ISSA JOURNAL

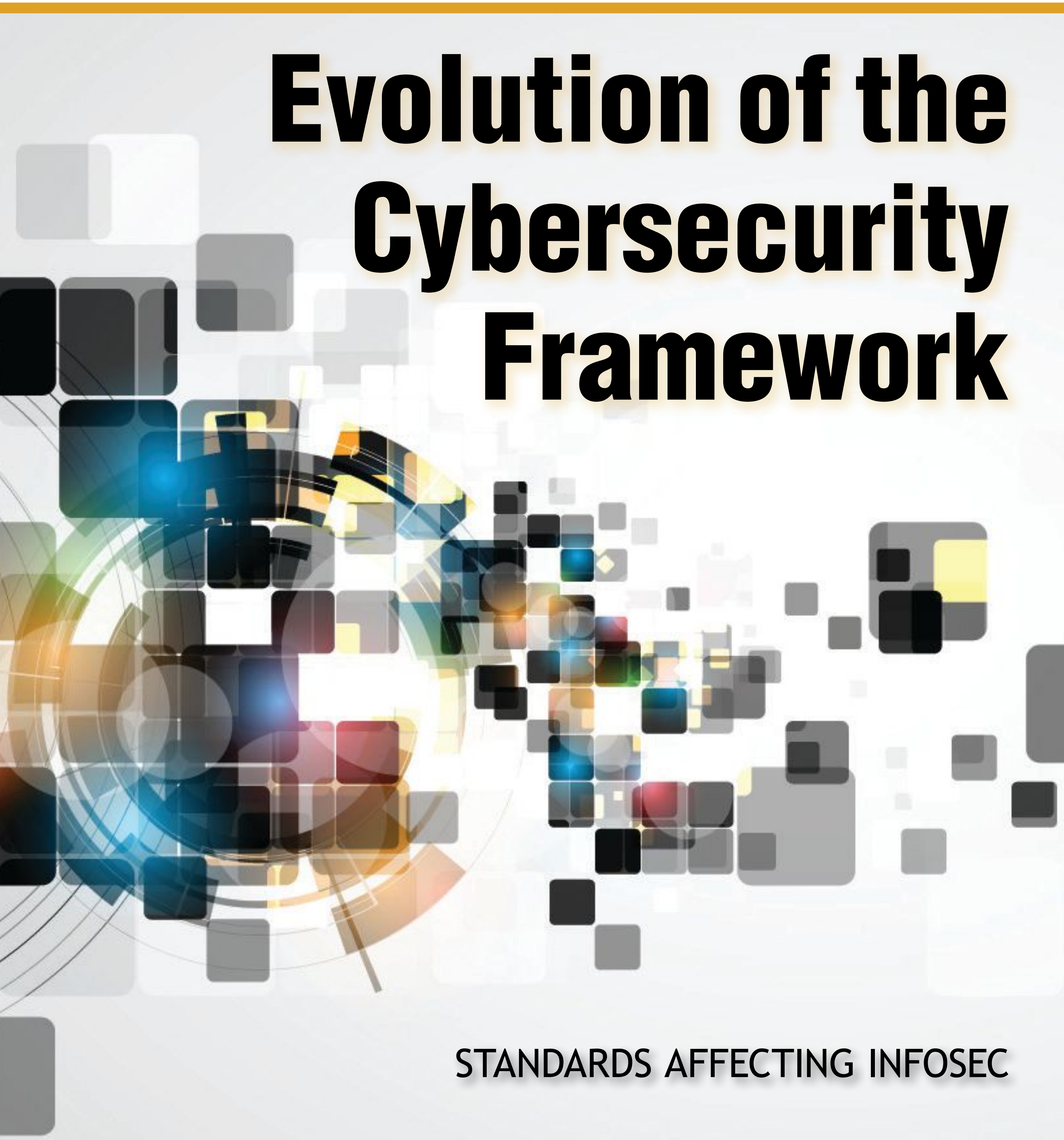
July 2018
Volume 16 Issue 7

A Multi-Pronged Approach to GDPR Compliance

Information Security Standards: Differences, Benefits, Impacts, and Evolution

Net Neutrality: What Is It and Is It Necessary?

PCAP Next Generation: Is Your Sniffer Up to Snuff?



Evolution of the Cybersecurity Framework

STANDARDS AFFECTING INFOSEC

Table of Contents

DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

Feature

Articles

Also in this Issue

ISSA JOURNAL
July 2018
Evolution of the Cybersecurity Framework
STANDARDS AFFECTING INFOSEC

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

The ISSA Journal (1949-0550) is published monthly by
Information Systems Security Association
1964 Gallows Road, Suite 310, Vienna, VA 22182
+1 (703) 382-8205 (local/international)

Hello, ISSA Members and Friends

Keyaan Williams, International President

The Future Is Bright

Things continue to change for the association. Although we've had a few hiccups in 2018, the future of the association is bright. As we prepare for the new association year and a new cadre of directors on the International Board, I'd like to provide some information and context about notable items coming up in conversation around the membership right now.

ISSA website

The URL that members are accustomed to visiting, www.issa.org, was automatically redirecting to https://issa.site-ym.com. Although the temporary address was legitimate, we did a poor job of communicating what was going on for our members. We hoped to resolve the situation faster than we did. Now that things are back in order, I think an explanation is still worthwhile.

The backend provider for the ISSA membership website recently transitioned its original data center to Amazon Web Services (AWS). ISSA received limited notice about the change. When we were notified, we had to quickly choose between continuing to manage our own DNS or giving DNS control to a third party. We decided to go with the former option for the following reasons:

- We were concerned about the possible risk of interruption or disruption to services made available to chapters within our current environment
- We are in the early stages of planning a new website and did not want our options to be limited
- We did not want to rebuild various chapter subdomains and other services within the new hosting environment

A consequence of the transition to AWS and our decision to continue to self-manage our DNS was that the ISSA website temporarily redirected to a site that led many people to think the ISSA website was compromised. We apologize for the confusion this caused. This experience provided a good opportunity to update our communication procedures to avoid repeating the same mistakes when another situation arises.

Changing the bylaws

The International Board is made up of dedicated volunteers who are doing their best to serve the interests of the association and our members.

The way the ISSA operates has changed significantly since changes to the bylaws were last ratified in 2001. During ISSA's 2018 election cycle, members had an opportunity to vote to accept or reject amendments that modernize the association bylaws and reflect the way ISSA currently operates. The amendments that members saw were the final recommendations that received approval following their review by a special meeting of chapter presidents. The changes on the ballot are the only proposals that received majority support from the International Board and the chapter presidents who participated in the review process.

One of the more controversial changes was the proposal to extend the term of service for members of the International Board. The board manages the official business of the association during eight days of face-to-face meetings (two days each quarter), and one-hour web calls hosted each month to address critical items. Extending the two-year term to three years provides time for the elected members of the board to accomplish their goals, projects, and initiatives before their terms expire.

Monthly chapter leaders call

I encourage all chapter leaders to participate in the regular chapter leaders calls that the ISSA Chapters Committee offers. We have significant participation from some chapters, but many chapters are not taking advantage of this opportunity to collaborate and receive advance information about important events and activities at ISSA that affect the membership. Participation provides the best opportunity for chapter leaders to discuss what is happening behind the scenes and relay that information to their chapter members.

Thank you, *Keyaan Williams*

How Do You Read Your ISSA Journal?

- **BlueToad online magazine**: all issues are fully searchable
- **ePub or PDF**: download to your device for anytime, anywhere access
- **Printed hard copy**: delivered to your mailbox quarterly

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, Distinguished 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
1964 Gallows Road, Suite 310, Vienna, VA 22182
+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.

Animal, Vegetable,…or Infosec Standard?

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

I know that many of you have probably heard that old adage: "If you ask 10 infosec professionals for the most important or universal infosec standard, you will get 20 answers." OK, so maybe it's not exactly an old adage, but you get the idea. The landscape of infosec standards contains a tremendously wide assortment of numerous different kinds of documents.

To me, the gauge of how a particular standard affects infosec correlates directly with how often I run into said standard during contract negotiations. Let's take a look at a few, but arranged in an order that is reflective of what I see and work on most frequently:

General Data Protection Regulation (GDPR) – As we all know, GDPR is NOT a standard (as aren't many of the entries in this list), but it sure feels like a standard at times. It mandates using a reasonableness approach to security. It also results in negotiations of several different contractual obligations, including standard contractual clauses, data processing addendums, and a host of other obligations. Note that I was tempted to fill out my column by simply listing the GDPR about 23 times, but I knew my editor would have a conniption.

Payment Card Industry (PCI) Data Security Standard (DSS) – Though many people often call this a law or regulation, it's actually a creature of contract. Developed by the major credit card companies (including Visa, American Express, and MasterCard), the DSS sought to bring at least some commonality to credit card security. It's also a favorite component for contractual wrangling, whether for services or (increasingly) in just about every M&A deal.

NIST 800 Series – Just as PCI often gets mislabeled as a "law," the NIST 800 series of documents often gets mislabeled as the "NIST Standards." In fact, the excellent series of what are known as "Special Publications" has a wide variety of documents ranging from highly detailed technical security specifications, to broad security frameworks. The two I run into most frequently are:

- **NIST SP 800-53** – Titled "Security and Privacy Controls for Federal Information Systems and Organizations," SP 800-53 provides a set of security and privacy controls that can be applied to both federal and commercial information systems and organizations. It also includes a process for selecting controls to protect a variety of stakeholders from a diverse set of threats including hostile cyber attacks, natural disasters, structural failures, and human errors.
- **NIST SP 800-171** – Titled "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," SP 800-171 focuses on what is necessary to protect information determined to be controlled unclassified information (CUI).

ISO/IEC 27000 family of Information Security Management Systems - The ISO/IEC 27000 family of documents comprises a set of standards and guidelines for information security governance, including focusing on an information security management system (ISMS).

- **ISO 27001** provides the requirements for establishing, implementing, maintaining, and continually improving an ISMS within the context of the organization.
- **ISO 27002** introduces the code of practice for infosec controls.

NIST Cybersecurity Framework – Again, not really a standard but a framework that allows infosec to be abstracted to five activities: Identify, Protect, Detect, Respond, and Recover. From that abstraction, a practitioner can delve deeper and deeper,

COBIT – The Standards Board of the Information Systems Audit and Control Association (ISACA) publishes a standard called Control Objectives for Information and related Technology (COBIT). COBIT provides a control framework for IT governance.

OWASP Top Ten Project – This web application security project resulted in a publication by the Open Web Application Security Project (OWASP) of the top ten most critical web application security flaws, which is often used in contracts as a way of ensuring at least some level of app security.

WebTrust program – The WebTrust audit, if successful, leads to a seal on a website indicating the company complies with the WebTrust principles related to security, online privacy, business practices and transaction integrity, and availability.

So that's my list of standards that help drive the infosec field. Now I'm going to throw one more old adage at you: "When you finish you ISSA column, it's time for a cold one in the heat of a Washington, DC, summer." OK, that one I TOTALLY made up, but that's what is needed with the temperature in the 90s and the heat index in the low 100s. Stay cool everyone—see you next month!

About the Author

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

Fine, I'll Comply

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

Another year, another standard. 2018 brought us the General Data Protection Regulation (GDPR), and within hours of its enforcement period coming live lawsuits were predictably filed against Facebook and Google. While this particular one has a privacy theme, section two does lay out three security requirements ranging from processing to notification to communication requirements.

But let's back up for a moment.

In 2004 when I was starting do a lot of payment security work, I had a key conversation with a security leader in a large retailer. This leader said to me, "I can't wait until we are done with this CISP/PCI stuff so we can get back to doing real security."

At the time, I discovered that I was capable of Oscar-worthy acting in which I maintained my composure and said, "I hear you." On the inside, I was laughing uncontrollably. Why? Because in this particular instance, this company needed PCI to bring them to the appropriate security levels for the time. And those that remember PCI DSS in 2004 should remember that while it was far reaching for many retailers at the time, it still was only scratching the surface of what needed to happen from a security perspective.

Today, however, I see more companies that are correct in saying "Man, I'll be glad when we're done dealing with $X standard so we can get back to real security work."

The problem with standards that have teeth to them is they set a bar that seems high or unreasonable to firms comparing their posture against them. Our response to new standards follows exactly the Ross & Kessler Five Stages of Grief:

- **Denial:** We don't have to comply with this; it doesn't apply to our business.
- **Anger:** Who the heck do these people think they are, telling me how to run my shop?
- **Bargaining:** What if I carve out this network, outsource this process, or divest this business?
- **Depression:** This standard is going to cost us millions and end my career.
- **Acceptance:** OK fine! You wore me down. Reluctantly, I'll comply.

For standards of sufficient size and impact, getting to the *I'll comply* phase generally creates a mass of companies that now have some level of expertise or dependence on it. It will move markets in cases, which then brings in some difficult questions from Congress or other legal entities.

I agree that some regulation is required to force managers to invest in technologies and systems that will work to protect their electronic assets. The collateral damage from free market capitalism here is too devastating and ultimately impacts you and me once the pwned company shuts its doors.

But what happens when technology improves? If I would have told you in the year 2000 that the company responsible for powering some of the largest Internet properties fifteen years into the future is the same one that ships books, DVDs, and CDs to your home, would you have believed me? The world moves faster than regulation or standards, and those regulations and standards are always playing catch-up—often times becoming obsolete before their framers intend them to.

Or, perhaps more accurately, the high bar of compliance that we vaulted over before is now something we trip over as we shuffle our feet toward the next checkpoint.

I've been writing this column for a decade now, and one thing continues to ring true from my years as a consultant and someone who helped companies interpret and build programs around standards such as PCI DSS, ISO 27001 (or ISO17799 back then), and NERC CSS: compliance and standards will come and go, but good security practice is here to stay.

Security practice must evolve over time. Consider applying the Toyota production system's implementation of kaizen, or the concept of continuous improvement you see as part of the DevOps movement. If you are not changing your internal security programs to match current threats, you are at risk of being the slowest hiker running away from the attacking bear.

When you get a free moment, consider honing your Google-Fu to see the myriad of standards that either directly apply or have partial applicability to information security. In most cases, the baselines of those standards have a lot in common. It's only the nuances specific to the industry or process it is targeting that add the variability that makes up the difference.

About the Author

Branden R. Williams, DBA, CISSP, CISM, is a seasoned infosec and payments executive 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/.

Infosec Standards

By Mark Anderson – ISSA member, Australia Chapter

My first use of infosec standards occurred when I was providing advice on architecting a system for government use and was confronted with the Rainbow Series. Diligently applying the *Orange Book* and *Red Book* after an exposure risk analysis from the *Yellow Book*, I quickly discovered everything verged to an "A1" requirement where the security model itself had to be mathematically verified. Given that perhaps only one system existed at the time with such an evaluation level, and did not meet even 10 percent of the functionality requirements, things didn't look too promising.

Perhaps the most fundamental issue was the interweaving of functionality with assurance, and the assumption that everyone ran a military grading classified system based on Unix. This approach clearly does not work in highly networked heterogeneous environments.

After the *Orange Book*, came a range of attempts to fix the obvious deficiencies such as Information Technology Security Evaluation Criteria (ITSEC), which at least tried to separate functionality from assurance and move away from specifying functional policies. But it fared no better for widespread take up and unsurprisingly so since the cost for non-trivial assurance levels quickly required an additional thousands of dollars per line of code to verify. The NSA had another try with the Common Criteria, which superseded ITSEC, and one of my inventions was apparently the first official device to receive the highest (EAL7) rating and went onto operational deployment. While products are evaluated under the criteria, we do not hear that much about it in the broader community.

So, what went wrong with all these standards?

Firstly, with my device (the actual evaluation work was undertaken by others but as the original inventor I was of course a most-interested observer) as just one example, the pain of going through the Common Criteria process was massive and required huge amounts of time. While that did not kill off my device since at the time it solved a serious national security problem and ended up being used by various governments and their agencies, it simply would not have been commercially viable to the larger business community if you had to add two to three years to the backend of your product development before going to market. And that was just for a particular version. I do note, however, that the Common Criteria process did try partially to solve the version issue with methods to streamline evaluation across versions in order to maintain its accreditation status.

Secondly, the standards were developed primarily under the custodianship of the intelligence community. At first this would seem to be sensible, given the expertise base. But in doing so, the practical, everyday drivers facing the broader commercial community can be too easily ignored, resulting in a standard that can be quite applicable to the high-grade secure needs of government departments, but less so for a commercial community with a broader array of functions. The end result was a move away from evaluation to a "risk managed" approach, which unfortunately resulted, in reality, to a "completely ignore risk" approach.

Unless the application of an infosec standard does not cost as much as the development of the system itself and does not require huge investment to be maintained, a standard, no matter its field of application, is unlikely to achieve widespread take up across an economy.

Where standards have been more successful has been in the crypto area such as NIST's DES and AES, which defined an algorithmic standard. Nevertheless, there is the cautionary tale with OpenSSL FIPS140-2. However, the lifetime of a protocol can amortize the cost of the proving the integrity of the protocol. But there has been a much lesser amount of success for systems and applications. Trying to apply a rigorous standard to software under today's DevOps regime where updates can occur almost daily would seem steered to failure unless the infosec standard testing compliance can be totally automated. Good luck with that.

My view is that an overarching infosec standard for systems once envisaged by the *Orange Book* is still not viable. There needs to be a much greater effort at secure architecting with standards of assurance focusing on longer life cycle, more primitive building bricks, and protocols that supply specific functions to support the architect. But, of course, we then still have the dreaded composability problem, but that is part of the art of secure architecting.

About the Author

Gray Hat is an ACM Distinguished Engineer and principal inventor for several patented devices and major systems that have entered operational service with the US Armed Forces, as well as other national governments for high-grade information security purposes. He can be contacted at msanderson@ieee.org.

The Failure of Compliance

By Luther Martin – ISSA member, Silicon Valley Chapter

High-profile data breaches at US federal agencies have undermined public confidence in the government. And although the Cybersecurity Act of 2015 requires federal agencies to encrypt or otherwise render indecipherable sensitive data that is stored on or transiting agency information systems, many federal agencies address this requirement in a way that provides little or no meaningful protection against data breaches. To understand the limitations of the approach that they typically use, it is helpful to understand a notional "encryption stack" that is conceptually similar to the familiar Internet protocol (TCP/IP) stack that provides the basis for today's Internet.

One notable feature of TCP/IP is how it abstracts the functionality of a computer network into four layers that we think of as comprising a "stack." In this notional stack, we have multiple logical layers that process information in a way in which information only gets passed between adjacent layers of the stack.

The TCP/IP stack comprises four layers:[1, 2] Application, Transport, IP, and Network Access (sometimes called the Link layer). Information is only passed between adjacent layers of the TCP/IP stack. A process running at the transport layer can pass information to a process running one layer away at the IP layer but not to one running two layers away at the network access layer, etc.

Similarly, it can be useful to think of encryption as taking place either relative to or at different levels in the TCP/IP stack, thus creating a notional "encryption stack" that closely parallels the TCP/IP stack. TLS encryption that is used by secure websites, for example, operates between the application layer and the transport layer. Internet Protocol Security (IPsec) encryption that is used to create virtual private networks (VPNs) operates at the IP layer. Link encryptors encrypt at the network access layer. Full-disk encryption (FDE) operates below the network access layer, as does transparent database encryption (TDE).

There are good reasons to encrypt at different places relative to the TCP/IP stack, but it is important to understand that when you encrypt at a particular place in the stack, the encryption only protects against threats that target layers at or below where the encryption takes place.

If you protect data with full-disk encryption, for example, the encryption will protect the data while it is stored on the encrypted disks. When the data leaves the disks and is handed off to the network access layer, that particular form of encryption no longer protects it. If a cybercriminal manages to steal a hard disk that is encrypted with FDE, he will probably be unable to read its contents. But if a cybercriminal intercepts information being transmitted across a network, the FDE provides absolutely no protection to the data. Similarly, malware that reads data from a hard drive that is protected with FDE will be totally unaffected by the FDE – once the encrypted data is read from the hard disk, the FDE no longer protects it.

And if you are using TLS to encrypt data between the transport and application layers, the TLS encryption will protect against attacks that target the transport layer, the IP layer and the network access layer, but it will not protect against attacks that target processes running at the application layer. Once data that is encrypted using TLS gets passed up the stack to the application layer, the TLS encryption no longer protects it.

But the biggest and most severe data breaches that have affected both the public and private sector all operate at the application layer. This includes almost all types of malware and advanced persistent threat (APT) attacks. Because of this, encrypting at the application layer is the only form of encryption that will address these important threats. TLS encryption does not protect against threats that operate at the application layer. Nor does FDE. Nor does TDE. But since these are the most common forms of encryption currently used by federal agencies, most of the use of encryption that they use is ineffective at protecting against the most serious threats that they face.

Federal agencies do indeed use encryption as the Cybersecurity Act of 2015 requires, but the most common forms of encryption that are used (TLS, FDE, and TDE) provide minimal protection for the most serious threats that the agencies face. And it seems likely that these technologies will also continue to provide an inadequate level of protection against malware and APT attacks in the future.

About the Author

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

[1] Braden, Robert. "RFC-1122: Requirements for Internet Hosts." *Request for Comments* (1989).

[2] Braden, Robert. "RFC-1123: Requirements for Internet Hosts – Application and Support." *Request for Comments* (1989).

If the Cyberspace Frontier Has Closed, Why Is the Internet Still Such a Dangerous Place?

By Geordie Stewart – ISSA member, UK Chapter

Some of us are old enough to remember when the cyberspace frontier was pronounced "closed." The frontier of the American Wild West was an apt metaphor. The early days of the Internet was a time of rapid expansion and relative lawlessness. It wasn't always clear what the rules where or who the sheriff was. As law enforcement trained up, jurisdictions were agreed and sheriffs were appointed, it seemed for a time like the lawless days were numbered, if not over. However, there are a number of reasons why the closing of the cyberspace frontier didn't work out as we thought.

Firstly, we had no idea the extent that intelligence agencies, both friendly and hostile, were dedicating themselves to undermining the security of the Internet. The applications we use, the encryption we depend on, and the network backbones we traverse were under wide-scale systematic attack. The problem is the ubiquity of security protections. The same security protections that provided us security for our private information and our commercial interests also prevented intelligence agencies from gathering the information they needed to perform their missions. We'll probably never know how much harm has been caused by this. Consider the impact of this on civil litigation and the right to seek redress, which is a key aspect of the rule of law. If you suffer harm or loss as a result of the activities of an intelligence agency, how would you seek redress? Would you even know in the first place?

Secondly, globalization, the force that has powered so much of the world's commerce, has also meant opportunities for illicit profit for individuals and groups in developing countries. Although numerous international treaties exist, there is a threshold for when it's cost effective for law enforcement to get involved across international borders. To make the best use of their limited resources, cyber law enforcement needs to concentrate on major crime groups. This means that large numbers of small-time criminals are free to operate across borders with impunity. In fact, some countries have a history of ignoring cyber criminals residing in their country so long as their targets are in foreign nations.

