ISSA JOURNAL

June 2020
Volume 18 Issue 6

Why Top Management Must Now Stop the Drift to Chaos and Disorder

Sophisticated Tools Alone Cannot Prevent Advanced Persistent Threats: What's Next?

Python Programming: Processing NVD Data

★ ★ ★ ISSA ★ ★ ELECTION ★ ★ 2020 ★ ★ ★

# Ethical Hacking from Vulnerability Scanning to Adversary Emulation

The Infosec Toolbox: Basics to the Bleeding Edge

# Table of Contents

## DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

### Feature

20 **Ethical Hacking from Vulnerability Scanning to Adversary Emulation**
*By Jorge Orchilles – ISSA Fellow, South Florida Chapter*
One continually hears "ethical hacking" or "offensive security" terminology used incorrectly by regulators, customers, etc. This article attempts to clarify the definition so that we can all speak and push the industry to use the correct terminology.

27 **Why Top Management Must Now Stop the Drift to Chaos and Disorder**
*By Charles Cresson Wood – ISSA member, San Francisco Chapter and Perry Carpenter*
Entropy is a law of nature which specifies that, over time, unless work is undertaken to reverse the trend, things will wind-down, become disorganized, and move into what appears to us to be chaos. This article discusses the need for the new management techniques that must be adopted to reverse the drift into entropy.

33 **Sophisticated Tools Alone Cannot Prevent Advanced Persistent Threats: What's Next?**
*By Srinivasulu Vuggumudi – ISSA member, Silicon Valley Chapter and Yong Wang*
This article introduces different groups of cybersecurity tools, discusses challenges with them, identifies the possible reasons why they are not enough to defend against advanced persistent threats, and discusses the research in progress to complement existing cybersecurity tools.

40 **Python Programming: Processing NVD Data**
*By Constantinos Doskas – ISSA Senior Member, Northern Virginia Chapter*
This article continues our discussion on database programming by exploring methods of downloading data from websites, loading them on databases, and analyzing them. In past articles we had an overview of NVD database data and the data was downloaded in local storage. In this article we will be loading some of the data on a table and present ways of creating visualizations from it.

### Also in this Issue

3 **From the President**

5 **Sabett's Brief**
Inside the Lawyer's Infosec Toolbox

6 **Herding Cats**
Contain This

7 **Open Forum**
Mindlessly Following "Best Practices"

8 **Women in Cybersecurity**
Orchestrating a Communication Cadence in Hybrid Environments

9 **The Cryptic Curmudgeon**
Thoughts on Disasters, Planning, and Training

10 **Open Forum**
Can You Handle a Nation-State Cyber Attack?

11 **Crypto Corner**
Asteroids

12 **Security in the News**

14 **2020 International Election**

44 **Career Center**

ISSA JOURNAL
June 2020
ISSA ELECTION 2020
Ethical Hacking from Vulnerability Scanning to Adversary Emulation
The Infosec Toolbox: Basics to the Bleeding Edge

*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

Candy Alexander, International President

## It's June and that must mean it is time to vote in the ISSA International Elections!

This is one of the most important things that you can do to support our association! I ask that you please, take a moment and learn about those individuals who have stepped up to the plate and are willing to dedicate hours each month to serve us—and vote. It will only take you a couple of minutes and voting is absolutely important. So, show us your support by voting and remember every vote counts! Find voting information and candidate profiles here.

Since I am running for re-election, I am going to ask for your forgiveness in having an extremely short president's letter this month. I want to ensure that there are no conflicts and perceptions of unfair campaigning.

I will catch you up on the president's message in July, as normal. Until then I hope that all of you stay safe and stay healthy in our COVID-19 pandemic world.

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

# DEVELOPING AND CONNECTING CYBERSECURITY LEADERS GLOBALLY

ISSA
Information Systems Security Association

**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

## Services Directory

**Website**
webmaster@issa.org

**Chapter Relations**
chapter@issa.org

**Member Relations**
memberservices@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.

# Inside the Lawyer's Infosec Toolbox?

**By Randy V. Sabett** – ISSA Distinguished Fellow, Northern Virginia Chapter

A variety of tools exist and can be deployed by an infosec lawyer, depending on the role being played by that lawyer (i.e., in-house, private practice, lawyer/consultant, etc.) In most scenarios, the contract remains most basic and fundamental tool to address a variety of infosec issues. In my practice, contracts span from commercial transactions (such as M&A and financings), to service provider contracts, to data sharing agreements, and a whole host of other scenarios. Although the provisions in this broad range of agreements may differ in terms of the obligations of the parties, at their essence they focus on (a) the protection of information and (b) the repercussions if problems arise related to that information being protected.

In the corporate world, the funding/acquiring entity seeks reasonable assurances (through due diligence) and adequate protection (through representations and warranties) from the target company such that an infosec issue will not create unreasonable exposure. During the diligence process, the target's infosec documentation will be reviewed and inquiries will be made about any issues of interest to the lawyers for the funding/acquiring entity. As a result of those inquiries, certain changes may be made to the deal contracts.

In the technology transactions arena, companies and service providers typically address numerous infosec issues in their agreements with each other. In these scenarios, the company acquiring services typically seeks appropriate protection for its information, while the service provider tries to maintain an acceptable amount of liability. In regulated scenarios, these might take the form of a business associate agreement or BAA (under HIPAA) or a data protection addendum or DPA (under the GDPR).

While regulations or other legislative requirements that require use of a BAA or DPA can be helpful in addressing infosec issues in specific environments, I sometimes find in non-regulated situations that companies either (a) don't think through how their information should be protected or what tailored provisions to include for their specific needs or (b) if they do include infosec provisions, they don't exercise their rights under those agreements. One of the perhaps most overlooked provisions involves audit rights that companies may have negotiated that will allow them varying degrees of insight into what the other party does with their sensitive information. I am consistently amazed at situations where a company has run into a situation involving their data with their service provider. They will ask me to review the contract and when I ask if they have exercised their audit right over the past X years (where X may be anywhere from one to four or more years), they say they have not. Why not?? That's an excellent way to understand what is happening to the company's sensitive data.

