ISSA JOURNAL

July 2021
Volume 19 Issue 7

2021 ISSA International Election
COVID-19's Impact on Organizational Cybersecurity Posture

Security Implications of an Interconnected World

Table of Contents

DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

Feature

Also in this Issue

The ISSA Journal (1949-0550) is published monthly by
Information Systems Security Association
1964 Gallows Road, Suite 210, Vienna, VA 22182
+1 (866) 349-5818 (local/international)

Greetings ISSA Members

Candy Alexander, International President

Welcome to Summer!

I am so excited to announce our plans for fall events include the first in-person event in more than a year! For an organization known for the value of networking among members, it is excellent news for us all!!

The event I am referring to is InfoSec World in Orlando! ISSA will be on the show floor, providing a session on our research, running our Cyber Executive Summit, and holding an Awards Gala during this event. Stay tuned for dates and details!

I am looking forward to the opportunity to get out there and talk with all of you and share knowledge and experiences! If you are planning on attending, please stop by and say hello to me!!

July is a significant time of year for us in the ISSA, as it brings the annual International Board Elections. It provides each of you an opportunity to let your voice be heard. As members, you are eligible to vote for the candidate(s) you believe will best suit your interests on the International Board of Directors. To find out more about this year's candidates, visit https://www.members.issa.org/page/2021ISSAElection and then cast your vote!

We send our deepest sympathy to the family of Phillipe Courtot. We have been inspired by Phillipe's energy and passion for the ISSA membership, ISSAEF program support, and the cybersecurity industry. We have a special tribute in the ISSAEF column in this issue of the Journal. He will truly be missed by everyone.

Please continue to reach out and participate in ISSA initiatives, such as our Special Interest Groups. Take advantage of member savings and join in our discussion on Social Link and LinkedIn.

We love to hear from you!

Check out the ISSA Community Corner in this issue for the latest on events and programs.

I wish everyone a wonderful summer season. Getting out and about with friends and family again as we get our lives back to a sense of normal is truly a blessing.

Sincerely,

Candy Alexander, CISSP CISM
ISSA International President
Candy.Alexander@ISSA.org

Flexibility is an Important Component of Cyber Resilience... and this Journal!

Jack Freund – Editor, the ISSA Journal

Welcome to the July Issue of the ISSA Journal!

This month we had wanted to share with you works documenting the intersection of privacy and security. However, it appears that the authors this month wanted to write about other topics, so we decided to be flexible. Indeed, we often publish articles that are off topic, contemporary, and well-written. In many ways this is like us all in our security careers: remaining flexible.

So, this month we have another review of the effects of COVID-19 on the cyber security, this time in a two-part series. Tune in to the August edition of the Journal for part two. We also have writings by our amazing columnists and open-forum contributors covering topics from search warrants, quantum security keys, connecting security to the businesses they support, and applying AI to opt-in and opt-outs.

Next month we want to focus on disruptive technologies. Disruptive technologies not only change technology, but it also modifies business, markets, and networks. This type of technology is innovative and advances our society and even our lives. So, if you have a story to share we are looking for information on experiences with what is considered disruptive technology and how it has impacted security teams and how it could change the world.

ISSA JOURNAL

Now Indexed with EBSCO

Editor: Jack Freund, PhD
editor@issa.org

Advertising: vendor@issa.org

Guessing Keys

By Luther Martin – ISSA Member, Silicon Valley Chapter

One of the more frustrating questions that I get asked is about the ability of hackers to guess an encryption key. "But," says a CISO, "a hacker could guess the right key with a single guess, couldn't they? How can that be secure?"

It's hard to come up with a good answer to questions like that without simplifying things so much that they're no longer really true. And this situation isn't limited to just discussions of encryption.

Hot water freezes faster than cold water. This is the "Mpemba effect," named after the Tanzanian scientist who noted the phenomenon when he was still in middle school. It's hard to state this effect precisely. If you have two otherwise identical cups of water, one at 1 degree Celsius and the other at 99 degrees Celsius, the colder of the two will freeze first. Or if you have a cup of hot water and a thin film of cold water then the cold water will freeze first. It's surprisingly difficult to get a precise statement of the Mpemba effect that is actually true. So while it's not quite true that hot water freezes faster than cold water, the statement seems to be true often enough to be interesting, even if it's not quite accurate.

You get the same problem when talking about quantum computing. Unless a statement about quantum mechanics is full of lots of math that most people don't understand, then it's probably not very accurate. Any discussion of entanglement that doesn't talk about tensor products is probably not quite true. And any discussion of superposition that doesn't talk about complex probability amplitudes is probably not quite true. But because the average person who wants to understand how quantum computing might affect the future of their business's use of encryption doesn't care about those sorts of details, it's necessary to create a simpler version for them. But when you do that, what you're saying isn't quite true. The best that you can hope for is being true enough, whatever that means.

But at least we understand quantum computing. It's hard to imagine a more active area of scientific research, and that's because of the potential economic payoff from having big, general-purpose quantum computers. And you don't need thousands of qubits to do this. Even 100 qubits would let you solve very interesting optimization problems that are worth billions of dollars (random circuit sampling is not one of these). Encryption may not be quite as well understood.

A hacker might guess an encryption key on his first attempt, but we don't let that stop us from saying that encryption is secure. So when we say that encryption is secure, what does it really mean? That's not as hard to understand as quantum mechanics, but it's still fairly hard.

There are actually many different definitions for what it means for an encryption scheme to be secure, depending on what you think that an attacker might be able to do. If you are just concerned about an attacker decrypting your encrypted data, then a type of encryption that resists that attack is enough. But most forms of encryption provide a higher level of protection, and this is usually defined by one of the indistinguishability criteria: indistinguishability to a chosen-plaintext adversary (IND-CPA), indistinguishability to a chosen-ciphertext adversary (IND-CCA), etc. These formalize the intuitive ideas of being resistant to chosen-plaintext (dictionary) attacks, chosen-ciphertext attacks, etc.

But they also seem to have an extra level of complexity that other tricky areas don't. In quantum mechanics, once you learn that the funny bracket notation (those things like <A|B>) is just a different notation for what you learn in linear algebra class, the rest isn't too hard to follow. With the indistinguishability definitions, however, there's an abundance of confusing script letters, backward-pointing arrows, and other things that seem to be roughly as understandable as Babylonian cuneiform.

But the good news is that with the confusing definitions comes the ability to very carefully state things and to prove that they're true. By making mathematical definitions for the notions of security for encryption, we can actually make sure that various ways to use encryption are secure. If you use the CBC mode of AES, for example, then it's possible to prove that that particular mode is IND-CPA secure, which is the precise way of saying that it's secure against dictionary attacks. And that's not just someone's opinion. It's a rigorously proven fact. (Unfortunately, the classic proof is also very hard to follow.)

So even if a hacker could guess a key on their first attempt, it's still reasonable to say that AES-CBC is secure. It's IND-CPA secure, which means that it's secure against dictionary attacks, even if that's obscured a bit by the definitions and the math.

About the Author

Luther Martin has survived over 30 years in the information security industry, during which time he has probably been responsible for most of the failed attempts at humor in the ISSA Journal. You can reach him at lwmarti@gmail.com.

Opting-in or Opting-out: An Innovative Use for AI

By Curtis Campbell, ISSA Fellow, Chattanooga Chapter

Where does your company fall under privacy law in their op-in or opt-out requirements? As a consumer, do you know where to go to make your choice? AI makes it easier. This article looks at an innovative use of AI-as-a-Plug-In to make it easier for users to locate these requests buried within privacy notices.

In the U.S., the California Consumer Privacy Act of 2018 (CCPA) gives consumers more control over the personal information that businesses collect about them, and the CCPA regulations provide guidance on how to implement the law. This landmark law secures new privacy rights for California consumers, including:

- The right to know about the personal information a business collects about them and how it is used and shared;
- The right to delete personal information collected from them (with some exceptions);
- The right to opt-out of the sale of their personal information; and
- The right to non-discrimination for exercising their CCPA rights.

It mandates that businesses are required to give consumers certain notices explaining their privacy practices. In addition to businesses, the CCPA also applies to data brokers. [1]

When it comes to choosing, there are privacy rules with opt-in requirements and those with opt-out requirements. Company behavior for these requirements depend on whether that company falls under a privacy law for opt-in versus opt-out.

With GDPR, companies must adhere with opt-in and the onus is on website administrators and service providers. Under the CCPA in California, Controlling the Assault on Non-Solicited Pornography and Marketing Act of 2003 and the Gramm-Leach-Bliley Act, other companies may face opt-out requirements. But, opting out is not always as visible to users. While the choices are there, they may be buried or hard for users to find, and there is no real pressure to correct this.