Thirdly, due to privacy laws we've seen very little cooperation in industry to combat cyber attackers. The problem is that rather than risking oversharing personal information, it's in the interests of most organizations to only share the information they have under court order. This means that in Europe, should you contact an ISP and make an allegation that criminal activity has been conducted using their services, you are unlikely to get any cooperation other than the suspension or disabling of the service that was causing the problem. It's very difficult to get any information, let along something that is personally identifiable and might help you hold someone accountable for their actions. For example, can an ISP tell you something generic like which city an IP address was used from? The answer is no from bitter experience. Sure, organizations can be compelled to share what they have in terms of logs, but this creates a very high bar where only very serious or repeat crimes are investigated properly. There has long been an exception under data protection laws to be able to share information for the purposes of crime prevention, but most organizations choose not to go down this route. So long as we have organizations with a vested interest in not cooperating to hold people accountable, this won't change any time soon.

To complete the metaphor of frontier justice, we now have serious proposals to make it legal to "hack back." US lawmakers have proposed the Active Cyber Defense Certainty Act. Basically, it would be legal to access systems that don't belong to you as long as certain conditions are met. Ultimately of course, it doesn't solve the problem of attribution. Was the source of a connection made to your network the source of the attack or was it in turn another third party that has been compromised by an attacker? Hacking back could be causing further harm to another party which has itself been a victim of a cybercrime. If the idea of organizations hacking back doesn't sound like the Wild West, then I don't know what is. The solution? There's no such thing as a "safe" Internet and the price of Internet freedom is eternal vigilance, security awareness, and computer-based training.

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.

News That You Can Use...

Compiled by Kris Tanaka – ISSA member, Portland Chapter and Stephen Teppler

GDPR Oddsmakers: Who, Where, When Will Enforcement Hit First?

https://www.darkreading.com/risk/compliance/gdpr-oddsmakers-who-where-when-will-enforcement-hit-first-/d/d-id/1331898

Now that the GDPR grace period has ended, experts take their best guesses on when data protection authorities will strike and what kind of organizations will be first to feel the sting of the EU privacy law. Worried? You may have good reason—investigations have already started. However, if you have begun your compliance process, you may be able to relax a bit. Regulators are currently focusing on those organizations that show blatant disregard and willful neglect for the law and its intent.

Compliance Is Not Synonymous with Security

https://www.securityweek.com/compliance-not-synonymous-security

Most of us agree that compliance does not equal security. Furthermore, as the author states, most breaches occur at places that are compliant to something. That said, compliance requirements, whether from the private world or international standards bodies, do tend to reduce risks and vulnerabilities.

We're Losing the Race to Patch Known Security Flaws: Will GDPR Help?

https://www.infosecurity-magazine.com/opinions/losing-patch-known-security-flaws/

Will GDPR change the world? Maybe. We will have to wait and see. However, one security area that GDPR might be affecting is patching. According to the article, "GDPR fines are designed to change behavior, not just appeal to enlightened self-interest. European regulators have already sent signals that they believe a failure to patch on a timely basis is an infraction under GDPR." As organizations look for better ways to deal with too many unapplied software fixes, virtual patching is emerging as possible solution to help speed up the patch cadence.

The Messy, Musical Process behind the Web's New Security Standard

https://techcrunch.com/2018/06/11/the-messy-musical-process-behind-the-webs-new-security-standard/

If you're a security standards geek, this is a good read. And for those who want to see how IETF uses GitHub, don't miss this article. Quite frankly, anyone who has ever participated in the creation of any standard will appreciate this quote, "the process of creating TLS 1.3 took four years, which for people in the security world is simultaneously forever and no time at all."

Supply Chains Brace for New Data Standards

https://www.supplychaindive.com/news/GDPR-compliance-logistics-right-to-be-forgotten/524071/

Let's face it, GDPR is currently the hot topic for the *ISSA Journal*. On a personal note, I was drawn to this article since I have worked in different aspects of supply chain. Bottom line: When a website called "supplychaindrive" states, "many US companies are simply not prepared to fully comply with GDPR by the deadline," you know we're in trouble.

Trudeau Government to Kick Off Talks towards National Strategy on Big Data

http://ottawasun.com/news/national/trudeau-government-to-kick-off-talks-towards-national-strategy-on-big-data/wcm/a220bb28-3209-4dd4-a891-862774e5cbcb

In order to avoid potential pitfalls in the growing global data-driven economy, Canada has issued a political call to action to create national strategy on big data. What is most encouraging is that they want security and privacy considered in the early stages rather than as an afterthought.

Will Blockchain Power the Next Generation of Data Security?

https://www.helpnetsecurity.com/2018/06/18/blockchain-next-generation-data-security/

As an unrepentant lover of all things blockchain, I had to throw this one in the mix. Here is a good discussion on why blockchain has so much more potential than cryptocurrencies. The author states, "Because blockchain had to be built to be impenetrable, and it can conceptually store any type of data, its applications in data security are profound." Profound indeed. Enjoy.

A Hard Look at Software Risks

https://automotivelogistics.media/intelligence/a-hard-look-at-software-risks

Few people realize how much software runs in today's cars. How true. Thanks to the growing connectivity in automobiles, there are many similarities to the smartphone experience. Carmakers can learn a great deal from the evolution of that industry—especially when it comes to dealing with cyber threats.

Deleting Your Online DNA Data Is Brutally Difficult

https://www.bloomberg.com/news/articles/2018-06-15/deleting-your-online-dna-data-is-brutally-difficult

Think before you spit into that test tube. As the direct-to-consumer genetic-testing industry continues to grow by leaps and bounds, it is important to remember that your genetic data may be used in unexpected ways by people you had no idea you were sharing it with. Never forget, "Once you share something online, you can't really ever unshare it."

Interview: Donn Parker

Information Security Pioneer

Donn Parker, CISSP retired and ISSA Distinguished Fellow, has specialized in information security consulting for many of the largest corporations and engaged in computer crime research at SRI International for 35 of his 50 years in the computer field. His sixth book, *Fighting Computer Crime, a New Framework for Protecting Information*, was published in 1998. Among numerous industry awards, he received the 1992 ISSA Award for Outstanding Individual Achievement and was inducted into the ISSA Hall of Fame in 2000. *Information Security Magazine* identified him as one of the five top information security pioneers (1999) and (ISC)^2 presented him with the Harold F. Tipton Lifetime Achievement Award in 2003. Donn formerly served on the *ISSA Journal* editorial advisory board.

It's been a while since you've served with the EAB; thank you for this opportunity to catch up.

You have been involved in information security for longer than most anyone. What is the greatest challenge you faced as an information security professional?

My greatest challenge was convincing information security professionals that making security decisions based on security risk is not viable. Information security risk is not determinable because we don't know how many loss incidents occur. Decisions should be diligence-based on many factors: Vulnerability and threat analysis, laws and regulations, policies, standards, contracts, insurance, tradition, audits, generally accepted practices, current trade literature and expert recommendations, available products, vendors' input, experience, and experimentation, available talent, business conditions, timing, stakeholders' acceptance, and control principles.

Can you tell us what is the most important aspect of information security you have had to deal with?

An important aspect is finding and understanding the perpetrators of harmful acts and effective security safeguards against them.

We are seeing more and more sophisticated cyber attacks as time goes by. What are our greatest challenges in combating cyber attacks and how can we address these going forward?

We can't adequately protect our stored information assets and systems against all kinds of cyber attacks. Some are unknown or unanticipated long after they occur. This makes timely system and data backup, detection, recovery, and correction important.

Today, many people think that we do not have any privacy and we should not have any expectation of ever having it. What are your thoughts?

We should stick to our expertise protecting the confidentiality, possession, and control of information and leave the different subject of human rights privacy to the lawyers and privacy experts.

Looking forward from a technological perspective, what areas of information security (networking, operating systems, encryption, access controls, etc.) do you see having the most promise?

The greatest promise is in artificial intelligence applied to loss incidents detection and system and data backup, recovery, and correction. Some loss events occur at computer speeds and require attention in that same time frame.

Ultimately system architecture must be changed so that a trusted and authorized user would be required to have phys-

ical access and presence and use physical locks and keys to make any changes or additions to the software in a computer system. This adds a layer of physical security on top of the logical security that we have today. Software must only be physically accessible to facilitate much stronger physical security safeguards.

Given the limited resources most organizations have for addressing information security and considering current trends, where do you recommend investing for the future?

First invest in detection, backup, and recovery; and second, implement all the applicable fundamental and known basic controls. I found that in more than 200 large companies they had excellent security in many ways but poor or non-existent security in at least one aspect.

Many research companies have their favorite top security issues, threats, and trends. What are yours?

In retirement my information security expertise has come and gone. However, I still encourage security researchers to seek, interview, and understand the people causing our losses in order to apply knowledge learned to the design of information security. I find that few information security specialists have this important insight.

You've talked about the criminals you interviewed and said they mostly succumbed to unlawfully solving all kinds of intense personal difficulties such as involving errors, sex, money, and competition, choosing cybercrime as a way out—insiders. What do you see motivating insiders today?

An important information security safeguard is making available free confidential problem-solving services (psychological, financial, medical, etc.) to trusted people. People violating their positions of trust ("insiders") today have the same old objectives but on much larger scale (e.g., the Madoff investments case).

What advice (or words of wisdom) do you have for those who are just starting their journey in information security? What is the most important characteristic needed to be successful in information security?

Know your employers' enemies to defeat them. You are not a fully equipped information security expert until you have spent some significant time with the perpetrators of cybercrime. Seek and maintain a consulting role to managers responsible for the safekeeping of information systems and assets by their trusted employees.

Thank you for your insights, Donn, and your many years of information security expertise.

Between February 2014 and August 2015, Donn Parker wrote "Donn's Corner," a monthly collection of his ofttimes controversial information security maxims. We've gathered the full series for your edification and enjoyment. See page 44.

ISSA CISO FORUM

The CISO Executive Forum is a peer-to-peer event. The unique strength of this event is that members can feel free to share concerns, successes, and feedback in a peer-only environment. Membership is invitation only, subject to approval.

DevOps: Developing Secure Applications in an Insecure World

August 16-17, 2018

Marriott Denver Tech Center, Denver, CO

DevOps practices focus on building quality into the code, on automated testing, and on a culture of continuous improvement that leads to improved security, stability, and throughput. Using continuous deployment techniques, DevOps practitioners have found a way to improve both speed and stability in the systems they support, but developing applications quickly may introduce security issues. We will dive into the concept of DevOps to improve application development processes while ensuring the applications are secure, stable, and resilient.

To register or for more information, click here.

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
- Health Care Needs Your Help! 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
- And more…

News from the Foundation

ISSA has once again demonstrated the importance of investing in our next generation of cybersecurity professionals by funding the Foundation's scholarships through its annual $10,000 donation.

The ISSA Education Foundation (ISSAEF) has extended the application deadline for the 2018 Foundation scholarships to July 15, 2018. Visit issaef.org/student_scholarships to obtain the form and read up on the requirements. If you are thinking you don't have a snowball's chance in the Sahara of winning a scholarship, you are wrong! A straight-A grade average is **NOT** required. We have three scholarships to give away. But you can't win unless you apply for this opportunity to receive FREE MONEY for your education. If you are reticent to apply, please send an email to our scholarship director at lfrost@issa-foundation.org and tell us the reason why.

Sandra Lambert [right] and Lorraine Frost greet conference goers at ISSA-LA's 10th Annual Information Security Summit

MAY WAS A BUSY and successful month for ISSAEF! At the ISSA Los Angeles' tenth annual Information Security Summit, our chairperson, Sandra Lambert, was a panelist on "Building Personal Brand and Visibility in Cybersecurity," and moderated a panel on "Future Trends in Cybersecurity," both of which were part of the Women in Security Forum offerings.

Having a presence at two ISSA chapter conference events—Denver's Rocky Mountain Information Security Conference (RMISC) and Los Angeles' Information Security Summit—the Foundation was able to collect nearly $2,000 in donations.

The winners of ISSAEF's opportunity drawing were Devroy Barnett [right] ($50 Amazon gift card) and Edmond Momartin (Amazon Echo Dot) at ISSA-LA's 10th Annual Information Security Summit

SMILE WHEN YOU SHOP at Amazon, knowing 0.5 percent of your eligible purchases will be donated to our scholarship fund! Better yet, it won't cost you a dime. All you have to do is start your purchase from smile.amazon.com and select "ISSA Education and Research Foundation Inc" (one time). Don't forget to tell your family/friends to do the same.

SEEKING VOLUNTEERS to participate in short-term projects, scholarship publicity, fundraising, and governance of the Foundation. Those interested in joining a truly dedicated and enthusiastic group, please contact Steve Haydostian at steve.haydostian@nbcuni.com or 818-777-8171.

Like us on Facebook and LinkedIn.

Member Benefit

20% Discount on Professional Development Programs Offered by the InfoSec Institute

Offering over 95 training courses, InfoSec Institute is the trusted choice for security and IT education. We'll help you boost your infosec skills, achieve certification, and advance your career—guaranteed. Ninety-three percent of our students pass their certification exams on the first attempt!

All ISSA members receive a 20 percent discount on any InfoSec Institute Boot Camps including CISSP, Ethical Hacking, Computer and Mobile Forensics, Reverse Engineering, Data Recovery, CISM, CISA, Security+, and many more. Check out the complete catalog of in-person and online courses. To claim your 20 percent discount, call your enrollment representative today at 708-315-6366 or complete this form.

ISSA International Web CONFERENCE

ISSA International Series

Trials & Tribulations of Social Engineering

2-hour Live Event: Tuesday, July 24, 2018

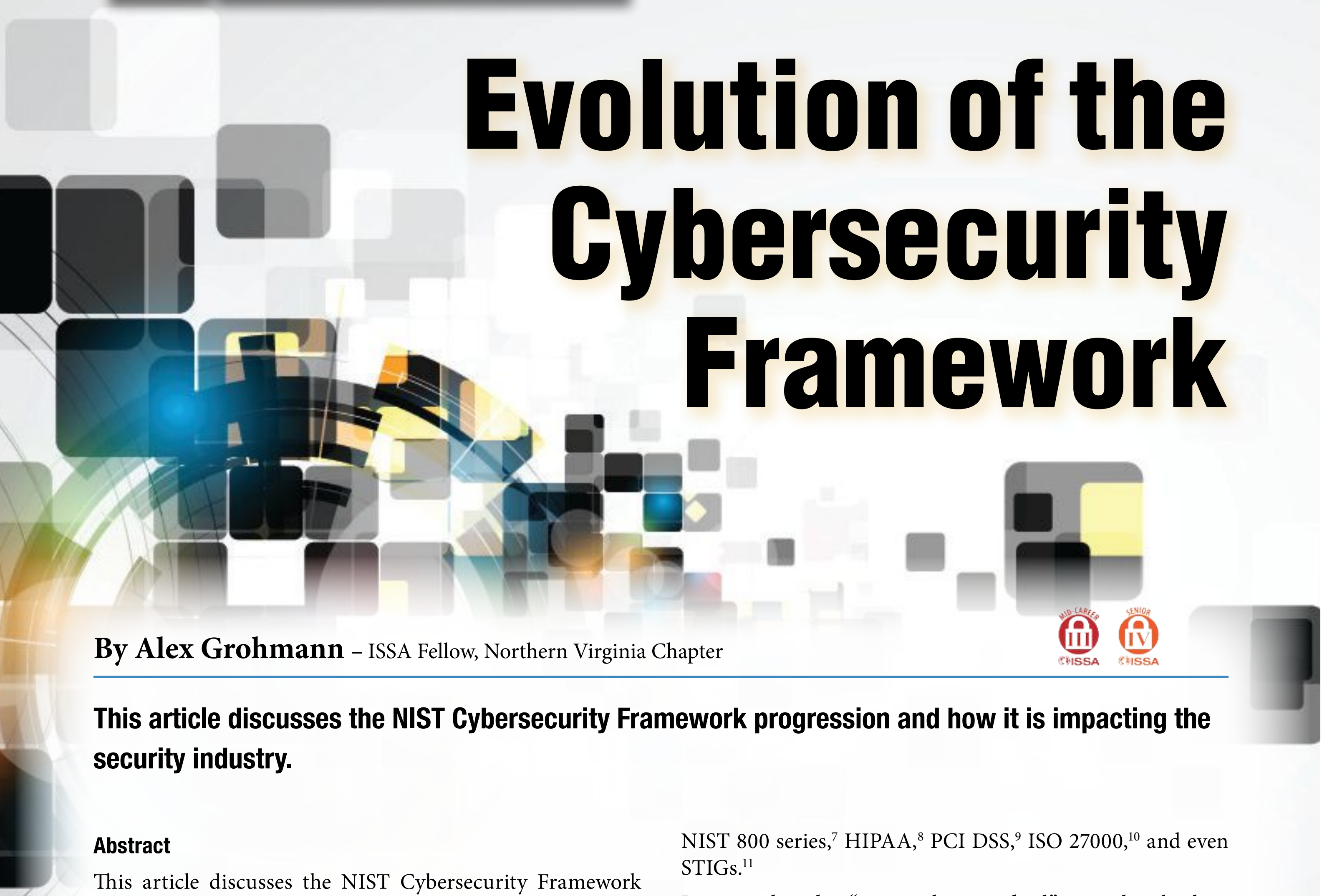
9 a.m. US-Pacific/ 12 p.m. US-Eastern/ 5 p.m. London

We all know about social engineering and phishing, but is it as simple as sending an email or asking for a click? Probably not. As hackers and attacks evolve, they will go from simple tricks to very sophisticated attacks. So how do we know what these attacks will be? Simply, we can't. So how can we detect the new attacks? This session will cover the state of the attacks and the directions they are taking. Ultimately, we will discuss strategies and how we can define the science that will evolve to thwart the evolving various attacks

Generously supported by KnowBe4 Human error. Conquered.

Click HERE to register.

For more information on this or other webinars:
ISSA.org => Events => Web Conferences



Evolution of the Cybersecurity Framework

By Alex Grohmann – ISSA Fellow, Northern Virginia Chapter

This article discusses the NIST Cybersecurity Framework progression and how it is impacting the security industry.

Abstract

This article discusses the NIST Cybersecurity Framework progression and how it is impacting the security industry. For the last four years the framework has proven to be a solid framework for risk management across all types of industries throughout the entire globe. It has just received its first update but still proves to be a valuable resource in the planning and building of a successful cybersecurity program.

Andrew Tanenbaum, author and computer science professor, is famously quoted as saying "The nice thing about standards is that you have so many to choose from." And so it is with the cybersecurity industry. Auditors have standards and guidelines from places like the FFIEC,[1] PCAOB,[2] ISACA,[3] IIA,[4] and COSO,[5] and cybersecurity professionals can choose from standards such as COBIT,[6] NIST 800 series,[7] HIPAA,[8] PCI DSS,[9] ISO 27000,[10] and even STIGs.[11]

It was within this "yet another standard" mentality, back in 2014, that the Cybersecurity Framework (CSF) [7] was initially introduced. This publication from the National Institute of Standards and Technology (NIST) quickly differentiated itself, however, because it was not just another detailed set of standards and guidelines around specific security processes and procedures but was the high-level strategy framework that had always been missing. This was the frame to the puzzle in which any set of standards could be fit, and the details of the framework requirements could be set by the CISO and driven by business needs instead of the old one-size-fits-all checklist.

For four years NIST's CSF has sat atop of the cybersecurity landscape as the framework for integrating standards into an overall strategy, and in that time many practitioners have been using the CSF in some form or fashion. The CSF was

[1] FFIEC - Federal Financial Institutions Examination Council – https://www.ffiec.gov/.

[2] PCAOB – Public Company Accounting Oversight Board –https://pcaobus.org/.

[3] ISACA – https://www.isaca.org.

[4] IIA – The Institute of Internal Auditors – https://na.theiia.org.

[5] COSO – Committee of Sponsoring Organizations of the Treadway Commission – https://www.coso.org.

[6] COBIT - Control Objectives for Information and Related Technologies – http://www.isaca.org/cobit.

[7] NIST 800 series – https://csrc.nist.gov/publications.

[8] HIPAA - Health Insurance Portability and Accountability Act of 1996 – https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

[9] PCI DSS - Payment Card Industry Data Security Standard – https://www.pcisecuritystandards.org/pci_security/.

[10] ISO 27000 – International Organization for Standardization, 27000 family, Information Security Management Systems – https://www.iso.org/isoiec-27001-information-security.html.

[11] STIGs - Security Technical Implementation Guides – https://iase.disa.mil/stigs/Pages/index.aspx.

originally intended to be an optional tool for the creation, management, and refinement of security programs and to provide the basis for any company or entity to create a strategy of how to approach information security [2]. It was this initial version of the CSF that famously came up with the identify-protect-detect-respond-recover cadence, which allows for the neat integration with the NIST risk management framework [4].

In December 2016, the White House Cybersecurity Commission Report [1] called for the CSF to be the dominate strategy framework used by federal CISOs, and in May of 2017 an executive order [3] was issued that did just that by mandating, among other things, protection of federal networks using the NIST CSF. In April of 2018, after long series of drafts and open discussions, NIST released version 1.1 of the CSF, which strengthened the framework by reinforcing some of its existing concepts (such as authentication and identify proofing) and adding some new ones (including supply chain risks, self-assessments, and vulnerability disclosure). The use of the CSF has since grown to be used across industries and academia as well as by the governments of different states and multiple nations.

How the framework works

While the CSF is a framework for detailed standards, it is not a small document, nor a small undertaking to implement. The "core" of the CSF is broken down into five general functions of cybersecurity: Identify, Protect, Detect, Respond, and Recover.

In the original version of the CSF, the five functions were then broken down into 22 categories and 98 subcategories, but with the release of version 1.1, a 23rd category was added that focuses on supply chain risk (table 1).[12] In addition to the five subcategories that were added to support the new supply chain category (table 2), there were new subcategories added to clarify and improve the requirements for identity proofing, multifactor access control, integrity checking, resilient mechanism design, and vulnerability disclosures, adding a total of 10 new subcategories, bringing the overall total to 108 subcategories. Each of these subcategories needs to be evaluated by the security team to define how they wish to address the requirement by using COBIT, NIST, ISO, ISA, or one of many other control definitions available in their industry, or by even defining their own custom solutions. Each subcategory includes what NIST has labeled "informative references" that map the specific controls from these different controls documents to the subcategory level, giving the implementation team an understanding of what the different control documents advocate for the possible control implementation for each subcategory.

