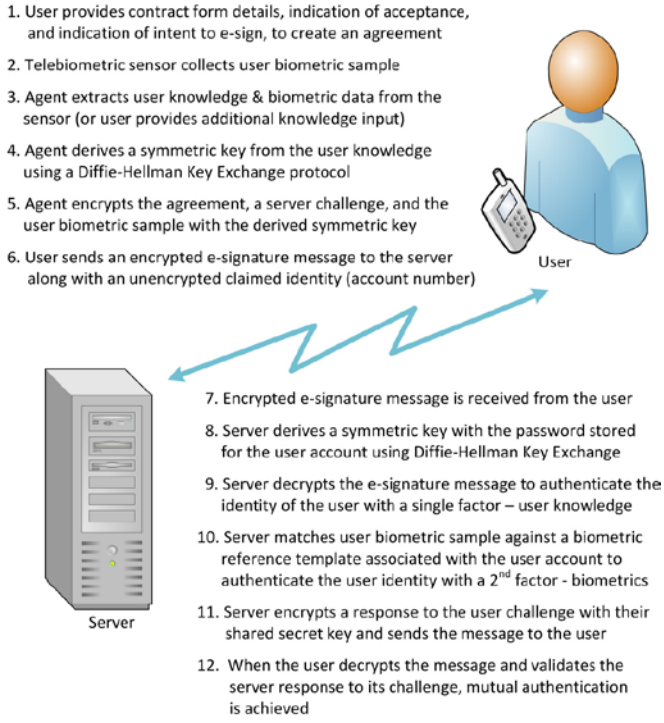


Figure 3 – Biometric electronic signature authenticated key exchange (BESAKE)

8 "Electronic Transactions Act Summary," Uniform Law Commission, http://www.uniformlaws.org/ActSummary.aspx?title=Electronic Transactions Act.

9 GPO, "Public Law 106 - 229 - Electronic Signatures in Global and National Commerce Act," US Government Publishing Office , https://www.gpo.gov/fdsys/pkg/PLAW-106publ229/content-detail.html.

10 ANSI, "ANSI X9.84-2010 (R2017): Biometric Information Management and Security for the Financial Services Industry," ANSI, https://webstore.ansi.org/RecordDetail.aspx?sku=ANSI+X9.84-2010+(R2017).

```
BiometricData ::= SEQUENCE {
   version      Version,
   templateID   BiometricReferenceTemplateID  OPTIONAL,
   bsp          BiometricServiceProvider  OPTIONAL,
   type         BiometricType  OPTIONAL,
   biometric    BiometricData
}

Version ::= INTEGER { v1(1) } ( v1, ... )

BiometricReferenceTemplateID ::= OCTET STRING

BiometricServiceProvider ::= URI

URI ::= VisibleString (SIZE(1..MAX))

BiometricType ::= OBJECT IDENTIFIER -- Any identified type

BiometricData ::= OCTET STRING (SIZE(1..MAX)
```

Figure 4 – BESAKE biometric data schema

one of the BESAKE process can contain any type value object (i.e., a deed of trust) or transfer instrument permitted by an application. This might be in the form of digital currency, fiat currencies issued by governments, or commercial products such as zCash[11] or Bitcoin. Digital documents, including electronic checks and payment card authorizations and other promises to pay or transfer value may also be used.

Step 10 in figure 3 describes the second phase in multi-factor authentication of the user identity. The user may be enrolled in a biometric system local to the relying party server or enrolled with a third-party biometric service provider (BSP). Third-party enrollment and verification would require that the relying party server trust the BSP. One possible abstract syntax notation one (ASN.1) schema [6] to support user biometric matching portability is described in figure 4.

Here, an optional biometric reference template identifier can be provided to speed up locating the template of the claimed identity during the biometric matching process. When necessary, an optional URI can be included that locates the BSP needed to perform the matching using a specific template. Finally, an optional biometric technology type identifier can be included to identify the type of biometric sample data in the message.

Conclusion

Authenticated key-exchange protocols such as PAKE-based BAKE can be used to achieve strong, two-factor user authentication. BAKE can be implemented by pairing biometric matching data and user knowledge extracted from a single biometric sensor. Many different biometric technology types can provide two authentication factors, all without the overhead of TLS, digital certificates, and a properly functioning PKI.

The BAKE protocol can be used to create low cost, convenient-to-use, access control systems that can "help manage the security risk of unauthorized access" [3] to information resources and to provide secure communications in resource-constrained environments unable to support certificate-based solutions. BAKE can also help to improve the user authentication experience, building user trust through mutual authentication, assurance that users are "actually connected to the systems they intended to connect to—systems that they can trust" [3].

BAKE ensures that user authentication credentials and other sensitive data are protected from man-in-the-middle and phishing attacks during the transfer of user authentication credentials, and during subsequent communications. BAKE can be extended into a protocol for e-signatures, BESAKE, to support e-signing documents in any format and type. Encrypted BESAKE message tokens are suitable for use in elec-

11 zCash, "Internet Money," zCash, https://z.cash/.

Continued on page 40

ISSA International Web CONFERENCE

Click here for On-Demand Conferences

www.issa.org/?OnDemandWebConf

Mobile Device Security
2-Hour Event Recorded Live: September 26, 2017

Untraceable Currency
2-Hour Event Recorded Live: August 22, 2017

Here Come the Regulators
2-Hour Event Recorded Live: July 25, 2017

Building Security in a Business Culture
2-Hour Event Recorded Live: June 27, 2017

Breach Report Analysis
2-Hour Event Recorded Live: May 23, 2017

Evolution of Cryptography
2-Hour Event Recorded Live: April 25, 2017

Internet of Things
2-Hour Event Recorded Live: March 28, 2017

Cyber Residual Risk
2-Hour Event Recorded Live: February 28, 2017

When TLS Reads "Totally Lost Security"
2-Hour Event Recorded Live: January 24, 2017

When TLS Reads "Totally Lost Security"
2-Hour Event Recorded Live: November 15, 2016

How to Recruit and Retain Cybersecurity Professionals
2-Hour Event Recorded Live: October 25, 2016

Security Architecture & Network Situational Awareness
2-Hour Event Recorded Live: September 27, 2016

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

Securing the Vendor

Changing the Dynamic of the Infosec Relationship

By Curtis Campbell – ISSA Senior Member, Chattanooga Chapter

This article discusses securing third-party vendors and the need for protecting organizational information wherever it is located. It focuses on the infosec relationship with internal business groups through cybersecurity discussions and risk analysis.

Abstract

This article discusses securing an organization's cybersecurity environment with third-party vendors. It considers the need for cybersecurity discussions and risk analysis when monitoring and evaluating vendors. It touches on the importance of changing the dynamic in information security roles to create a trust relationship with internal units for protecting organizational information, wherever it is located.

It's a great thing when an internal business group comes to you for advice on a third-party vendor, isn't it? Or, do we find ourselves wondering what else is beneath the tip of the iceberg we didn't know about?