Likely not surprising to anyone in this audience, infosec also has a whole assortment of cutting edge issues and technologies, many of them unique and often needing specialized contracts that are tailored to either the parties, the technology, or both. For example, PKI (though a technology that has been around for over 30 years) continues to evolve around new business models that require customized documentation and contracts. For two different engagements recently, I had to write a tailored certificate policy (CP) for a novel application of PKI to combat a significant masquerading problem and then had to write a certification practice statement (CPS) for a company looking to break into the embedded certificate market. In the past, I have had to write subscriber agreements, relying party (RP) agreements, and operating policies for other PKI applications; information sharing guidelines and associated agreements for industry information sharing efforts; and agreements covering government/commercial cooperation efforts (what today might be called defend forward).

The takeaway from all of this should be clear—infosec tools for lawyers may involve traditional and straightforward contractual mechanisms (very much resembling what I call "NDAs on steroids"). Sometimes, however, they could also involve very specific and particularized concepts that cannot be addressed by a form or template agreement. That's where the lawyer really needs to pull out his or her specialized tools and take particular care to accurately capture what the client needs. On that note, I'm off to talk to a client about an employee who downloaded almost half a terabyte from the company's servers…just before leaving the company. Have a great month and stay safe!

## About the Author

*Randy V. Sabett, J.D., CISSP, is an attorney with Cooley (www.cooley.com/rsabett), a member of the advisory board of the Georgetown Cybersecurity Law Institute and the RSA Selection Committee, a member of the Cyber Leadership Council in the U.S. Chamber of Commerce, and is the former Senior VP of ISSA NOVA. He can be reached at rsabett@cooley.com.*

# Contain This

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

I just recently was asked to put together a course for executives around cybersecurity, and the particular module they wanted me to build was around tools, technologies, and solutions. What started as a "Yeah, I think I can do that," quickly turned into a "What did I sign up for?!" Building a course where you cover these topics turned out to be much more difficult than I had imagined, but it reminded me of the challenges that we all face when we try to marry a capability to a product.

For this column, however, I want to write about a technology we see on the IT side that has some interesting security implications—both as a defensive tool as well as a potential hiding spot for critical vulnerabilities. So buckle up, we're talking containers.

Container, or OS-level virtualization, capabilities have been present for decades. Perhaps the chroot command could be the first containerization capabilities in the Unix world. Originally found in the early 1980s, it would essentially put a user into a chroot "jail" once they logged into a machine for interactive usage or file transfer. There would be static binaries for common commands like ls dropped in a bin directory, and the user would not see any of the rest of the operating system.

It wasn't until 2000 that we started to see more practical OS-level virtualization in a product from Virtuozzo that started to hint at where this could possibly go from a features and security perspective. Looking back over the last 20 years, it is clear that being able to contain software into some kind of a sandbox became more desirable. Zoom[1] ahead to 2013 and the technology that might have the most familiar name to you is introduced—Docker.

Docker by itself is pretty cool. If you have not tried it, go grab the binaries and install them on whatever test machine you are using. Then go browse the vast number of tools that can be deployed as a Docker container. It's a lightning fast way to deploy, test, and remove software to tinker with it before moving to production. Containers help to create resiliency and a deploy-anywhere mindset. What about security pros and cons?

On the pro side, one thing that makes Docker containers desirable is their immutable file system. The base file system is not changed unless you update the container build itself, and you can see everything done while the container has been running by using docker diff. This is good because you know you are starting from a known good place, and any changes the application or attacker makes are logged.

There is also another benefit in that containers are meant to be ephemeral (fancy word for temporary with an undefined lifespan). So if you were under attack because of some vulnerability inside your container, you could kill and respawn every five minutes (the time frame varies) and force the attacker to start over. If the attack takes 10 minutes to complete, they will move off to another target. I had a former client that ran known vulnerable code that way in production to buy their developers time to fix the issue properly. They destroyed and respawned containers to get the attacker to move on.

Let's talk some cons. Network scanning containers is not very effective because network ports that get bridged from the inside world to the outside world have to be defined. So even though you have a PostgreSQL database running inside the container and listening on TCP port 5432, we wouldn't be able to access it unless you specifically bridge that port from inside to the outside of the container. Instead, you would need to conduct periodic scans of your container manifests to determine where vulnerable software might be living. There are plenty of vendors that have services to check your container security, as well as some open source options (Clair comes to mind).

Which leads us to another con, vulnerabilities can hide inside containers based on dependencies from various components that are inside your container—both from a configuration perspective as well as an outdated software perspective. Can you exploit it? Perhaps, but it won't be easy or as straightforward as if it were not containerized.

The Docker universe is vast and I'm just scratching the surface here. Given the nature of software deployments happening now and in the future, it would be a good investment of your time to learn all you can about containers and how they can be used to help or harm your enterprise.

## About the Author

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

[1] I'm cracking up as I wrote that. The word *zoom* will never be the same.

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

# Mindlessly Following "Best Practices"

**By Steve Kirby** – ISSA member, Greater Spokane Chapter

There are many buzzwords and security strategies that a security professional should be aware of. The details of these strategies matter but mindlessly following best practices may result in your systems actually becoming less secure. It is important to keep an eye on the overall strategy. This article is a deconstruction of some decisions that a company I work with made. These decisions significantly reduced security rather than improved it.

To set up the story, a company whose net worth is over $1B and employs roughly 50,000 people was spending a lot of money on security. It's an older company and the IT staff was not generally strong. The reason for the big push in security was that they were hacked, and a lot of internal information was shared. The company implemented a concerted program for over two years on upgrading their security.