Function: ID	Categories
Identify: ID	Asset Management, Business Environment, Governance, Risk Assessment, Risk Management Strategy, Supply Chain Risk Management
Protect: PR	Identity Management and Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, Protective Technology
Detect: DE	Anomalies and Events, Security Continuous Monitoring, Detection Processes
Respond: RS	Response Planning, Communications, Analysis, Mitigation, Improvements
Recover: RC	Recovery Planning, Improvements, Communications

Table 1 – Cybersecurity Framework Functions and Categories

The CSF is not intended to say how to meet the requirement—only what the requirements are—and allows the dif-

CATEGORY	SUBCATEGORY	INFORMATIVE REFERENCES
Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.	**D.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	CIS CSC 4 COBIT 5 APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 ISA 62443-2-1:2009 4.3.4.2 ISO/IEC 27001:2013 A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 SA-9, SA-12, PM-9
	ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	COBIT 5…
	ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	COBIT 5…
	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	COBIT 5…
	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	COBIT 5…

Table 2 - Supply chain risk management subcategories and sample informative references

[12] Images and tables are reprinted courtesy of the National Institute of Standards and Technology, U.S. Department of Commerce.

ferent control documents to drive the how, which will be determined by the individual organization (by defining it based on their understanding of the risk and their accepted risk posture). This is an important distinction; it is the organization that defines what level they expect the control to meet, based on the level of risk that they are willing to accept, which is driven by applying a cost-benefit analysis to their own situation. In other words, the security leadership can customize their controls by building a common control framework that meets their specific requirements and risks. This concept can give the CISO the opportunity to take some of the checklist-mentality away from the auditor and ensure that they are being audited on the control levels that they have set for themselves, customized for their own environment.

This allows senior management…to give direction on security settings based on their understanding of business priorities.

However, while the core functions of the CSF have caught on, there are two other components that are intended to support the core functions: tiers and profiles. These are not as well-known as the CSF's main core component. NIST has defined a four-level tier structure with the purpose of describing "…an increasing degree of rigor and sophistication in cybersecurity risk management practices" [7]. These tiers are intended to be signposts as to the state of each of the cybersecurity subcategories. Though NIST explicitly calls out that this tier structure (from level 1 – partial to level 4 – adaptive) is not a maturity level, the increase in levels is clearly the result of a more mature level of processes that may be worth attaining if it provides a "…cost-effective reduction of cybersecurity risk" [7]. In an ideal setting, senior management would dictate what tier level they would like to operate each subcategory at (based on risk and cost-benefit), with a supporting team to translate the assigned tier level to appropriate technical control implementations. This allows senior management, who may not be familiar with the details of security language and technology, to give direction on security settings based on their understanding of business priorities.

ISSA International Web
CONFERENCE

ISSA Thought Leadership Series

Is DNS a Part of Your Cybersecurity Strategy?

60-minute Live Event: Wednesday, July 11, 2018

10 a.m. US-Pacific/ 1 p.m. US-Eastern/ 6 p.m. London

Detecting malware, helping to prevent and disrupt C&C communication, ransomware, and phishing attacks—DNS can help with this and much more. But are you leveraging it as part of your security controls and processes? DNS is the perfect choke point to stop not just data exfiltration but also to detect and stop malware from spreading and executing. Join us for a discussion on this often overlooked topic and learn:

- The value of DNS as part of your cybersecurity strategy
- How DNS can provide SIEM with actionable intelligence
- How DNS can add value to other security controls, such as vulnerability scanners and end point protection

Generously supported by Infoblox CONTROL YOUR NETWORK

Click HERE to register.

For more information on this or other webinars:
ISSA.org => Events => Web Conferences

This prioritization of the subcategories by tier can be a major undertaking, which is why NIST decided to integrate profiles in with tiers. In the original version of the CSF, target profiles were pre-canned implementation risk-level recommendations for a specific sector, business, or industry. This allowed supporting organizations to publish the priority of subcategories that they thought should be put in place for a specific group of businesses. For example, NIST has published a target profile for the manufacturing industry to highlight which subcategories were of higher importance based on the business objectives common to the manufacturing industry [8]. In this situation, under the business objective of "Maintain Human Safety" in the category of Asset Management, the subcategories of ID.AM-1 (physical device inventory) and ID.AM-5 (resources are prioritized) would be considered a priority in the target profile.

In version 1.1, this concept of profiles was expanded to include tiers, where the characteristics of a target profile would be reflected to support the desired tier level. As in the above example, management might feel that the implementation of physical device inventory should be a tier-four control because of the high risk of injury associated with manufacturing equipment, which would lead to extensive processes of checks and balances to ensure that the physical device inventory was rigorously maintained at all times. This would likely be a time-consuming and expensive set of processes but considered worth the potential cost based on the calculated benefits and priority within the organization. In contrast, Asset Management subcategory ID.AM-2 (software inventory) is a lower priority in the profile and might only rate a tier-one investment in a control solution (relying on a much looser and informal process for tracking). For each of the 108 subcategories, once a target profile was established, a current profile would need to be developed based on the current state of the control, followed by a gap analysis between the two, and a remediation plan—all part of the CSF seven-step process to improve the cybersecurity program.

Future of the framework and next steps

NIST has stated that the CSF is a living document and has published a road map [6] of the next topics to be addressed, including "international aspects, impacts, and alignment" and "small business awareness and resources." NIST plans

CIS Controls™

Start Secure & Stay Secure

with the New CIS Controls Version 7

The CIS Controls V7 are the newly updated prioritized set of actions any organization can follow to improve their cybersecurity posture. The CIS Controls V7 provide clear, step-by-step guidance to tackle the most pervasive cybersecurity threats. Best of all, they're a free cybersecurity resource everyone can download and implement.

CIS Controls V7 separates the controls into three distinct categories:

Basic: Key controls which should be implemented in every organization for essential cyber defense readiness.

Foundational: Technical best practices provide clear security benefits and are a smart move for any organization to implement.

Organizational: These controls are more focused on people and processes involved in cybersecurity.

Basic

- 1 Inventory and Control of Hardware Assets
- 2 Inventory and Control of Software Assets
- 3 Continuous Vulnerability Management
- 4 Controlled Use of Administrative Privileges
- 5 Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
- 6 Maintenance, Monitoring and Analysis of Audit Logs

Foundational

- 7 Email and Web Browser Protections
- 8 Malware Defenses
- 9 Limitation and Control of Network Ports, Protocols, and Services
- 10 Data Recovery Capabilities
- 11 Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
- 12 Boundary Defense
- 13 Data Protection
- 14 Controlled Access Based on the Need to Know
- 15 Wireless Access Control
- 16 Account Monitoring and Control

Organizational

- 17 Implement a Security Awareness and Training Program
- 18 Application Software Security
- 19 Incident Response and Management
- 20 Penetration Tests and Red Team Exercises

Version 7 of the CIS Controls keeps the same 20 controls that businesses and organizations around the world already depend on; however, the ordering has been updated to reflect today's current threat landscape. We've also updated the sub-controls to be more clear and precise, implementing a single "ask" per sub-control.

The CIS Controls V7 were only possible through the collaboration of CIS and a global community of cybersecurity experts in academia, industry, government, and more. Over 300 individuals contributed to help improve cybersecurity for all.

CIS® Center for Internet Security®
Confidence in the Connected World

To learn more about the CIS Controls and download a copy, visit:
https://www.cisecurity.org/controls/

on addressing privacy engineering, cybersecurity workforce, and the life cycle of cyber attacks in future updates, with the option to add or reprioritize topics as they gain or lose importance. As with the version 1.1 update, it is likely that the core of the CSF will remain relatively static so that while any new version will offer some new features, it will also allow the continued use of previous versions without impact.

It is therefore incumbent on the organization to start to integrate some type of risk management framework into their environment. In order to be successful in this regard, the organization needs to understand its own regulatory requirements and be able to address specific industry priorities. It is here that pre-built profiles by industry experts would be a huge step forward—published either by NIST or by separate independent industry specialists. In addition, the organization needs to have an understanding of its industry's risk environment in order to consider unique risks that they may be facing. In the long run, perhaps this is something that the industry-specific information sharing and analysis centers (ISACs) would be better equipped to manage and maintain across their specialty sectors. Lastly, an organization needs to understand what its current level of maturity is in these different cybersecurity areas to be able to know where to move toward. NIST has tried to bridge this gap by teaming with the Baldridge Performance Excellence Program to create a set of resources that can assist the management team in defining their overall cybersecurity strategy and mapping the current and future state of their cybersecurity program [5].

Conclusion

The Cybersecurity Framework is an elegant document that provides the skeleton on which a solid cybersecurity program can be built. Meeting all the requirements of an individual control document can be a cost-prohibitive project that absorbs countless man-hours with little return on investment in many of the control areas, so being able to build a customized set of controls that is specifically adapted to meet the needs of an organization is both cost effective and maximizes risk reduction.

References

1. Commission on Enhancing National Cybersecurity, "Report on Securing and Growing the Digital Economy," (December 1, 2016) – https://www.nist.gov/sites/default/files/documents/2016/12/02/cybersecurity-commission-report-final-post.pdf.
2. Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," US Federal Register (February 12, 2013) – https://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf.
3. Executive Order 13800, " Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," Federal Register (May 11, 2017) – https://www.gpo.gov/fdsys/pkg/FR-2017-05-16/pdf/2017-10004.pdf.
4. Joint Task Force Transformation Initiative, "Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach," NIST (updated 6/5/140 – https://csrc.nist.gov/publications/detail/sp/800-37/rev-1/final.
5. [NIST, "Baldrige Performance Excellence Program," National Institute of Standards and Technology (March 2017) – https://www.nist.gov/baldrige.
6. NIST, "Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1," National Institute of Standards and Technology (December 5, 2017) – https://www.nist.gov/sites/default/files/documents/2017/12/05/draft_roadmap-version-1-1.pdf.
7. NIST, "Framework for Improving Critical Infrastructure Cybersecurity (version 1.1)," National Institute of Standards and Technology (April 16, 2018) – https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
8. Stouffer, K., et al, "NISTIR 8183: Cybersecurity Framework Manufacturing Profile," National Institute of Standards and Technology (September 2017) – https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8183.pdf.

About the Author

Alex Grohmann, CISSP, CISA, CISM, CIPT, is an independent consultant and information security professional with nearly 25 years of experience. He is an ISSA Fellow and a member of the Honor Roll. He may be reached at grohmann@sicherconsulting.com.

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

A Multi-Pronged Approach to GDPR Compliance

By Mark Shriner – ISSA member Puget Sound Chapter

This article looks at a comprehensive, holistic strategy to GDPR compliance that includes best practices related to people, processes, technology, legal, and business insurance. Specifically, we discuss why a multi-pronged or "team" approach towards GDPR compliance is the most effective method to prepare for the GDPR.

GDPR compliance is a timely, relevant, and possibly mission-critical objective for many organizations around the world. Just the mention of those four letters, G-D-P-R, can cause severe anxiety among compliance directors, CISOs, entire C-suites, BoD members, and shareholders.

Some organizations, such as Microsoft, have made a public commitment to be GDPR compliant and have adopted comprehensive compliance planning and activities across their entire enterprise. Other organizations have chosen to adopt a potentially risky "wait and see" position. And some very "risk tolerant" groups have selected what is possibly the worst approach, that is, to do nothing.

Why is there such a variance in strategies adopted for GDPR compliance?

For starters, many organizations aren't exactly sure if GDPR applies to them. **Note:** If your organization controls or processes data that relates to EU residents, it is subject to GDPR. Data can take the form of emails, databases, metadata, customer feedback forms, images, and even CCTV scans.

Even when it's clear that an organization does fall under the purview of GDPR, the actual wording of the regulations is oftentimes quite vague, leaving a great deal open to interpretation. For example, Article 37 of GDPR requires a data protection officer (DPO) in cases where certain types of data are processed "on a large scale." There is no definition of what "a large scale" is. Thus, in many cases it really isn't clear if a DPO is required [1].

And, even when an organization does commit to work towards GDPR compliance, it may receive guidance from an advisor that only addresses one part of the overall GDPR compliance puzzle. A lawyer, for example, may be inclined to focus on the crafting of GDPR-compliant documents such as personal data protection policy, privacy notice, employee privacy notice, data retention policy, data retention schedule, data subject consent form, parental consent, supplier data processing agreement, data breach response and notification procedure, data breach register, data breach notification form, etc.

A process consultant may focus on things such as breach notification, the handing of data subject access requests, or the implementation of the policies that were described during the creation of the above mentioned documents. Technology providers may be inclined to be more focused on introducing security and data protection services or technologies to either protect data and the IT infrastructure or facilitate processes that need to be followed such as breach notifications.

Because of the built-in ambiguity of the GDPR articles and due to the disparate approaches towards compliance that various GDPR consultants espouse, even those firms that are firmly committed to GDPR compliance can find that objective overly complex.

A team approach towards GDPR compliance

It is exactly for the above mentioned reasons that a "team" or "multi-pronged" approach towards GDPR compliance is commonly advocated by many compliance experts. This is the same approach that Microsoft has strongly promoted at recent GDPR events and one that our company has successfully introduced to a variety of organizations around the globe to help them quickly move toward GDPR compliance.

What does the team approach entail? For starters, it means that your organization should identify key stakeholders, bring them together, and provide them with enough autonomy, visibility, and support to make meaningful progress towards GDPR compliance. An example could be an organization that brings together representatives from the compliance, IT, and marketing teams to craft an overall strategy and then communicate that across the enterprise.

> "I've seen what happens when an isolated group tries to make decisions affecting the whole business—usually it involves everyone going back to the drawing board after wasting a lot of time!" – Jake Bernstein, Privacy Attorney [2]

If you fail to include all the relevant stakeholders from the start, you run a high risk of overlooking key issues and possibly facing internal roadblocks later in the process. For example, one organization that we work with had approached compliance solely from a legal perspective and had created a long list of action items that included setting up processes to respond to data subject access requests (DSARs) and insuring that personal data was encrypted.

When they went to their board of directors to get signoff on the plan, they met a lot of resistance because they hadn't discussed those action items and several others with the IT leadership. It turned out that they were competing priorities for a limited IT budget, and it wasn't feasible to automate the DSARs with existing infrastructure. Nor was it clear exactly what data should be encrypted and how the encryption policy could be automated. So, the original GDPR compliance team had to be expanded to include representatives from IT and essentially start their whole planning process from the beginning.

Washington-based privacy attorney Jake Bernstein advises, "The most important first step is to put someone with authority in charge of achieving GDPR compliance. If there's no leadership, there will be no compliance. GDPR affects nearly every aspect of a modern business's operations and without someone to guide the ship, it will overwhelm you. And because GDPR compliance involves nearly every aspect of business operations—from product concepts to development to marketing—your GDPR compliance team must cross all those internal boundaries" [2].

Building your external compliance team

Once the internal team is assembled, it will most likely need to leverage the guidance of lawyers, GDPR process consultants, and IT vendors to help them understand the most relevant solutions in each one of those arenas. And while insurance is not technically part of GDRP compliance, it is an important part of any GDPR preparation plan. Therefore, it would be wise to loop in your business insurance provider to insure that your existing breach coverage includes GDPR-related damages and fines. There may be some overlap in the work these consultants perform, but that can be helpful as it allows for cross checking and validation of the guidance you are receiving in the context of your current situation and business objectives.

Again, it may seem obvious, but if you fail to leverage the guidance from a variety of external subject matter experts, you run the risk of implementing a GDPR compliance plan that overlooks key areas of compliance or is too heavily focused on a narrow set of activities. This often happens when a firm solely relies on its legal advisor. The result can be a long list of action item that are difficult to prioritize since many of the action items will involve very specific technical capabilities or processes related to privacy, security, and compliance.

Automated processing of DSARs would again be relevant example. Your attorney may have added that to your list, but your firm may not be in a position to immediately act on that. However, your external IT consultant should be able to look at your exiting IT platform and future strategic road map and then help you figure out some quick and easy wins that might not result in automated DSAR processing, but instead significantly strengthen your IT security posture and privacy controls.

And that leads to a widely accepted best practice. Don't try to do everything at once. As a team, get an understanding of where you are and what your risks are and prioritize your action items based upon your current ability to complete them and the overall risk to your organization. Then get started on the highest priority items.

Brian King of insurance brokerage AHT advocates taking a multi-pronged approach for GDPR preparation, "First and foremost, our recommendation is to focus your efforts on compliance and then your legal contracts with your customers/vendors. Insurance should only be considered a financial backstop to these efforts and then it becomes a philosophical discussion on how companies want their insurance to respond to GDPR—particularly for those with high-deductible programs" [4].

Seattle-based attorney Cecilia Jeong also recommends a holistic approach, "In order to be in compliance with the GDPR, companies will need to take a holistic approach, working closely with its internal divisions (i.e., IT, operations, sales, legal) as well as with outside vendors. Among its requirements the GDPR expects companies to provide a 'reasonable' level of protection for data subjects' personally identifiable information without interpreting what 'reasonable' means" [3].

Even subject matter experts from the same field may advise different strategic approaches to GDPR compliance. For example, while some attorneys are focused the creation of compliant documents and communications, others take a more structural approach towards risk mitigation.

Lisa Schaures, attorney at Schwabe Williamson & Wyatt, states, "Companies may have functions or data collection that can be separated out—we are considering how to structure

Save $200 on your Briefings pass
with discount code **ISSABR18**

black hat®
USA 2018

AUGUST 4-9, 2018

MANDALAY BAY / LAS VEGAS

https://www.blackhat.com/us-18/

UBM

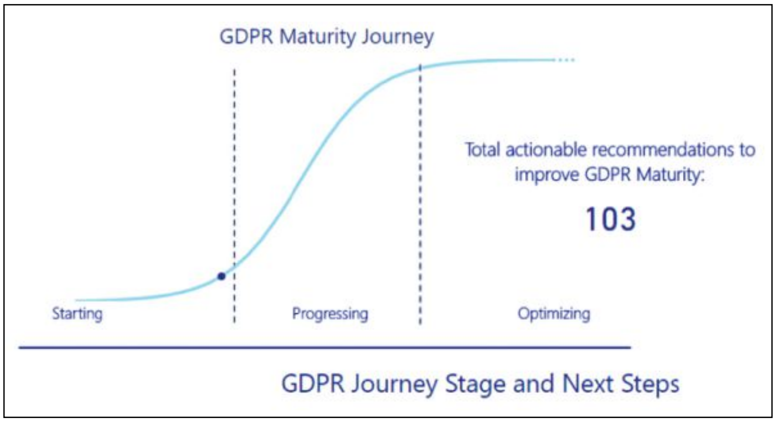


Figure 1 – Microsoft's GDPR detailed assessment measures an organization's maturity level across four key areas of compliance. Source: Microsoft Partner Presentation Slides

companies to facilitate compliance in a streamlined manner. This structuring will be further developed as the GDPR is interpreted by the various regulatory bodies" [10].

On the technology front, the diversity of approaches and solutions is even greater than other areas. As an example, the average fortune 500 company works with 50-70 different IT security vendors [5]. Then there is a whole other set of technology products that simply enable or facilitate compliance-related processes. We will look at both sets of solutions in the following paragraphs.

IT security is heavily dependent upon the action or inaction of the people in an organization, the processes that are followed, and the deployed technology. Potential issues in these areas can't be resolved by simply buying the latest "security tool." Organizations need to carefully match the appropriate solution for their needs and business requirements.

GDPR assessments

With that in mind, a good way to get a grip on your current GDPR readiness and IT security posture is with an assessment that can help you document what actions you have taken and identify and prioritize any major compliance-related gaps.

There is a wide variety of assessments available to help organizations quickly get a picture of where they stand in relation to GDPR compliance. Each has a specific purpose and can be used by itself or in combination with the others.

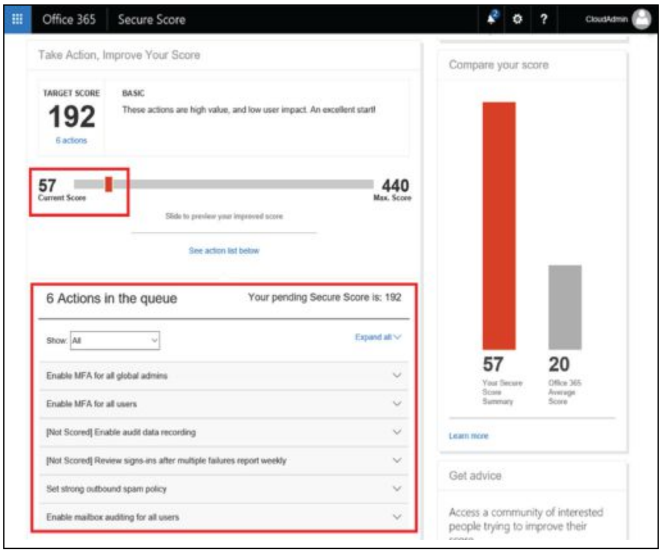
For example, Microsoft created the GDPR Detailed Assessment (figure 1), which is publicly available to any organization. The assessment is a 160 yes-no question survey that provides a snapshot of where an organization currently stands in terms of people, processes, and technology in relation to GDPR compliance. Specifically, the questions do a deep dive into a firm's ability to discover, manage, protect, and record data and events related to GDPR. All the questions are mapped to specific GDPR regulations and the output is linked to specific process and technology solutions [6].

There are also data discovery tools (DDT) that help companies identify what data they have and where it resides. During the scanning process the DDT also facilitates the automatic tagging of data that is important, as will be discussed later, for enabling policies that limit sharing, force encryption, or enact other protective measures.

If your organization is running Office 365 and you just want to get an assessment of your current IT security posture, you could run the O365 Secure Score [6] (figure 2). This assessment is free and only take a few minutes to run. The output makes recommendations that are aligned and prioritized according to business and compliance objectives. This can be a very low-cost way to quickly improve the IT security posture since most of the recommendations involve activating security functions that are baked into Office 365 such as multifactor authentication (MFA) and don't require the purchase of any additional products or services [8].

There are plenty of GDPR readiness assessments available and choosing the most appropriate one(s) may be the most difficult part of the assessment process. But that's where working with an external subject matter expert can really be helpful. They should be help you to decide what type of assessments you should run and then identify the specific ones that would be most appropriate for your organization.

Your legal, insurance, or process advisor might not be familiar with the GDPR assessment landscape. However, your external IT security or compliance advisors should have a good list to work from. The important thing is to be sure to cover all the bases. That is, you need to understand what if any gaps you may have related to people, processes, and technology. You need to know what types of data you have, and where they are. You also need to attach tags to that data. Finally, you will want to look at your IT security posture to see how secure your data and IT platform is against breaches.



TARGET SCORE 192 6 actions

BASIC These actions are high value, and low user impact. An excellent start!

57 Current Score — 440 Max. Score

Slide to preview your improved score

6 Actions in the queue — Your pending Secure Score is: 192

Show: All

- Enable MFA for all global admins
- Enable MFA for all users
- [Not Scored] Enable audit data recording
- [Not Scored] Review signs-ins after multiple failures report weekly
- Set strong outbound spam policy
- Enable mailbox auditing for all users

57 Your Secure Score Summary — 20 Office 365 Average Score

Access a community of interested people trying to improve their score

Figure 2 – O365 Secure Score recommendations. Source: Microsoft Partner Presentation Slides

Strengthening your IT security posture

After you've completed your assessment(s), you will definitely want to consider implementing some type of data loss prevention (DLP) solution. DLP allows you to auto-classify data and documents and then either force or suggest specific actions such as encrypt or prohibit sharing. For example, if the DLP detects personally identifiable information such as national ID numbers, it can insure that the info is encrypted, thus protected, to safeguard against inadvertent or purposeful sharing outside an authorized team.