Recently, I was asked by someone in our digital group if it was okay to give a vendor "Edit" access on the organization's Google Analytics page of the website domain in order to set up new remarketing lists. The business owner went on to state the vendor had previously been given "Edit" access but was later downgraded to "Collaborate" status, although the business owner didn't remember why, and did Information Security see any problem?

Securing the vendor is more important than ever before as more data is shared electronically between supply chains and organizations. In the first half of 2017, a reported 1.9 billion data records were lost or stolen by cyberattacks, consisting of 918 separate data breaches.[1] Reports indicate cloud data traffic will increase over three times the current amount by 2020, and that represents a huge challenge for information security professionals. New technologies such as machine-to-machine connectivity and the Internet of things that link consumer products are contributing to these risks of accessing data. To protect organizations, restricting data access where applicable and vetting third parties is an ongoing process.[2]

The sheer number of increasing vendors may make it hard to audit everyone thoroughly. Many organizations may not be fully staffed for performing due diligence and risk modeling for hundreds of vendors. Acceptable metrics to assess risks and the added complexity of participant departments within the organization also make it tough. And, in regulated environments, management is held accountable by the board or appropriate board-approved committee for implementing information security programs and compliance, governed by regulatory audits from participating agencies.[3]

Saying "no" isn't our job; identifying and communicating risk so the business can understand it, is.

As Information security professionals, we must understand our role in helping the business balance risk versus reward. We are responsible for helping business leaders understand cybersecurity risks and should serve as an enabler of the business, not a road block. When we can do this in a serving capacity, we can be a very trusted and useful resource. Saying "no" isn't our job; identifying and communicating risk so the business can understand it, is. Providing options for

1 Luke Graham, "The Number of Devastating Cyberattacks Is Surging – And It's Likely to Get Much Worse," CNBC, September, 2017, https://www.cnbc.com/2017/09/20/cyberattacks-are-surging-and-more-data-records-are-stolen.html.

2 Financier Worldwide, "Dealing with cyber breaches in the supply chain," Financier Worldwide, June, 2017, https://www.financierworldwide.com/dealing-with-cyber-breaches-in-the-supply-chain/.

3 FFIEC. "Federal Regulatory Agencies Administrative Guidelines," Implementation of Interagency Programs for the Supervision of Technology Service Providers, October 2012 – https://ithandbook.ffiec.gov/media/153533/10-10-12_-_administrative_guidelines_sup_of_tsps.pdf.

accomplishing tasks at hand with less risk is an opportunity to guide and build trust and respect from those around us.

Accountability and compliance

Securing the vendor has primarily been access driven, either "on" or "off," whereby vendor access pathways are controlled by enforcing access control policies and recording all third-party activity. The discussion around securing the vendor now is extremely relevant as third-party suppliers continue to grow and access some portion of company networks every single week. To add to the complexity, some vendors may share an integration with importing or exporting files on the network. The business may not know the right questions to ask their vendors regarding technology and tools being used to access company networks. Organizations may understand company credential policies around secure remote access, but information security professionals can help address risks and concerns around vendor vulnerability when approached.

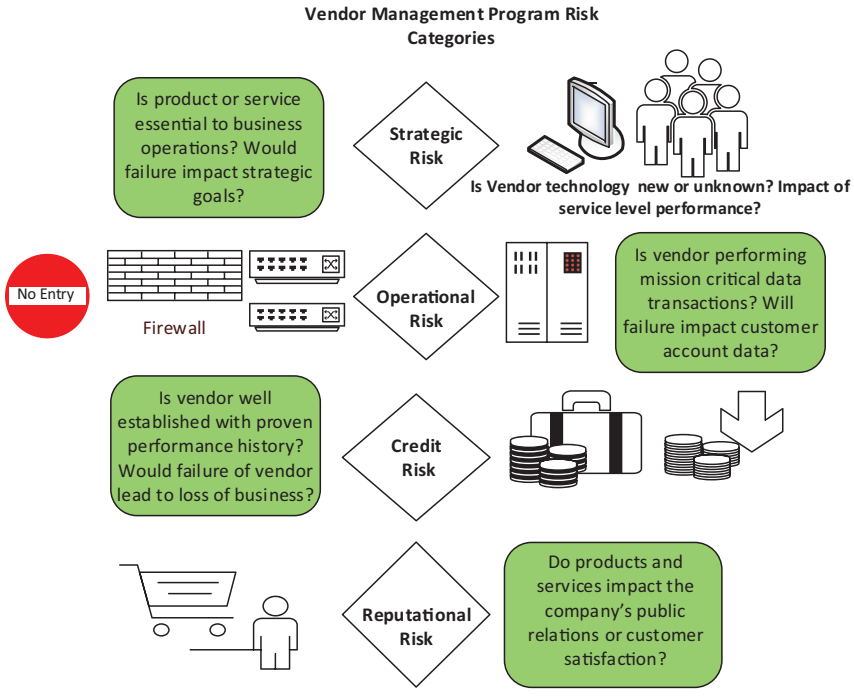


Figure 1 – Risk categories used in vendor management programs

Maintaining ongoing due diligence to assess information security risk that identifies, prioritizes, and assesses the risk to critical systems, including threats to external websites and online accounts, is important.[4] Not only does this benefit the company in gaining risk intelligence and insight for non-compliance or unethical behavior, but it also protects the organization against potential fraudulent activity.

Vendor management

Vendor risk management programs serve to monitor risk classification and maintain third-party governance by incorporating vendor management policies, processes, and guidelines set by regulatory agencies. Organizations face challenges of reviewing and analyzing hundreds of critical and non-critical vendors each year. In an enterprise, a vendor risk management program touches procurement, information security, physical security, legal, compliance, IT, HR, and even sales. A cost-effective vendor risk management program is complex, and the mere task of performing due diligence and risk modeling with shrinking budgets presents a challenge to all.

In the particular scenario mentioned at the beginning, the search engine optimization vendor was used on a need-be basis by the business and not included within the vendor management program due to its specialty service offering, small size (picture geeky millennials in a storefront), and non-critical core or critical system status. While achieving success in raising websites to the forefront of the search pages, the vendor was a small shop with no certificate of insurance, SOC1 or SSAE16 type report, bridge or gap letter, or financial report.

As information security professionals, the responsibility for vendor management programs may be well out of our purview, but maintaining an awareness of specific vendor management program components collected for attestation and

4 FFIEC. "Joint Statement Distributed Denial=of-Service (DDoS) Cyber-Attacks, Risk Mitigation, and Additional Resources," April 2014, https://www.ffiec.gov/press/pdf/ffiec ddos joint statement.pdf.

ISSA SPECIAL INTEREST GROUPS

ISSA Special Interest Groups

Security Awareness
Sharing knowledge, experience, and methodologies regarding IT security education, awareness and training programs.

Women in Security
Connecting the world, one cybersecurity practitioner at a time; developing women leaders globally; building a stronger cybersecurity community fabric.