Some of the work has been pretty solid, mostly a bit traditional. They have reconfigured their network to follow the network security model. They unified logins to make auditing easier. The company started internal scans for file system changes, looked for out-of-date software, and began flagging for upgrade. An internal scan of open ports was also performed, looking for vulnerabilities. Additionally, the company started forcing usernames that are not based on a pattern (e.g., first initial/last name) to make guessing logins harder. It was surprising that they had not had these tools in place before, but senior management had thought it was a waste of money until the penetration.

One area that failed, for reasons we will get into, was the use of two-factor authentication, which is where a user has to "know" something (password) and then "have" something like a phone or RSA token. Two-factor authentication is generally stronger than "single-factor" authentication, but the details matter and in this case the company, in my opinion, now is less secure. Previously the company required that users connect to the server using their own credentials and then switch to an administrative user. Shared accounts had no password, and there was no way to connect to the accounts other than by being on the server.

As a hacker, there were multiple challenges: he needed to find a username, guess the password, hope it had some sort of elevated access that he wanted to use, and then do the work. The servers, generally UNIX servers, were well hardened with minimum packages installed and few network-exposed services that might be used for an exploit. If a hacker, or disgruntled employee, were able to guess a username, guess a password, find a user that had elevated privileges on a server, and then run whatever scripts they had, there were still ways to catch him.

Auditing would allow you to see who was logged in at the time of escalation after the fact. The auditing is very robust between external Splunk servers to encrypted on-disk auditing that would be difficult to forge. Clues such as questioning the users logged on at the time, unusual IP addresses, unusual commands, will likely allow the company, at worst after the fact, to determine what happened. So, what is the downside of going to two-factor authentication? It can really be screwed up at implementation. How?

In this case, the company bought a "check-out" system whose sole job was to manage access. Only a few admin accounts could be in use at a time. Users were required to check in and check out of accounts, and the accounts were set for a limited duration in which the account could be used. The new system allowed a number of logins per shared user before preventing further logins without a "check in" of the shared user and the admin session had a timeout. The tool could even be configured to allow access only during certain times. It could manage security keys if those were used for connections. The tool would log every keystroke to make auditing simple. So, how was this weaker than the prior configuration?

If configured correctly, and without the messiness of operations, it would probably be a really good tool, but let's ask a couple of questions. How does the UNIX server authenticate the user? Well, it turns out, the company servers were not using SSH keys; instead they were using the username and password for admin UNIX accounts. Why a username/password? Because they had several very old servers they were unwilling to decommission. These outdated servers could not support keys and they did not have a good key management system to roll keys over frequently. To harden the password management for normal users, the company opened admin users to remote access, using passwords.

Previously servers required an identified user to connect to the server first; now an admin user connects directly. The network address still provided a clue as

Continued on page 38

# Orchestrating a Communication Cadence in Hybrid Environments

By Curtis C. Campbell – ISSA Senior Member, Chattanooga Chapter

*Millions of workers are working remotely; some will be phasing back into the workplace, creating a hybrid environment needing efficient communications in which the feeling of connectedness will be more important than ever. This article provides insight and tips for rules of engagement and consistency in communication for remote teams and hybrid environments.*

The past 90 days have created a huge cultural shift in working arrangements. Commutes are non-existent and so are dry cleaning bills. It's getting harder to remember traffic jams and rush hour. What to wear to work? No worries, shorts will do. We have adopted our own virtual routines, and if our routine seemed awkward at first, it now seems very normal. The pandemic caught us a little off guard, but we have taken the ball and ZOOM-ed with it. Now, certain teams are beginning to slowly phase back into the workplace, creating a percentage of those who will remain working from home. Setting the tone for communications in hybrid environments while managing and hiring both teams is important.

While we have sheltered in place, have you noticed any different (did I mean lax?) social behaviors? As in those who keep their camera off when Zoom-ing versus those who do not? Notice any difference in length of time responding to email? A favorite one-liner response in today's current email environment is " Sorry….I just saw your email" (from email sent days ago). If your teams communicate in many different channels (Slack, Teams, Email, Zoom, etc), and time zones, the rules for response times or reachability status need to be adopted by all. It may be time to tweak your virtual-now-becoming hybrid culture.

Think of a communication cadence in terms of rhythm. In remote/hybrid environments, leaders should communicate guidelines/best practices or workplace etiquette in responding to teammates, clients, and others. Leaders who facilitate and encourage communication will build trust wherever teams are located. Those organizations who have had hybrid environments with remote teams in the past have already done this.

## Working remotely

Most meetings are happening synchronously and virtually. This is not anything new, but face-to-face meetings and events (less than six feet apart) have been replaced with virtual ones. However, back and forth chit chat and follow ups are still asynchronous. A remote working environment can produce a healthy culture through consistent communications. All it takes is focusing on the same shared goals.

While working remotely is now being adopted and properly planned, this sudden shift overnight to 100 percent remote during the pandemic did not give a lot of preparation time. In a hybrid environment, break rooms may be closed. We can't set up a ping pong table, or play corn hole, celebrate monthly birthdays with a cake in the break room, stock the drink cooler, and call it a day. Since we are well accustomed to communicating through technology, we should create a consistent communication cadence through media platforms for people to do at work what many of them already do in their personal lives—interact with all kinds of people. This means reaching out or responding to people all over the world, whether we know them well personally or not.

While many organizations are phasing back into working at the office, many teams may have the option to enter a permanent work-from-home arrangement. This is a shift from traditional communications and team meetings in the conference room. For remote working staff, knowing what is expected and following protocol to avoid misconceptions are crucial.

## Hiring remotely

Hiring managers experienced in staffing remote environments already know what skills and traits they look for in candidates. Remote.co is a popular website focusing on remote jobs posted by remote companies seeking remote candidates.[1] On the site, company testimonials describe qualities and soft skills they are seeking as well as job-related requirements. Some rank great communication skills as crucial for joining a distributed team. Others companies gauge a candidate's timely responses as a screening tool for those that move forward in the hiring process. Self-starter and self-motivation traits are sought after along with tech savvy abilities for knowledge in software programs used to run the business. Team players and a strong work ethic with a "get it done" attitude also make the list. Hiring managers say professionalism and passion come across on video, and they watch and listen to candidates expressing themselves in video interviews.[2]

[1] Remote.co. "What Traits Do You Look for in Candidates for a Remote Job?" https://remote.co/qa-leading-remote-companies/what-traits-do-you-look-for-in-candidates-for-a-remote-job.