Another key technology to consider is multifactor authentication (MFA) and its cousin, conditional access. MFA forces a second layer of authentication such as a pin, or a code received by text or voice message or an authenticator app when accessing a user account. Conditional access operates in the same manner as MFA but can be flexibly deployed in preset scenarios depending on the location of the device, the OS of the device, the apps being accessed, and the user's profile.

MFA and conditional access protect against breaches that originate from stolen or compromised passwords and can also be used as a part of a "just-in-time" permission process to elevate a user's credentials to an admin level in order to complete a specific task or for a limited time. Some companies have implemented MFA enterprise-wide. However, the majority of MFA implementations are focused on high-value accounts such as global admin, those with access to important data, and users who have the ability to enact financial transactions.

Technology can also be used to track and record an organization's compliance posture in relation to GDPR. For example, Microsoft's Compliance Manager informs users of all relevant processes that need to be implemented, allows for delegation, tracking, and alerts based upon regulatory changes for GDPR, and several other regulatory and compliance objectives including HIPAA, ISO 27001, ISO 27018, and NIST.

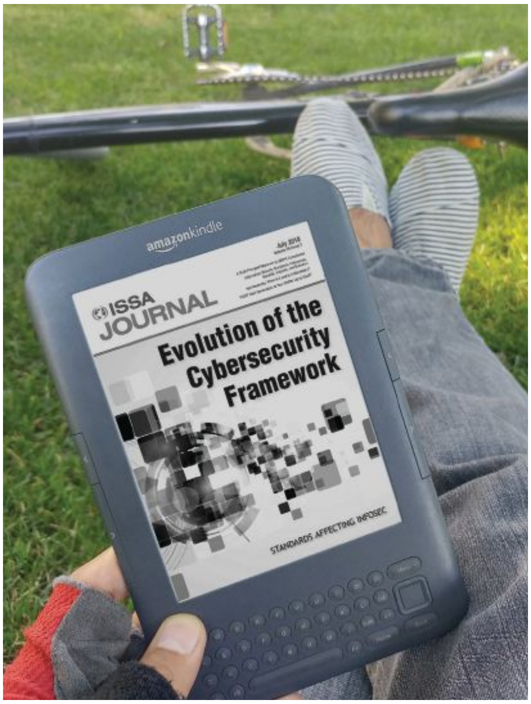
Again, the takeaway is that there are some really useful security and process tools available on the market, or maybe already available in your organization, but unless you include representatives from the IT team and leverage external IT security advisors, you might not be aware of their existence.

But, no matter what technologies you adopt, technology is just one piece of the compliance puzzle. Hiram Machado, CEO of adaQuest, advises, "Any organization that is concerned about GDPR compliance should assemble a team of advisors to develop a holistic compliance plan that incorporates legal, process, technology, training, and insurance." He continues, "If you don't include the guidance of several domain subject matter experts, you risk having large gaps, possibly even unknown, in your GDPR compliance posture."

Some activities fall under more than one domain. For example, creating and following a patch policy is a "process" that might be monitored by the compliance team but implemented by the IT security team.

Likewise, programs designed to create awareness and educate employees on the dangers of phishing campaigns would most likely be run by the IT security team, but may involve stakeholders from the training and compliance teams.

And, speaking of education, it is becoming increasingly common for organizations to provide some basic GDPR training for all employees. A good example is Microsoft's four-hour GDPR Fundamentals program [7] that can be delivered live via webinars or videos. Again, we recommend that you don't try to create a GDPR, privacy, or security training program on your own. Instead, it can be much easier and cost effective to leverage some of the off-the-shelf programs that are widely available to companies around the world [9].


amazonkindle
ISSA JOURNAL
Evolution of the Cybersecurity Framework
STANDARDS AFFECTING INFOSEC

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…

A role for cyber insurance

An oft overlooked piece of the GPDR preparation plan is business insurance to cover breach-related damages and fines. While not a requirement of GDPR compliance, most companies carry some sort of business insurance, and the majority of those policies will provide some cyber protection related to data loss and security breaches. However, there is a vast discrepancy as to what actually triggers those policies.

According to AHT's Brian King, "We spend a lot of time discussing with our clients how they want their cyber policies to trigger to GDPR, whether it is to have their cyber policy respond only to claims arising from breaches or potential breaches vs. affirmatively providing coverage for fines arising out GDPR audits." King continues, "Some larger clients may only want their policy to trigger in the event of breach in order to preserve policy limits and assume the risk from the audit. Others prefer not to run that risk out of the financial or job security fear from a potentially large or "catastrophic" GDPR fine" [4].

One thing for sure, anyone who is involved in their organization's GDPR compliance efforts should be sure to request a review of the firm's business and cyber insurance to see if damages and/or fines related to breaches and specifically the GDPR are covered. Again, this is made easier if you have a trusted advisor with subject matter expertise as part of your GDPR compliance team.

Conclusion

In conclusion, if your organization is concerned with GDPR compliance, your first step should be to assemble an internal team of stakeholders across all relevant teams who are enabled to implement and drive a compliance plan. The next step would be consult with advisors and subject matter experts from the legal, technology, compliance, process, and insurance fields to put together a fully comprehensive plan that aligns with your organization's business objectives and risk appetite.

ISSA JOURNAL

Infosec Book Reviews

Have you read an excellent information security book of value to ISSA members? You are invited to share your thoughts in the ISSA Journal.

- Summarize contents
- Evaluate interesting or useful information
- Describe the value to infosec professionals
- Address any criticisms, omissions, or areas that need further development

Review should be 500-800 words, including short bio, photo, and contact email. Submit your review to editor@issa.org.

ISSA Information Systems Security Association

DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

References

1. Article 37 EU GDPR "Designation of the Data Protection Officer," SecureDataService (07.06.2018) –http://www.privacy-regulation.eu/en/article-37-designation-of-the-data-protection-officer-GDPR.htm.
2. Bernstein, J., privacy attorney at Newman DuWors, unpublished, subject matter expert email – http://www.newmanlaw.com/jake-bernstein/.
3. Jeong, C., attorney at Schwabe Williamson & Wyatt, unpublished, subject matter expert email –https://www.schwabe.com/attorneys-cecilia-jeong.
4. King, B., AHT Insurance, unpublished, subject matter expert email/conversation – https://www.ahtins.com/team/brian-king/.
5. McLean, A., "Security Landscape Plagued by Too Many Vendors: Cisco," ZDNet, November 23, 2016 – https://www.zdnet.com/article/security-landscape-plagued-by-too-many-vendors-cisco/.
6. Microsoft, "GDPR Detailed Assessment Toolkit," Cyber Training 365 (nd) – http://m365.cybertraining365.com/m365/CourseInfo/Microsoft_GDPR_Detailed_Assessment_Toolkit.
7. Microsoft, "General Data Protection Regulation," Microsoft 365 for Partners – https://www.microsoft.com/microsoft-365/partners/GDPR.
8. Microsoft, "Introducing the Office 365 Secure Score," Microsoft Office Support –https://support.office.com/en-us/article/introducing-the-office-365-secure-score-c9e7160f-2c34-4bd0-a548-5ddcc862eaef.
9. Privacy Compliance Hub, "Training Your Staff for the GDPR: Data Protection in Your Organization," Privacy Compliance Hub – https://www.privacycompliancehub.com/gdpr-resources/gdpr-training-your-staff/.
10. Schaures, L., attorney at Schwabe Williamson & Wyatt, unpublished, subject matter expert email – https://www.schwabe.com/attorneys-lisa-schaures.

About the Author

Mark Shriner is Director North America for Wordbee, a Luxembourg-based SaaS provider, and is responsible for client engagement and partner development at adaQuest, a Microsoft Security & Compliance Partner. Mark is a regular speaker on the topic of GDPR and has recently given presentations at the Microsoft Technology Centers in Bellevue and Mountain View and at the ISSA Puget Sound Chapter meeting. Mark can be contacted at marks@adaquest.com.

Information Security Standards

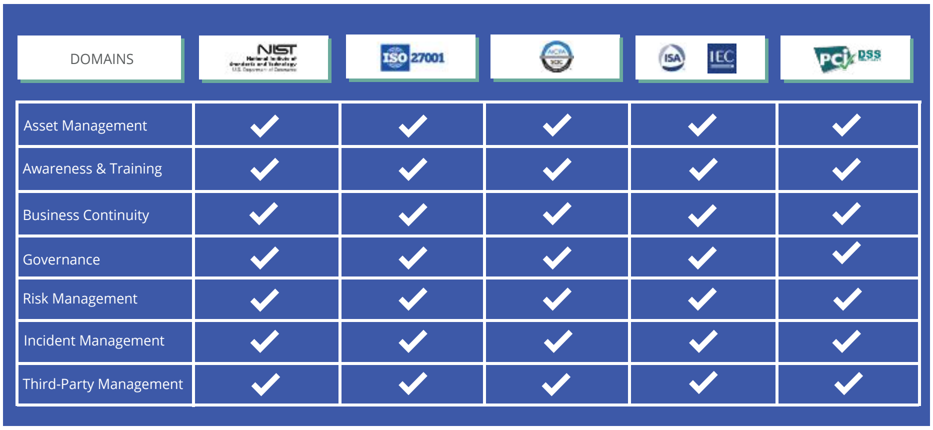
Differences, Benefits, Impacts, and Evolution

By Antonella Commiato – ISSA member, Los Angeles Chapter and Michael Sturgill

This article compares five common information security standards, discusses the benefits and challenges of adopting and maintaining a standard, and outlines factors for organizations to consider when deciding to adopt a standard.

Abstract

With a wealth of standards, frameworks, regulations, and guidelines available to the infosec community, each option can bring a variety of challenges and benefits to an organization. This article compares five common information security standards, discusses the benefits and challenges of adopting and maintaining a standard, and outlines factors for organizations to consider when deciding to adopt a standard.



DOMAINS	NIST	ISO 27001	AICPA SOC	ISA IEC	PCI DSS
Asset Management	✓	✓	✓	✓	✓
Awareness & Training	✓	✓	✓	✓	✓
Business Continuity	✓	✓	✓	✓	✓
Governance	✓	✓	✓	✓	✓
Risk Management	✓	✓	✓	✓	✓
Incident Management	✓	✓	✓	✓	✓
Third-Party Management	✓	✓	✓	✓	✓

Figure 1 – Domain coverage for infosec standards

Information security (infosec) standards bring structure to an organization's security initiatives and are essential in defining and maintaining the security functions, policies, and protocols necessary to protect and manage information.

There are a wealth of standards, frameworks, regulations, and guidelines available to the infosec community. While there is no denying the value that an established standard can bring to an organization, infosec professionals often find that many of the standards used today are pertinent to their business or industry and cover multiple domains. Furthermore, today's portfolio of standards often provides duplicate benefits, which may cause redundancy or confusion to stakeholders (figure 1).

Becoming familiar with available standards and understanding which are appropriate to adopt is vital for an organization, both to develop its security posture and maintain the security of its information, as well as support on-going assessment, monitoring, and improvements.

Which standards "stand-out"?

With so many different standards available, it is critical to the understand differences, recognize the benefits each standard provides, and identify the potential value it can bring to your organization.

Five of the most prominent, internationally-recognized organizations for establishing standards and guidelines for security controls are outlined below.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800 Series of Standards – NIST 80-53A

NIST SP 800 provides solid support for frameworks such as the Cybersecurity Framework (CFS) and the Risk Management Framework. The standards in this series also provide best practices for information security domains. Within NIST, the Computer Security Resource Center provides cybersecurity and information security material to the US government, educational institutions, and civilian industries.[1] Compliance with NIST standards is mandatory for federal agencies, but they can also be a great source of information to all enterprises regardless of affiliation or size by tailoring the NIST SP 800 series to fit their requirements.

A well-known standard for infosec is NIST 800-53A "Assessing Security and Privacy Controls in Federal Information Systems and Organizations." According to the special publication outlining the standard, it "provides a set of procedures for conducting assessments of security controls and privacy controls employed within federal information systems and organizations. The assessment procedures, executed at various phases of the system development life cycle, are consistent with the security and privacy controls in NIST Special Publication 800-53, Revision 4."[2]

International Organization for Standards (ISO)

ISO 27000 Series of Standards – ISO 27001

The ISO/IEC 27000 family of standards is designed to help organizations secure their information assets and covers areas such as developing an information security management system (ISMS), implementing controls, managing risk, conducting audits, and more. Combining multiple ISO 27000 standards can be a valuable way to create and maintain a holistic, effective infosec program. These standards are especially useful to security managers looking to implement a framework that can be audited and compliance that can be verified through certification.

ISO 27001 is recommended to organizations interested in implementing infosec best practices regardless of their vertical or size. ISO 27001 prescribes management clauses and security controls from ISO 27002 that guide organizations in the implementation of an information security management system (ISMS) designed to safeguard the confidentiality, integrity, and availability of sensitive information. The management clauses provide a solid framework on the following components: leadership, planning, support, operation, performance evaluation, and improvement. The ISO 27002 "Code of Practice for Information Security Controls" outlines 114 safeguards for organizations to consider as part of the ISMS implementation in order to mitigate risk to meet the organizations' risk appetite such as encryption and access control. ISO 27001 also provides a solid base for compliance with regulatory requirements or laws such as the EU General Data Protection Regulation (GDPR) and the New York Department of Financial Services cybersecurity requirements, since it covers many controls that overlap with these regulations including breach notification, asset management, and vendor management for the protection of sensitive data.[3]

According to ISO, as of 2016, more than 33,000 organizations held an ISO 27001 certification. This number represents a 21 percent increase from 2015. The growth trend is projected to continue at a fast pace given that ISO 27001 provides a solid base for compliance with several significant regulations.[4]

American Institute of Certified Public Accountants (AICPA)

Statement of Standards for Attestation Engagement (SSAE) 18

The Auditing Standards Board (ASB) of the AICPA created the SSAE regulation to redefine and update how service com-

[1] "Computer Security Resource Center," NIST, accessed on June 18, 2018, https://csrc.nist.gov/.

[2] NIST, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," NIST (December 2014) – https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final.

[3] Richard Menear, "How ISO 27001 Can Help Your Organisation Meet GDPR Requirements," SC Media UK, last modified on December 21, 2017 – https://www.scmagazineuk.com/how-iso-27001-can-help-your-organisation-meet-gdpr-requirements/article/712142/.

[4] IAPP, "IAAP and OneTrust Map ISO27001 to the GDPR," March 2018, https://iapp.org/news/a/iapp-and-onetrust-map-iso-27001-to-the-gdpr/.

ISSA International Web CONFERENCE

Click here for On-Demand Conferences

www.issa.org/?OnDemandWebConf

Cloud Services and Enterprise Integrations
Recorded Live: June 26, 2018

Making sense of Fileless Malware
Recorded Live: June 13, 2018

Breach Report Analysis
Recorded Live: May 22, 2018

Why Automation is Essential to Vulnerability Management
Recorded Live: May 10, 2018

IoT/Mobile Security
Recorded Live: April 24, 2018

Blockchain & Other Mythical Technology
Recorded Live: March 27, 2018

Security Awareness Strategies
Recorded Live: March 21, 2018

Privacy vs. Security
Recorded Live: February 27, 2018

A Cure for the Common SOC
Recorded Live: February 14, 2018

2017 Year in Review & Predictions for 2018
Recorded Live: January 23, 2018

Mobile Device Security
Recorded Live: September 26, 2017

Untraceable Currency
Recorded Live: August 22, 2017

A WEALTH OF RESOURCES FOR THE INFORMATION SECURITY PROFESSIONAL

panies report on compliance controls. SSAE 18 became effective in May 2017 and was preceded by SSAE 16 (effective in 2011), and SAS 70 (effective April 1992).[5]

Organizations achieve SSAE and infosec compliance through SOC 2 reporting. Organizations that are SOC 2 compliant demonstrate the ability to address criteria for managing customer data across five principles:

- Security
- Availability
- Processing integrity
- Confidentiality
- Privacy

As it pertains to information security, organizations are audited on controls related to the protection of assets including network and application firewalls, two-factor authentication, and intrusion detection.

PCI Security Standards Council
PCI Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) details the infosec standards for securing credit card data for merchants that process credit card information. This industry-specific security standard is managed by the PCI Security Standards Council, which was founded by five major credit payment brands.[6] PCI DSS focuses on six primary goals:

- Maintaining a security network
- Protecting cardholder information
- Protecting systems against hacking
- Restricting and controlling access to system information and operations
- Monitoring and testing networks
- Defining and maintaining a formal information security policy[7]

International Society of Automation (ISA)
ANSI/ISA-62443 Series of Standards

ISA is a leader and expert source for creating American National Standards Institute (ANSI) accredited standards that cover safety, efficiency, and profitability for the management of automation and control systems.[8] The ISA 62443 series of standards provide infosec best practices and controls for industrial automation control systems. These standards address requirements and controls that support the C-I-A triad throughout the entire life cycle of an automation control system. In addition to providing guidance and information sharing, the 62443 series provides the framework for product assessments and cybersecurity certificate programs.[9]

The Evolution of Infosec: The Standards' Role

Using an information security standard will create a strong foundation for managing an organization's information security program. Even more importantly, successfully complying with existing standards will provide an easier pathway to meet new regulatory requirements. Current standards play a role in the evolution of information security in three ways:

- **Evolution is often expected and built into the road map.** Many standards have mandatory review dates to ensure that the standard's content is still relevant to current technology and security trends. For example, ISO 27001 has a predefined life cycle of five years to ensure the document undergoes a complete review and update.
- **Expert collaboration and feedback polling drives change.** Members of the infosec community voluntarily collaborate on understanding security vulnerabilities and steps to mitigate them. For example, since 2010 the Open Web Application Security Project (OWASP) has published a top 10 report that identifies critical security risks to web applications based on a consensus of security experts.[1] The "OWASP Top 10" reports are always free to download and provide valuable information to help identify the details of each risk, from exploitation to prevention strategies.
- **Breaches shine the light on vulnerabilities and improvement opportunities.** Major infosec breaches bring to light vulnerabilities and force updates to infosec standards. The credit industry implemented PCI DSS to combat credit card fraud against older cards without chip technology. Laws are established to enforce infosec in the government and civilian sectors, and standards are created to provide compliance guidance.

[1] OWASP, "Open Web Application Security Project Top Ten Project," last modified June 3, 2018, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

Should your organization adopt and follow a standard?

Standards bring practices recommended by experts, create common ground between and within organizations, and provide a sense of trust and confidence—especially when an organization certifies its compliance. In addition, there are a

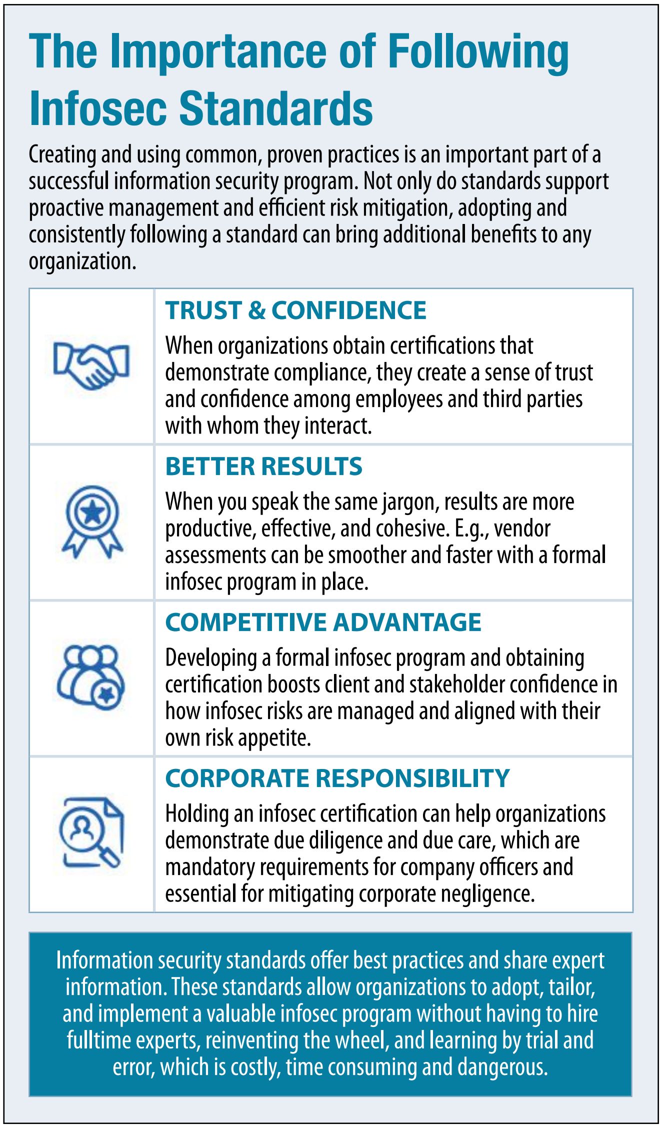
[5] Jaike Hornreich, "Understanding the New SSAE 18 – What You Need to Know," Skoda Minotti, April 2017, https://skodaminotti.com/blog/understanding-new-ssae-18-need-know/.

[6] PCI Security Standards Council, "About Us," accessed on June, 18, 2018, https://www.pcisecuritystandards.org/about_us/.

[7] Margaret Rouse, "PCI DSS (Payment Card Industry Data Security Standard)," TechTarget, May 2009 – https://searchfinancialsecurity.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard.

[8] International Society of Automation, "ISA Standards," ISA, accessed on June 18, 2018 – https://www.isa.org/standards-and-publications/isa-standards/.

[9] ISA, "ISA/IEC 62443 Cybersecurity Certificate Programs," ISA – https://www.isa.org/training-and-certifications/isa-certification/isa99iec-62443/isa99iec-62443-cybersecurity-certificate-programs/.



The Importance of Following Infosec Standards

Creating and using common, proven practices is an important part of a successful information security program. Not only do standards support proactive management and efficient risk mitigation, adopting and consistently following a standard can bring additional benefits to any organization.

TRUST & CONFIDENCE
When organizations obtain certifications that demonstrate compliance, they create a sense of trust and confidence among employees and third parties with whom they interact.

BETTER RESULTS
When you speak the same jargon, results are more productive, effective, and cohesive. E.g., vendor assessments can be smoother and faster with a formal infosec program in place.

COMPETITIVE ADVANTAGE
Developing a formal infosec program and obtaining certification boosts client and stakeholder confidence in how infosec risks are managed and aligned with their own risk appetite.

CORPORATE RESPONSIBILITY
Holding an infosec certification can help organizations demonstrate due diligence and due care, which are mandatory requirements for company officers and essential for mitigating corporate negligence.

Information security standards offer best practices and share expert information. These standards allow organizations to adopt, tailor, and implement a valuable infosec program without having to hire fulltime experts, reinventing the wheel, and learning by trial and error, which is costly, time consuming and dangerous.