Health Care
Driving collaborative thought and knowledge-sharing for information security leaders within healthcare organizations.

Financial
Promoting knowledge sharing and collaboration between information security professionals and leaders within financial industry organizations.

Special Interest Groups — Join Today! — It's Free!
ISSA.org => Learn => Special Interest Groups

validation by the organization may be helpful. Listed are six documentation areas commonly used in vendor management programs for vendor onboarding and annual risk reviews.

Corporate governance/vendor policies

Are strong governance policies in place? Good policies create a solid foundation with expectations and guidelines. Most policies should be reviewed and approved annually.

Executed vendor NDA and contracts

Is there an executed NDA and contract for each approved vendor with the "right to audit," periodic security reports, terms, termination, and renewal sections signed by both parties? These documents should be executed by both parties and stored in multiple places (perhaps specified in the policy).

New vendor onboarding and annual risk assessments

Strategic risk, operational risk, credit risk, and *reputational risk* are categories for measuring vendor risk. Is there a template or living document that can be updated each year for tracking risk calculations, updates, and "red flags" within the vendor's environment?

Figure 1 shows vendor risk categories for ongoing evaluation and monitoring.

Onsite visits/audits

Are site visits required to a vendor's office or data center? A prepared checklist with questions is helpful, and a best practice is to make a site visit to a third party's data center. If a third-party vendor uses a fourth party, a site visit to see where your organization's data is kept is a good idea. Help the business partner understand that "in the cloud" is not a literal answer.

Expenses are not always budgeted for site visits, but for core systems and critical network vendors, a best practice would be to include a line-item expense in the budget that can provide company representatives access to see and evaluate firsthand the third party's secure environment. This is an important due diligence step best made by key IT or information security staff tasked with the day-to-day engagement of the vendor.[5] Of course, it is not always feasible to visit out-of-the-country locations, and a work-around option would be to have prospective vendor teams come to your location or conduct video conferencing.

Audit/reporting

Audit reports provide strong areas and weak areas of compliance. Archiving reports by annual year of review provides guidance and identifies any sudden change within the reporting categories. In situations of vendor acquisitions, due diligence is extremely important and can significantly increase or decrease the risk the vendor poses.

Consistent oversight and monitoring

Key areas are vendor's financial health, business continuity and contingency plans, security controls—both technical and non-technical—and proof of insurance, including cybersecurity insurance.

Cybersecurity liability insurance has been included in the products within the insurance market in recent years. Insurance companies now offer a variety of cyber liability insurance in addition to common categories such as general liability, automobile, and errors and omissions (E&O). Although it will not protect the organization or supply chain against attackers, cybersecurity liability coverage can help organizations recover financially when breached.[6] As security professionals, we can help the business understand the need for added cybersecurity liability coverage.

Changing the dynamic of the infosec relationship

A vendor management risk program cannot stand alone. As security professionals and leaders, we are encouraged to display a leadership attitude in helping business leaders balance the risk versus reward, liability versus value, especially in a time where cyberattacks are surging. This includes being approachable and authentic, adaptive, and willing to connect with others through various communication methods and technology.[7]

Our true role in partnering with the business groups is to move the needle toward a balance in securing the vendor while allowing the business to grow and rapidly adapt to market and environmental changes. Securing the vendor includes governing vendors' access, collaborating on contractual terms and conditions, and auditing security attestations and financials. The dynamic of the infosec relationship with internal business groups changes when we:

1. **Communicate with a helpful, open attitude.** By listening and asking questions, an open dialog can establish or reestablish a good internal business partner relationship.
2. **Pick our battles.** Being seen as inflexible and unwilling more often than not alienates those who seek us out for advice. Not saying "no" initially will go a long way to keep the lines of communication open.
3. **Provide options.** Options that protect while allowing the business to grow is a win-win. Alignment with the core business strategy while critically thinking through the issues is a must.
4. **Impact change.** Resist complacency and stay engaged to impact change. Helping facilitate secure options for business goals drives change at an organizational level.

5 Stefanie Overby, "How to Get the Most Out of an IT Outsourcing Visit," CIO.com. November26, 2015, https://www.cio.com/article/3008414/outsourcing/how-to-get-the-most-out-of-an-it-outsourcing-vendor-visit.html.

6 Steve Sanders, "Demystifying Vendor Management," March 09, 2016, CSI.com, http://www.csiweb.com/resources/blog/post/2016/03/09/demystifying-vendor-management.

7 Amy Jen Su, "How New Managers Can Send the Right Leadership Signals," Harvard Business Review, August 8, 2017, https://hbr.org/2017/08/how-new-managers-can-send-the-right-leadership-signals.

5. **Build trust.** Align words and actions to model the behavior you seek from others. When the business trusts you, your position on the issue is respected as a trusted advisor and not a road block to change.

In the end, the millennial-owned search engine vendor mentioned in the beginning was granted "Edit" access to the Google Analytics section of the company website to refresh the marketing list. The business owner requested the vendor to come onsite, complete the task at the company location, and make the changes in a controlled, monitored environment within the security and perimeter of the corporate network. Being a local vendor, that was a simple, effective resolution. However, if vendors are located in geographically diverse areas, finding the right solution takes critical thinking outside the box.

Conclusion

Changing the dynamic of information security roles involves a willingness to switch gears and focus on helping internal business groups understand cybersecurity risks when dealing with vendors. A great way to facilitate discussions with internal business groups is to address new and emerging risks associated with business strategies. Protecting information wherever it is located requires a fundamental shift in thinking for organizations, and discovering ways to relay answers regarding third-party providers will reap great rewards.

Starting a conversation the next time the business comes knocking with a potential vendor or security-related issue may produce more than just collaborative thought. It may serve to change the dynamic of the relationship. Working with the business on ways to secure the vendor not only protects our organization's confidential information but, more importantly, builds a culture of trust. Ultimately, it's knowing that information security isn't only about control; it's about changing the dynamic of the relationship to provide value and knowledge in the business environment.

About the Author

Dr. Curtis C. Campbell, DM/IST, is a VP and IT procurement manager at a financial institution, co-founder and VP, Programs of the ISSA Chattanooga Chapter, ISSA Small Chapter of the Year 2017. She is a member of the Financial, Security Awareness, and Women in Security Special Interest Groups. Her professional background includes audit and compliance, risk management, cybersecurity, procurement, and IT project management in the enterprise. She can be reached at curtis@mprotechnologies.com.

Biometric Electronic Signatures

Continued from page 36

tronic commerce transactions and to authorize the transfer of value in smart contracts and other distributed-ledger technologies.