[2] Ibid.

Continued on page 26

# Thoughts on Disasters, Planning, and Training

By Robert Slade

You don't think I can get through this without mentioning it, do you?

As I write this, I am huddled in social isolation, while armed bands are roving the countryside, desperately searching for the last hoards of toilet paper. We are stacking the dead bodies of the victims in the forests, waiting for wildfire season, which now starts earlier every year, to deal with them. This is what disaster recovery has become: an attempt to use one crisis to deal with the outcomes of another. I am writing this in the hopes that future generations may learn the folly of placing shredded or crumbled cheese into plastic bags for convenience, and Make Civilization Grate Again.

One of the tools that we surprisingly, in my view, don't put into the toolbox is that of emergency management. We don't think about emergencies in advance, which is when we **should** think of them. This past year we had a seemingly unending stream of disasters, topped off with a global one. Are you willing to think about them **now**?

Those of us in the security communities are always interested in disasters. We are forever dealing with crises, both large and small, assessing risks, planning and comparing mitigation strategies, and looking at the management of it all. When we hear of the latest disaster on the news, someone always challenges us to make contributions to charity. I up the stakes. I challenge everyone to get trained for disasters.

Unfortunately for the point I'm trying to make, I am speaking from a position of privilege. Canada has the best emergency structure in the world. British Columbia has the best emergency response management system in Canada. And the North Shore, where I live, has the best disaster training regime in BC.

Emergency response, in a major disaster, is not simply a matter of having water, generators, blankets, and rescue dogs. It has to do with organization, co-ordination, management, and, particularly, trained people—most of them volunteers, since nobody can afford to pay for a full-time staff of all those you need to have ready in an emergency.

That's where you come in.

Get trained.

There is some emergency measures organization that covers your area, regardless of where you live. Your local municipality probably has an office. They need volunteers. And they provide training.

If you volunteer, you will probably get trained. For free. (You may also get additional perks. I get my flu shots paid for every year, since I'm an emergency worker.)

First of all, you'll probably get trained on what you need for you and your family. What do you need to survive the first 72 hours (or seven days, or two weeks) following a disaster? Do you know how much water, what type of food, etc. you need in the event of a total failure of utilities and other factors we rely on?

Then there are the skills you need to help other people. Sometimes this might relate to first aid, or structural assessment of buildings after an earthquake, etc. However, there are many necessary skills that are not quite so dramatic. Most emergency response, believe it or not, has to do with paperwork. Who is safe? Who needs care? Do families need to be reunited? Documentation of all of this is a huge effort, which goes on long after the bottles of water and hot meals have been distributed.

Then there are management skills to co-ordinate all of the other skills. An awful lot of "charity" gets wasted because some people get too much help, and others don't get enough. Someone needs to oversee the efforts.

Training in all of this is available. And, in an emergency, having trained people is probably more important than having stockpiles of tents. Trained people can make or improvise shelter.

Maybe your municipality or county doesn't have a formal emergency structure. In that case, there are organizations covering the gap. In Canada, the government doesn't do it all. The Red Cross and Salvation Army are two of the groups that have been working on this for years, and have specialists.

(For those who have security related certifications, like the CISSP, ongoing professional education is a requirement. A constant complaint is that training is expensive, and getting the credits costs too much. I get all kinds of training related to business continuity and disaster recovery. I get almost all of it free.)

Get trained. Volunteer. You'll get a wealth of experience that will help you plan for all kinds of events, not just for major disasters, but for the minor incidents that plague us and our companies every day. You'll be ready for the big stuff, too. You'll be able to keep yourself and those near to you safe. You'll be able to make a difference to others, certainly reducing suffering, and possibly saving

Continued on page 44

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

# Can You Handle a Nation-State Cyber Attack?

**By Gordon Lawson** – ISSA member, National Capital Chapter

Theft of technology from China alone is estimasted to cost the United States as much as $600B annually, according Attorney General William Barr.[1] If you're wondering if your company is a target, the FBI identifies the high-priority areas of interest—as identified by PRC national policies—as clean energy, biotechnology, aerospace, IT, and manufacturing.

Even if you're not in a targeted market, if you have valuable IP to protect, the chances are high your business will be targeted. As has been widely stated, an attacker need only be right once to penetrate a system, while defenders must be right all the time. In the past, companies concerned about IP theft and business disruption responded by relying primarily on tools and technologies. With $124B spent on products and services in 2019 amidst an escalation of high-powered attacks, I believe two realities are clear: 1) No matter what products you have deployed, the enemy has inevitably learned about them and knows how to exploit or bypass them; 2) Since nation-state and other high-level attackers are constantly changing methodologies and finding new exploits, no one is fully prepared to stop them.

Another reality is that, while the frequency of attacks on business has been relatively consistent, their nature, which has become not only more sophisticated but in constant evolution, has not.

Examples abound. Crowdstrike's *Global Threat Report 2020* notes the alarming trend in targeted ransomware operations specifically focused on managed service providers (MSPs). "Subsequent use of remote management software can enable the spread of ransomware to many companies from a single point of entry."[2] The Crowdstrike report also points to the relentless and more challenging DoppelPaymer ransomware group. Using a name-and-shame website, this group has published data stolen from at least six companies, promising to hold it hostage until payments are received.[3] This scenario has been confirmed by security firm Emsisoft as apparently being behind the supply chain attack on Lockheed-Martin, Boeing, and SpaceX via its partner Visser Precision.[4]

We will increasingly have to deal with such tactics, techniques, and procedures. Handling these advanced targeted attacks does not mean stopping them because, as we've learned, this is near impossible. Rather, we must *and can* learn to contain them and limit their damage.