Figure 2 – The importance of following infosec standards

variety of benefits and challenges to consider when deciding to follow a standard (figure 2).

Benefits of speaking the same infosec language

When stakeholders and team members speak the same infosec language, the results are often more productive, effective, and cohesive. For example, companies performing vendor assessments to vet the information security posture of suppliers benefit from vendors that hold an infosec certification like ISO 27001 or are compliant with a mainstream infosec framework. Because their policies and practices are already well documented, evaluating vendors with an established program is often smoother and faster compared to assessing a company that does not have a formal infosec program in place.

Organizations that create standards and security professionals know the importance of establishing common ground between security standards and using hybrid control maps to show how standards are comparable with each other. For example, AICPA offers Trust Service Criteria mappings to show how their security controls are similar to the NIST CSF and ISO 27001 frameworks.[10]

We can also look to the federal government to see an illustration of adopting infosec standards to improve communication and increase efficiency. Along with other benefits, in 2014 the US Department of Defense (DoD) decided to adopt NIST to be more compatible with civilian companies.[11]

Competitive advantages

Adopting infosec standards makes good business sense for private organizations. Compliance with or certification of an infosec standard provides customers and stakeholders with confidence in how a company is managing information security-related risks in accordance with the organization's risk appetite. Compliance and certification offer an advantage over competitors that haven't adopted an infosec standard. In some instances, compliance is expected or required by potential clients, such as financial institutions, banks, and insurance companies.[12]

Demonstrating corporate responsibility

Compliance with infosec standards also demonstrates corporate responsibility. Company officers are ultimately responsible for information security at their organizations and can be held liable for negligence and be fined significant penalties in case of a breach. Due diligence and due care are mandatory processes that must be identifiable to mitigate corporate negligence. Demonstrating due diligence and due care by holding an infosec standard certification can help mitigate these circumstances by demonstrating commitment through these efforts. In addition, insurance companies might offer cybersecurity at a lower premium to certified organizations.

Challenges of implementing and maintaining standards

While there are real, valuable benefits to implementing one or more standards, organizations should be aware of potential challenges related to implementation and maintenance.

- **Time:** Implementing and maintaining information security standards is not a one-time project. Rather, it is a process that requires dedicated, qualified personnel, support from senior leadership, and continuous monitoring and improvement. A successful effort will require buy-in from the entire organization.
- **Cost:** Standards can be expensive to implement and just as costly to maintain. In the case of ISO 27001, for example, in addition to the time and effort necessary to meet the

[10] AICPA, "Mappings Relevant to the SOC Suite of Services," AICPA, accessed on June 18, 2018, https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/mappingsrelevanttothesocsuiteofservices.html.

[11] Joey Cheng, "DOD Switches to NIST Security Standards," Defense Systems, April 2014 – HTTPS://DEFENSESYSTEMS.COM/ARTICLES/2014/04/03/DOD-ADOPTS-NIST-SECURITY-STANDARDS.ASPX.

[12] Certification Europe, "ISO 27001:2013 – Information Security Management Systems," https://www.certificationeurope.com/certification/iso-27001-information-security/.

standard requirements, organizations must budget for annual audit fees, which can be substantial.

- **Buy-in:** Senior leadership buy-in and program ownership at the C-level are critical elements for an organization to deploy an information security program effectively. The information security team must share metrics, report the effectiveness of the program, and demonstrate its value and strategic alignment with the organization's business objectives to maintain senior leadership support.
- **Change management:** In general, everyone appreciates the value of securing information until it requires a change. Security teams implementing standards are challenged to strike a delicate balance between security and convenience.
- **Continuous improvement:** Standards have life cycles. When a standard is updated, it is the responsibility of all compliant organizations to be aware of the updates and implement them by specified dates, or as soon as possible if a time line is not mandated. In some cases, a standard might become obsolete, and a new standard must be researched and presented to senior leadership for approval for implementation.

Deciding which standard is right for your organization

With many varying standards and guidelines available, choosing the right fit and best value for your organization can be a time-consuming task. Whether you require a standard specific to your industry or need a customized solution, start by educating yourself and understanding all the options. Research established standards, frameworks, and best practices so you can tailor components to meet your company's requirements and overall business strategy. Key considerations include:

- **Hybrid approach:** Some organizations may need to select specific components from a variety of standards and frameworks and tailor them to meet their specific needs because of gaps of standard coverage for organizations involved within multiple industries or compliance requirements
- **Alignment with business strategy:** Examine the requirements and determine which standards are compatible with current business operations
- **Leverage in-house expertise:** When regulatory or client requirements don't impact the decision, organizations may choose to select a standard based on the experience of in-house subject matter experts
- **Client requirements:** To do business within a particular market, a company might need to hold a certification or show compliance with a standard to be eligible or competitive
- **Regulatory compliance or compulsory requirements:** Some organizations, depending on the industry or gov-

The Experience-Sharing Platform for IT Leaders
451 Research
Wisegate
Wisegate helps IT leaders achieve more – by thinking **together**
Benefit from online discussions, live peer calls, peer-tested work product
Get trusted, firsthand insights directly from your peers
Stay connected between conferences and meetings
Request an invitation today
WWW.WISEGATEIT.COM

ernment regulations and laws, will not have a choice and must implement standards and frameworks to demonstrate compliance

- **Implementation and maintenance costs:** The cost of deployment, maintenance, and continuously improving compliance with a standard can be a significant factor in selection and budgeting
- **Build your knowledge:** Join organizations such as ISSA to continue learning and share knowledge and experiences with the infosec community
- **Supporting technology:** Identify and adopt tools and platforms that automate your processes and communications, and support the efficient development, maintenance, and improvement of your information security program
- **Organizational awareness:** Provide regular updates and training to build a culture of information security among all team members and ensure all stakeholders are informed so they make take leadership roles and establish themselves as a cohesive part of the solution

Conclusion

Information security standards have proven to be valuable resources for sharing information best practices as established by industry experts. Specific infosec guidance is available for government agencies and civilian organizations and varies depending on factors such as industry, laws, and regulatory compliance requirements. When selecting a standard, organizations should consider the importance of certification as a way to demonstrate infosec compliance and perform a cost-benefit analysis to determine if certification is the right path. The process of selecting the appropriate infosec standard can be intimidating, but with careful research, any organization can choose the right standard to achieve its goals.

About the Authors

Antonella Commiato, Chief Technology Officer/Chief Information Security Officer EXTEND Resources, has 23 years of IT leadership experience across a broad range of disciplines that include marketing, social expression, transportation, and logistics. With her technological expertise and guidance companies are able to support their complex business initiatives, grow their businesses, and implement efficient internal operations. She may be reached at acommiato@extendresources.com.

Michael Sturgill, CISM, CEH, and SEC+, Information Security Manager EXTEND Resources, has more than 15 years of experience in information systems, program management, security, and technical solutions for the US government and civilian sector. He may be reached at msturgill@extendresources.com.

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

⬇ APRIL
Internet of Things

⬇ MAY
Health Care & Security Mangement

⬇ JUNE
Practical Application & Use of Cryptography

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

Net Neutrality: What Is It and Is It Necessary?

By **Nima Zahadat** – ISSA member, Northern Virginia Chapter

This article presents an examination of the laws regarding net neutrality and deliberates both sides of the divide in terms of how net neutrality and its regulations impact consumers and end users, companies that depend on the Internet and its services, and the ISPs that provide broadband and other services.

Abstract

The net neutrality debate's argument revolves around whether high-speed broadband services provided by ISPs such as Verizon to content providers such as Netflix need regulating in order to prevent bias based on price discrimination and preferential treatment based on tier pricing. Supporters of net neutrality reason that the regulations keep the Internet free and fair by deterrence of discriminatory practices. Opponents claim that the regulations cost the providers of broadband services a great deal, forcing them to pass those charges downstream.

Any policy effort regarding net neutrality must go outside of ordinary arguments and must comprise serious studies of the technical and societal aspects of the situation, instituting a discussion surrounding policies and regulations involving the public, consumer advocates, developers, service providers, content providers, and federal and state-level government regulators.

In its simplest form, "net neutrality" refers to the principle that Internet service providers (ISPs) must not discriminate against the data that's transmitted through their networks. This means allowing all content and web applications to be uniformly accessible to customers, regardless of their source or destination, and also not to block specific websites the ISPs dislike or disagree with in any shape or form.

The central argument of this debate revolves around the conflict to protect freedom, as advanced by both proponents and opponents, each side citing its own version of freedom. The proponents of net neutrality argue that this is all about the freedom of using the Internet and its resources without permitting ISPs and service providers to "discriminate among Internet packet streams to selectively block, adjust quality of service, or adjust prices" [11], and in doing so, allow the broadband service providers to charge content providers or even charge different prices to different providers for the same or similar service or to block content of content providers to advance their own, in effect crippling the Internet [2]. Opponents of net neutrality advance the argument that it is really about the freedom of the markets by not allowing governments to regulate how ISPs and service providers deliver their services and by "allowing experimentation with new business models," which they assert are "key to the Internet innovation and the deployment of expanded networks needed to handle rapidly growing Internet traffic" [2].

Undoubtedly at its face, there certainly appears to be valid arguments in both camps and certainly both sides have partial validity to their respective opinions. This article presents an examination of the laws regarding net neutrality and deliberates both sides of the divide in terms of how net neutrality and its regulations impact consumers and end users, companies that depend on the Internet and its services, and the ISPs that provide broadband and other services. The article concludes with a focus on whether or not net neutrality should be preserved and if so, whether or not regulations should be the methodology in preserving it.

Literature review

Net neutrality has become an intense and touchy topic of debate in the United States. In the United States, the Federal Communications Commission (FCC) is tasked with regulating and supervising ISP behavior and conduct, though some opponents of net neutrality argue that the Federal Trade Commission (FTC) should be tasked with regulating power. The extent of this purview itself is subject to controversial deliberation, but that is not an emphasis of this article.

On December 21, 2010, the FCC issued the FCC Open Internet Order, which was to be "in the matter of preserving the open Internet broadband industry practices" [6]. This order was a package of regulations designed to prevent ISPs and broadband service provides from blocking users' access to their competitors' services and websites. The FCC went further by providing a consumer guide as to what an open Internet refers to, describing the regulations in place to prohibit the following actions by broadband service providers: blocking of "access to lawful content, applications, services, or non-harmful devices"; prevention of throttling, where Internet traffic is deliberately targeted "to be delivered to users more slowly than other traffic"; and prevention of paid prioritization, where some Internet traffic, or the content and services of providers' affiliates, are favored "in exchange for consideration of any kind" [9].

The December 2010 regulations were revised on September 23, 2011, by adding directives expressing that broadband providers must be transparent in their network practices, not block lawful content, applications, or services and not discriminate in transmitting lawful network traffic [7]. This order originated as the result of *Comcast Corp. vs. FCC*, which was decided by the United States Court of Appeals for the District of Columbia on April 6, 2010, and in which the FCC lost. The court ruling was that because the FCC had classified cable Internet providers as "information services" and not "telecommunications services," the actions of cable Internet providers, such as Comcast, did not fall under the FCC's jurisdiction as defined in the prevailing Telecommunications Act of 1996 [13].

Following the Comcast case, another decisive case to test the limits of FCC's net neutrality enforcement abilities was *Verizon Communications, Inc. vs. FCC* [14]. Verizon sued the FCC arguing the 2011 order exceeded FCC authority while violating Verizon's constitutional rights and at the same time creating ambiguity within the communications industry. Again, the court ruled against the FCC, maintaining that the FCC did not have the authority to enforce net neutrality rules because the service providers were not classified as "common carriers," (i.e., telecom companies). Having lost two cases against two giants of the industry, the rulings signaled to the ISPs that the FCC order in effect had no teeth. In order to combat these giants, the FCC first attempted in May 2014 to issue new policies while complying with the court's rulings. Under the new rules, ISPs including Comcast and Verizon would be allowed to build faster service connection ("service lanes") for businesses willing to pay for those services and speed, receiving preferential treatment. These rules prompted an overwhelming backlash from the supporters of net neutrality which caused the FCC to issue a news release on February 26, 2015, ruling in favor of net neutrality by reclassifying the broadband service providers as telecommunications services (common carriers) that now fell squarely under the purview of the Telecommunications Act of 1996 [8].

So, what does the future look for net neutrality? The regulations placed by the FCC were instituted and supported by the Obama administration. Those rules and regulations were reconsidered by the Trump administration under the new FCC chairman, Ajit Pai, who began the process of rolling back the open Internet rules that were instituted since 2015. It must be noted that Ajit Pai was a lawyer working for Verizon during its lawsuit with the FCC. Pai's goal has been to reclassify broadband service providers as information service provides and end regulations placed by the FCC since 2015. Research suggests that one single policy will not be effective in achiev-

ISSA JOURNAL

Legal, Regulations, Ethics
Operational Security — the Basics of Infosec
Internet of Things
Health Care & Security Mangement
Practical Application & Use of Cryptography
Standards Affecting Infosec
Foundations of Blockchain Security
Privacy
Security Challenges in the Cloud
Impact of Malware
The Next 10 Years

Write for your ISSA Journal…

Advance your career • Gain chapter, national, and global recognition
Help others benefit from your expertise • Indexed in EBSCO database

- **Monthly topics**
  Expanded theme descriptions here.
- **Choose your own topic**
  Have a different infosec topic in mind? Go ahead and submit it.
- **Mentor program**
  We will pair you up with an experienced writer in Friends of Authors

If you have an infosec topic that does not align with the monthly themes, please submit. All articles will be considered.

~Thom Barrie, Editor

It's Your Journal – Contribute Your knowledge & Expertise

ing the political and economic objectives that are core to the debate and instead, "safeguarding multiple goals requires a combination of instruments that will likely involve government and nongovernment measures" [1].

Pro net neutrality

Most organizations in favor of net neutrality are human rights groups, consumer advocates, smaller organizations, and content providers. In a survey by Consumer Reports, nearly 70 percent of Americans seemed to agree that ISPs should not be allowed to determine what applications and what streaming services or websites customers can access, and over 60 percent agreed that ISPs should be prohibited from modifying or editing content that consumers may want to access on the Internet [16].

One of the more active proponents of net neutrality is the American Civil Liberties Union (ACLU). Part of what the ACLU wants to thrust forth is for the public to believe that net neutrality rules prevent sinister conduct by telecom companies. These include acts such as scrutinizing personal data or interference with the normal stream of data by blocking or slowing down traffic from sites that are competitors or ones they may dislike (e.g., for political reasons). Such actions are considered to violate the First Amendment rights of Americans. Perhaps this view is not sufficiently academic, but the ACLU does make a serious point that academic analyses have borne out: data manipulations by broadband service providers is not always detectable and can be carried out in subtle ways as to not be obvious to consumers. Further, as the barriers to establishing high-speed broadband service are very high, there aren't likely to be alternatives that consumers can choose from in the event they believe their provider is active in snooping and manipulating their data and service quality.

Anti net neutrality

The opponents of net neutrality rules commonly argue on the basis of economics to the ISPs. Keith Hylton points out the weakness of arguing for net neutrality regulations as protectors of consumer rights by drawing comparison between the use of toll bridges and the use of broadband services [10]. He presents the case that if a toll operator would charge the same amount for a heavy truck that he charges for a regular sedan, the car is in effect subsidizing the cost of maintaining the bridge as trucks are costlier maintenance factors to the bridge. He contends that this analogy is similar to how broadband service providers are being dealt with under net neutrality rules; that is, consumers are in effect subsidizing lower costs for the large content providers such as Amazon and Netflix. Permitting some content providers that use up a lot of broadband, such as Netflix, to be charged the same as other content providers that use only a fraction of that, means that "net neutrality is not neutral at all: it forces A to pay for the consumption of B." Another argument advanced by Tim Wu, who coined the term *net neutrality*, is that the current Internet even in the best effort implementation favors file transfer or other non-time-sensitive traffic over real-time communications; therefore, it is not as neutral as one would like to believe [17].

Fact is, the revised open Internet put out by the FCC in 2015 and lauded as "improved" may not have much meaning to investors or consumers in the short term. What is indeed true is that all large ISPs have done what they could so as to avoid implementing services and strategies that might make them targets for net neutrality regulations. Ample debate has centered around how consumers on one hand and the ISPs on the other would likely be impacted by the regulations. In these disputes, much less has been brought to the surface as how these regulations or their lack of would impact companies, small and large, that rely on the Internet for their businesses. Several open questions remain on this topic, and they need consideration in further debate, assessment, and formulation of policy as correlated to net neutrality.

The first question is what type of organization or business would benefit (or not) from net neutrality regulations? It is clear that companies such as Netflix, Google, Amazon, Facebook, and smaller companies that use the Internet for their day-to-day businesses benefit from net neutrality. Companies that use very high bandwidth, notably Netflix, would have the greater benefit than their smaller counterparts. In a sense, as described previously, this may not be fair to smaller businesses that use far less bandwidth but end up paying the same while not getting the usage.

FORTINET
WITH THE FORTINET SECURITY FABRIC
Networking leaders can confidently meet the demands of network performance and security effectiveness while scaling to meet exponential growth in traffic and a proliferation of devices, users, and applications.
BE READY.
TO ENABLE SD-WAN WITHOUT SACRIFICING SECURITY
Learn more at www.fortinet.com » Products » SD-WAN

The second question is what will the revenue models be that content-providing companies may utilize for their services? Depending upon whether net neutrality regulation is maintained, and if the ISP chooses to impose more delivery charges to the content provider, the latter may change its model from, say, bundling content and advertising, to one that is subscription based. Therefore, net neutrality may impact the content provider's revenue model. Similarly, an ISP cannot guarantee quality of service under net neutrality, so a large content provider may have to develop its own content delivery networks just outside the ISP's network, and these costs will be distributed somehow, perhaps some to the end user (consumer), but it is for now an unknown.

Key findings

Net neutrality is intensely debated with those who know anything about it, having strong opinions for or against it. Companies and businesses that heavily depend on the Internet such as e-commerce, television, telephone, and streaming service providers will be especially impacted, feeling the reverberations as applications and devices become increasingly Internet Protocol (IP) based. Given this fact alone, all politics aside, any policy formulation will have to take into account the impact of these areas on not just consumers and ISPs but decision makers such as executives and investors of companies whose services will depend upon the transfer of data within the Internet [12].

Mainstream opponents of net neutrality oppose it on economic bases, advancing that it stifles innovation and investment. Some argue on ideological bases, that governments should not interfere with the operation of broadband service providers in a free market. One such economist, Gerald Faulhaber, a professor of business economics and public policy, posited that the "economics of two-sided market" could provide an objective and politics-free view of the Internet market and in particular the ISP market. Faulhaber's market is one where "an intermediary offers interconnection services to two (or more) distinct groups together for purposes of communication and transaction" [5]. As an illustration, Comcast could be considered an intermediary connecting content, network, and application providers to retail consumers while connecting retail consumers with each other through email and social networks.

Faulhaber's argument details that from an economic perspective, intermediaries have a vested interest in increasing their customers on both sides of the Internet market, the idea being that the larger the customer base the more the profit. The rationale goes that as such broadband providers like Verizon would want more content providers and more consumers to join their network and utilize their services. Since broadband ISPs have been in business for well over two decades as of this writing, one would expect all the discriminatory, anticompetitive, and predatory practices that net neutrality regulation aims to prohibit to have been widespread during this period and abundant cases documented. Instead, Faulhaber cites the FCC as having produced only four such cases of ISP misconduct in a decade [5]. FCC regulations, in his view, are thus only "prophylactic remedies to non-problems," and he questions their necessity.

One of the exceptions among economists who have declared pro-net neutrality regulation views is Nicholas Economides, economics professor at NYU. Economides stresses that abolishing net neutrality will profit the ISPs in the long-term while hurting content providers and consumers, even if the ISPs claim that consumers will end up paying less [4]. The danger of this system of prioritization, as he reasons, is that

LOOKING AHEAD – JOURNAL THEMES

September: Privacy

Every year seems to be noted as "the worst year in online privacy." Globally, big breaches continue to occur (Equifax in 2017), we see an increase in government privacy laws (GDPR, government censorship and surveillance increase), more people are online and through more devices (mobile devices in even the youngest hands), and companies can't get to the cloud fast enough (AWS v. Azure). All of these trends effect online privacy which in turn effects our individual online privacy. Do fewer hacks give us privacy? Do more laws give us privacy? Is the private cloud any more private than your publicly-connected mobile phone? This is a call for articles in the ISSA Journal on Privacy - Examples; GDPR, mobile ransomware, Cloud privacy, IoT malware.

SUBMIT ARTICLES TO EDITOR@ISSA.ORG.

October: Security Challenges in the Cloud

No matter where you are in your migration to the cloud - public, private or hybrid - it is almost universally accepted that the security of data, along with the underlying system and network components, is a work in progress. In addition to the use of different virtualization techniques that are the foundation for the different cloud forms, there are technical as well as legal, regulatory and governance aspects to the data protection models that make things quite complicated. Do you "speak cloud?" If so, we are looking for your input, ideas, experience and observations as to what works and what doesn't. Avoiding the cloud is not the answer. Therefore, here's your chance to weigh in regarding what standards should be applied and what considerations a security practitioner should keep in mind. What practical solutions do you have to help meet the business requirements while keeping your organization secure?

the ISPs will become the dictators of the terms of competition in Internet services such as search, news, e-commerce, etc. As an illustration, picture if a competitor to eBay launches a similar website. Since eBay can pay the higher fees for higher speeds and this new market entrant cannot, consumers will naturally stay with eBay because they can purchase items faster, checkout faster, have their auction bids registered faster, etc. Eventually, that new competitor will lose customers, suffer losses, and leave the market—unless it begins to pay the higher-tiered fees. Economides argues that this is how monopolies and duopolies are maintained.

Assessing the viewpoints of both sides of the net neutrality debate, it appears that the pro camp is largely comprised of content providers, other businesses that use the Internet extensively for their operations, activist organizations, and consumers. The anti camp is largely comprised of ISPs, economists, and free market economics proponents. A debate between Christopher Yoo (anti net neutrality regulation) and Timothy Wu (pro net neutrality regulation) sums up each side's main argument for being against or for net neutrality regulations [18]. The anti-regulations camp, which Yoo represents, contend that regulations will halt technology advances by discouraging investment and innovation. The pro-regulation camp, which Wu represents, draws a portrait of mammoth-sized ISPs giving preferential treatment to content that's paid for, given the privilege of being loaded faster versus smaller, new market entrants who are relegated with slow load speeds, losing their audiences in the processes, with the ISPs maintaining a grip on the "last mile" pipeline to computers.

A thought-provoking study by Cheng et al. [3] devised a game-theoretic model to determine who would gain or lose if there were no net neutrality regulations, and if broadband service providers and ISPs would be incentivized to expand their broadband network capacity in the absence of regulation. The outcomes were quite interesting, to say the least. Their framework exhibited that consumers either experience no difference, or the majority are better off, but there is a minority who would experience far worse wait times. The most interesting finding of their model, however, was that broadband service providers demonstrated an "unambiguously higher" incentivized behavior to expand their network capacity under regulation-based model than when they are not being regulated. This is contrary to the ISPs' assertion that they would not be incentivized to expand if they were regulated. This finding certainly deserves further research.