References

1. Griffin, P.H. (2015). "Transport Layer Secured Password-Authenticated Key Exchange," Information Systems Security Association Journal, Vol. 13, No. 6 (ISSA), The ISSA Journal, June, 2015. Retrieved September 12, 2017, from http://www.issa.org/?x9.
2. Manulis, M., Stebila, D., & Denham, N. (2014). "Secure Modular Password Authentication for the Web Using Channel Bindings," in *Security Standardisation Research: First International Conference*, SSR 2014, London, UK, December 16-17, 2014. Proceedings (Vol. 8893, pp. 167-189). Chen, L., & Mitchell, C. (Eds.). Springer International Publishing. Retrieved September 13, 2017, from http://www.springer.com/us/book/9783319140537.
3. Griffin, P.H. (2017). "Secure Authentication on the Internet of Things," IEEE SoutheastCon 2017. Retrieved October 2, 2017, from http://ieeexplore.ieee.org/abstract/document/7925274/.
4. Griffin P.H. (2018) "Adaptive Weak Secrets for Authenticated Key Exchange," in Nicholson D. (eds) *Advances in Human Factors in Cybersecurity.* AHFE 2017. Advances in Intelligent Systems and Computing, vol 593. Springer, Cham. Retrieved October 4, 2017, from https://link.springer.com/chapter/10.1007/978-3-319-60585-2_2.
5. Fong, S., Zhuang, Y., & Fister, I. (2013). "A Biometric Authentication Model Using Hand Gesture Images," Biomedical engineering online, 12(1), 111. Retrieved October 1, 2017, from http://www.biomedical-engineering-online.com/content/12/1/111/.
6. Larmouth, J.L. (2000). "ASN.1 Complete," Morgan Kaufmann. Retrieved October 3, 2017, from http://www.oss.com/asn1/resources/books-whitepapers-pubs/larmouth-asn1-book.pdf.
7. Vicars, W. (2011). Fingerspelling & Numbers: Introduction, American Sign Language University (ASL). Retrieved October 4, 2017, from http://www.lifeprint.com/.

About the Author

Phillip H. Griffin, CISM, has over 20 years experience in the development of commercial, national, and international security standards and cryptographic messaging protocols. Phil has a Master's of Information Technology, Information Assurance and Security degree and has been awarded 10 US patents at the intersection of biometrics, radio frequency identification (RFID), and information security management. He may be reached at phil@phillipgriffin.com.

When You Cannot Be Silent: Whistle-Blowing 2.0

By Avani Desai – ISSA Women in Security SIG member

When we think of whistle-blowing, it tends to have a negative connotation—sometimes for the right reason. This article discusses how whistle-blowing has changed in the online world to "cyber whistle-blowing" or whistle-blowing 2.0.

Tell-tale tit, yer mither cannae knit, Yer father cannae walk wi a walkin-stick.

Abstract

This article discusses how whistle-blowing has changed in the online world to "cyber whistle-blowing" or whistle-blowing 2.0. When we think of whistle-blowing, it tends to have a negative connotation—sometimes for the right reason. We have seen this blurred line between the good and bad whistle-blowing and even with the awareness and education from high-profile cases in 2017 that perception seems to not have changed in our online world. With an appropriate structure and process to bestow protections for the individual we will see an increase in the "good" whistle-blowing and stronger shields in place for those who are defending the good in the world.

The words above come from a Scottish (with English variations) nursery rhyme that was often sung in the playground. It was used to taunt any child that dared to speak out about something—to discourage one from telling the teacher that "little Susie had stolen a pencil from their school desk," that sort of thing. The idea of a *tell-tale* is something that sweeps across human culture and has for decades. "Snitch," "snarc," and "squealer" are all words used in a more modern context to describe a person who "tells tales out of school"—and none of those words carries positive connotation.

In the same vein, now in our modern world the words used to describe people who "whistle-blow" are often harsh and applied in a very negative way. In the world of crime, the term is used as a way of controlling people, making sure that no one "snitches" about a crime, and those who do may well be punished in some manner—typically by being ostracized by their peers (or worse). The same concept now applies to the online world as well; if the *tell-tale tit* is the equivalent of whistle-blowing 1.0, then we now have the cyber whistle-blower—or whistle-blowing 2.0.

In recent years, we have seen some very high-profile versions of whistle-blowing 2.0. Often, this has been directed at the very highest offices in the country. During the recent US election, thousands of Democratic National Committee emails were hacked and passed onto Wikileaks for the world to see, though the impact on the election outcome remains up for debate. And then there are the infamous Edward Snowden leaks around the NSA's use of surveillance. Snowden leaked documents showing the NSA misusing powers to gather information on individuals without permission in a highly invasive and privacy-compromising manner. These are modern versions of the tell-tale, a sort of "digital-snitch." But is a cyber whistle-blower good or bad?

The modern take on "the snitch"

The modern-day version of the tell-tale has become known as the cyber whistle-blower. With technological advancement, our personal data, whereabouts, and financial information have become and are now part of the wider digital world. Various protective measures are applied to this sensitive data, and regulations enforce that protection; but, as in the non-digital world, these things are not always rigorously fool-proof. High-profile whistle-blowers like Snowden and Wikileaks' founder Julian Assange have had very bad press after their

leaks became public. However, their information alerted the public and other officials to many security and privacy issues that had been previously kept in the dark. Moreover, whistle-blowing isn't limited to politics or intelligence—it is trickling down the chain from the highest office to the common enterprise. Whistle-blowing 2.0 is becoming part of the very framework of our organizations across the land.

As employees, we may well find ourselves in situations where we can see poor practice or sensitive information being compromised. What we do in that situation is something that needs to be handled at a cultural level. A friend who works in health care recently told me that within that sector whistle-blowers are frowned upon as interfering with the job—within that industry at least, there is a culture of "just getting on with it" and ignoring the issue. This is perceived as a pragmatic and "hardworking" approach to these problems—whistle-blowers are an inconvenience getting in the way of people just doing their job. The result of this kind of culture, however, is that best practice is often broken.

The US EEOC… recorded retaliation charges in 44.5 % of claims by employees wanting to blow the whistle in 2015.

In the cyberworld, the same is true. You can picture this hypothetical scenario:

> A system administrator working for a large enterprise, or perhaps a government department, realizes that the organization has not applied the correct security measures to consumer accounts—accounts that hold personally identifiable information (PII) such as name, social security number, credit card details, and so on. This system administrator has been telling the company for two years that they must put these security measures in place. But it continually falls on deaf ears—the person in charge does not want to listen, as this problem makes him look bad. Finally, a memo mentioning the security issue but dismissing it as "too costly" appears in the system administrator's inbox...what should this admin do?

These hypotheticals exist for smaller enterprises as well: for instance, a large online firm that offers an app to use in booking taxi cabs, but has such lax protection of its users' PII that employees can track well-known users for fun. You watch as this happens, day in and day out—what do you do?

Taking the leap into this kind of territory—the kind that could end with you annoying colleagues at best or losing your job at worst—is not something that everyone feels comfortable doing. When we can switch on the TV news and see Edward Snowden, effectively exiled from his home and family, it's not hard to understand having second thoughts about blowing the whistle on bad company data practice. This mentality is supported by figures from the US Equal Employment Opportunity Commission [9] which recorded retaliation charges in 44.5 percent of claims by employees wanting to blow the whistle in 2015.