International bank Barclays is using a cloud-based training program and cyber range to develop skills to learn how to better handle the latest attacks and vulnerabilities. Leadership wants ongoing assurance that security team members are not seeing such attacks for the first time when they are unfolding. This type of preparedness goes far beyond awareness or compliance because it involves setting specific goals for improved security procedures, cooperation, and resilience across global teams.

## Lessons in operational training from NATO's cyber range

My company was part of the team that built the cyber range and cyberattack simulations for the NATO Cooperative Cyber Defense Center of Excellence (CCDCOE). NATO members' IT and critical infrastructure covers over 29 member countries, 603.8 million people, and 13.66 million sq. km of the world. Over the past decade, these entities have increasingly been the target of attacks, many of them nation-state sponsored. Designed as a safe "red team/blue team" space to play out realistic, in-the-moment" attacks, the NATO cyber range aims to allow faster and more effective detection and containment operations to be developed. Member countries take part in these simulations to help train their cyber defenders to be prepared for future critical infrastructure attacks. They are especially focused on attacks that are a precursor to possible invasion.

Such simulation and cyber range training is now being adopted by businesses like Barclays that want their teams to develop the same critical operational skill sets NATO members use.

## Barclays ongoing experiential learning

As is the case at other companies, Barclays' security team recognizes that even the most sophisticated security stacks operated by exceptionally skilled professionals with the highest security credentials are vulnerable to targeted, multi-stage attacks.

To address this, Barclays sought to hone and measure the skills of their cyberse-

Continued on page 25

[1] "China Initiative Conference" Keynote Address, William Barr, U.S. Attorney General, Center for Strategic and International Studies (Feb. 6, 2020) – https://csis-prod.s3.amazonaws.com/s3fs-public/event/200206_Keynote_Address_William_Barr.pdf?R0G7Wa05hL6kbqX1kEtOrjp2udfcK8id.

[2] "Cybersecurity Trends Around the World in 2019," CrowdStrike – https://www.crowdstrike.com/resources/crowdcasts/global-threat-report-webinar-2020/, p. 16.

[3] "DoppelPaymer Ransomware Slams Supplier to Boeing and Tesla," Bank Info Security, https://www.bankinfosecurity.com/tesla-boeing-supplier-hit-by-doppelpaymer-ransomware-a-13838.

[4] "DoppelPaymer Ransomware Used to Steal Data from Supplier to SpaceX, Tesla," threat Post – https://threatpost.com/doppelpaymer-ransomware-used-to-steal-data-from-supplier-to-spacex-tesla/153393/.

# Asteroids

By Luther Martin – ISSA member, Silicon Valley Chapter

Key management is almost never cryptographically strong (taking roughly 2^80 calculations or more to defeat). This means that it is easier to get a key by subverting key management processes than to get it through a cryptanalytic attack. General William Barrow, former Commandant of the Marine Corps, once noted that "Amateurs talk about tactics, but professionals study logistics." Similarly, information security amateurs talk about encryption, but professionals talk about key management. But because key management may not be as interesting as encryption, we will cheerfully ignore this and talk about the security of encryption anyway.

There are many reasons to believe that encryption is very secure. Incredibly powerful computers are unable to crack a 128-bit key (such as an AES key) within a reasonable time. A calculation that takes a billion years or more will essentially never be completed, and that is roughly what it will take to crack a 128-bit key using technology that will be available for the next several lifetimes.

There are also reasons to believe that cracking a 128-bit key will never finish, beyond limits imposed by available computing power: asteroid impacts on the Earth will see to that. This should give you an idea of the likelihood of an attacker cracking a 128-bit AES key.

There at least two ways in which asteroid impacts could affect the ability of a computer to continue work on cracking a key: the computer itself could be destroyed by the impact of an asteroid, and the civilization that is needed to support and maintain the computer could be wiped out. And it turns out that these events happen with a frequency that is not cryptographically low (having a probability of roughly 2^-80 or less). In any particular year, they are much more likely to happen than an adversary with a very powerful computer is likely to crack a cryptographic key.

The Earth encounters millions of asteroids every year. Most do not make it through the atmosphere and hit the ground. In fact, it takes a fairly big asteroid to make it through our atmosphere. Using Isaac Newton's ideas and lots of assumptions, it is not hard to estimate how big such a rock must be. We know the air pressure at sea level. From that we can estimate the mass of the air above a unit area. To reach the ground, an asteroid will need to be large enough to push that air out of the way on its way down.

> **…if you start cracking a 128-bit key, you will probably never finish because something more important will end up distracting you.**

If you are not fond of such calculations, searching the NASA website for this information provides an easier, if less interesting, alternative. Either way, we find that it takes an asteroid roughly the size of a big house (about 25 meters in diameter) to survive the trip through the atmosphere. That is fairly big for an asteroid; most are much smaller, and simply burn up in the atmosphere without endangering any computers on the ground that might be cracking cryptographic keys. But it's hard to think of a reasonable way to estimate the chances of a computer being destroyed by an asteroid impact in any given year. Maybe it makes sense to worry less about a computer being directly destroyed by an asteroid impact and worry more about bigger asteroids that would affect people's ability to support and maintain the computers doing the cracking.

Bigger asteroids hit the Earth only rarely, but they can have impressive effects. Every million years or so an asteroid impact occurs that would dramatically affect civilization, if not destroy it entirely. Every 100 million years there is an asteroid impact that would definitely destroy both civilization as we know it and most life on Earth.

So if there is an asteroid impact every million years that will make people suddenly lose interest in cracking a key, that means that in any given year there is about a one in a million chance having a key cracking project interrupted by such a disaster. And if it takes about a billion years to crack a key (a reasonable estimate for a 128-bit key with 21st century technology), there is about a one-in-a-billion chance of the key-cracking project being successful in any given year.

In any particular year, the chances of cracking a 128-bit key being interrupted by an asteroid impact are about 1,000 times greater than the right key being found. Thus if you start cracking a 128-bit key, you will probably never finish because something more important will end up distracting you. So don't worry about AES being cracked. It's not going to happen.