Given the varied ways that opt-out options are presented, an amazing innovation has been created using artificial intelligence to focus on locating opt-in and opt-out links. A team of researchers from Carnegie Mellon's CyLab Security and Privacy Institute have trained AI to search and find opt-out links in thousands of privacy notices. [2] Should these op-out links be buried deep within privacy notices, the Opt-Out Easy browser plug in quickly finds it for you.

The interesting aspect is the use of AI, machine learning, and natural language processing to scan a site's privacy notice. For the past seven years, the research team has been training the AI to automatically read the text of privacy notices. The machine learning specifically looks for different types of opt-out choices and the consumer is spared from laborious browsing and searching.

Called the Opt-Easy browser plug in, its task is to scan around 7,000 most popular websites. More websites will be added over time. Estimated time once a new site is added is around a week from the time a new website request is sent to when the AI recognizes the site. [2}

The California Consumer Privacy Act (CCPA) explains how to submit the opt-out request: "Consumers should ensure you submit your opt-out request through the "Do Not Sell My Personal Information" link or through another method that the business designates for opt-out requests, which may be different from its normal customer service contact information." [1] It further states: "If you can't find a business's "Do Not Sell" link, review its privacy policy, which must include that link." Additionally, this statement adds: "Make sure you submit your opt-out request through the "Do Not Sell My Personal Information" link or through another method that the business designates for opt-out requests, which may be different from its normal customer service contact information. If you can't find a business's "Do Not Sell" link, review its privacy policy which must include that link." [1]

The problem becomes that these choices are hard to find, not as visible to users. It is assumed AI and machine learning will not produce 100% accuracy, but they may be able to get the number as close as possible." [2] For now, it is a way to simplify and speed up your search. There are plans in the works to lobby in public policy circles for the development of a standard method to convey opt-out links to the user. So, next time you're deciding whether you should stay or you should go, check out the Opt-Easy browser plug in. Let AI do the work for you!

About the Author

Dr. Curtis C Campbell, C|CISO, is VP of Atlantic Capital Bank in Atlanta, GA, serves as Director on the ISSA International Board, and is President of the ISSA Chattanooga Chapter. Curtis holds a Ph.D. in Organizational Leadership in Information Systems Technology, and serves on the advisory board of University of TN-Chattanooga, a national Center for Academic Excellence for Cyber-Defense (CAE-CD) studies. She was named ISSA Fellow in 2020. Connect with Curtis via curtis@mprotechnologies.com.

References

1. Retrieved from https://www.oag.ca.gov/privacy/ccpa
2. Chavietta, R. (1-29-2021) Researchers' browser extension uses AI to unearth opt-out links, Privacy Tech, https://iapp.org/news/a/researchers-browser-extension-uses-ai-to-unearth-opt-out-links/

~~Search~~ Patch Warrants

By Karen Martin – ISSA Member, Silicon Valley Chapter

The recent hack that affected Microsoft's Exchange Server led to an interesting legal maneuver by the US government: to deal with the results of the hack, the FBI obtained a search warrant that let them remotely modify affected software by implementing a patch to it. That doesn't sound like a search.

Judges do have the authority to issue warrants. Rule 41 of the Federal Rules of Criminal Procedure gives magistrate judges the authority to "use remote access to search electronic storage media and to seize or copy electronically stored information" if, in an investigation of a violation of the Computer Fraud and Abuse Act, "the media are protected computers that have been damaged without authorization and are located in five or more districts." Accessing a "protected computer" without authorization and causing damage and loss is a violation of the Computer Fraud and Abuse Act, and the definition of a protected computer is pretty broad, as it includes computers that are "used in or affecting interstate or foreign commerce" even if they are outside the United States.

So, the FBI probably had the authority to get the necessary warrants to seize or copy any information on the affected servers. But this raises obvious questions about the limits of this authority. It's not clear to me that FRCP 41 gives a judge the authority to modify any information on the affected servers, nor that it should.

With a search warrant, you need a certain level of specificity and probable cause. The warrant application says that the FBI identified certain Exchange Servers that were compromised and their justification of probable cause is based on the fact that "these victims are unlikely to remove the remaining web shells because the web shells are difficult to find due to their unique file names and paths or because these victims lack the technical ability to remove them on their own." The FBI noted that "by deleting the web shells, FBI personnel will prevent malicious cyber actors from using the web shells to access the servers and install additional malware on them." That is certainly a worthy goal, but is it a good justification for a search warrant?

Secondly, even if we knew the FBI had good intentions, how safe is their patch? When it comes to software, we know that testing is hard and getting harder by the day. I've heard more than a few stories about how even trivial changes ended up causing lots of unexpected downtime because of unexpected interactions. Even the smallest change to software can require tens of thousands of tests to make sure that the change doesn't cause a problem somewhere else.

Doing adequate testing is hard and expensive. And it's almost impossible to do perfectly. In commercial software development, the effort spent on testing software is roughly comparable to the time spent developing it. It wasn't always that way. Back in the dot-com era, software was much simpler, and so was testing. Back then, there were legendary (and possibly apocryphal) programs that were built from one million lines of code. Today, it's easy to find open-source projects about that big. The very first one that I checked, the Expat XML Parser has almost that many, and that just parses XML. Imagine the complexity required to do a full operating system.

But with the patch to this hack of Exchange Server, how much testing did the FBI do? Would their testing meet the "commercially reasonable" standards we require of software vendors?

My understanding of search warrants is that they are used to gather evidence that can be used to prosecute criminals, not to patch software, even if there's a very good reason for that patch to be installed. This analogy isn't perfect, but changing software with a search warrant seems a bit like using a warrant to search your car, and then swapping your 2015 Toyota into an unmarked 1987 Yugo. I'm not a lawyer, but that doesn't sound like a search or seizure. And if you bought that Toyota because you liked its reliability, you wouldn't want to be saddled with maintaining an '87 Yugo.

Even though the government's intentions seem to be good, in this particular case, it's not clear that what they did was a proper use of a search warrant. Requiring search warrants is an important protection of our privacy and we should be concerned when the government extends their ability to do searches and seizures in ways that seem to be an innovative interpretation of the law, and this seems to provide a good example of a case that we should indeed worry about.

About the Author

Karen Martin is a San Jose based information security engineer. She may be reached at kjlmartin@gmail.com.

Applied structured analytic techniques for cyber: How not to Break the Business

By Elizabeth Fulp

Practitioners and leaders in cybersecurity face decisions daily. The fidelity of cyber decisioning does not improve with repetition, it is a skill that must be developed intentionally. In this article, we will explore diagnostic and decision support analytic techniques to better enable you to conduct structured analysis and make calculated decisions for cyber-centric problems. By applying structured analytic techniques, your decisions will be defensible and pragmatic.

There are a multitude of structured analytic techniques, so how do we choose the right one? Let's define core techniques into two main types: diagnostic and decision support. By classifying analytic techniques, the decision-maker can quickly route decisions through the proper channel, avoiding delays and ensuring an appropriate decision is executed.

Diagnostic techniques help you define and scope a problem using the scientific process (formulating and testing hypotheses). Some diagnostic techniques include competing hypotheses, blackhat analysis, and premortem analysis.

- Competing hypotheses is a method of scientific reasoning where the practitioner generates multiple competing hypotheses and systematically eliminates them, keeping only the ones that cannot be refuted (Pherson & Heuer, 2020). The remaining hypotheses help to frame the uncertainty of the problem and help the decision maker to categorize and triage relevant information to identify analytic paths to reduce that uncertainty.
- Blackhat analysis is organic to cybersecurity- it is focused on thinking like the adversary and anticipating their behavior. This technique is great for perceiving and forecasting threats.
- Premortem analysis is the pause before deciding to ask "what could go wrong." This technique encourages you to challenge your conclusions and entertain the possibility that you could be wrong-to deconstruct the failure before it occurs to ensure you are considering all known failure points.

Each of the structured analytic methodologies offers unique values surrounding evidence identification and consideration. Competing hypotheses are compatible with technical decisioning, and when the decision is so important that you cannot afford to be wrong (Pherson & Heuer, 2020). This analytic method is particularly useful when you need an auditable trail to show relevant information considered. The Blackhat analytic technique enables a leader to leverage the adversary's perspective to identify root cause, predict future actions (next moves), and progress toward attribution. The Premortem analysis technique reduces the element of surprise by reverse engineering potential failures to account for causes of error.

Decision support techniques serve as mental whiteboards to examine the contextual variables of a decision. Some decision support techniques include Force Field analysis, Impact Matrix, and SWOT analysis.

- Force field analysis is essentially a weighted pros and cons list which informs the decision-making strategy concerning which situational variables will strengthen their position or which ones to focus on to mitigate opposing forces.
- Impact matrix aims to estimate the impact of a decision beyond the immediate participants, and how it will affect the future state of things.
- SWOT analysis technique examines the strengths and weaknesses affecting a team's ability to achieve a goal. Strengths and weaknesses are compared against identified opportunities and threats that would either facilitate or impede reaching that goal.