However, despite the personal reservations, that doesn't mean whistle-blowing cannot necessarily be a tool for good. A PWC report [4] into economic crime found that larger organizations (1000+ employees) were more susceptible to fraud, with hackers being able to circumvent normal control frameworks. When asked, 42 percent of these organizations found that monitoring whistle-blowing hotlines was an effective control.

When good whistle-blowing goes bad

Even if it can be used for good, the fears around whistle-blowing are deep within our psyche, as that "tell-tale tit" rhyme demonstrates. The way whistle-blowers are handled plays into this. Snowden's story demonstrates this keenly. In June 2013, the British newspaper *The Guardian* [5] leaked NSA documents showing an order to Verizon, a multinational telecommunications conglomerate, to disclose data from millions of US citizens' phone calls. Shortly after Snowden's identity was disclosed, the US government filed criminal charges against him, including a charge of espionage.

In the case of Snowden, whistle-blowing changed his life forever, but he continues to maintain that he disclosed the information for the good of everyone. A pinned tweet from Snowden's Twitter account states the following:

> **"Speak not because it is safe, but because it is right."**

Unfortunately, not all whistle-blowers have such good intentions—just look at the security firm Tiversa Inc., which used whistle-blowing to create revenue. Tiversa [8] acted as a proxy whistle-blower to the Federal Trade Commission (FTC). Tiversa would claim that certain companies had breached data protection laws, offering the FTC doctored documents that evidenced alleged data breaches. This instance of perceived whistle-blowing was, in fact, vengeance against a company that had refused to take on Tiversa as a contractor. Tiversa is notably making amends, having sacked the CEO, and is fully cooperating with the ongoing federal investigation [3] into the allegations. Still, their false whistle-blowing plays into the negative association many have with the act.

Whistle-blowing isn't limited to American enterprise; blowing the whistle on bad practices is something that is taken very seriously in other parts of the world too. In the UK, the National Health Service (NHS) has recently created a new role called the Freedom to Speak Up Guardian (FTSU) [2]. The FTSU offers a confidential service to employees who are concerned about patient safety and bad practices within a healthcare community. The remit of the guardian is to create a more transparent workplace where employees feel safe to speak up about problems. This "hand-to-hold" approach is a vital help line that can prevent uncontrolled whistle-blowing and whistle-blowing for vengeance.

Forming structures for whistle-blowing

The problem as we have seen with unsupported whistle-blowing is that it can backfire, not only on the whistle-blower but also to preventing the resolution of the issue itself. The Na-

tional Whistle-blower Center [7], a not-for-profit organization, does offer advocacy for whistle-blowers, and it provides a list of references that offers protection for whistle-blowers. However, we need to have further structures in place to prevent the misuse of whistle-blowing freedoms, but that maintain support to allow whistle-blowers to speak out safely without fear of retaliation.

Currently in the US, whistle-blowing as a right has protection under the Civil Rights Act of 1964, and the Equal Employment Opportunity Commission is set up to cover discrimination against employees [1]. However, this act is currently specific to discrimination and does not extend to whistle-blowing about the misuse of data or security/privacy issues. In terms of cybersecurity and data privacy, whistle-blowing has no national overarching legislation to protect those who would speak out against bad practices. However, two regulatory frameworks do have provisions for cyber whistle-blowing:

- **The Sarbanes-Oxley Act** – offers protection to persons wishing to expose fraud, such as wire, mail, and securities fraud. It offers protection against retaliation of whistle-blowers [6].
- **The Dodd-Frank Act** – offers monetary rewards for whistle-blowers who provide information on cybersecurity issues that violate securities laws or regulations to the government [10].

Perhaps these, along with the protection within the Civil Rights Act of 1964, could act as a framework to extend the protection of discrimination and also to those who try and uphold an individual's privacy and security. If anything, it's clear that the black and white lines of good and bad whistle-blowing continue to be blurred, and we should push for more extensive legislation to help clarify what to do and how one would be protected in the event.

Conclusion

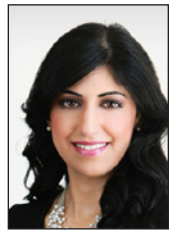
When organizations large and small, whether governmental, public, private, or even non-profit, engage in practices that violate laws and regulations, putting personal information and privacy at risk, employees should have recourse—without fear of retribution or retaliation—of exposing those practices to proper authorities. In the US, the Civil Rights Act of 1964, the Sarbanes-Oxley Act, and the Frank-Dodd Act provide limited protections for the whistle-blower; the UK Freedom to Speak Up Guardian provides more.

It is time to develop a framework to extend these protections afforded to the cyber whistle-blower—whistle-blowing 2.0—to those who would try and uphold an individual's privacy and security. A whistle-blowers charter could create an environment where telling tales was not a negative but a positive for society. As long as we can build in checks and balances to prevent malicious use of the charter, we could, as a whole, benefit from a clearer view of our organizations and societal structures.

References

1. "The Civil Rights Act of 1964 and the Equal Employment Opportunity Commission," National Archives – https://www.archives.gov/education/lessons/civil-rights-act.
2. CQC, "National Guardian's Office," Care Quality Commission – http://www.cqc.org.uk/national-guardians-office/content/national-guardians-office.
3. Fair, M. "LabMD Slams Bid to Extend Stay in Tiversa's Defamation Suit," Law 360 – https://www.law360.com/articles/888265/labmd-slams-bid-to-extend-stay-in-tiversa-s-defamation-suit.
4. Global Economic Crime Survey 2016, "Adjusting the Lens on Economic Crime Preparation Brings Opportunity Back into Focus," PWC – https://www.pwc.com/gx/en/economic-crime-survey/pdf/GlobalEconomicCrimeSurvey2016.pdf.
5. Guardian, "NSA Files Decoded: Edward Snowden's Surveillance Revelations Explained," The Guardian – https://www.theguardian.com/us-news/the-nsa-files.
6. Marshall, D. editor, "American Bar Association Section of Labor and Employment Law Committee on Federal Labor Standards Legislation 2016, Midwinter Meeting Report," Subcommittee on the Sarbanes-Oxley Act of 2002 – https://s3.amazonaws.com/zuckermandev/wp-content/uploads/2016-Annual-Update-on-the-Whistle-blower-Provisions-of-SOX.pdf.
7. NWC, "Federal Whistle-blower Protections," National Whistle-blower Center – http://www.whistle-blowers.org/index.php?option=com_content&view=article&id=816&Itemid=129.
8. Staff Report, "Tiversa, Inc.: White Knight or Hi-tech Protection Racket?" US House of Representatives, January 2, 2015 – http://michaeljdaugherty.com/wp-content/uploads/2015/05/2015.01.02-Staff-Report-for-Rep.-Issa-re-Tiversa.pdf.
9. US EOPC, "EEOC Enforcement Guidance on Retaliation and Related Issues," US Equal Opportunity Commission, August 25, 2016 – https://www.eeoc.gov/laws/guidance/retaliation-guidance.cfm.
10. US HR, "Dodd-Frank Wall Street Reform and Consumer Protection Act," Office of the Legislative Counsel of the US House of Representatives, December 16, 2016 – https://legcounsel.house.gov/Comps/Dodd-Frank Wall Street Reform and Consumer Protection Act.pdf.