## 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.*

# News That You Can Use…

Compiled by Kris Tanaka – ISSA member, Portland Chapter

## CISA Releases New Cybersecurity Essentials Toolkit

https://www.securitymagazine.com/articles/92491-cisa-releases-new-cybersecurity-essentials-toolkit

The first "essential element" of the Cybersecurity and Infrastructure Security Agency's (CISA) Cyber Essentials Toolkit is now available for download. The resource is a set of modules designed to break down security components and directives into bite-sized actions for IT and C-suite leadership to work toward full implementation in their organizations. New toolkits that correspond with each of the six essential elements will be rolled out each month.

## Choosing a Safe Conferencing Tool in the Era of Mass Telework

https://federalnewsnetwork.com/cybersecurity/2020/06/choosing-a-safe-conferencing-tool-in-the-era-of-mass-telework/

When organizations had to figure out how to securely move their workforces from an office environment to employee homes at the start of the COVID-19 pandemic, one of the biggest challenges involved how to enable safe communication and collaboration outside of the corporate security perimeter. With so many options to choose from, how do you know what conferencing tool is right for your company? Luckily the US National Security Agency (NSA) has put together a guide to make the selection and implementation process easier.

## Centralized or Decentralized, All Tracking Apps Fall Foul of the Same Vulnerability – User Error

https://www.cpomagazine.com/data-privacy/centralized-or-decentralized-all-tracking-apps-fall-foul-of-the-same-vulnerability-user-error/

Useful tool that will help halt the spread of COVID-19 or invasion of privacy? This is the dilemma that people face when it comes to using contact tracing apps. As governments move toward implementing these new tools, they have quite a few hurdles to clear regarding how these apps will function and if they truly will provide value.

## China's Military Is Tied to Debilitating New Cyberattack Tool

https://www.nytimes.com/2020/05/07/world/asia/china-hacking-military-aria.html

Infosec tools are not only for the good guys. Researchers have identified a particularly malicious new tool called Aria-body, which allows hackers to remotely take over a computer to copy, delete, or create files, as well as carry out extensive searches of the device's data. It also has new ways of covering its tracks to avoid detection. The weapon has been connected to a group of hackers, called Naikon, which was previously traced to the Chinese military. Although China insists that it is opposed to cyber attacks of any kind, researchers claim that group is responsible for China's cyber operations and technological espionage in Southeast Asia and the South China Sea.

## What The COVID-19 Pandemic Teaches Us about Cybersecurity – And How to Prepare for the Inevitable Global Cyber Attack

https://www.weforum.org/agenda/2020/06/covid-19-pandemic-teaches-us-about-cybersecurity-cyberattack-cyber-pandemic-risk-virus/

What if COVID-19 was a cyber pandemic instead of a biological virus? Would we be ready for the impact it would have on our lives? Probably not. Should we be preparing for such a crisis? Absolutely. According to the article, the economic impact of a widespread digital shutdown would be of the same magnitude or greater than what we are currently experiencing. And if the cyber attack had characteristics like the coronavirus, it would spread faster and further than any biological virus. The key takeaway here is that it is not a matter of if we will have a cyber pandemic, but when. Therefore, we need to use what we are learning now to help us be better prepared for the future.

## The Definitive Cybersecurity Statistics Guide for 2020

https://securityboulevard.com/2020/05/the-definitive-cyber-security-statistics-guide-for-2020/

Data is one of the most powerful tools you can have in your cybersecurity toolbox. To help you in your quest for information, here is a collection of links to the top 122 cybersecurity statistics for 2020 and beyond.

## Cybersecurity: Half of Employees Admit They Are Cutting Corners When Working from Home

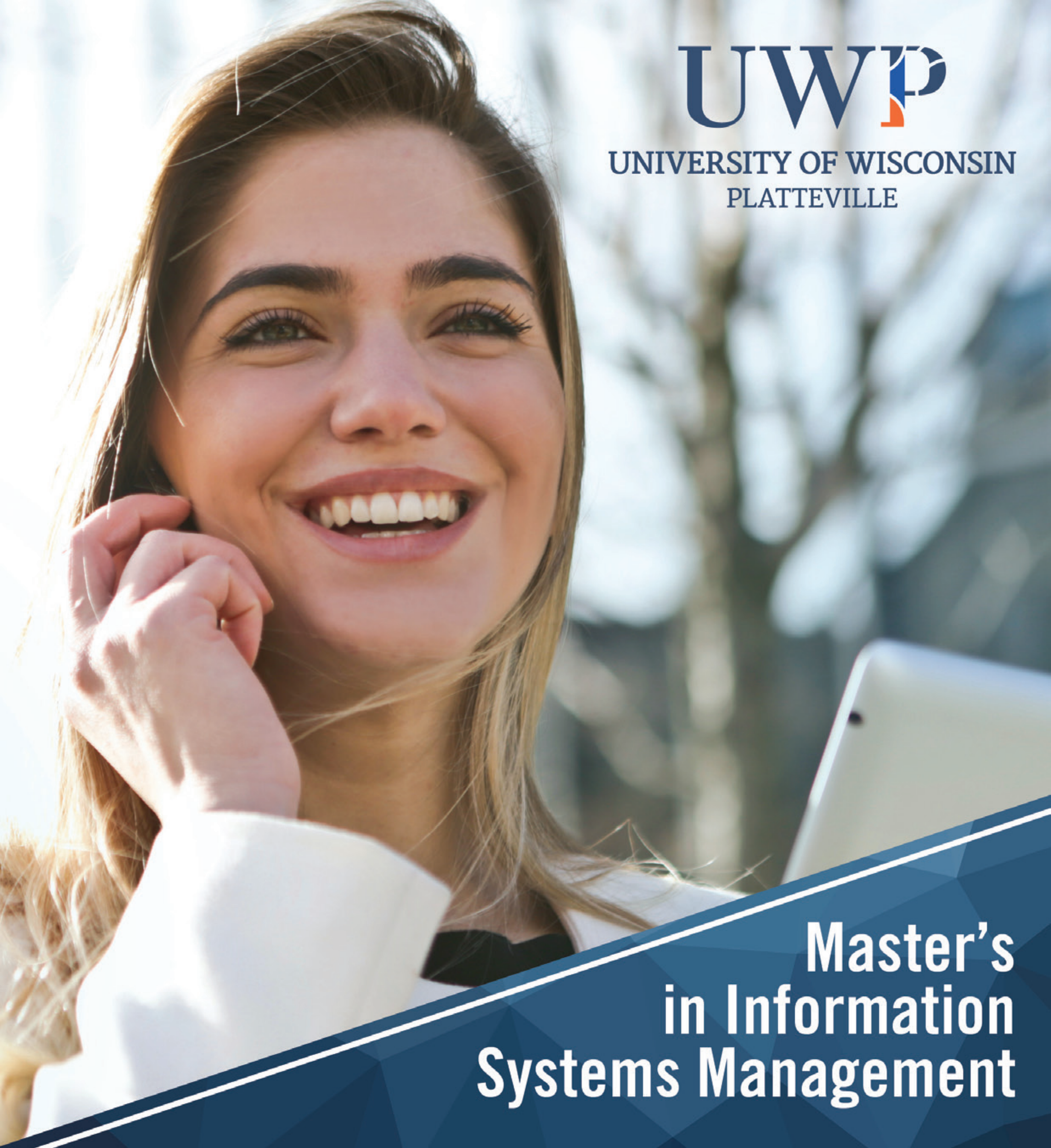
https://www.zdnet.com/article/cybersecurity-half-of-employees-admit-they-are-cutting-corners-when-working-from-home/