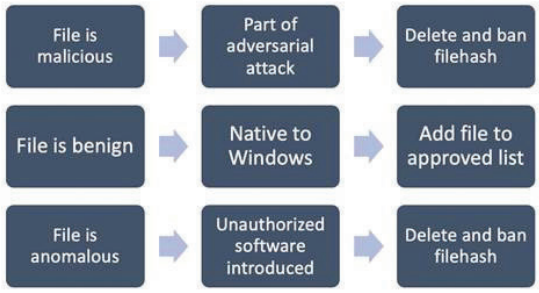
When utilizing these structured analytic techniques for solving cyber problems, recognize and consider the below to avoid pitfalls in your decision process.

- Competing hypotheses is subjective to human error (bias, assumptions). Unbalanced or incomplete data to refute hypotheses is likely to occur.
- Predicting an opponent's moves using Blackhat analysis is difficult. It requires understanding the adversary (with high accuracy) with limited insight of guarded information.
- Premortem analysis provides a variety of input from team members, this can snowball into a multitude of "what if" scenarios resulting in delayed decision making. Further, as new information is contributed, it may prompt recalculations of data or reexamination of evidence, adding time to the decision process.

Below are three cybersecurity operational questions which will require important decisioning. As a leader or analyst, you will be faced with similar problem sets. Here are examples of how to apply structured analytic techniques to help make informed and defensible decisions.

Cyber Decision 1: Should I ban this malicious file hash across the enterprise?

A malicious filehash is discovered via Endpoint Detect and Response (EDR). Corroborating cyber threat intelligence indicates the filehash has been involved in reported adversarial attacks as part of Tactics, Techniques, and Procedures (TTPs). Using the competing hypothesis technique, the analyst can discern if the filehash is a key component of this attack method or a native Windows process, and therefore should not be deleted from the environment.



Cyber Decision 2: Should we be threat hunting for malicious PowerShell?

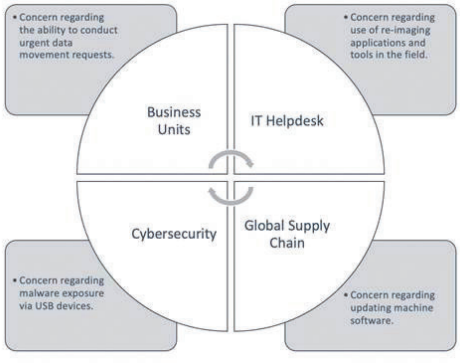
PowerShell can be used by threat actors for advancing against malicious objectives. PowerShell is used legitimately for business purposes by internal teams. Currently Powershell logging is not enabled. By using Impact Analysis matrix, you can visualize the stakeholders, levels of interest, and impact to make the best overall decision.

Stakeholder	Level of Interest	Impact
Cyber Team	High	Mostly Positive
Internal Partner Teams	Low	Mostly Negative
Executive Leadership	Low	Neutral

Cyber Decision 3: Should external media usage be blocked?

A policy amendment was recommended which would deny external media usage in the production environment. Premortem analysis can allow consideration of multiple stakeholder perspectives and respective concerns to inform the decision.

- What could go differently than expected?
- What unintended consequences could occur?
- Will this be an issue in the future?



About the Author

Elizabeth Fulp received her associate's degree in Network Security/Data Assurance at Guilford Technical Community College. She is currently working as a Security Analyst II at a Fortune 500 company and holds the following certifications: AWS Cloud Practitioner, CompTIA Security+, and CompTIA CYSA.

Resources:

1. Pherson, R. H., Heuer, R.J. (2020). Structured Analytic Techniques for Intelligence Analysis. CA: SAGE Publications.

The 'Sort of' Book Report: Reading ISSA International's Chapter Manual

By Jay Carson, Security+, CIPP/E, Semper Sec LLC, ISSA-COS Member-at-Large

When I started volunteering for our chapter, despite the efforts of two great mentors and multiple supportive colleagues, I felt overwhelmed. I am primarily a learn-by-reading person. I felt I must be missing some information about the inner workings of ISSA chapters generically. Since ISSA has been around over 30 years, they must have the 'things I wanted to know' written down. What about a manual explaining things? Why should I feel I was in new territory, as certainly things with which I was dealing had been experienced before?

Answers: I did not have to be concerned! Things are indeed written down! There is a 136-page manual of recommendations on how to do things, and it is easily available to ISSA members!

To access the manual, just go to the ISSA International website, log in, and go to the 'Chapters' pull down tab. Click on 'Chapter Resources,' and you will see it.

Please do not feel bad if you may not have yet heard about the manual! I attended a recent ISSA International Chapter Leader's Meeting where I learned others have not heard about it. Even the current Chapter of the Year nomination application has an (if applicable) block to check for the chapter manual marked "Did not know it exists." Despite being three years since the last edition (I know, cybersecurity pros consider anything from even last month out-of-date!), the manual is full of reasonable expectations, and useful techniques to achieve those expectations.

While I personally think every board member and all of the key personnel would find it worth their time to read the basic 136-page manual cover-to-cover, it is designed as a reference tool. If your time does not allow that level of study, skimming the manual for situational awareness is also valuable. There are terrific sections on the duties of the chapter treasurer (be appreciative of your chapter treasurer, they have a complicated and very detailed job!), tax status, chapter insurance details, other legal considerations, finding presentation speakers, etc., etc. Also, while I confess I have not yet read them all, there are supplemental documents full of detail and templates on:

- Chapter Organization & Governance Membership
- Leadership & Engagement Meetings
- Sponsorship & Vendor Relations Communications & Marketing Awards & Recognition
- Financial Management Conferences & Events
- Exhibiting at Conferences or Trade Shows Partnering with other Organizations Special Interest Groups
- ISSA Education Foundation

An administrative manual is not a page-turning spy story. But if you want to know 'why we do what we do,' this document will help you!

I saved the best for last! ISSA International is sponsoring work in 2021 on a revision to the manual, as well as a chapter playbook! There are plenty of volunteering opportunities for you clear-headed writers!

ISSA Journal 2021 Calendar

JANUARY
Best of 2020

FEBRUARY
Regulation, Public Policy, and the Law

MARCH
Preparing the Next Generation Security Professional

APRIL
Cyber Warfare: Nation State Actors and Corporate Espionage

MAY
Encryption, Blockchain, and Hardware Security

JUNE
Cybersecurity Impacts of COVID-19

JULY
Security Implications of an Interconnected World

AUGUST
Disruptive Technologies
Editorial Deadline 7/1/2021

SEPTEMBER
Shifting Security Paradigms in the Cloud
Editorial Deadline 8/1/2021

OCTOBER
The Business Side of Security and Risk Management
Editorial Deadline 9/1/2021

ISSA Community Corner

ISSA Board Elections Now Open through July 18! Let Your Voice Be Heard!

- You should have received your voting information and instructions from noreply@directvote.net by June 28. Please check your spam/junk mail if you have not received it and were a member in good standing by June 14, 2021
- For more information on the current candidates Meet the Candidates Webinar Replay is available at https://www.members.issa.org/page/2021ISSAElection

Chapter Leader Meetings Schedule

- July 30, 2021 - 1:00 PM Eastern Time. Register here.

Find out more at https://www.members.issa.org/page/ChapterLeadersSummit

Upcoming Events and Conferences

Cyber Executive Forum – Virtual Summit

August 19, 2021 is the next Cyber Executive Virtual Summit. Registration now open

We welcome guests (ISSA general members and non-members interested in the Cyber Executive Forum and Cyber Executive Membership) to put in an application to join these sessions.

All ISSA Cyber Executive Members are invited to attend and invite guests.

Find out more at https://www.issa.org/event/august-19-virtual-cyber-executive-forum-2021/

ISSA Members receive discounts to a variety of industry events and conferences such as:

- WSJ Pro Cybersecurity Executive Form June 2, 2020 - Complimentary passes for ISSA members
- Blackhat
- InfoSec World
- SECtor

To learn more visit: https://www.members.issa.org/general/custom.asp?page=SpecialOffers

Visit our new community events page to find local and virtual events.

https://www.members.issa.org/events/event_list.asp

There's always a webinar worth viewing either live or On Demand.

Visit and bookmark our events page to see our latest offerings. https://www.issa.org/events/

Visit our past webinars and view them on demand. https://www.issa.org/past-web-conferences/

Join a Special Interest Groups Available Only to ISSA Members

ISSA Cyber Resilience SIG Join here:

https://www.members.issa.org/members/member_engagement/groups.aspx?code=Cyber+Resilience

ISSA Privacy SIG Join here: https://www.members.issa.org/members/member_engagement/groups.aspx?id=229802

ISSA Women in Security Sig Join here: https://www.members.issa.org/page/WomenInSecurity

Looking for Journal Authors and Contributors

Want to get your thoughts and opinions published? We are looking for you!