About the Author



Avani Desai is a Principal and the Executive Vice President at Schellman. Avani has more than 15 years of experience in IT attestation, risk management, compliance, and privacy. Avani's primary focus is on emerging healthcare issues and privacy concerns for organizations. She may be reached at avani.desai@schellmanco.com.

Cybersecurity Risk in Health Care

By Barry S. Herrin – ISSA member, Metro Atlanta Chapter

This article discusses the current state of healthcare data privacy and security, the legal issues requiring attention, risks of the growing use of remote and wearable technologies, and cybersecurity insurance.

Abstract

The need for constant availability and integrity of patient data means that many organizations compromise on privacy and security, often to their detriment. This article discusses the current state of healthcare data privacy and security, examines the legal issues requiring attention, discusses risks of the growing use of remote technologies, mHealth, and wearable technology, and finally discusses cybersecurity insurance as a way to mitigate the financial costs of breach.

The current state

Notwithstanding the imperative of the federal Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its Privacy and Security Rule,[1] the era of interoperability has created a de-emphasis on the confidentiality of medical information while, at the same time, creating a tremendous emphasis on integrity and availability.

Findings from the Health Care Industry Cybersecurity Task Force in its final report of June 2, 2017,[2] show that "of the three aims of cybersecurity (confidentiality, integrity, availability), availability is the most important. You cannot take care of patients without having availability of information. Having high availability of patient information is especially important with hospitals that operate 24x7 and 365 days a year." Second to availability was integrity of data. The HCIC report specifically stated that "integrity of data is important for protecting patient safety," which is "directly implicated when it comes to connected medical devices and patients whose health can be directly impacted by the operation of the medical device." However, the report recognizes that the drive to interoperability has resulted in the confidentiality of medical information being de-prioritized and asserts that "healthcare data confidentiality must remain top of mind."

A 2017 KLAS survey reports that 41 percent of respondents said their health systems dedicate less than three percent of the IT budget to cybersecurity, primarily because IT leadership has been focused on implementing electronic health record systems and dealing with interoperability challenges.[3]

Task Force Imperative 4 calls for an "increase [in] healthcare industry readiness through improved cybersecurity awareness and education." However, the increase in readiness "requires a holistic cybersecurity strategy. Organizations that do not adopt a holistic strategy not only put their data, organizations, and reputation at risk, but also—most importantly—the welfare and safety of their patients."

In the healthcare industry specifically, the financial impact of cybersecurity breaches is grim. One in three Americans was affected by healthcare breaches in 2015, according to a report from Bitglass.[4] That's more than 113 million individuals. Each lost or stolen medical record costs a healthcare organization

1 45 CFR Parts 160 and 164; the enabling legislation is found at 42 U.S.C. Section 1320a-7c.

2 "Report on Improving Cybersecurity in the Health Care Industry," Health Care Industry Cybersecurity Task Force (June 2017) – https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf.

3 Center for Connected Medicine report, "The Internet of Medical Things: Harnessing IoMT for Value-Based Care," July 2017 – https://www.connectedmed.com/files/assets/common/downloads/publication.pdf.

4 Bitglass. "Bitglass Healthcare Breach Report 2016," Bitglass – https://pages.bitglass.com/BR-Healthcare-Breach-Report-2016_PDF.html.

$363 per record on average, per a Ponemon Institute report.[5] The anecdotal record is not any more pleasant: Hollywood Presbyterian's information systems were held hostage in February 2016 for $3.6 million in Bitcoin,[6] and more and more healthcare enterprises are creating reserves for data ransom. A 2016 IBM study quoted by *SC Media UK* showed that in the United States 70 percent of businesses receiving a ransomware demand paid to get their data back, with 50 percent of those paying more than $10,000 and a further 20 percent paying more than $40,000.[7]

No matter the technology used in the healthcare industry today—e-signature software, EHR platforms, wearable devices, smartphones, tablets, or other software or hardware—providers can either work to mitigate risk or watch the organization spiral into potentially uncontrollable vulnerability. Today's electronic environment leaves little room for laissez-faire security efforts if a healthcare provider wants to remain safe from attack and protected from the financial consequences of the inevitable.

Why HIPAA still matters

HIPAA in general, and the Security Rule in particular, imposes specific compliance burdens on healthcare "covered entities." Any use or disclosure of electronic protected health information (ePHI) not in compliance with the Privacy and Security Rules or more stringent state law constitutes a violation of HIPAA.[8] The failure of a covered entity to implement sufficient security measures regarding the transmission of and storage of ePHI to "reduce risks and vulnerabilities to a reasonable and appropriate level" is also a violation.[9] Likewise, a failure to implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of its facility, and the movement of these items within its facility, are violations.[10] And, once a security incident occurs, the failure to "timely identify and respond to a known security incident, mitigate the harmful effects of the security incident, and document the security incident and its outcome" are all violations.[11]

At the time of writing, most of the Security Rule fines and penalties assessed by the US Department of Health and Human Services Office for Civil Rights (OCR) relate solely or primarily to either (1) theft of devices containing unsecured ePHI or (2) failure to conduct a security risk assessment that is discovered when another privacy or security breach is investigated. Examples of such "traditional" enforcement activity in recent times include the August 2015 announcement of a $750,000 settlement against Cancer Care Group, P.C., for the theft of an employee laptop containing ePHI on 55,000 individuals, the December 2013 announcement of a $150,000 settlement against Adult & Pediatric Dermatology, P.C., for the theft of a thumb drive containing ePHI on 2,200 patients, and the announcement of settlements by Idaho State University and University of Washington Medicine for failure to conduct privacy and security risk assessments and failure to adequately adopt security measures. Were this still the level of involvement by OCR in ePHI enforcement, a shrug of the CIO's shoulders and a promise to encrypt all ePHI data at rest would be the universal response.

However, in recent times the enforcement focus has shifted to more "core" system security functions and away from the "low hanging fruit" of lost or stolen data-carrying devices. For example, a $850,000 settlement paid by Lahey Clinic Hospital in 2015 specifically references the failure "to assign a unique user name for identifying and tracking user identity" with respect to a particular workstation,[12] failure to have a working audit trail capability with respect to workstation activity,[13] and the failure to restrict physical access to workstations generally to authorized personnel. A similar enforcement activity against South Broward Hospital District in February 2017 resulted in a $5,500,00 settlement payment based on improper access to ePHI by over a dozen individuals exposing in excess of 80,000 patient records and the failure of the covered entity to "implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports"[14] and "to implement policies and procedures that establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process."[15] Several enforcement activities also resulted in settlements for failure to have business associate agreements in place with third-party vendors responsible for storing ePHI.[16] Just as the environment for bad cyber behavior has matured, so has the OCR's level of understanding of system and enterprise failures of the healthcare community.