During these challenging times, we have proven that remote work is possible. In fact, our work environment may be permanently changed thanks to the success of this new digital transformation. However, can we really be confident that our teams are making the right choices and keeping cyber safe when they are not at the office?

## Top 5 Must-Use Cybersecurity Tools

https://www.techradar.com/news/top-5-must-use-cybersecurity-tools

Although this list is meant for cybersecurity newbies, it can be a useful starting point as you create or evaluate your security tool checklist. Do you agree with author's recommendations? What things are missing? Security in the News would like to know what is in your cybersecurity toolbox. Share your "most valuable tools" list with Editor Thom Barrie.



★ ★ ★ ISSA ★ ★ ELECTION ★ ★ 2020 ★ ★ ★

# 2020 International Election

## Candidate Profiles

The election of the International Board of Directors will take place online June 15 – July 3. From the following slate of candidates, you will select the following positions:

**International President and Five International Directors**
Profiles on following pages.

Eligible voters include General, CISO Executive, Lifetime, and assigned Corporate and Government Organizational members as of June 7. Voting information will be sent to your primary email address on file. Please update your member profile to ensure you receive your credentials. If you have questions regarding your membership status, contact elections@issa.org.

### President

**Candy Alexander**
**Shawn P. Murray**

### Five Director Positions

**Curtis Campbell**
**Mary Ann Davidson**
**John Dyson**
**Alex Grohmann**
**Lee Neely**
**Michael Rasmussen**
**Jimmy Sanders**

*Watch "Meet the Candidates" June 12, 12:00 PM EST.*
*The recorded version will be available shortly thereafter.*

GoToWebinar

## Your Vote Will Make a Difference

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

The ISSA elections open at 12:01 AM Eastern Time on June 15, 2020, and will close 11:59 PM Eastern Time, July 3, 2020.

All eligible voters will receive an email on June 10 with their credentials to vote from noreply@directvote.net. The email contains your unique voter login URL and your unique login credentials. The email will be sent to the primary email address we have on file for you. If you do not see this email in your in-box, please check your junk folder and/or spam filter for your login credentials.

If you do not receive your credentials or need assistance, please contact support@directvote.net.

JUNE 15 – JULY 3

## President Candidate
## Candy Alexander
CISSP, CISM

Candy has been working in cybersecurity for over 30 years, growing up within the profession. She's held several positions as CISO, consults with international organizations, and is considered one of cybersecurity's valued thought leaders.

Candy has received numerous awards including ISSA Distinguished Fellow and the ISSA Hall of Fame. She is often asked to speak at various events and two that remain most memorable are being a featured speaker at a United Nations event and receiving an invitation to the Offices of the White House.

Candy's passion is demonstrated through her work in the ISSA including being the current international president, chief architect for the Cyber Security Career Lifecycle, and long-standing dedicated member of the international board. She is also the inaugural president and past board member of the ISSA Education Foundation. Candy's home chapters are New England and New Hampshire.

Through Candy's leadership and direction, the association has regained back office accountability and stability in business processes, substantial improvements of technology (website, financial, and membership management systems), ongoing chapter leaders support with improved communications, tools, and processes—all of which enable our chapters success—and most recently the ability to sustain a healthy organization and uninterrupted support system through our unprecedented times brought on by the pandemic.

### Statement of Goals

The past two years have focused on formalizing processes in order to run the ISSA International as a business, as was promised in my first campaign as president.  Now, let's make ISSA shine! If re-elected I plan to:

- Continue to focus on stability and accountability
- Emphasize a culture of service, continuous improvement, and collaboration
- Ensure open and bi-directional communications
- Deliver the tools that chapters need to succeed
- Increase member value through services that are relevant to member needs
- Continue the use innovation and technology to deliver services to chapters and members
- Expand on our partnerships with organizations such as IAPP and CSA to drive our profession forward, based on research, needs identified, and collaboration
- Through the ESG/ISSA research study, identify our collective challenges and offer actionable solutions for our members
- Celebrate our members and their accomplishments and make an association you are proud to say you are a member of

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

## President Candidate
## Shawn P. Murray
C|CISO, CISSP, CRISC

Shawn Murray is a principal scientist with the United States Missile Defense Agency and an officer in the US Civil Air Patrol. Previous assignments include work with Army Cyber Command in Europe, US Air Force, and 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, holds several degrees to include a doctorate in computer science. He is an ISSA Executive Member, chapter advisor, ISSA Honor Roll recipient, and 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, and volunteers with youth soccer in his community.