For more information on how to contribute and what we are looking for visit:

https://www.members.issa.org/page/journal-contribute

ISSA Education Foundation

News from the Foundation

Passing Of a Great Benefactor and Friend

The ISSA Foundation lost one of its big supporters and a great, treasured friend, Philippe Courtot. Starting in 2013, the Chairman and CEO of Qualys continued an annual donation to ISSAEF to fulfill his passion for cybersecurity education, which funded the ISSAEF Howard Schmidt Memorial scholarship. The Foundation Board and scholarship awardees are forever grateful for his generosity. In 2020, he was named an ISSAEF Benefactor, the Foundation's highest award. Pictured is Mr. Courtot, with Foundation Vice President, Debbie Peinert, receiving his award.

In recognition of Phillipe's enormous generosity, the Foundation will offer a special, one-time scholarship in his memory for 2022. Donations in his memory can be made at The Foundation website www.issaef.org/donate. Further details of this scholarship will be announced in a future communication.

HEARING FROM OUR SCHOLARSHIP RECIPIENTS

One of Foundation's 2020 scholarship recipients, Abhishek Soni, recently sat down with ISSAEF Board members Lorraine Frost and Edmond Momartin to share insight from his study towards a Master's degree in Information Security and how ISSA and the Foundation's scholarship helped support his academic goals. Look for the full interview in a future article.

Continued on page 21

2021 ISSA International Election

Meet the Candidates for 2021

Nominations for this year's International Board elections are now closed and we have confirmed our candidates.

To learn more about this year's candidates, check out their biographies and goals for the position in the following pages. You can also view the profiles and the Meet the Candidates Webinar at our election page found at https://www.members.issa.org/page/2021ISSAElection.

Candidates and Positions

COO/Secretary

Dr. Shawn Murray *

Director

Alex Grohmann

Debbie Christofferson

Lee Neely

Robert Martin

* Please Note: As there was only one nomination made for COO, there will be no official vote required.

Official Voting Window is Now Open

Our election is run by an experienced third-party, Survey and Ballot Systems.

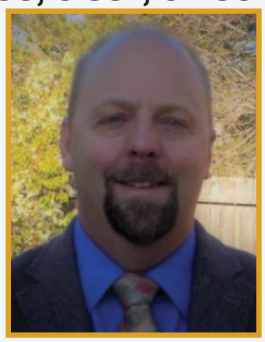
If you were an active member in good standing by June 13, 2021 your election specific broadcast should have arrived safely in your inbox on June 27, 2021 from: noreply@directvote.net. If you do not receive your election email by June 28, 2021, please contact support@directvote.net If you have not received your election email please contact support@directvote.net.

Questions?

For any questions, please contact the Election Committee Chair at electionschair@issa.org.

COO/Secretary

Dr. Shawn P. Murray, CICISO, CISSP, CRISC



Shawn Murray currently serves as COO/Secretary for ISSA International. He is a Principal Scientist with the United States Missile Defense Agency and is an officer in the US Civil Air Patrol. Previous assignments include work with Army Cyber Command in Europe, US Air Force, and with commercial industry in various roles in information assurance and cybersecurity. He has traveled the globe performing physical and cybersecurity assessments on critical national defense and coalition systems. Dr. Murray has worked with NSA, FBI, CIA, and the US Defense and State Departments on various cyber initiatives and has over 20 years of IT, communications, and cybersecurity experience. He enjoys teaching and presenting as guest lecturer on cybersecurity, business, and computer science courses for several universities. He has several industry recognized certifications to include C|CISO, CISSP, and CRISC. He holds several degrees including a Doctorate in Computer Science. He is an ISSA Executive Member, chapter advisor and ISSA Fellow. He is also a professional member of IEEE, ACM, (ISC)2, and an FBI InfraGard partner. He enjoys traveling with his family, researching and collaborating with other professionals in cybersecurity, and is a principal backer of a youth sports non-profit organization as well.

Statement of Goals

As a practitioner and educator, I'm passionate about the current and future state of cybersecurity and collaborate with people leading the charge in this profession. I bring experience in applying information security concepts and educating future cybersecurity professionals expected to fill widening gaps in our career field. My contributions to members include travelling to help establish new chapters, collaborating with other chapters to help solve problems, and representing our association as a keynote presenter at the European CISO summit in The Hague. I've met and spoken to members of Congress and advocated for information and cybersecurity to other US Government leaders. I've worked with board members through significant association realignment initiatives that has made our association stronger and directly benefits the membership as a whole. If re-elected, I will continue to serve and represent the best interest of our members internationally and work with other board members to steer ISSA into the future. Additional goals next term include: Working to find solutions to address gaps in skill sets to address shortages while educating new professionals and identifying resources for ISSA programs and work with chapter leaders and members to bring more value. I will continue to be the voice of our members!

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

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

Director Candidate

Debbie Christofferson

More than 25 years in the industry, as a senior security manager and leader globally, currently an IT security consultant and business owner. Certifications: CISSP, CISM, CCSK. Previous employers include Intel Corporation, State of Arizona, Cloud Security Alliance, and other large organizations across sectors.

Ten years board experience on ISSA Phoenix Chapter, including four as President, when our chapter won its first Chapter of the Year. Current Co-Chair of ISSA's Women in Security SIG, an ISSA Distinguished Fellow, and past recipient of the Honor Roll Award for significant ISSA service.

For ISSA International, led the RFP process for outsourcing ISSA's management capability, led the Advisory Council for ISSA's CISO Executive Forum, led the first 5 years of ISSA's Chapter Leader Forum, led the hiring committee for ISSA's current Executive Director, and led the committee for ISSA's 25th Anniversary during Howard Schmidt's 2nd term as President.

Founder of the Cloud Security Alliance Southwest Chapter, and currently serving the ISC2 Phoenix Chapter Board. Author of a Women in Security book that showcases 14 women in different cybersecurity career paths. Fully engaged in the industry and giving back, including speaking, and writing about our field.

Statement of Goals

Help drive activities that enhance member value. Support the Association's strategic goals for partnerships, relationships, membership, revenue, global relevance and visibility, and member outreach and touch. Engage actively in high ROI activities where my skills and passion will make a difference for ISSA and its members.

Identify high value opportunities within the Board and ISSA's SWOT (Strengths, Weaknesses, Opportunities, Threats) for post-pandemic re-emergence and growth--with fresh eyes and ears--on new ways of conducting business for new results. Pare down best options to start, stop and for leveraging my own skills and passion for ISSA, in concert with current ISSA leaders.

Actively engage with members and chapters to identify and meet their needs. Participate in relevant communities supporting and engaging our current and future members. Identify and prospect where ISSA can expand our member engagement and footprint. Seek speaking and writing options to showcase our field and ISSA, including a speaker directory.

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

Director Candidate

Alex Grohmann

Alex Grohmann has served on the ISSA International board for two terms and would like to serve a third.

As a security and privacy professional for over 25 years, he has helped to promote the profession through professional and personal contributions. He volunteers a great deal of his time to make the profession stronger through his efforts in ISSA.

During Alex's time on the international board, he has helped foster relationships with the IAPP, acted as the POC for ISSA's Privacy special interest group, created a legal and regulatory forum, contributed to the Awards committee, and has acted as the direct representative for the Mid-Atlantic chapters.

As a 20-year member of the Northern Virginia chapter, Mr. Grohmann has volunteered on its board for 9 years, with 3 of those as chapter president. During that time, the chapter won the Chapter of Year, and he collected the Honor Roll and Fellow designations.

Outside of ISSA, Alex has served on several boards and/groups including Washington DC InfraGard, NIST's NICE and the IT-Sector Coordinating Council.

Alex is a proud Seminole and graduate of Florida State University in MIS. He still considers Florida his home.

His desire is to continue to help the profession through contributions via the International Board of Directors.

Statement of Goals

If elected to a third term, I plan to continue the initiatives I started as a member of the current board. The board has the vision and roadmap in place to make the association stronger. As a newer member, I bring fresh ideas.

Individually, I plan on strengthening ISSA relationships with entities including the IAPP (Privacy), NIST, CISA and CyberWatch. My contributions to ISSA online web conferences will remain active.

I will also be working to reinforce our educational initiatives to help ensure our next generation of cyber professionals are well equipped for the challenges to come. My contributions to the National Initiative for Cybersecurity Education (NICE) has a special place in my heart.

My work with local chapters will continue and prosper by providing them a voice to the board as well informing them about new initiatives. This is also true of my work with organizations supporting minorities, especially the Hispanic community. I will resume my work to improve chapter resources such as management of chapter meeting registration, updating of board policies, and chapter websites. Lastly, I plan on visiting individual chapters again, as soon are we are officially clear of COVID.