The healthcare Internet of things

The task of HIPAA compliance and compliance with cybersecurity "best practices" is being made harder with the proliferation of Internet-connected devices in the healthcare industry. As recently as 2012, a Ponemon Institute survey reported that 69 percent of respondents did not even address

5 Larry Ponemon, "Cost of Data Breaches Rising Globally, Says '2015 Cost of a Data Breach Study: Global Analysis,' " Security Intelligence, May 27, 2015 – https://securityintelligence.com/cost-of-a-data-breach-2015.

6 Vincent Lanaria, "Hackers Hold Hollywood Hospital's Computer System Hostage, Demand $3.6 Million As Patients Transferred," Tech Times, 16 February 2016 – http://www.techtimes.com/articles/133874/20160216/hackers-hold-hollywood-hospital-s-computer-system-hostage-demand-3-6-million-as-patients-transferred.htm. The hospital eventually paid $17,000 in Bitcoin.

7 Max Metzger, "Your Money or Your Files: Why Do Ransomware Victims Pay Up?" SC Magazine UK, May 25, 2017 – https://www.scmagazineuk.com/your-money-or-your-files-why-do-ransomware-victims-pay-up/article/664211/.

8 45 C.F.R. §§ 160.103 and 164.502 (a). NOTE: CFR 45, Parts 160 and 164 can be found at US Electronic Code of Federal Regulations: Title 45—Public Welfare, Subchapter C—Administrative Data Standards and Related Requirements: 160-164 – https://www.ecfr.gov/cgi-bin/text-idx?SID=fbc57ba7be313c69e19aa1e78ac97adf&mc=true&tpl=/ecfrbrowse/Title45/45CsubchapC.tpl.

9 45 C.F.R. §164.308(a)(1)(ii)(B)

10 45 C.F.R. § 164.310(d)(1)

11 45 C.F.R. § 164.308(a)(6)(ii)

12 45 C.F.R. § 164.312(a)(2)(i)

13 45 C.F.R. § 164.312(b)

14 45 C.F.R. §164.308(a)(l)(ii)(D)

15 45 C.F.R. § 164.308(a)(4)(ii)(C)

16 As examples, see the July 18, 2016 Resolution Agreement with Oregon Health & Science University in which $2,7 million was paid and the September 23, 2016 Resolution Agreement with Care New England Health System in which $400,000 was paid.

the security of US Food and Drug Administration (FDA) approved medical devices in their IT security or data protection activities.[17] Since that time, over five billion devices—*not including smartphones*—have connected to the Internet, and that number is expected to grow to between 25 billion and 50 billion by 2025.[18]

The healthcare industry has particular patient safety risks associated with these devices, as revealed in a 2012 US Government Accountability Office report on the lack of action by the FDA to expand its consideration of information security for medical devices.[19] A November 2015 Wired.com survey listed the seven healthcare device types most vulnerable to hacking or other violation, which included drug infusion pumps, Bluetooth-enabled defibrillators, blood refrigeration units, and CT scanners—the failure of any of which would create tremendous patient risk. We have grown far beyond the fear of hacking the vice president's pacemaker.[20]

Eighty-four percent of health applications for smartphones that were approved by the FDA were found to create HIPAA violations and were "hackable."

The fact that smartphones are not included in this total is worrisome, as the growth in potential cyber risk due to smartphone use is even more troubling. Eighty-four percent of health applications for smartphones that were approved by the FDA were found to create HIPAA violations and were "hackable."[21] Also worrisome is the continued increase in the use of smartphones to transmit and receive unsecured ePHI (primarily by text message) for patient treatment by healthcare professionals, in spite of HIPAA's requirements and facility rules attempting to limit such activity.[22] Most health care enterprises gave up the fight over "bring your own device," or BYOD, rules due to provider pressure a long time ago anyway. Although study results vary, as of 2014 "upward of 90 percent of healthcare organizations permit employees and clinicians to use their own mobile devices to connect to a provider's network or enterprise systems."[23]

One has to wonder what OCR's response to all of this would be in light of the settlement agreements mentioned earlier: the decision not to impose device accountability for provider convenience may be fertile ground for future fines and penalties. And there is always the modern privacy paradox: health care consumers voluntarily share endless amounts of personal health information with applications on their smartphones, resulting in data being stored who-knows-where on the Internet without them thinking if it is convenient for them[24]; however, these same consumers continue to resist the same sharing activities by their own healthcare providers, even if such activity would result in faster and better health care.[25]

Cybersecurity insurance

In October of 2002, *The Economist* magazine opined[26] that "total security was impossible" and that insurance would be the way that businesses mitigated the financial risk caused by this lack of security. Since that time, both security defenses and security attacks have proliferated, changed, and become more aggressive and complex. However, the cybersecurity insurance market, though maturing, is not developing at as rapid a pace. Some issues that remain to be explored are due to the relative newness of the coverage and the lack of good predictive actuarial models.[27]

While the market matures, there are various factors that potential insureds should evaluate closely as they shop for and price out cybersecurity insurance. The first and most important of these coverages should be the coverage of costs related to managing breaches, to include expenses related to the investigation, remediation efforts, and patient notification. Other costs that may also be incurred are credit monitoring services,[28] damages associated with identity theft, damages associated with recovery of data, damages incurred due to having to reset EHR systems, and damages to reconstruct or recover websites and other Internet presences. Business continuity expenses related to workarounds or loss of revenue due to a cybersecurity incident might also need coverage, especially as most commercial policies of this type are figuring out how to exclude cyber-related risks from their covered losses. Finally, but not least importantly, coverage for rogue employees and insider threats needs to be a part of the insurance package.

17 John Glaser, "The Risky Business of Information Security: With Growing Threats to Patient Privacy and Increasing Sanctions by Regulators, Make Data Security Central to Your Business," Hospitals & Health Networks, August 12, 2014 – http://www.hhnmag.com/articles/4064-the-risky-business-of-information-security.

18 The Florida Bar, "8th Annual FUNdamentals: The Legal Implications of the 'Internet of Things'," Course 2232R (September 16, 2016)

19 GAO, "Report to Congressional Requesters: Medical Devices: FDA Should Expand Its Consideration of Information Security for Certain Types of Devices," United States Government Accountability Office, August 2012 – http://www.gao.gov/assets/650/647767.pdf.

20 Lisa Vaas, "Doctors Disabled Wireless in Dick Cheney's Pacemaker to Thwart Hacking," Naked Security, Sophos, 22 Oct 2013 – https://nakedsecurity.sophos.com/2013/10/22/doctors-disabled-wireless-in-dick-cheneys-pacemaker-to-thwart-hacking/.