Conclusion

Ultimately, given there are arguments for and against both sides of net neutrality and most of them making sense to the common observer, the policies that need be debated and perhaps eventually enacted are ones that can allow for beneficial traffic discrimination while protecting consumers from harmful traffic discrimination [11]. The net neutrality discussion, in its most universal sense, is an endeavor to determine the organization of the vertical relations between the broadband service providers and content providers such that efficiency and welfare effects are maximized for all. The range of options lay on a spectrum involving minimal constraints (no regulation, network providers can differentiate services and prices within the limits of competition laws) on one end, and maximal constraints (full regulations) on the other end, with a variety of regimes in between. The issue, as this researcher sees it, will endure for some time since the existing literature on the topic contains many persuasive and convincing arguments to support both sides of the debate. It looks that a conclusive answer can only come from more empirical-based research, not theoretical arguments unsupported by scientific research based on empirical evidence. Since projected future changes cannot be proved empirically because future events have not taken place, experiential evidence must be based on sound economic models that can unequivocally validate how differentiation strategies on the part of ISPs will alter the freedom of the Internet or not.

ADVERTISE STRATEGICALLY

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

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

Kai Zhu believes that "Internet traffic prioritization can both coexist with and encourage Internet innovation" and "some minimal regulation is needed to prevent market power abuses and usage discrimination in the Internet service market" [19]. He maintains that many arguments inserted into both sides of the debate are "misplaced, prejudiced or hyperbolic," the reason being because of the many technical details of the Internet that need to be understood well, first and foremost. Therefore, it is not enough for economists to take a stance either way without understanding those details, and likewise it is not sufficient for IT experts to take a stance either way without understanding market and economic implications. There is, according to Zhu, a "technically feasible middle-ground solution to the debate," one that uses "bandwidth reservation to protect garage innovation under QoS [quality of service] provision," [19].

It is a reasonable assumption that any policy must address this trade-off between prioritizing innovation by broadband network providers and prioritizing innovation by small, independent content and application providers [15]. Furthermore, the efforts must go beyond mere discourse and diatribe and ought to encompass a serious study of the technical aspects of the situation, meaning the discussion surrounding policy and regulation must involve public administrators, IT developers and professionals, economists, consumer groups, and other stakeholders in the Internet market. Obviously, the long-term goal is to maintain a free market economy that is regulated as little as possible, but also provide enough sensible regulation that is not going to present a choke-hold to investment and innovation, and at the same time protect the smaller competitors so that the market can truly be "free" and not dominated by only one or two major players. There is no doubt that more research is required to further apprise the debate, with the ultimate goal of formulating a fair and equitable policy for all stakeholders.

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 1,057 job listings [7/1/18] you will find the following:

- Senior Security Engineer/Analyst, Equity Residential – Chicago, IL
- Senior Cyber Security Engineer, Oak Ridge National Laboratory – Oak Ridge, TN
- Senior Security Operations Engineer, AllClear ID, Inc. – Austin, TX
- President and CEO (Company Not Listed) – Fairfax, VA, United States
- Director, Security and Privacy, Ministry of Transportation and Infrastructure – Victoria, BC
- Sr. Information Security Analyst, Puppet – Portland, OR
- Director Information Security and Compliance, KLDiscovery – Eden Prairie, MN
- VP, Operational Risk – Information Security (L13), Synchrony Financial – Multiple Locations
- Information Security IAM Analyst Level 1, Cadence Bank N.A. – Houston, TX
- Information Security Analyst, Tufts Health Plan – Watertown, MA
- Healthcare Information Security Engineer, Booz Allen Hamilton – Charleston, SC
- IT Specialist II - Information Security Specialist, Orange County Sheriff's Office – Orlando, FL
- Information Security Archive Specialist, Mutual of America – New York, NY
- HPE Information Security Analyst, Hewlett Packard Enterprise – Roseville, CA
- Instructor, Cybersecurity - BAS (Job #0761), Pasco Hernando State College – New Port Richey, FL

References

1. Bauer, J.M. and Obar, J.A. (2014). "Reconciling Political and Economic Goals in the Net Neutrality Debate," Information Society, 30(1), 1-19. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2910104.
2. Baumol, W. J., et al (2007). "Economists' Statement on Network Neutrality Policy," – https://papers.ssrn.com/sol3/papers.cfm?abstract_id=976889.
3. Cheng, H.K., Bandyopadhyay, and Guo, H. (2008). "The Debate on Net Neutrality: A Policy Perspective" (last revised 21 Apr 2013). Department of Decision and Information Sciences, Warrington College of Business Administration, University of Florida. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=959944.
4. Economides, N. (2007). " 'Net Neutrality', Non-Discrimination and Digital Distribution of Content Through the Internet," NYU Law and Economics Research Paper No.07-13. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=977096.
5. Faulhaber, G.R. (2011). "Economics of Net Neutrality: A review," Communications & Convergence Review 2011, Vol.3, No.1, 53-64. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1894286.
6. FCC (2010). "In the Matter of Preserving the Open Internet Broadband Industry Practices," FCC 10-201, December 21, 2010. Retrieved from https://apps.fcc.gov/edocs_public/attachmatch/FCC-10-201A1.pdf.
7. FCC (2011). "Preserving the Open Internet," Federal Register Vol.76, No.185, September 23, 2011. Retrieved from https://www.gpo.gov/fdsys/pkg/FR-2011-09-23/pdf/2011-24259.pdf.
8. FCC (2015). "FCC Adopts Strong, Sustainable Rules to Protect the Open Internet," News release February 26, 2015. Re-

Continued on page 43

PCAP Next Generation: Is Your Sniffer Up to Snuff?

By Scott D. Fether

The PCAP file format is widely used for packet capture, but it is not the only standard. The PCAP next generation (PCAPng) capture file format is a refreshing improvement that adds extensibility, portability, and the ability to merge and append data to a wire trace. This article describes the new format, displays methods to take advantage of new features, introduces scripting that can make the format usable, and makes the argument that migration to PCAPng is necessary.

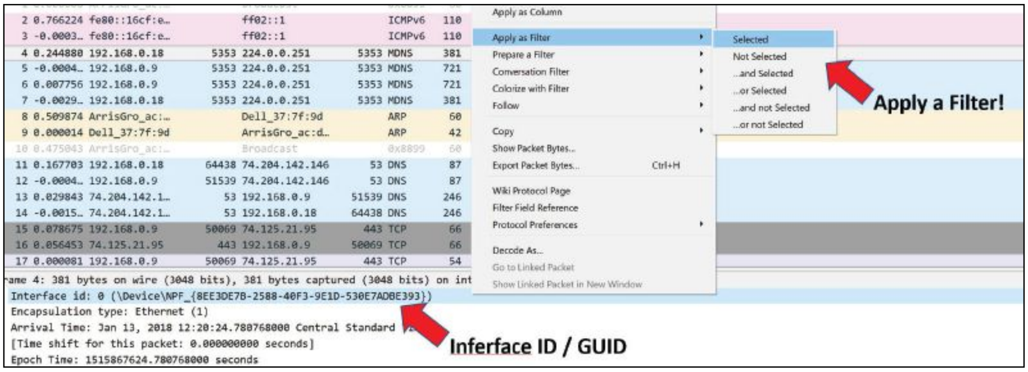
Abstract

The PCAP file format is widely used for packet capture within the network and security industry, but it is not the only standard. The PCAP next generation (PCAPng) capture file format is a refreshing improvement that adds extensibility, portability, and the ability to merge and append data to a wire trace. While Wireshark has led the way in supporting the new format, other tools have been slow to follow. With advantages such as the ability to capture from multiple interfaces, improved time resolution, and the ability to add per-packet comments, support for the PCAPng format should be developing more quickly than it has been. This article describes the new format, displays methods to take advantage of new features, introduces scripting that can make the format usable, and makes the argument that migration to PCAPng is necessary.

PCAP Next Generation (PCAPng) is a new file format that is used to conduct and analyze packet captures. PCAPng is an attempt to improve the traditional PCAP format by introducing new features. The three goals of the PCAPng file format are extensibility, portability, and the ability to merge or append data. These goals address shortfalls of the PCAP format. PCAPng attempts to improve upon the PCAP file format through the use of blocks that provide useful metadata about the capture. By using blocks, PCAPng prevents its file structure from being constrained to the contents of a single header. Blocks can be inserted to provide more metadata about the capture as necessary. The most important blocks and their descriptions are as follows:

- **Section Header Block (SHB)** – This block is mandatory for all captures and must appear at least once. It defines general characteristics about the file that are necessary for readability.
- **Interface Description Block (IDB)** – Contains metadata about the interface that performed the capture. There may be multiple IDBs in a capture, which enables multiple interface captures, regardless of link-layer type.
- **Enhance Packet Block (EPB)** – Serves as a container for a single captured frame. It may also include optional metadata that enables per-packet annotations.
- **Name Resolution Block (NRB)** – Contains information that maps IP addresses to host names. The metadata is included in the PCAPng file itself, so the mapping is available even if the DNS server is not.
- **Interface Description Block (ISB)** – Provides statistics about the capturing interface such as number of dropped packets.

The introduction of these blocks allows for additional metadata to be included in the capture, which translates to more functionality than PCAP currently provides. One problem with PCAP is that it does not allow for capturing on multiple interfaces when the link-layer types are different. For example, PCAP does not allow for the capture of traffic on wired and wireless interfaces simultaneously. PCAPng fixes this limitation through the ISB. Because a PCAPng file can include multiple ISBs, it can capture on many interfaces regardless of link-layer type while maintaining the interface-to-packet mapping. This is not possible in PCAP because the interface mapping is defined in a global header.



```
 2 0.766224 fe80::16cf:e…              ff02::1                   ICMPv6   110
 3 -0.0003… fe80::16cf:e…              ff02::1                   ICMPv6   110
 4 0.244880 192.168.0.18         5353 224.0.0.251           5353 MDNS     381
 5 -0.0004… 192.168.0.9          5353 224.0.0.251           5353 MDNS     721
 6 0.007756 192.168.0.9          5353 224.0.0.251           5353 MDNS     721
 7 -0.0029… 192.168.0.18         5353 224.0.0.251           5353 MDNS     381
 8 0.509874 ArrisGro_ac:…              Dell_37:7f:9d             ARP       60
 9 0.000014 Dell_37:7f:9d              ArrisGro_ac:d…            ARP       42
10 0.475043 ArrisGro_ac:…              Broadcast                 0x8899    60
11 0.167703 192.168.0.18        64438 74.204.142.146          53 DNS       87
12 -0.0004… 192.168.0.9         51539 74.204.142.146          53 DNS       87
13 0.029843 74.204.142.1…          53 192.168.0.9          51539 DNS      246
14 -0.0015… 74.204.142.1…          53 192.168.0.18         64438 DNS      246
15 0.078675 192.168.0.9         50069 74.125.21.95           443 TCP       66
16 0.056453 74.125.21.95          443 192.168.0.9          50069 TCP       66
17 0.000081 192.168.0.9         50069 74.125.21.95           443 TCP       54
rame 4: 381 bytes on wire (3048 bits), 381 bytes captured (3048 bits) on int
 Interface id: 0 (\Device\NPF_{8EE3DE7B-2588-40F3-9E1D-530E7AD8E393})
 Encapsulation type: Ethernet (1)
 Arrival Time: Jan 13, 2018 12:20:24.780768000 Central Standard
 [Time shift for this packet: 0.000000000 seconds]
 Epoch Time: 1515867624.780768000 seconds
```

Figure 2 – Filter on interface ID

PCAP also lacks statistical information about the capture itself. PCAPng addresses this through the use of the ISB, which provides information on dropped packets and other statistics. Time resolution is improved in PCAPng as well. To improve upon the PCAP time resolution of microseconds (which can easily reduce the accuracy of timestamps even on a 1Gbps link), PCAPng stores timestamps in 64-bit blocks that provide a time resolution of nanoseconds. Finally, PCAP does not provide a way to include portable comments on a per-packet basis. However, PCAPng allows for optional data in the EPB so that portable comments on a per-packet basis can be included. Unfortunately, many applications do not support the features that PCAPng provides, so to demonstrate functionality, Wireshark's suite of tools is used in this research.

Wireshark

Wireshark started as a project called Ethereal, which was released in 1998 under the GNU Public License by Gerald Combs. Ethereal was rebranded in 2006 under the name Wireshark, and today it has more than 500 developers who actively contribute to the project [7]. A typical Wireshark install includes TShark, which is a full-featured command line tool. TShark has all the same capabilities that Wireshark does, as it can take advantage of the ability to read and write PCAPng. It also comes with tools such as EditCap, MergeCap, ReorderCap, which assist in editing and manipulating captures. Wireshark's popular GUI makes it easy to take advantage of the features PCAPng introduces. For example, figure 1 shows the ability to capture from multiple interfaces. An analyst can choose one of the active interfaces on a machine, hold CTRL, and click on a second interface. Wireshark will capture traffic from both interfaces at the same time—a feature not possible without PCAPng's ability to distinguish between interface IDs.

In this case, the analyst can capture on the wired and wireless interfaces simultaneously, which saves a significant amount of time. It is evident how easily this concept could be applied in a situation where the behavior of two networks, separated by physical interfaces, might need to be captured at the same time. Distinguishing the traffic is as simple as applying a display filter when the capture is complete. Figure 2 shows that each packet is given an interface ID—a direct benefit of the fields available in the IDB and EPB provided by PCAPng. Because this information exists in the capture, analysts can distinguish between the two interfaces and capture at the same time. Timestamps can be compared with more accuracy using this method, and merging becomes less necessary.

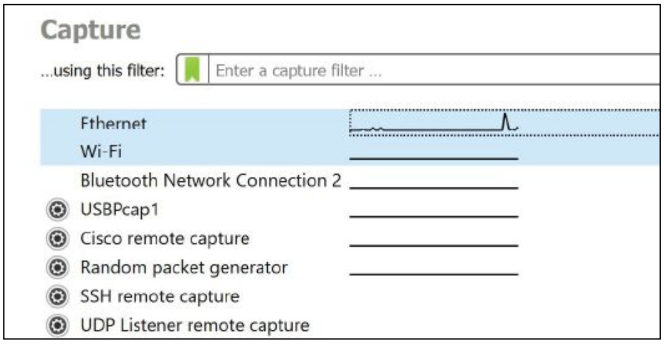
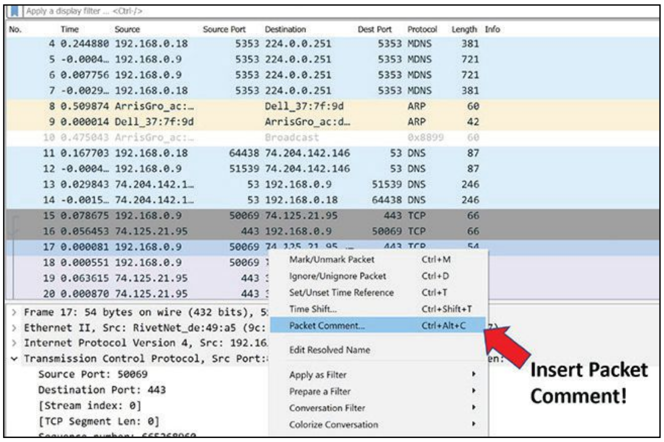


Figure 1 – Perform a capture

Filtering the capture to display information from only one interface is simple. As displayed in figure 2, an analyst can simply right-click on the interface ID and choose to filter on that interface alone. This is considered a "display filter" and can be defined at any time after a capture is complete. Wireshark also provides the ability to apply a "capture filter," which tells the application to save only the information defined by the filter. For example, one could sniff a wireless network, but choose to save only http traffic to the PCAPng produced from the sniffing session.

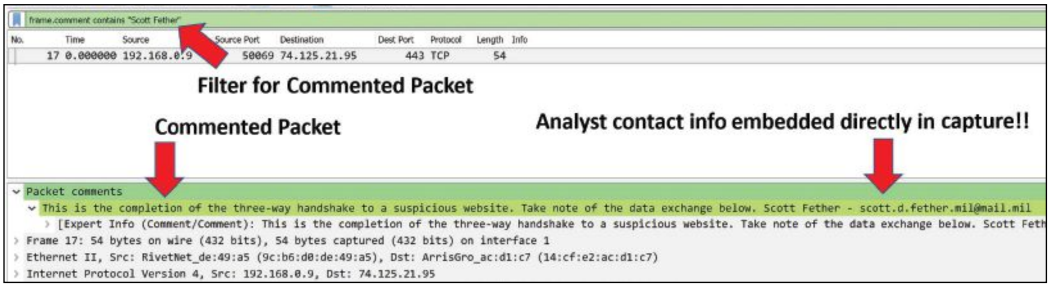
Another capability of the PCAPng file format is making per-packet comments. The opt_comment option allows the file format to accept a UTF-8 human-readable string. Since each packet has a header capable of being edited by an upper-level application, it's easy to place analytical notes directly into a PCAPng file. Wireshark takes advantage of this capability, and comments can be added directly to a packet. By right-clicking on any packet the user will be given the option to add a comment. Figure 3 shows the act of adding comments to packet number 17, the completion of a TCP three-way handshake.

For this example, a comment has been added to packet 17 that includes a name and email address. This displays how an analyst would take advantage of the commenting feature that PCAPng provides. If an analyst expects that other analysts will view his comments, he could make it standard practice to add contact information to those comments. Analysts could also add comments to each packet to identify who captured the packet and when the capture took place. The additional metadata contributes to shared information and collaboration among analysts. Once a comment has been applied, a



```
Apply a display filter ... <Ctrl-/>
No.     Time      Source          Source Port  Destination      Dest Port  Protocol  Length  Info
      4 0.244880 192.168.0.18          5353 224.0.0.251          5353 MDNS       381
      5 -0.0004… 192.168.0.9           5353 224.0.0.251          5353 MDNS       721
      6 0.007756 192.168.0.9           5353 224.0.0.251          5353 MDNS       721
      7 -0.0029… 192.168.0.18          5353 224.0.0.251          5353 MDNS       381
      8 0.509874 ArrisGro_ac:…              Dell_37:7f:9d             ARP         60
      9 0.000014 Dell_37:7f:9d              ArrisGro_ac:d…            ARP         42
     10 0.475043 ArrisGro_ac:…              Broadcast                 0x8899      60
     11 0.167703 192.168.0.18         64438 74.204.142.146         53 DNS         87
     12 -0.0004… 192.168.0.9          51539 74.204.142.146         53 DNS         87
     13 0.029843 74.204.142.1…           53 192.168.0.9         51539 DNS        246
     14 -0.0015… 74.204.142.1…           53 192.168.0.18        64438 DNS        246
     15 0.078675 192.168.0.9          50069 74.125.21.95          443 TCP         66
     16 0.056453 74.125.21.95           443 192.168.0.9         50069 TCP         66
     17 0.000081 192.168.0.9          50069 74.125.21.95 …        443 TCP         54
     18 0.000551 192.168.0.9          50069
     19 0.063615 74.125.21.95           443
     20 0.000870 74.125.21.95           443
> Frame 17: 54 bytes on wire (432 bits), 5
> Ethernet II, Src: RivetNet_de:49:a5 (9c:
> Internet Protocol Version 4, Src: 192.16
v Transmission Control Protocol, Src Port:
    Source Port: 50069
    Destination Port: 443
    [Stream index: 0]
    [TCP Segment Len: 0]
```

Figure 3 – Packet comment



```
frame.comment contains "Scott Fether"
No.     Time      Source          Source Port  Destination      Dest Port  Protocol  Length  Info
     17 0.000000 192.168.0.9          50069 74.125.21.95          443 TCP         54
v Packet comments
  v This is the completion of the three-way handshake to a suspicious website. Take note of the data exchange below. Scott Fether - scott.d.fether.mil@mail.mil
    > [Expert Info (Comment/Comment): This is the completion of the three-way handshake to a suspicious website. Take note of the data exchange below. Scott Feth
> Frame 17: 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface 1
> Ethernet II, Src: RivetNet_de:49:a5 (9c:b6:d0:de:49:a5), Dst: ArrisGro_ac:d1:c7 (14:cf:e2:ac:d1:c7)
> Internet Protocol Version 4, Src: 192.168.0.9, Dst: 74.125.21.95
```

Filter for Commented Packet
Commented Packet
Analyst contact info embedded directly in capture!!

Figure 4 – Filter for commented packet

great benefit is the ability to filter on those comments. This is shown in figure 4.

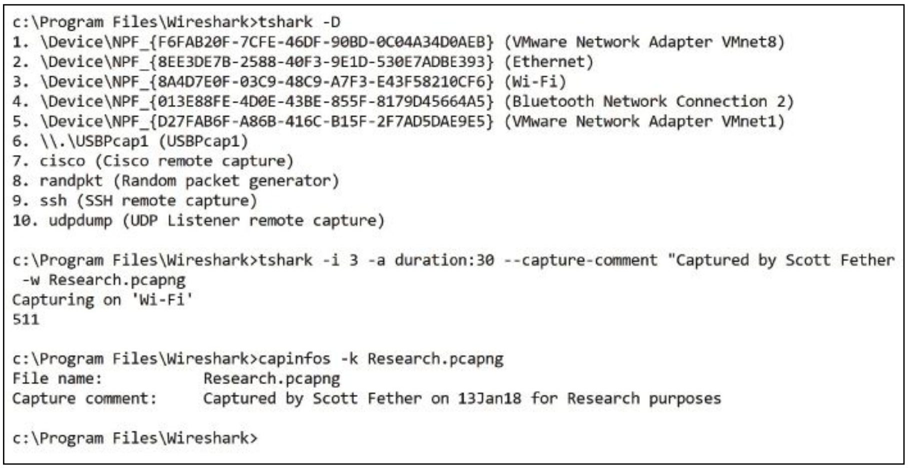
All of these features are portable, and they are carried along as a PCAPng file is transported from application to application. If the application supports the reading of the PCAPng file format, comments will carry over as part of that file. TShark, Wireshark's command line version of Wireshark, can be implemented to further display how analysts can take advantage of these new features. TShark has the added advantage of being able to read and write to the PCAPng file format, which brings all the additional features to a CLI environment capable of automation through scripting.

TShark and other command line tools

TShark has many options that can manipulate the display of a PCAPng file based on an analyst's need. The capture used in the previous section was saved to a file called "CommentedCapture.pcapng" and was moved into the directory where TShark is installed. A simple TShark command that displays commented packets shows that the packet comment used in this example was transported along with the PCAPng file. It is readable by TShark and would be readable to any application that can read the file format, as figure 5 shows. As expected, frame 17 contains the comment created in the Wireshark GUI.