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

Director Candidate
Robert Martin

Robert Martin is a Certified Information Systems Security Professional with over fourteen years of experience in information security. He holds a Master of Science in Network Technology with a concentration in Information Security. He also holds a Cyber Security Masters Certification. He works as a Sr. Security Engineer at Cisco System Inc. in RTP, NC. Robert specializes in such areas as risk management, regulatory compliance, security solutions architecture, security audits, vulnerability assessments, and penetration testing. He serves as a Director of the Information Systems Security Association International Board.

Statement of Goals

His goals are to work with all the ISSA Chapters to provide training opportunities for the members and guests to drive membership and development of new skill-sets in an ever-changing IT Security landscape.

Director Candidate
Lee Neely

Lee Neely is a senior IT and security professional at LLNL with over 30 years of extensive experience with a wide variety of technology and applications from point implementations to enterprise solutions. He currently leads LLNL's Entrust team and is the CSP lead for new technology adoption specializing in mobility. He teaches cyber security courses, and holds several security certifications including GMOB, GPEN, GWAPT, GAWN, GPYC, GEVA, CISSP, CISA, CISM and CRISC. Lee is a past ISSA International Board member, Treasurer and co-founder of the Boise Cloud Security Alliance chapter, current director for Uncle Credit Union and holds the CCUB and CCUSC certifications. He is a past President for the ISC2 Eastbay Chapter, Member of the SANS NewsBites Editorial Board, GIAC Advisory Board member, GIAC Ethics Committee Member, SANS Analyst and co-host of Paul's Security Weekly podcast. He is also a member of and co-leader for the ISSA Webinar and Content committees.

Statement of Goals

My goals taking a leadership role and give back to the ISSA:

1. Help the board operate effectively, enabling forward progress of strategic initiatives.
2. Ensure that the board is driving value back to chapters to achieve operational excellence.
3. Continue to bring current industry leaders to ISSA leadership forums and webinars to benefit our members.
4. Find initiatives to make ISSA first choice of professional organizations for information security professionals, including relevancy and supporting resources.

Your Vote Will Make a Difference

Did you know that on average, among professional associations from five to seven percent of the membership actually make the effort to vote? That's right! Less than 10 percent of the membership is deciding who will lead your association into the future. Voting only takes a few minutes. Make your voice heard this year— and make a difference. The ISSA elections is open now and runs until July 18th 2021. So take a few minutes and make your voice heard!

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

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

Protecting Users Against Modern, Invisible Cyber Threats

Babur Nawaz Khan
Product Marketing Manager
A10 Networks

A security strategy is only as strong as its weakest point. No matter how extensive your network defenses are, if there is even one blind spot, you are still vulnerable to attacks. This is true even for the Zero Trust model, at the core of modern cybersecurity. Fortunately, there is a way to fix it.

Zero Trust Model: The Perfect Security Strategy…with a Catch

Zero Trust security / Zero Trust model has become a critical element of network defense. Its rise has been driven by the way traditional concepts of secured zones, perimeters, network segments—even "inside" and "outside"—have been rendered outdated by the modern cyberthreat landscape. After all, you can't count on walls to keep you safe from insider attacks by people with legitimate access, prevent multi-level attacks designed to bring networks down, or stop lateral movement during the course of an attack.

The Zero Trust model responds to these challenges by adopting the approach of "trust nobody"—inside or outside the network. Cybersecurity strategies are redesigned accordingly along four key principles:

- Create network micro-segments and micro-perimeters to restrict east-west traffic flow and limit excessive user privileges and access as much as possible.
- Strengthen incident detection and response using comprehensive analytics and automation.
- Integrate solutions across multi-vendor networks with ease, so they can work together seamlessly, enabling compliance and unified security. The solutions should also be easy to use so that additional complexity can be removed.
- Provide comprehensive and centralized visibility into users, devices, data, the network, and workflows.

This sounds good in principle. Even the name "Zero Trust Security" is reassuring, with absolute terms that suggest absolute protection. But there is a catch: The Zero Trust model works only when you have full visibility into people and their activities. If something is invisible, there is no way for you to ensure that it does not pose a risk. And that is true for the vast majority of network traffic thanks to the widespread use of encryption.

Zero Trust Model / Zero Trust Security Blind Spot

Encryption is now ubiquitous across the internet. Google reports that over 90 percent of the traffic passing through its services is encrypted, and the numbers are similar for other vendors as well. This trend has been great for privacy—but it is devastating for security, whether you are implementing a Zero Trust model or something different. As encryption renders network traffic invisible to legacy solutions, your network's security stack is effectively useless.

In response, many security vendors incorporate TLS (Transport Layer Security) inspection into their solutions. In effect, they decrypt traffic, inspect it, and then re-encrypt it before passing it on. But this "distributed TLS inspection" approach, in which decryption and re-encryption happens separately for each device in the security stack, brings problems of its own. Network bottlenecks and performance problems typically compromise service quality for business users and customers—an unacceptable penalty in today's competitive business environment. What is more, the need to deploy private keys in multiple locations across the multi-vendor, multi-device security infrastructure expands the attack surface, increasing risk.

For the Zero Trust model to deliver on its promise, companies need a way to eliminate the Zero Trust model blind spot without sacrificing service quality.

Full Encrypted Traffic Visibility via TLS inspection

A10 Networks closes this Zero Trust blind spot. To avoid the downsides of distributed encryption, we provide full visibility to the enterprise security infrastructure through a dedicated, centralized SSL decryption solution. This is complemented by a multi-layered security approach for optimal protection.

For more information about SSL/TLS visibility, visit: www.a10networks.com

A10 | Always Secure. Always Available.

COVID-19's Impact on Organizational Cybersecurity Posture

By Douglas Shuman https://www.linkedin.com/in/douglas-shuman-06221b122/

Part one of this two-part article looks at some of the rapid changes that happened in the work place due to COVID-19 and their implications to cybersecurity.

Abstract

Organizational cybersecurity landscapes changed as a result of employees working from home during the COVID-19 pandemic. Abruptly sending employees to work from home resulted in many quickly implemented changes. This research is a review of the cybersecurity landscape of the transformed workforce. This includes the scope of pandemic telework, how threats changed, and the cyber-attacks observed. Organizations need to continually evaluate how they secure their environment to allow for remote work and ensure best practices are in place.

Introduction

When the significance of COVID-19 ("the coronavirus") became clear in early 2020, many organizations' cybersecurity landscapes changed as a result of sending employees home to work remotely. Government mandates were largely the source of sending employees home, with the purpose to stop the spread of a deadly virus which we knew little about. This introduced two new threats; "a high-profile event and a rapid change in computing habits." [1] While working from home is not a new concept, starting in March and April of 2020, most U.S. organizations (e.g., businesses, government agencies) needed to continue operations with most or all employees now working from home. In the United States especially, organizations had little time to prepare for a crisis response that suddenly sent employees to work remotely.

To those who were uninvolved in making changes, the situation may seem like Information Technology (IT) departments simply made a few networking changes to implement remote work solutions or expand capacity. However, this assumption ignores the variety of decisions with serious cybersecurity implications that organizations faced because of increased remote work. This is apparent from a survey by the Information Systems Security Association (ISSA), which was sent to people working in cybersecurity and IT positions. Twenty-seven percent of respondents willingly indicated their organizations were underprepared to secure the devices and applications employees would use at home. [2]

At the time of writing, organizations have mostly moved on from the changes required to enable high-volume remote work to supporting remote work over the long term. Regardless, decisions with cyber-implications made during the beginning of 2020 are likely still putting organizations at risk. This begs the question: in light of COVID-19, how have organizations' cybersecurity postures changed due to the influx of people working from home? There are many issues worth investigating because of the pandemic, but the focus of this research is on the impact of COVID-19 on organizations' cybersecurity postures and how they have changed.

Literature Review

Significance and Scope of COVID-19 Work from Home

Not every company could allow employees to work from home when COVID-19 began affecting everyone. The U.S. Bureau of Labor Statistics finds that working from home is generally feasible in "management, professional, and administrative support jobs, but not in most service, construction, transportation, and production jobs." [3] This study found that before the pandemic, about 45% of the U.S. employment population were in positions where telework (i.e. working from home) was feasible. [3] Of that surveyed population, the work from home "takeup rate" (spending a significant amount of time doing remote work) was about 22% or 25% depending on the survey. [3] To summarize, less than half the workforce had the capability to work from home, and about a quarter of those people took advantage of work from home.

Once the pandemic required organizations to enable work-from-home, employment drastically changed. Stanford research found that regardless of current occupation or employment status, in June 2020, 43% of the U.S. labor force was working from home. [4] A Gallup poll found that remote work leveled off around mid-April with a total of 63% of employed adults having worked from home at some point. [5] PricewaterhouseCoopers (PwC) performed a survey of office workers from May to early June and found every employee was working from home. [6] Of those PwC surveyed, 70% of workers were required to work from home due to shelter-in-place mandates (and they did not work from home before), while the other 30% were able to easily switch to full work from home given existing flexible arrangements with employers. [6]

The above statistics show that the organizations which allowed working from home before COVID-19 were accustomed to only a small amount of their workforce utilizing remote work. As a result, most organizations were unprepared for the massive amount of remote work that suddenly needed to be enabled. This encouraged hasty decisions with cybersecurity implications.