21 Ibid.

22 Ibid. (citing a 2015 University of Chicago survey finding that over 70 percent of its medical residents improperly sent ePHI by text messages).

23 John Glaser, "The Risky Business of Information Security: With Growing Threats to Patient Privacy and Increasing Sanctions by Regulators, Make Data Security Central to Your Business," Hospitals & Health Networks, August 12, 2014 – http://www.hhnmag.com/articles/4064-the-risky-business-of-information-security.

24 Shannon Barnet, "Millennials and Healthcare: 25 Things to Know," Becker's Hospital Review, August 04, 2015 – http://www.beckershospitalreview.com/hospital-management-administration/millennials-and-healthcare-25-things-to-know.html. 71 percent of Millenials surveyed by Harris would use a mobile app to share health care data with providers. See also Mintel, "Sixty Percent of Millennials Willing to Share Personal Info with Brands," Mintel, March 7, 2014 – http://www.mintel.com/press-centre/social-and-lifestyle/millennials-share-personal-info, in which the study reports that 60% of Millennials would be willing to provide details about their personal preferences and habits to marketers, and, of those that would not initially provide such information, 30% would do so after receiving an incentive offer such as a discount off future purchases.

25 Denver Nicks, "Survey: Millennials Care about Privacy (But Not So Much in Japan), Time, Nov. 07, 2013 – http://techland.time.com/2013/11/07/survey-millennials-care-about-privacy-but-not-so-much-in-japan/. Only 4% of respondents would be comfortable with data being used for a purpose outside of its original context. The study also says that these preferences vary by economic status, with high-income worried more about data privacy than low-income people.

26 "Putting It All Together," The Economist (October 24, 2002)

27 Koo, "More Incident Data Needed for Cybersecurity Insurance," Bloomberg BNA (March 28, 2016)

28 Even though there is almost a universal recognition in the law enforcement and security communities that these programs do no good at all, as the sophisticated hacker knows to wait out the 1-2 years of service before making use of the stolen data.

The type of coverage a healthcare enterprise can obtain, and the premiums therefore, may be affected by certain underwriting considerations, all of which should inform the enterprise's compliance efforts:

- The enterprise should be able to show that it is in compliance with HIPAA, including those provisions that require security and privacy risk assessments and proof of a plan of mitigation and remediation. Insurers likely will not cover losses resulting from a gap in HIPAA compliance, especially because there is a legal obligation on the enterprise to find out what those are.
- The potential insured needs to know what the insurer's requirements are for encryption beyond those mandated by HIPAA. Some coverages require more secure and more robust email systems that are more resistant to phishing and spoofing, and even other coverages may require intentional phishing attacks by the insured's IT department or vendors to gauge compliance with training.
- The training requirements for new employee onboarding and access by non-employee contractors may need to meet certain criteria beyond HIPAA workforce awareness training.
- Insurers may require that contractors providing "business associate" services be separately insured as a first layer of defense against cost.
- The potential purchaser needs to be on the lookout for what is referred to in the industry as "cannibalizing" coverage, in which the costs of defense reduce the limits available to pay damages or judgments. The best coverage separates costs of defense from claims expenses.
- The purchased coverage, as with certain types of malpractice insurance, should be based on the "date of detection" as opposed to "date of intrusion." It is so difficult, even with the best system monitoring tools, to determine when a breach or incident actually first occurred, so the enterprise does not want to be locked into a technical dispute with the insurer about when the hack "should have been" detected.
- The prospective insured needs to know whether offshore operations will be covered. Significant risks are associated with outsourcing certain data manipulation and management functions to countries or regions that have stronger privacy and data security rules than the United States. In particular, the European Union takes a dim view of American-style discovery and most likely will not permit the compelled return of data from an EU vendor in litigation pending in United States courts.

Conclusions

The growth of connected devices, connected physicians, and connected patients will continue to push healthcare facilities to provide more interoperability for health data than ever before. These same technological pressures will make it more and more easy for cybercriminals and disgruntled employees to compromise the data upon which everyone relies for reliable patient care, because an increase in interoperability in most cases creates an increase in gaps in security. Healthcare systems need to recognize this risk as a direct threat to patient care, and not just to its financial and technology resources. A holistic security approach, combining effective cybersecurity practices, HIPAA training and compliance, and appropriate insurance coverages will be the best way to address this growing area of opportunity—and risk—in the future.

About the Author

Barry S. Herrin, JD, FAHIMA, FACHE, is the founder of Herrin Health Law P.C. in Atlanta, Georgia. Herrin has over 25 years of experience practicing law in the areas of healthcare and hospital law and policy, privacy law and health information management, among other healthcare-specific practice areas. He is both a Fellow of the American College of Healthcare Executives and a Fellow of the American Health Information Management Association. He may be reached at barry.herrin@herrinhealthlaw.com.

ISSA
CAREER CENTER

The ISSA Career Center offers a listing of current job openings in the infosec, assurance, privacy, and risk fields. Among the current 871 job listings [12/30/17] you will find the following:

- **Assistant Director Faculty Position,** University of West Florida Center for Cybersecurity – Pensacola, FL
- **Assistant/Associate/Full Professor in Computer Science,** United States Coast Guard Academy – New London, CT
- **Broadband System Maintenance Technician (BB Specialist IV),** Mediacom – Saint Peter, MN
- **Penetration Tester,** Palindrome Technologies – Hazlet, NJ
- **Cyber Security Manager and Chief Information Security Officer,** National Renewable Energy Laboratory (NREL) – Golden, CO
- **Information Security Analyst - Cryptographic Key Management,** American Express – Phoenix, AZ
- **Information Security Specialist,** American Express – Phoenix, AZ
- **Cybersecurity Service Provider Information Security Analyst in Fort Meade, MD at Booz Allen Hamilton,** Booz Allen Hamilton – Fort Meade, MD
- **Information School Assistant Professor Tenure Track,** University of Washington Information School – Seattle, WA

ISSA
Information Systems Security Association

2018 ISSA International Conference:

SECURING TOMORROW TODAY

October 15-17, 2018
Westin Peachtree Plaza, Atlanta Georgia

The Information Systems Security Organization's seventh annual flagship conference is a world-class event bringing together cyber, information, software, and infrastructure security professionals from 92 countries around the world. The two-day conference delivers practical sessions and no-nonsense insights that give cybersecurity professionals the tools to strengthen their security without restricting their business.

Conference Highlights

- 800+ attendees spanning all levels of IT and InfoSec
- Six education tracks totaling 40+ sessions
- Expert keynote program on the latest information security trends and technologies
- Intimate roundtables and panel discussions
- Expo floor featuring more than 35 leading technology companies
- Networking lunches, general sessions, and evening receptions and award parties
- Career center

Topics

- Emerging technologies (with real-world applications)
- Application security
- Business skills
- Cloud security
- Digital forensics
- APT defense
- Mobile devices and BYOD
- Incident response

Registration opens soon. For more information, visit www.issa.org