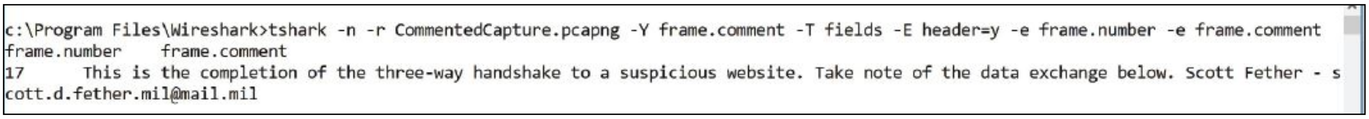
TShark can also can write a comment to an entire capture when TShark is the tool being used to perform the capture. This is different than a per-packet comment, however, and if a capture is split into two files at a later time, this metadata might be lost. As an example of TShark's implementation of a capture comment, figure 6 shows a typical capture process. The first command uses the "-D" option, which displays all the interfaces available on which to capture. In this case, interface 3 is used, which is Wi-Fi. Using a typical capture command along with the "—capture-comment" option, TShark can comment on a capture as a whole. An analyst then has the opportunity to add his or her name, date, and purpose of capture. Finally, using another tool that is provided with Wireshark called CapInfos, the comment that was created during the capture is displayed.

In order to add per-packet comments to a capture, one must use EditCap, which is another tool that comes with a basic Wireshark installation. EditCap can add, delete, or modify information on a previously saved PCAPng file. For example, if an analyst wants to comment his name on the very first packet in the capture that was edited in Wireshark, he can use EditCap as shown in figure 7. With the "-a" option in



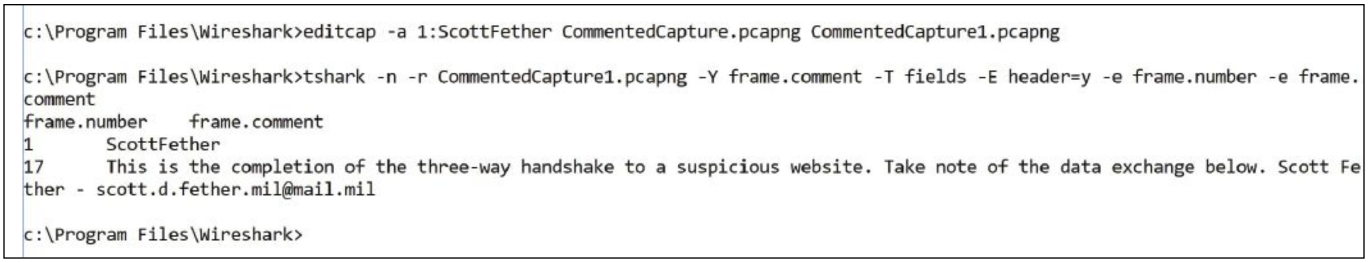
```
c:\Program Files\Wireshark>tshark -D
1. \Device\NPF_{F6FAB20F-7CFE-46DF-90BD-0C04A34D0AEB} (VMware Network Adapter VMnet8)
2. \Device\NPF_{8EE3DE7B-2588-40F3-9E1D-530E7ADBE393} (Ethernet)
3. \Device\NPF_{8A4D7E0F-03C9-48C9-A7F3-E43F58210CF6} (Wi-Fi)
4. \Device\NPF_{013E88FE-4D0E-43BE-855F-8179D45664A5} (Bluetooth Network Connection 2)
5. \Device\NPF_{D27FAB6F-A86B-416C-B15F-2F7AD5DAE9E5} (VMware Network Adapter VMnet1)
6. \\.\USBPcap1 (USBPcap1)
7. cisco (Cisco remote capture)
8. randpkt (Random packet generator)
9. ssh (SSH remote capture)
10. udpdump (UDP Listener remote capture)

c:\Program Files\Wireshark>tshark -i 3 -a duration:30 --capture-comment "Captured by Scott Fether
 -w Research.pcapng
Capturing on 'Wi-Fi'
511

c:\Program Files\Wireshark>capinfos -k Research.pcapng
File name:           Research.pcapng
Capture comment:     Captured by Scott Fether on 13Jan18 for Research purposes

c:\Program Files\Wireshark>
```

Figure 6 – TShark capture with capture comment



```
c:\Program Files\Wireshark>tshark -n -r CommentedCapture.pcapng -Y frame.comment -T fields -E header=y -e frame.number -e frame.comment
frame.number    frame.comment
17      This is the completion of the three-way handshake to a suspicious website. Take note of the data exchange below. Scott Fether - s
cott.d.fether.mil@mail.mil
```

Figure 5 – Portable comments



```
c:\Program Files\Wireshark>editcap -a 1:ScottFether CommentedCapture.pcapng CommentedCapture1.pcapng

c:\Program Files\Wireshark>tshark -n -r CommentedCapture1.pcapng -Y frame.comment -T fields -E header=y -e frame.number -e frame.
comment
frame.number    frame.comment
1       ScottFether
17      This is the completion of the three-way handshake to a suspicious website. Take note of the data exchange below. Scott Fe
ther - scott.d.fether.mil@mail.mil

c:\Program Files\Wireshark>
```

Figure 7 – Comments with EditCap

EditCap, an analyst can add a comment to one frame. Now instead of having just one comment on frame 17, there is also a comment on frame 1. Unfortunately, there is no option to add the same comment to a range of frames. For example, it may be desirable to add capture information to each frame, which would ensure that the information would survive most variations done in EditCap. Currently, one must use scripting to accomplish this task

The TShark and EditCap tools both have limitations. TShark, for example, can only write comments on a per-capture basis. Even this "per-capture" commenting capability is limited because it can only be used at the time of capture. TShark cannot add comments to a previously saved file or per-packet comments. These limitations require the use of multiple tools within a command-line environment to take advantage of the commenting features provided by PCAPng.

EditCap has the ability to add comments to a packet, but there is no way to add comments to a range of packets. The "-a" option depicted in figure 7 only works one frame at a time. EditCap also requires an input file, which means that comments cannot be added during a capture. The PCAPng file must be fully written before it can be adjusted by EditCap. Clearly, the tools provided in Wireshark provide an analyst the most comprehensive ability to take advantage of additional options and fields that the PCAPng file format introduces.

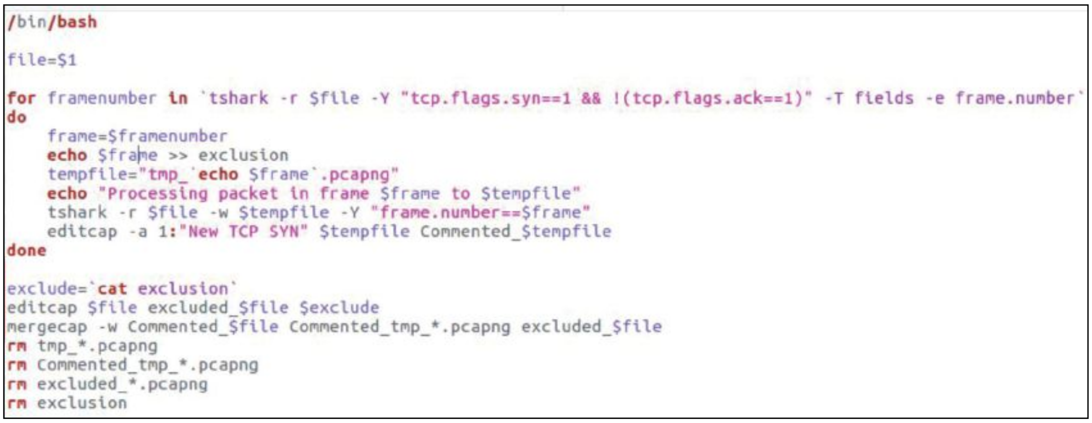
As a developing format, Wireshark could be improved to support more advanced operations, however. The ability to add per-packet comments at the time of capture would be a desirable improvement, for example. This capability applied to specific packets within a capture could help Wireshark take full advantage of commenting capabilities. In the meantime, analysts resort to scripting to take advantage of PCAPng's new features.

Scripting It Out

Although PCAPng has some advantages over its predecessor, the challenge for analysts becomes how to use these features while their favorite tools are slow to advance their capabilities. This section will focus on a Linux system to use the features of bash scripting. Since writing PCAPng files is not fully supported in some languages, scripting combined with Wireshark's tools can bring PCAPng features into action. This example will show how a script can be used to filter traffic from any capture, and how comments can be added to each of those packets. As stated previously, tools like EditCap rely on a fully written PCAPng file, so this is a post-capture task. It can save time and help the analyst comment on interesting traffic through automation.

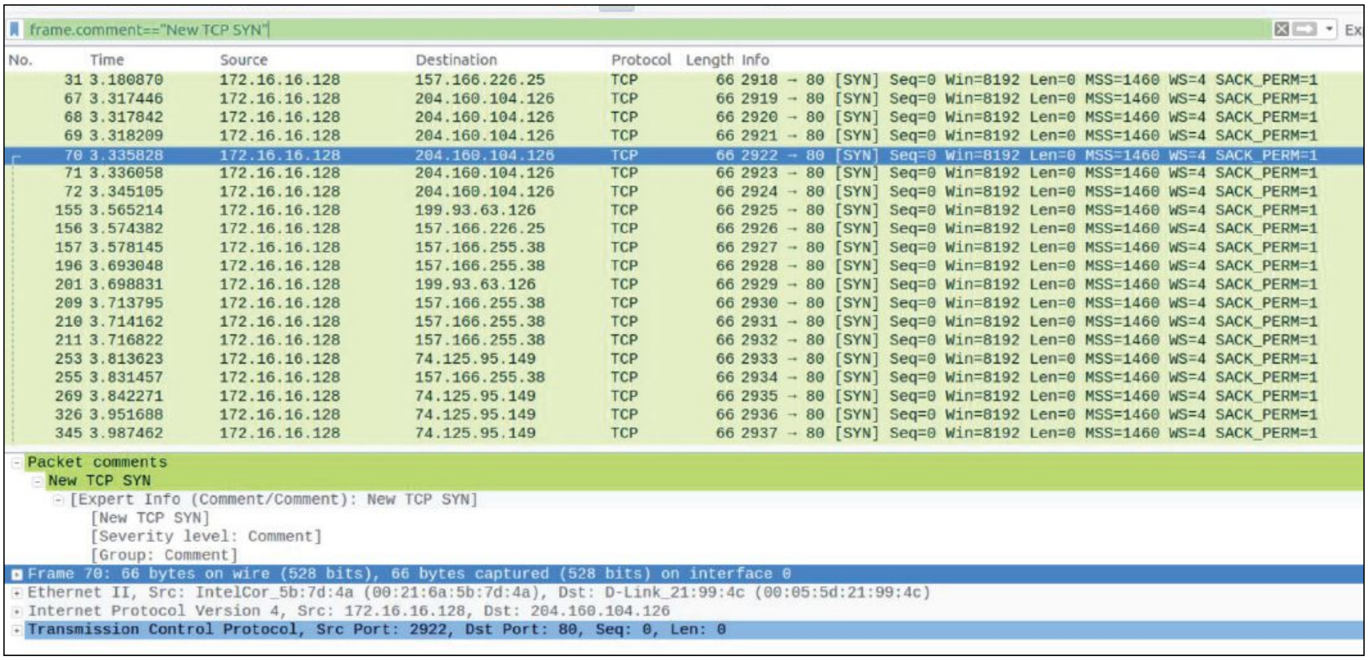
During script development, a Linux distribution that had Wireshark installed along with TShark, EditCap, and MergeCap was used. The script will also work on a Windows system with Bash installed. Bash provided the easiest way to manipulate the data and pass it between Wireshark's different tools. The SIFT workstation from SANS was downloaded for this example. This demonstration uses a previously captured PCAPng file that includes a large amount of web traffic. Chris Sanders, author of "Practical Packet Analysis: Using Wireshark to Solve Real Network Problems," has a multitude of PCAPng files posted on his GitHub. I chose one called "lotsofweb.pcapng" [6].

When analyzing new captures, one may spend time looking for new TCP connections. An analyst could be looking for connections to IP addresses that might be untrusted or adversarial. For captures that have many TCP connections, it can be helpful to add a comment to each new connection. Because of this, I decided to write the script so it filters on new TCP connections and creates a new PCAPng file that includes comments on the first SYN packet for new connections. In Wireshark, the filter for this type of traffic could be tcp.flags.syn==1 && !(tcp.flags.ack==1). This will filter out only the



```
/bin/bash

file=$1

for framenumber in `tshark -r $file -Y "tcp.flags.syn==1 && !(tcp.flags.ack==1)" -T fields -e frame.number`
do
    frame=$framenumber
    echo $frame >> exclusion
    tempfile="tmp_`echo $frame`.pcapng"
    echo "Processing packet in frame $frame to $tempfile"
    tshark -r $file -w $tempfile -Y "frame.number==$frame"
    editcap -a 1:"New TCP SYN" $tempfile Commented_$tempfile
done

exclude=`cat exclusion`
editcap $file excluded_$file $exclude
mergecap -w Commented_$file Commented_tmp_*.pcapng excluded_$file
rm tmp_*.pcapng
rm Commented_tmp_*.pcapng
rm excluded_*.pcapng
rm exclusion
```

Figure 8 – PCAPng comment script



```
frame.comment=="New TCP SYN"

No.     Time        Source          Destination       Protocol  Length  Info
     31 3.180870    172.16.16.128   157.166.226.25    TCP       66 2918 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
     67 3.317446    172.16.16.128   204.160.104.126   TCP       66 2919 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
     68 3.317842    172.16.16.128   204.160.104.126   TCP       66 2920 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
     69 3.318209    172.16.16.128   204.160.104.126   TCP       66 2921 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
     70 3.335828    172.16.16.128   204.160.104.126   TCP       66 2922 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
     71 3.336058    172.16.16.128   204.160.104.126   TCP       66 2923 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
     72 3.345105    172.16.16.128   204.160.104.126   TCP       66 2924 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    155 3.565214    172.16.16.128   199.93.63.126     TCP       66 2925 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    156 3.574382    172.16.16.128   157.166.226.25    TCP       66 2926 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    157 3.578145    172.16.16.128   157.166.255.38    TCP       66 2927 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    196 3.693048    172.16.16.128   157.166.255.38    TCP       66 2928 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    201 3.698831    172.16.16.128   199.93.63.126     TCP       66 2929 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    209 3.713795    172.16.16.128   157.166.255.38    TCP       66 2930 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    210 3.714162    172.16.16.128   157.166.255.38    TCP       66 2931 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    211 3.716822    172.16.16.128   157.166.255.38    TCP       66 2932 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    253 3.813623    172.16.16.128   74.125.95.149     TCP       66 2933 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    255 3.831457    172.16.16.128   157.166.255.38    TCP       66 2934 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    269 3.842271    172.16.16.128   74.125.95.149     TCP       66 2935 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    326 3.951688    172.16.16.128   74.125.95.149     TCP       66 2936 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
    345 3.987462    172.16.16.128   74.125.95.149     TCP       66 2937 → 80 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1

- Packet comments
  - New TCP SYN
    - [Expert Info (Comment/Comment): New TCP SYN]
        [New TCP SYN]
        [Severity level: Comment]
        [Group: Comment]
+ Frame 70: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
+ Ethernet II, Src: IntelCor_5b:7d:4a (00:21:6a:5b:7d:4a), Dst: D-Link_21:99:4c (00:05:5d:21:99:4c)
+ Internet Protocol Version 4, Src: 172.16.16.128, Dst: 204.160.104.126
+ Transmission Control Protocol, Src Port: 2922, Dst Port: 80, Seq: 0, Len: 0
```

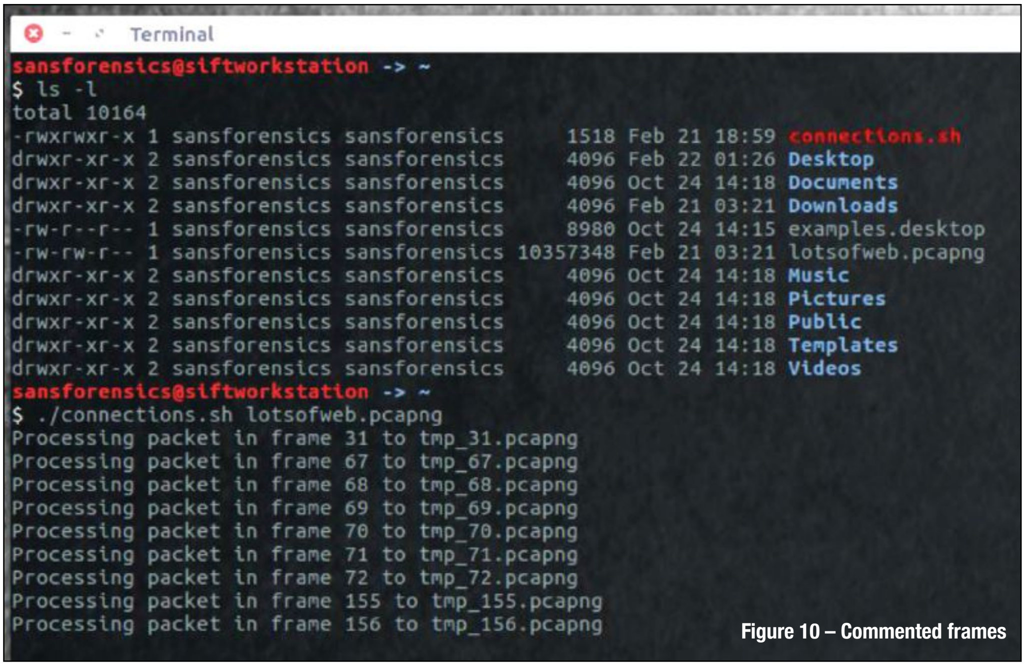
Figure 9 – Running the script

initial SYN packet from a TCP three-way handshake. The script is posted in figure 8.

The FOR loop utilizes TShark to filter on TCP SYN connections and extracts the frame number for each of those frames. The frame number is important because it uniquely identifies each frame. Within the loop, the frame number is appended to a file called "exclusion" for later use. Each frame that was identified in the filter is temporarily written to its own individual file. After it has been written to an individual file, EditCap is used to add the comment "New TCP SYN" to the frame. At the end of the FOR loop, each frame exists in its own temporary file which has been commented on. Frames are broken out into individual files because EditCap requires an input and output file and can only add comments one frame at a time. Using it in a FOR loop seemed the most efficient way to do it with those limitations.

Once the FOR loop has commented on the individual frames, the script has to merge the data back together. Simply using MergeCap to add the individual files to the original capture results in duplicate frames. This cannot be resolved by using the "-d" deduplicate option in EditCap because the additional comment changes the md5 hash of the duplicated packet. For this reason, the script keeps track of which frames were edited in the "exclusion" file. This makes it simple to remove the edited frames from the original capture and rename it "excluded_$file." The script then merges all the commented temporary files and the excluded_$file to produce the final product. The end result of the script is a new PCAPng file named "Commented_$file." The only difference in the new file is that all initial SYN packets are commented on. All temporary files are removed upon completion of the script. The only files that remain are the original capture and the newly commented capture files.

In order to run the script, the capture file is placed in the same directory as the script. Simply run the command "./connections.sh inputfile.pcapng." Figure 9 shows the process.



```
sansforensics@siftworkstation -> ~
$ ls -l
total 10164
-rwxrwxr-x 1 sansforensics sansforensics     1518 Feb 21 18:59 connections.sh
drwxr-xr-x 2 sansforensics sansforensics     4096 Feb 22 01:26 Desktop
drwxr-xr-x 2 sansforensics sansforensics     4096 Oct 24 14:18 Documents
drwxr-xr-x 2 sansforensics sansforensics     4096 Feb 21 03:21 Downloads
-rw-r--r-- 1 sansforensics sansforensics     8980 Oct 24 14:15 examples.desktop
-rw-rw-r-- 1 sansforensics sansforensics 10357348 Feb 21 03:21 lotsofweb.pcapng
drwxr-xr-x 2 sansforensics sansforensics     4096 Oct 24 14:18 Music
drwxr-xr-x 2 sansforensics sansforensics     4096 Oct 24 14:18 Pictures
drwxr-xr-x 2 sansforensics sansforensics     4096 Oct 24 14:18 Public
drwxr-xr-x 2 sansforensics sansforensics     4096 Oct 24 14:18 Templates
drwxr-xr-x 2 sansforensics sansforensics     4096 Oct 24 14:18 Videos
sansforensics@siftworkstation -> ~
$ ./connections.sh lotsofweb.pcapng
Processing packet in frame 31 to tmp_31.pcapng
Processing packet in frame 67 to tmp_67.pcapng
Processing packet in frame 68 to tmp_68.pcapng
Processing packet in frame 69 to tmp_69.pcapng
Processing packet in frame 70 to tmp_70.pcapng
Processing packet in frame 71 to tmp_71.pcapng
Processing packet in frame 72 to tmp_72.pcapng
Processing packet in frame 155 to tmp_155.pcapng
Processing packet in frame 156 to tmp_156.pcapng
```

Figure 10 – Commented frames

The script will display feedback to the terminal as each frame is processed.

When the script is complete, a new file called “Commented_$file.pcapng” will be placed in the current directory. In this case, the file is called “Commented_lotsofweb.pcapng.” Using Wireshark, opening the new file will display that all TCP SYN frames are now commented with “New TCP SYN.” An analyst can filter on the commented frames using the Wireshark filter frame.comment==”New TCP SYN.” This filter displays the initial connection to all TCP streams. This is just one way to take advantage of the PCAPng commenting feature. The filter is shown in figure 10.

Appendix A

Commenting Script

```
# Author: Scott Fether
# February 21, 2018
# This script will identify new TCP Connections and add per-packet comments to
# the initial SYN frame. The script filters specifically on new TCP connections, but
# it can be modified to filter on anything TShark accepts. Comments can be changed
# to describe the interesting traffic.

#!/bin/bash
file=$1
for framenumber in `tshark -r $file -Y “tcp.flags.syn==1 && !(tcp.flags.ack==1)” -T fields -e frame.number`
do
     frame=$framenumber
     echo $frame >> exclusion
     tempfile=”tmp_`echo $frame`.pcapng”
    echo “Processing packet in frame $frame to $tempfile”
      tshark -r $file -w $tempfile -Y “frame.number==$frame”
    editcap -a 1:”New TCP SYN” $tempfile Commented_$tempfile
done

exclude=`cat exclusion`
editcap $file excluded_$file $exclude
mergecap -w Commented_$file Commented_tmp_*.pcapng excluded_$file
rm tmp_*.pcapng
rm Commented_tmp_*.pcapng
rm excluded_*.pcapng
rm exclusion
```

The script can automate comments for various types of filters that need to be applied. The only necessary changes would be to change the filter used on the original TShark command in the FOR loop, then change the comment in the EditCap line to whatever the analyst desires. The script is a great way to take advantage of commenting features of the PCAPng file format. Until other tools incorporate some of these features, scripting enables access to portions of the PCAPng file format that are otherwise inaccessible. The full script is included in Appendix A.