Need for Agility

IT departments need to respond quickly and flexibly given customer and business requirements. A pandemic is an extreme example of changing requirements warranting flexibility and timely responses. This is the purpose of the agile development process. Working from home during the pandemic has further reinforced the need for agility, especially regarding cybersecurity. [7] Even in 2021 Gartner is saying, "the pandemic has highlighted the challenges resulting from rigorous, inflexible security programs," which shows the need for agile cybersecurity programs. [8]

Non-security IT teams often do not consider cybersecurity until after deployment, which is sometimes called "bolting on" security. This is the opposite of "baked in" security, which considers cybersecurity implications throughout changes and development, ideally in an agile manner. Lovejoy et al. found that just 36% of organizations say cybersecurity is built into their planning. [9] There are some significant concerns with considering security after planning, especially after deployments. Considering security after deployments can make implementation more difficult, and organizations are open to attack during the period where systems are vulnerable. We can expect cybersecurity was ignored regarding many changes due to COVID-19, because it is often initially overlooked in general.

Enabling Pandemic Telework

Organizations had to achieve many things to enable pandemic telework. At its simplest, working from home consists of an employee with an internet connection, a computer, and means to connect to their organization's resources (e.g. by virtual private network), without physically being in a traditional workplace. The focus here will be the concerns of new working locations, types of devices connecting to the organization network, and types of remote access.

New Location Concerns

Working outside of the regular workplace (e.g. office) introduces different threats. Many organizations that suddenly needed to enable telework did not have time to address newly introduced threats. A concerning pandemic statistic shows that 45% of employees had no training on how to ensure work device security. [10] Additionally, 53% of employees say their company has not provided new guidelines for managing sensitive personally identifiable information (PII). [10] This is especially important because some legislation, such as the General Data Protection Regulation (GDPR), requires strict management of data storage locations.

Due to using a personal network when working from home, if malware infects a home network it could spread and end up infecting the organization's network as well. [11] The number of home networks now connecting greatly expands this threat. Ensuring there are anti-malware controls installed on devices helps mitigate this threat. Current literature does not provide examples of organizations limiting employees from working at locations other than their home office. Working from locations other than the home office could expose more malicious networks to work devices. Additionally, the frequency of which employees connect to other people's networks for work is also unknown. By allowing employees to work anywhere other than their home, organizations expose themselves to the risks of additional untrusted networks. Organizations should evaluate if the risk is great enough to implement a policy restricting where remote work is allowed.

Another threat of note is regarding privacy concerns. With the popularity of smart-home devices (e.g. Alexa, Google Home) many people have a device constantly listening to them, including when they are discussing sensitive work information. Some organizations may not be comfortable knowing various third parties could be collecting data on their employees' work conversations. One U.K. law firm required during the pandemic that employees disable their smart home devices and remove them from the work room so sensitive conversations cannot be listened to. [12] Current literature is not clear on how widespread this requirement may be. Additionally, one would think the concern of smart devices listening would apply to cellphones as well, but current literature does not provide examples of organizations limiting this as a result work from home changes. Organizations should evaluate the risk of third parties listening through devices like smart speakers and cellphones to determine if these devices should be limited in work environments.

Types of Devices Connecting to the Network

Due to COVID-19, the personal computer (PC) market suffered a 12.3% decline in shipments in the first quarter (Q1) of 2020 compared to Q1 2019. [13] This was the largest decline in this market since 2013. [13] The pandemic caused supply chain disruptions, especially in China, so companies were unable to produce as many computers as normal. [13] There was also a surge in demand for computers because more people were working from home. Since many people suddenly needed to

work from home and there were supply chain problems, organizations were sometimes unable to provide standard corporate owned and managed devices where needed. This resulted in many employees needing to use personal devices for work. This is concerning because corporate owned devices are often much easier to secure than personal devices. [14]

Personal devices used for work are concerning for several reasons. To name a few examples, personal devices may not have standard security software such as endpoint protection programs, they might allow devices plugged in to run malicious executables, and organizations may not have as much visibility into device activity, such as if an employee began saving sensitive data on their personal device. Problems like these can be remediated through making a personal device "managed" by the employer, such as through installing device management software. Time and resources are required to enable an effective managed personal device program.

The previously referenced IBM Security and Morning Consult study found several interesting statistics on personal device use during the pandemic. Discoveries included that 53% of remote employees used personal laptops and computers for work. [10] Sixty-one percent of employees said their employers did not provide tools to secure those personal devices, such as endpoint protection software. [10] Fifty-three percent of those surveyed say their personal devices used for work were not administered at all by their employer. [10] Some good news is that those working with PII were more likely to have their personal devices administered by an employer, likely due to the importance of securing sensitive information. [10] From the above we see that many employees did not use a managed corporate device for work during the pandemic, but something not addressed in the existing literature is if organizations were able to provide corporate devices to employees who did not have them before COVID-19.

Types of Remote Access

There are various means available to connect to organization resources remotely for work. Historically, the most common option was to use a virtual private network (VPN), which has been relied upon for over the past 20 years. [15] Due to their architectural design, VPNs can be slow for end users, especially when organizations previously only had a small subset of their employees using them. [15] For VPNs, "the only way to effectively increase capacity was to add equipment", which is costly and not easy to do quickly. [16] VPNs are becoming a legacy remote access technology.

The main alternatives to VPNs are zero trust network access (ZTNA) solutions and virtual desktop infrastructure (VDI), although other solutions exist as well. VDIs run hosted virtualized desktop environments which can be internet accessible. This allows access to an organization's internal resources through the remote desktop environment. VDIs may not be as efficient as VPN since they add an additional barrier between the employee and organization resources. VDIs are more useful as dedicated environments with pre-installed resources or greater computing power than just as a remote access tool.

The zero-trust model enforces that access is denied until a user sufficiently proves their identity, hence "zero trust." With ZTNA, information such as application, location, device, network, or other elements can work together to verify a user's identity, which can provide for greater security. [16] Zero-trust networks allow users to make a secure connection to a specific resource, including cloud based and on-premise. ZTNAs are a "more flexible alternative to VPNs" which still protect traffic from attackers while offering scalability for the network. [17] Prior to the coronavirus, estimates showed that by 2023, 60% of enterprises will phase out their VPNs in favor of ZTNA. [17]

It is worth noting that remote access solutions are not required to access organization resources from the internet, such as software as a service (SaaS) solutions like Office 365 or Salesforce. This access can be secured through means like a cloud access security broker (CASB). CASBs give organizations greater visibility and control over resources that are in other cloud environments, which is a gap for VPNs. [16] While CASBs provide secure access to cloud-based resources, they do not provide remote access and cannot access on-premise datacenters.

Organizations that require solutions to access their internal networks should look at solutions like ZTNA, VPN, and VDI. Organizations need to evaluate what is best for them, because each of these solutions have different benefits, setup difficulty, and ongoing management needs. Most organizations must consider these options, because in 2019, survey results found 98% of businesses ran server hardware in an on-premise environment. [18]

Existing literature is unclear on how usage of remote access tooling options changed as a result of the pandemic. Because remote access tools were new to people beginning work-from-home, did organizations chose to relax security controls to be more accessible to all employees? For example, did organizations decrease frequency for initial authentication or multi-factor authentication (MFA)? Were controls weakened to ease impact on technology like VPNs, by organizations externalizing internal resources? Or could controls have strengthened by choosing to migrate to better, modern solutions? Another major gap includes employee personal reflections of how their employers dealt with cybersecurity as a result of COVID-19. For example, did rushed out telecommunication tools like Zoom make employees feel concerned about the organization's cybersecurity? Please look forward to part 2 of this series, where I present survey results which address some of the gaps identified in this research,

Threat Actor Tactics

Cyber threat actors took advantage of the chaos brought on by COVID-19 in attempts to exploit organizations. Microsoft claims there was not a surge in the overall quantity of cyber-attacks, but rather, the tactics used by threat actors changed given the introduction of COVID-19. [18] While the number of attacks has not significantly changed, Microsoft found that there were more successful attacks, especially in countries which had serious virus outbreaks. [18] Cybersecurity company Zscaler found a rise in COVID-19 related attacks from just

1,200 in January 2020 to 380,000 in March 2020. [20] Attacks were generally more successful due to fear and desire for new information. [18] Attackers achieving greater success further shows that organizations were unprepared for the pandemic and the ensuing changes. We will now explore some documented examples of COVID-19 enabled or themed attacks, primarily focusing on a study by Lallie et al., which documented information about public coronavirus related attacks. [21]

Cyber-enabled Crime

Of the cyber-attacks and campaigns in the Lallie et al. study, 86% of them included phishing. [21] Phishing is an extremely common tactic which preys upon human emotions to illicit responses, such as installing malware or sharing sensitive information. These scams targeted victims with lures like selling goods in high demand (e.g. masks, testing kits) and impersonating organizations such as the World Health Organization. [21] Some scams even used CAPTCHA to appear more legitimate and avoid detection from security crawlers. [20] Some recent phishing scams targeted government COVID-19 stimulus checks and vaccine distribution.

There were six pharming attacks documented in the Lallie et al. timeline. [21] Pharming is when a fake website is set up to appear legitimate. When unsuspecting users enter information, such as credentials, the information is sent to attackers. One large pharming campaign used a fake Office 365 login for access to a fake COVID-19 financial compensation website. [18]

Cyber-dependent Crime

The Cyber & Infrastructure Security Agency (CISA) says that threat actors are "taking advantage of this mass move to telework" by exploiting vulnerabilities in popular software used for working from home. [22] For example, remote access tools and telecommunication tools were exploited. [22] There was an increase in attacking insecure remote desktop protocol (RDP) endpoints as well. [22] The Lallie et al. study also found two COVID-19 hacking targets where attackers attempted to steal research on the virus. [21]

The Lallie et al. COVID-19 cyber-attack timeline found 65% of attacks involved malware. [21] Some common malware types included the "Agent Tesla" keylogger and Trojans like "GraceWire" and "TrickBot." [22] These Trojans install other malicious files, like Remote Access Trojans (RATs), desktop sharing clients, and ransomware. [22] Cybercriminals also developed fake VPN software that would install malware when downloaded. [20] Another malware example was a fake Android app for coronavirus tracking that, when installed, would download ransomware and demand payment to unlock the device. [20]

The Lallie et al. COVID-19 cyber-attack timeline found two distributed denial of service (DDoS) attacks, which targeted the U.S. Health Agency and a Chinese epidemic prevention unit. [21] Compared to the second quarter in 2019, security firm Kaspersky found a 217% increase in DDoS attack attempts during the second quarter of 2020, which they believe to be related to the coronavirus. [23] They found that the U.S. and China were victims of the most DDoS attacks, but most DDoS attacks were also launched from these regions. [23]

Conclusion

Because of the sudden shift to get employees to work from home, changes were made which posed cybersecurity risks. Organizations need to ensure their IT departments consider cybersecurity throughout an agile development processes, and cybersecurity programs ought to become more agile to meet business needs while ensuring appropriate security. Attackers will continue to take advantage of our mistakes and deliberation, so we need to remain diligent. We must continually evaluate and implement best practices for remote work cybersecurity, especially due to the changes made because of the COVID-19 pandemic.

About the Author

Author Douglas Shuman has about five years of experience working in cybersecurity, primarily as a cyber risk analyst. He recently completed his master's degree in Cybersecurity Analytics and Operations from Penn State University and is certified in Open Factor Analysis of Information Risk (FAIR). His focuses are on cyber risk assessments and cybersecurity consultation. He can be reached at his LinkedIn page.

References

1. Jaikaran, C. (2020, April 10). Federal telework during the covid-19 pandemic: Cybersecurity issues in brief. Congressional Research Service. https://crsreports.congress.gov/product/pdf/R/R46310/2
2. Oltsik, J. (2020, July). The Impact of the COVID-19 Pandemic on Cybersecurity. ISSA. https://www.issa.org/the-impact-of-the-covid-19-pandemic-on-cybersecurity/
3. Dey, M., Frazis, H., Loewenstein, M. A., & Sun, H. (2020, June). Ability to work from home: Evidence from two surveys and implications for the labor market in the COVID-19 pandemic. U.S. Bureau of Labor Statistics. https://www.bls.gov/opub/mlr/2020/article/ability-to-work-from-home.htm
4. Bloom, N. (2020, June). How working from home works out. Stanford SIEPR. https://siepr.stanford.edu/research/publications/how-working-home-works-out
5. Hickman, A., & Saad, L. (2020, May 22). Reviewing remote work in the U.S. under COVID-19. Gallup. https://news.gallup.com/poll/311375/reviewing-remote-work-covid.aspx
6. PricewaterhouseCoopers. (2020, June 25). Us remote work survey. PwC. https://www.pwc.com/us/en/library/covid-19/us-remote-work-survey.html
7. Scholtz, T., Addiscot, R., & Olyaei, S. (2020, September 8). Implement an agile cybersecurity program: Lessons learned from the COVID-19 pandemic. Gartner. https://www.gartner.com/document/3989976?ref=solrAll&refval=265556396
8. Kashyap, A., Scholtz, T., Addiscott, R., & Olyaei. (2021, March 2). The importance of an agile cybersecurity program: lessons learned from the COVID-19 pandemic. Gartner. https://ssofed.gartner.com/sp/startSSO.ping?PartnerIdpId=urn:mace:incommon:psu.

edu&TargetResource=https%3A%2F%2Fwww.gartner.com%2Fdocument%2F3998816%3Fref%3Dd-linkShare

9. Lovejoy, K., Burg, D., Hynes, M., Maddison, M., Pizzala, J., & Watson, R. (2020, February 18). How does security evolve from bolted on to built-in? EY. https://www.ey.com/en_us/consulting/how-does-security-evolve-from-bolted-on-to-built-in
10. IBM Security & Morning Consult. (2020, June). Work from home study. http://filecache.mediaroom.com/mr5mr_ibmnews/186506/IBM_Security_Work_From_Home_Study.pdf
11. Lakhani, A. (2020, August 7). IoT security during COVID-19: What we've learned & where we're going. Dark Reading. https://www.darkreading.com/iot/iot-security-during-covid-19-what-weve-learned-and-where-were-going/a/d-id/1338501
12. Liberatore, S. (2020, March 23). Hey Alexa, stop listening! Employees urged to turn off smart speakers while working from home. Daily Mail. https://www.dailymail.co.uk/sciencetech/article-8144713/Employees-urged-turn-smart-speakers-working-home-coronavirus.html
13. Costello, K., & Rimol, M. (2020, April 13). Gartner says worldwide pc shipments declined 12.3% in the first quarter of 2020 due to coronavirus pandemic. Gartner. https://www.gartner.com/en/newsroom/press-releases/2020-04-13-gartner-says-worldwide-pc-shipments-declined-12-point-3-percent-in-the-first-quarter-of-2020-due-to-coronavirus-pandemic
14. Costello, K. (2020, March 31). Ask these questions before deploying remote access technology. Gartner. www.gartner.com/smarterwithgartner/ask-these-questions-before-deploying-remote-access-technology/
15. Smith, R., Riley, S., Hill, N., & D'Hoinne, J. (2020, March 25). Solving the challenges of modern remote access. Gartner. https://www.gartner.com/document/3982521?ref=solrAll&refval=261625834
16. Chrisholm, M. (2020, July 23). What's the difference between a CASB, ZTNA, SDP and VPN, and when do you need them? NetMotion Software. https://www.netmotionsoftware.com/blog/remote-working/when-do-you-need-casb-ztna-sdp-vpn
17. Riley, S., MacDonald, N., & Orans, L. (2019, April 29). Market guide for zero trust network access. Gartner. https://ssofed.gartner.com/sp/startSSO.ping?PartnerIdpId=urn:mace:incommon:psu.edu&TargetResource=https%3A%2F%2Fwww.gartner.com%2Fdocument%2F3912802%3Fref%3Dd-linkShare
18. Tsai, P. (2019, March 4). The 2019 state of servers. Spiceworks. https://community.spiceworks.com/blog/3182-the-2019-state-of-servers
19. Lefferts, R. (2020, April 8). Microsoft shares new threat intelligence, security guidance during global crisis. Microsoft Security. https://www.microsoft.com/security/blog/2020/04/08/microsoft-shares-new-threat-intelligence-security-guidance-during-global-crisis/
20. Desai, D. (2020, April 23). 30,000 percent increase in COVID-19-themed attacks. Zscaler. https://www.zscaler.com/blogs/research/30000-percent-increase-covid-19-themed-attacks
21. Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. ArXiv:2006.11929 [Cs]. http://arxiv.org/abs/2006.11929
22. Cybersecurity & Infrastructure Security Agency. (2020, April 8). Alert (AA20-099A) COVID-19 exploited by malicious cyber actors. https://us-cert.cisa.gov/ncas/alerts/aa20-099a
23. Nair, P. (2020, August 11). Kaspersky: DDoS attacks spike during COVID-19 pandemic. InfoRisk Today. https://www.inforisktoday.com/kaspersky-ddos-attacks-spike-during-covid-19-pandemic-a-14805

ISSA Education Foundation

Continued from page 11

VOLUNTEER OPPORTUNITY TO JOIN ISSAEF

The Foundation is seeking volunteers for the following:

- Board Members: Director of Fundraising and Director, Special Fundraising Programs.
- Committee Members: Scholarship Review Committee and Professional Grant Review Committee.
- Short-term Projects, including scholarship publicity, fundraising, and governance of the Foundation.