Conclusion

There is no doubt that PCAPng is an improvement over the old PCAP file format. Its additional capabilities such as multiple interface capture, per-packet comments, and improved time resolution make the transition a worthy one. So far, packet capture applications have failed to fully implement the capabilities of the new format. Even Wireshark, which is responsible for much of PCAPng’s advancement to date, shows limitations in its ability to take advantage of the new fields. The necessity to pass a PCAPng file from tool to tool is unfortunate, and analysts could increase efficiency if tools were more supportive of the format.

Further research on this topic would seek to integrate the PCAPng file format into more tools so its new fields can be harnessed for advanced research and increased cyber forensic capability. As networks grow faster and more complex, cyber defenders’ capability to analyze threats must be accurate and provide as much metadata as possible. Packet analysis will continue to play an important role in defending networks and analyzing malware, especially with the increased use of fileless malware. It is important that projects such as PCAPng are supported so that they can continue to provide adaptable solutions to problems that defenders will face in the future.

References

1. Development/LibpcapFileFormat. (n.d.). Retrieved November 14, 2017, from https://wiki.wireshark.org/Development/LibpcapFileFormat - Libraries.
2. Koch, M. (2016). “Implementing Full Packet Capture,” Retrieved October 5, 2017, from https://www.sans.org/reading-room/whitepapers/forensics/implementing-full-packet-capture-37392.
3. NIST. (2016). NIST Special Publication 800-53 Rev4. Retrieved from NIST.gov: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.
4. “Pcapng/pcapng,” Github. Retrieved November 13, 2017, from https://github.com/pcapng/pcapng/wiki/Implementations.
5. Jasper, “The Trouble with Multiple Capture Interfaces,” Packet Foo (2014). Retrieved from https://blog.packet-foo.com/2014/08/the-trouble-with-multiple-capture-interfaces/.

6. Sanders, C. "Chrissanders/packets,"Github (June 19, 2017). Retrieved February 18, 2018, from https://github.com/chrissanders/packets.
7. Sanders, C. *Practical Packet Analysis: Using Wireshark to Solve Real-World Network Problems*. San Francisco, CA: No Starch Press (2017).
8. Sanders, C., and Smith, J. *Applied Network Security Monitoring*, Syngress (2014) pp. 37-38).
9. "TCPDUMP & LIBPCAP," TCPDUMP.org (n.d.). Retrieved November 14, 2017, from http://www.tcpdump.org/.
10. Tuexen, E., Risso, F., Bongertz, J., Combs, G., Harris, G., (2017). PCAP Next Generation (pcapng) Capture File Format. Retrieved October 10, 2017, from http://xml2rfc.tools.ietf.org/cgi-bin/xml2rfc.cgi?url=https://raw.githubusercontent.com/pcapng/pcapng/master/draft-tuexen-opsawg-pcapng.xml&modeAsFormat=html/ascii&type=ascii.
11. Walls, J. "Five Reasons to Move to the Pcapng Capture Format (by Jason Walls)," LoveMyTools.com (2012, October 02). Retrieved December 12, 2017, from http://www.lovemytool.com/blog/2012/10/five-reasons-to-move-to-the-pcapng-capture-format-by-jason-walls.html.

About the Author

Scott Fether is an Information Protection Warrant Officer for the United States Army. For the past 14 years he has worked in various information technology positions for the Army. Scott is a candidate for the Master of Science degree in Information Security Engineering from SANS Technology Institute. He may be reached at scott.d.fether.mil@mail.mil.

Net Neutrality: What Is It and Is It Necessary?

Continued from page 36

trieved from http://transition.fcc.gov/Daily_Releases/Daily_Business/2015/db0226/DOC-332260A1.pdf.

9. FCC (2016). "Consumer Guide – Open Internet." Last Reviewed 6/14/16. Retrieved from http://transition.fcc.gov/cgb/consumerfacts/openinternet.pdf.
10. Hylton, K.N. (2016). "Law, Social Welfare, and Net Neutrality," Boston University School of Law, Law & Economics Paper No. 16-08. Revised May 26, 2016. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2736541.
11. Peha, J.M. (2006). "The Benefits and Risks of Mandating Network Neutrality, and the Quest for a Balanced Policy," 34th Telecommunications Policy Research Conference, Sept 2006. Retrieved from https://www.researchgate.net/publication/228704027.
12. Peha, J.M., Lehr, W.H., and Wilkie, S. (2007). "The State of the Debate on Network Neutrality," International Journal of Communication 1 (2007), 709-716. Retrieved from https://www.researchgate.net/publication/254571226.
13. United States Court of Appeals for the District of Columbia Circuit (2010). "Comcast Corporation v. Federal Communications Commission and United States of America," Decision No. 08-1291. Retrieved from https://www.cadc.uscourts.gov/internet/opinions.nsf/EA10373FA9C20DEA85257807005BD63F/$file/08-1291-1238302.pdf.
14. United States Court of Appeals for the District of Columbia Circuit (2014). "Verizon v. Federal Communications Commission," Decision No. 11-1355. Retrieved from https://www.cadc.uscourts.gov/internet/opinions.nsf/3AF8B4D938CDEEA685257C6000532062/$file/11-1355-1474943.pdf.
15. Van Schewick, I.B. (2005). "Towards an Economic Framework for Network Neutrality Regulation." Paper presented at the 33rd Research Conference on Communication, Information and Internet Policy (TPRCC 2005), September 23-25, 2005, The National Center for Technology and Law, George Mason University School of Law. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=812991.
16. Willcox, J.K. (2017). "Survey: Consumers Favor Strong Net Neutrality Rules," Consumer Reports September 27, 2017. Retrieved from https://www.consumerreports.org/net-neutrality/most-consumers-still-want-strong-net-neutrality-rules/.
17. Wu, T. (2003). "Network Neutrality, Broadband Discrimination," Journal on Telecommunications and High Technology Law Vol.2, 141-178.
18. Wu, T. and Yoo, C. (2006). "Keeping the Internet Neutral? Tim Wu and Christopher Yoo Debate," Federal Communications Law Journal, Vol. 59, 575-592. Retrieved from http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1778&context=faculty_scholarship.
19. Zhu, K. (2007). "Bringing Neutrality to Network Neutrality," Berkeley Technology Law Journal Vol.22, Issue 1, Article 32, January 2007. Retrieved from http://scholarship.law.berkeley.edu/cgi/viewcontent.cgi?article=1697&context=btlj.

About the Author

Dr. Nima Zahadat is a professor of forensics, information systems, and data science. He has also held positions as chief security officer, chief information officer, director of security, director of training solutions, dean of computer science, program chair of information systems, and director of operations. Dr. Zahadat has worked extensively with public and private sectors throughout the years. His research interests are digital forensic, mobile security, information security, risk management, data mining, and information visualization. He may be contacted at nima@nima-zahadat.com.

Donn's Corner

Donn's Corner was published in the ISSA Journal as a monthly column February 2014 through August 2015

By Donn Parker – ISSA Distinguished Fellow, Silicon Valley Chapter

Information Security Maxims

This column in the ISSA Journal presented and briefly explained my sometimes controversial information security maxims (general rules, principles, or truths) for your edification. The topics I address start with cybercrime followed by information security solutions, advice for information security management, cybercrime predictions, and security future. A caveat is in order: for every maxim, there is an exception. ~ Donn Parker

Number 1 – The Golden age of Cybercrime

1. We are in the golden age of cybercrime between disaster and annihilation.

Number 2 – Cybercrime

2. Computers and devices using computers play just four roles in crime: Object, subject, tool, and symbol.
3. A cybercrime is an abuse or misuse where a computer or device containing a computer is the object, subject, tool, or symbol, and the perpetrator intentionally made or could have made gain.
4. Fragile computers as objects of great importance have been shot, blown up, kicked, shaken, drowned, electrocuted, fried, baked, burned, urinated upon, dropped, stolen, held for ransom, lost, irradiated, and sat on.
5. If it came from a computer, it must surely be correct, true, and significant.

Number 3 – Automated Crime

6. For the first time in criminal history, it is possible to possess a crime and execute it repeatedly as an app; not just do a crime one up.
7. Automated cybercrime provides the makings of perfect crime.

Number 4 – Errors and Omissions

8. Enterprises probably lose more from errors and omissions than they do from intentional acts.
9. Computers don't make errors or omissions; people do.
10. Assume loss incidents are intentional before accepting them as accidental.
11. It is better to concentrate first on preventing and mitigating intentional wrongdoings.
12. It is difficult at times to tell the difference between intentional and accidental wrongdoings.
13. Some intentional acts are derived from observed accidents.

Number 5 – Tabulating Cybercrimes

14. There are no known valid representative tabulations or cross tabulations of cybercrime.
15. The partial and biased tabulations that we have may be used for proof-of-existence.
16. The annual breach reports are excellent sources of "lower bound" tabulations of cybercrimes (known but more are unknown).
17. Viruses, worms, hacker intrusions, point of sale frauds, phishing, and software piracy are not risks; they are likely certainties.
18. Hackers and hacker attacks haven't gone away.

Number 6 – Checklists

19. At the right level of abstraction, detail, and comprehensiveness, security checklists are valuable aids, but only aids.
20. Remember, your adversaries use different checklists than yours.
21. Never assume a checklist is complete.

Number 7 – Cybercriminals

22. Employers don't hire crooks; people become trust violators in the course of their work.
23. Computers don't commit crimes; people do.
24. Cybercriminals think they are too smart to get caught.
25. Wrongdoers often become the equivalent of trusted people to execute their crimes.
26. Wrongdoers find computers are attractive targets; they don't show anguish, cry, or hit back.
27. Information security professionals are expert and highly trusted and, therefore, potentially highly dangerous.
28. Collusion should be suspected in complex cybercrimes.
29. One cybercrime attracts more cybercrimes. Cybercriminals are frequent copycats.
30. Restitution for harm done rarely occurs and is more difficult and dangerous.
31. Cybercriminals routinely lie and deceive.
32. Cybercriminals may be more dangerous in prison than out by educating other prisoners.
33. Recidivism is unlikely among amateur trust violators that are motivated by personal problems.
34. Violation of trust deceptively called "insider crime" is probably more frequent than reported.
35. Perpetrators are more likely to engage in crimes in familiar work environments.
36. Publicly revealing too much about an enterprise's security, vulnerabilities, and adversities is a grave danger.
37. Put your choice here.

Number 8 – Cybercrime Methods and Tactics

38. "How much electronic money, information, or software should I steal, modify, use, hide for extortion, plagiarize,

or destroy?" Since the effort is the same for any amount.

39. Perpetrators will gravitate to the simplest and safest methods first.
40. The salami technique of taking many small slices of the whole asset that goes unnoticed or ignored is profitable with computers.
41. The infamous accounting fraud of accumulating fractions of pennies after multiplication and division round-down is purely fictional.
42. Enterprise security policies, standards, and guides are excellent resources for planning cybercrimes.
43. Copy-cat cybercrimes abound: if done once, it will be done many times.
44. Attacks are plentiful and easy; defenses are limited and difficult.
45. We can't win for losing. Cybercrime happens.
46. Phishing (social engineering) is ultimately successful.
47. For perpetrators, one bug in their work and they go to jail.
48. A successful adversary must know the environment of his crime perfectly and completely.
49. Endangerment is an often overlooked but common cybercrime.
50. A clever form of sabotage is to blindly "work to rule" when exceptions occur.
51. Computers and networks free adversaries from geographic proximity to and real-time observation of their wrongdoings.

Number 9 – Classification of Enterprise Information

52. Two-level classification of information with applicable security labels is good enough except where multilevel is required by contract, law, or regulation.
53. Never use "confidential," "secret," and "top secret" labels except for government purposes.
54. Protect public information from plagiarism and unintended modification.

Number 10 – Limitations of the Need-to-Know

55. The need-to-know rule: Entrust only needed information.
56. The need-to-withhold rule: Withhold only specified information.
57. If more information is sharable than not, then need-to-withhold may be the better rule.

Number 11 – Ethical Conflicts

58. Seek informed consent of stakeholders to avoid unethical conduct.
59. People engaged in unethical acts often rationalize that they are solving a problem by causing the least harm to the least number of people.
60. Perpetrators act rationally from their perspectives but irrationally from victims' perspectives.
61. What is the security officer of a criminal enterprise to do (Enron for instance)?

Number 12 – Some Advice for Information Security Management

62. The enterprise's overall security effectiveness is only as strong as its unknown weakest link.
63. It is the nature of security that the best that security staffs can do is to go unnoticed.
64. CSOs may seem to become obsolete and their positions at stake when they are successful and adversities become infrequent. This is called "working your way out of a job."
65. Good security is when nothing very bad happens. And when nothing very bad happens, who needs security? Security seeks a "natural" lowest level. Periodic revitalization is necessary.
66. Security failures may be depicted as amusing but produce great personal anguish and suffering.
67. Even seemingly good security solutions may introduce unanticipated new vulnerabilities. For example, universal use of cryptographic protection in laptops in a large bank significantly increased the loss of laptops, because users assumed reduced need to protect them.
68. The security imperative: CSOs get only one chance to recommend security solutions to organizations because if they aren't accepted or effective, the organization stakeholders will use the failure as an excuse to preclude use of more security solutions. CSOs must be right the first time.
69. Diligent enterprise information security should be based on:
    a. A cooperative and understanding enterprise culture,
    b. Traditional controls and practices and loss experience,
    c. Compliance with requirements,
    d. Others' good practices, experience, and experimentation under similar circumstances,
    e. Standards, audit reports, and contracts,
    f. Cautiously used vendor advice and experimentation,
    g. Acceptance by management and stakeholders,
    h. Cost, and
    i. Cautious, proven, and selective use of current professional trade and research literature and news media.
70. Risk assessment dangerously provides management the opportunity and reason to accept risks and preclude acceptance of otherwise good security solutions.
71. Decisions by higher management fiat should be obtained when solution disagreements or intractable trade-offs occur.
72. Explicit information security compliance should be required in job descriptions and performance evaluations of all stakeholders.
73. The security of the information about the security of an enterprise is critically important and sensitive.

Number 13 – Cybercrime Predictions

74. We are approaching the total automation of crimes. For the first time in criminal history it is now possible to produce, package, possess, buy, and sell a crime, not just do a crime. This may be accomplished by selecting victims, perpetration, conversion to irreversible gain, and erasure of all evidence within a single uninterrupted software application that may be bought, sold, and improved upon by experts.
75. Automation will facilitate achieving the perfect crime where perpetrators know little or nothing about the

crimes they execute and the identity of the victims, gains are untraceable and irreversible, and no evidence remains of the event except the loss.

76. Many cybercrimes or aspects of them are unobservable at computer speeds far exceeding the time scale of human capability to mitigate them. This requires totally automated security without human intervention.
77. Many cybercrimes are now carried out as formal business ventures. They involve the use of packaged crime tools that are subject to continuing improvement and for which there is now an active and expanding market. The market is created by otherwise unqualified perpetrators willing to purchase and use them.
78. Older characteristics of past cybercrimes and adversaries such as malicious hackers and their games don't become obsolete. All types of criminals and their methods remain active and accumulate.
79. Much that is deducible from news or trade media reports of cybercrime is at most that something interesting may have happened.
80. Cybercrime is rapidly outpacing security and occupies the leading edge of information technology where criminal payoff is the greatest.

Number 14 – Limitations of Information Security

81. Try to remove an asset from the need for protection before protecting it.
82. Information security should include protection of possession (control), authenticity, and utility of information as well as confidentiality, integrity, and availability (CIA).
83. Information security is an unbounded and never complete art and practice.
84. Information security is a psychological discipline.
85. There always are more untreated vulnerabilities.
86. The effectiveness of security solutions is dependent on timely and sustained alertness, motivation, and commitment of trusted stakeholders.
87. Positive security motivation must be achieved with rewards for exemplary security and penalties for poor security before awareness training will be effective.
88. There are no known best security solutions.
89. Application of controls and practices add complexity and new vulnerabilities.
90. Information security ages and deteriorates and must be periodically renewed and reinvigorated.
91. With a big enough hammer you can break anything.

Number 15 – Information Security Solutions

92. Don't spend more protecting an asset than it is worth.
93. We must think like the enemy to overcome him.
94. Don't apply security solutions unless the stakeholders accept and support them.
95. Solutions and vulnerabilities are in one-to-many and many-to-one relationship.
96. The value of security solutions is usually unknown.
97. Security and the constraints impose unrecoverable costs and are universally hated.
98. The lack of quality security is primarily a "people problem."
99. Adding security solutions may reduce the value of other solutions, increase vulnerabilities, and even reduce overall security by providing a challenge to adversaries.
100. Properly used computers are often far superior anomaly detection devices than humans.
101. Attempting to forecast security risks (probabilities and impacts) of what unknown adversaries may do is fruitless and dangerous to careers when wrong.
102. Risk assessments may be achieved by providing simple and succinct expert opinion reports.
103. Segregation of duties or dual control and confidential personal advisory services for trusted people are important security solutions.
104. Multilevel classification of information in non-government enterprises ultimately deteriorates.
105. An objective of good enterprise security is at a minimum to have all appropriate accepted controls and practices in one's industry effectively in place or documented reasons why they are not in place.

Number 16 – The Trusted Persons Security Threat

106. Internal controls and catching trust violators protects trusted people.
107. Unusual efforts to gain trusted status, expertise, and special knowledge may be warning signs.
108. Security controls and practices in hiring, contracting, revealing secrets, and terminating employees should be commensurate with the degree of trust.
109. Balancing enterprise security with protection of trusted people's rights is the ultimate security control issue.
110. We are unable to anticipate sufficiently all of the unknown vulnerabilities and attacks before our increasingly intelligent and capable unknown cybercrime adversaries do.
111. Safety is a part of security.
112. Segregation of duties and dual control are sometimes effective alternatives to one another.
113. Ethics and law preclude enterprises from taking excessively vigorous security actions.
114. The security basics provide us with the equivalent of locked doors, moats, thick walls, auditors, forensics, and recovery, but with a big enough hammer and sufficiently effective deception, trusted people can break anything.
115. Deterioration and violation of controls and practices by trusted people is a constant problem and requires continued restrengthening.

Number 17 – CISO?

116. The qualified information security professional is a consultant and service provider to the enterprise.
117. The person accountable for a breach and loss is the person that could have prevented or mitigated it.
118. The title should fit the job, and the job should fit the title.
119. Chief and officer titles carry personal responsibility.
120. Policy should clearly state the security and loss responsibilities of all positions in the enterprise.

Donn Parker
ISSA Distinguished Fellow, Silicon Valley Chapter

ISSA CISO FORUM

The CISO Executive Forum is a peer-to-peer event – Members can feel free to share concerns, successes, and feedback in a peer-only environment.

ISSA CISO Executive Membership Program

The role of information security executive continues to be defined and redefined as the integration of business and technology as it evolves. While these new positions gain more authority and responsibility, peers must form a collaborative environment to foster knowledge and influence that will shape the profession.

The Information Systems Security Association (ISSA) recognizes this need and created the exclusive CISO Executive Membership program to give executives an environment to achieve mutual success. Connecting professionals to a large network of peers, valuable information, and top industry experts the program is a functional resource for members to advance personal and industry understanding of critical issues in information security.

Membership Benefits

- Free registration at four CISO Executive Forums per year, including lodging for one nigh and all meals at each Forum
- Extensive networking opportunities with peers and experts on an on-going basis
- Privileged access to online community
- Direct access to top subject matter experts through educational seminars
- An effective forum for understanding and influencing relevant standards and legislation
- A unified voice to influence industry vendors
- Basic Wisegate membership, including exclusive access to the Wisegate community and ISSA CISO Forum private group

Visit ISSA.org => Learn => CISO Executive Forum for more information or to register for the Forum.

ISSA Chapters around the Globe

Asia Pacific

Bangladesh
Chennai
Phillippines
Dehradun
India

Canada

Alberta
Vancouver
Ottawa
Toronto
Quebec City

Europe

Brussels
France
Germany
Irish
Italy
Netherlands
Poland
Romania
Spain
Switzerland
Turkey
UK
Ukraine

Latin America

Argentina
Barbados
Bolivia
British Virgin Islands
Chile
Colombia
Ecuador
Peru
Brazil

Middle East

Bahrain
Egypt
Israel
Kuwait
Saudi Arabia
Iran
Kazakhstan
Qatar

USA

Alamo
Blue Ridge
Boise
Buffalo Niagara
Capitol of Texas
Central Alabama
Central Florida
Central Indiana
Central Maryland
Central New York
Central Ohio
Central Pennsylvania
Central Plains
Central Texas
Central Virginia
Charlotte Metro
Chattanooga
Chicago
Colorado Springs
Columbus
Connecticut
Dayton
Delaware Valley
Denver
Des Moines
Eastern Idaho
East Tennessee
Fort Bragg Fayetteville
Fort Worth
Grand Rapids
Greater Augusta
Greater Cincinnati
Greater Spokane
Hampton Roads
Hawaii
Inland Empire
Kansas City
Kentuckiana
Kern County
Lansing
Las Vegas
Los Angeles
Melbourne, FL
Memphis
Metro Atlanta
Middle Tennessee
Milwaukee
Minnesota
Motor City
National Capital (DC)
New England
New Hampshire
New Jersey
New York Metro
North Alabama
North Dakota
North Oakland
North Texas
Northeast Florida
Northeast Indiana
Northeast Ohio
Northern Colorado
Northern New Mexico
Northern Virginia
Northwest Arkansas
Oklahoma
Oklahoma City
Orange County
Phoenix
Pittsburgh
Portland Oregon
Puerto Rico
Puget Sound
Quantico
Rainer
Raleigh
Rochester
Sacramento Valley
San Diego
San Francisco Bay Area
SC Charleston
SC Upstate SC
Silicon Valley
South Bend
Southeast Arizona
South Florida
South Texas
Southern Tier of NY
St. Louis
Tampa Bay
Texas Coastal Bend
Texas Gulf Coast
Triad of NC
Tucson
Utah
Ventura County
West Texas
Yorktown

ISSA.org => Chapters => Chapter Directory

ISSA
Information Systems Security Association

October 17–18, 2018
Georgia World Congress Center
Co-located with Cyber Security Atlanta

HOW TO FIGHT BACK:
nstrations of the Current
ou and Your Organization
HOW HACKERS ATTACK AND HOW
With Live Hacking Demonstra
cisco
Mera

2018 ISSA International Conference

SECURING TOMORROW TODAY

ISSA's eighth annual flagship conference is a world class event bringing together cyber, information, software, and infrastructure security professionals from 92 countries around the world. This 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

- 1000+ attendees spanning all levels of IT and InfoSec
- Expert Key Note Program
- Latest Information Security trends and techniques
- Intimate roundtables and panel discussions
- Networking lunches, general sessions, and evening receptions and award parties
- Career center
- VIP Lounge

Topics

- Application & Data Security
- Cloud Security
- Security Awareness
- Security & Privacy Collaboration
- Governance, Risk & Compliance
- Email & Endpoint Security
- Professional Development
- Threat Intelligence
- Emerging Technologies
- Bridging the Business Gap

The Expo floor will now feature more than 50+ leading technology companies

For registration and more information, visit www.issa.org