If you are interested in joining a truly dedicated and enthusiastic group, please send an email with your background to volunteer@issaef.org

SUPPORT US WHILE SHOPPING

Help spread the word about these great opportunities to your friends and family at no cost to you – just use Amazon Smile while shopping online and automatically, with absolutely no cost to shoppers a 0.5% of eligible purchases will be donated by Amazon to our scholarship fund! It's simple: start the purchase on https://smile.amazon.com, select "ISSA Education and Research Foundation Inc." (needs to be done only the first time), and shop as usual. Do not forget to tell your family/friends to do the same.

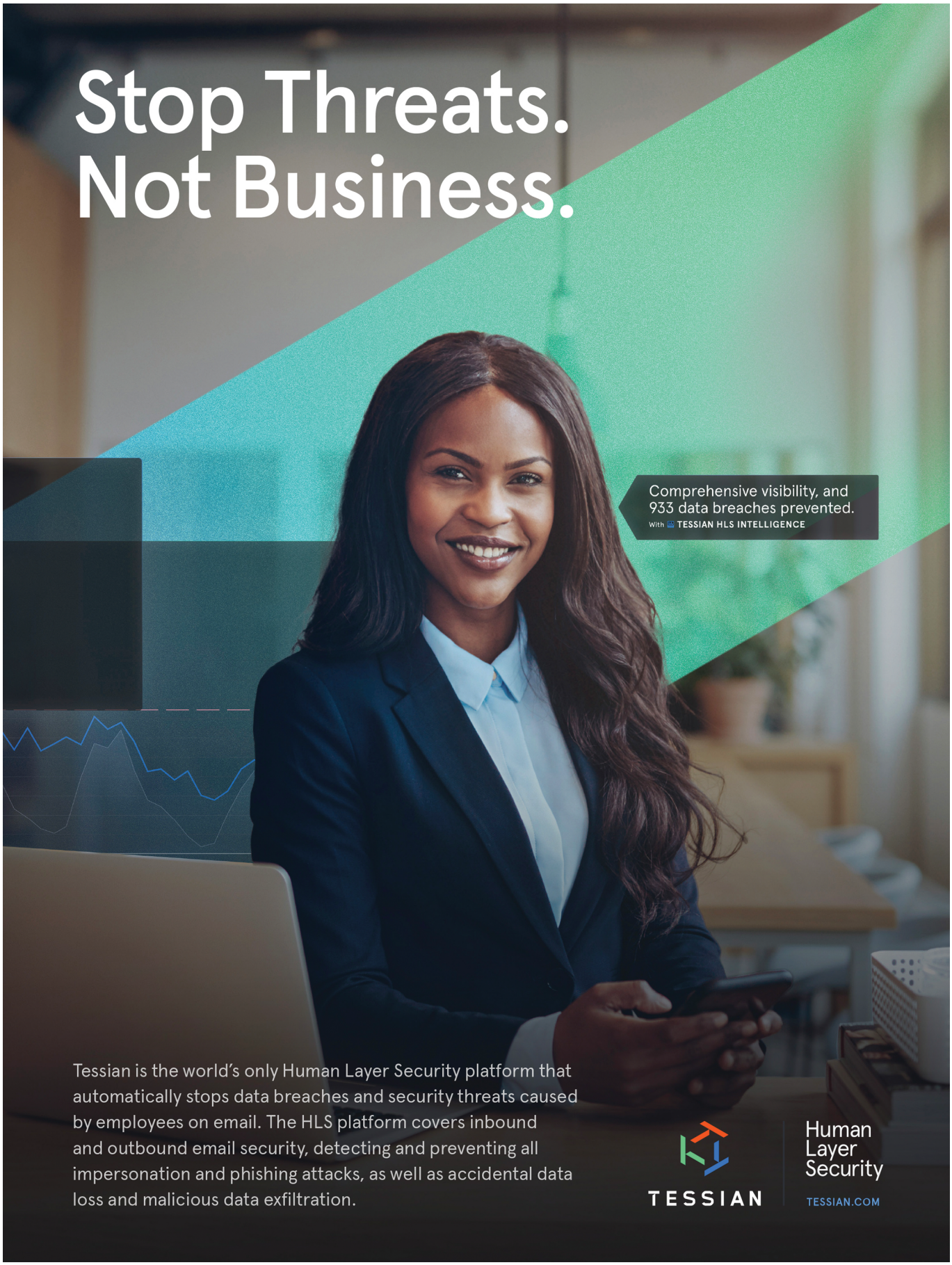
Like us on Facebook, Twitter and LinkedIn

Support us with amazonsmile
You shop. Amazon gives.

"Enjoying the Journal? Got ideas for how to improve it? Let us know by taking the official ISSA Journal Survey:

https://bit.ly/3powHrB

We want the Journal to reflect what you want and be a valuable part of your ISSA membership and security career."


Stop Threats.
Not Business.
Comprehensive visibility, and
933 data breaches prevented.
With TESSIAN HLS INTELLIGENCE
Tessian is the world's only Human Layer Security platform that automatically stops data breaches and security threats caused by employees on email. The HLS platform covers inbound and outbound email security, detecting and preventing all impersonation and phishing attacks, as well as accidental data loss and malicious data exfiltration.
TESSIAN
Human Layer Security
TESSIAN.COM

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…

ISSA JOURNAL

Write for your ISSA Journal…

- Regulation, Public Policy, And Law
- Preparing The Next Generation Security Professional
- Political Dimensions Of Cybersecurity: Elections, Cyberwarfare
- Cryptography/ Quantum Menance
- Toolbox: Basics To The Bleeding Edge
- Security Vs Privacy Tug Of War
- Disruptive Technologies
- Security Paradigms In The Cloud
- The Business Side Of Security
- Big Data/Machine Learning/ Adaptive Systems
- Looking Toward The Future Of Infosec

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 with Friends of Authors

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

~Jack Freund, Editor

It's Your Journal – Contribute Your knowledge & Expertise

ISSA
CYBER EXECUTIVE FORUM

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

ISSA Cyber 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 Cyber 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 Cyber Executive Forums per year, including lodging for one night and all meals at each Forum
- You'll be part of an effective forum for understanding and influencing relevant standards and legislation
- Extensive networking opportunities with peers and experts on an ongoing basis
- Direct access to top subject matter experts through educational seminars
- CPE credits you earn will be automatically submitted
- Vendor Influence: A unified voice to influence industry vendors
- Online Community: Privileged access to our online community

Visit Cyber Executive Forum for more information or to register for the Forum.

Asia Pacific
Bangladesh
Chennai
Dehradun
India
Philippines

Canada
Alberta
Ottawa
Quebec City
Vancouver

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

Latin America
Argentina
Barbados
Bolivia
Brasil
British Virgin Islands
Chile
Colombia
Ecuador
Peru

Middle East
Bahrain
Egypt
Iran
Israel
Kazakhstan
Kuwait
Qatar
Saudi Arabia

USA
Alamo San Antonio
Blue Ridge
Boise
Buffalo Niagara
Capitol of Texas
Central Alabama
Central Florida
Central Indiana
Central Maryland
Central New York
Central Ohio
Central Plains
Central Texas
Central Virginia
Charleston
Charlotte Metro
Chattanooga
Chicago
Colorado Springs
Columbus
Connecticut
Dayton
Delaware Valley
Denver
Des Moines
East Tennessee
Eastern Idaho
Eugene
Fayetteville/Fort Bragg
Fort Worth
Grand Rapids
Grand Traverse
Greater Augusta
Greater Cincinnati
Greater Spokane
Hampton Roads
Hawaii
Inland Empire
Kansas City
Kentuckiana
Kern County
Lansing
Las Vegas
Los Angeles
Metro Atlanta
Mid-South Tennessee
Middle Tennessee
Milwaukee
Minnesota
Motor City
National Capital
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 Virginia (NOVA)
Northwest Arkansas
Northwest Ohio
Oklahoma
Oklahoma City
Orange County
Phoenix
Pittsburgh
Portland
Puerto Rico
Puget Sound (Seattle)
Quantico
Rainier
Raleigh
Rochester, NY
Sacramento Valley
San Diego
San Francisco
Silicon Valley
South Bend - Michiana
South Florida
South Texas
Southeast Arizona
Tampa Bay
Tech Valley Of New York
Texas Coastal Bend
Texas Gulf Coast
Triad of NC
Upstate SC
Utah
Ventura County
West Texas
Wyoming
Yorktown

ISSA.org => Chapters