### 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 forth experience applying information security concepts and educating future cybersecurity professionals expected to fill widening gaps in our career field. My contributions to members as director and most recently COO over the past four and a half years includes traveling to help establish new chapters, collaborating with other chapters to help solve problems, and representing our association as a keynote presenter when invited to do so.

I've met and spoken to members of Congress and advocated for information and cybersecurity to other state and US government leaders. I've worked with board members through significant association realignment initiatives that have made our association stronger, which directly benefits the membership as a whole.

If elected president, I'll continue to serve and represent the best interests of our members internationally and work with other board members to steer ISSA into the future. Additional goals this term include identifying resources for ISSA programs and working with members to bring more value to our association. As president, I will work to ensure that our association is leading the industry by leveraging our members experience. I am honored and committed to continue service by leading ISSA, its chapters, and our members!

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

JUNE 15 – JULY 3

Director Candidate

## Curtis Campbell

C|CISO

Dr. Curtis Campbell is a 25-year information security professional, holds Bachelor and Master of Science degrees from the University of TN, and earned a PhD in organizational leadership/information systems technology.

Curtis works as vice president and manager of vendor management and information technology procurement at Atlantic Capital Bank, chartered with accountability and oversight of third-party risk to include regulatory audits. She works with executive leadership to minimize third-party risk, developing strategic improvements in evaluation, and monitoring processes and standards.

As president of ISSA Chattanooga, Curtis has been active leading the chapter she co-founded in 2012. During this time, she sought to increase membership by bringing national-level sponsors and speakers to local chapter events for robust education and training in mini conference-style quarterly events. During her roles as chapter VP and president, the Chattanooga chapter was recognized as Small Chapter of the Year in 2017 and again in 2019.

A Senior Member of ISSA International, Curtis chaired the 2018 Chapter Collaboration Committee, formed to bring chapters together for strengthened support, resources, and mentoring. Curtis has been active at local and international ISSA conferences and summits, moderating and participating on women in cybersecurity panels, championing women of all stages in their careers to power up their careers.

A thought leader, Curtis contributes a monthly *ISSA Journal* column, "Women in Cybersecurity" and has been recognized for her work in highlighting women's accomplishments, leadership, and issues facing the field today. She has published over 20 peer-reviewed journal articles including "Securing the Remote Employee: Protecting the Human Endpoint in the Cybersecurity Environment," "Inspiring and Preparing the Next Generation of Cybersecurity Professionals," and "Existential Risk: Women Fighting for the Future."

### Statement of Goals

- Assist board initiatives in promoting security education and skills development through virtual and face-to-face events
- Assist board initiatives to further develop and promote collaboration and communication through the website's collaboration platform
- Assist board initiatives for ISSA chapters desiring partnering or joint events to utilize shared resources for virtual and other face-to-face events
- Assist the board in ways to promote, recognize, and help strengthen chapters through highlighting chapter events and accomplishments

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

Director Candidate

## Mary Ann Davidson

Mary Ann Davidson is the chief security officer at Oracle Corporation, responsible for Oracle software security assurance. She represents Oracle on the board of directors of the Information Technology Information Sharing and Analysis Center (IT-ISAC), has been named one of *Information Security*'s top five "Women of Vision," is a Federal 100 award recipient from *Federal Computer Week*, and has been named to the ISSA Hall of Fame. She has served on the Defense Science Board and as a member of the Center for Strategic and International Studies Commission on Cybersecurity for the 44th Presidency. She has testified on cybersecurity to the US House of Representatives (Energy and Commerce Committee; Armed Services Committee; and Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology) and the US Senate Committee on Commerce, Science, and Technology.

Ms. Davidson has a BSME from the University of Virginia and an MBA from the Wharton School of the University of Pennsylvania. She has served as a commissioned officer in the US Navy Civil Engineer Corps.

### Statement of Goals

Many ISSA members work in regulated industries; the rest of us soon may, as incipient cybersecurity legislation emerges in multiple countries. While regulatory compliance is not optional—and often crowds out "real security"—we nonetheless have no choice but to meet it. The degree to which we can leverage other's experiences and knowledge in these areas helps us be smarter, faster. Furthermore, we must—without necessarily becoming a "lobby group"—weigh in on public policy issues that affect us as security practitioners, particularly as most regulators do not understand the practical limits of security and often have no idea of the cost of mandated measures vs. tangible benefits from those measures.

We must also strengthen our "pipeline" of new recruits by targeting universities. The next generation of practitioners may have as much to teach us as we have to teach them and will help us create the "ISSA community of tomorrow." We must use our interaction with universities to help improve security education in multiple disciplines such as computer science, software engineering, and related disciplines (e.g., control systems engineering and for that matter, business school curricula). If we do not change our collective mind-set—which means educational change—there are not enough IT security professionals in the world to secure critical IT-based infrastructure that was never designed as infrastructure.

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

JUNE 15 – JULY 3

Director Candidate

## John Dyson

CISSP, CISA, CISM, CCSP

John Dyson has 25 years of experience within information security in both private industry and government. His expertise includes security operations center support, cloud security, red teaming, incident monitoring, and NIST 800-53 security controls auditing. Currently John is one of the senior technical leaders for the corporate incident response team at a major global firm. He has also spent five years as an adjunct professor for the cybersecurity certification program at the local community college and has published in the *ISSA Journal*.

Through ISSA, John has been fortunate to support programs that promote cyber skills at the high school and college levels. ISSA has opened doors for him to lecture and speak with students about introductory skills and growth paths in the offensive and defensive cyber operations fields. He has had the opportunity to teach CISSP courses for ISSA, represent ISSA as a judge for high school-level cyber competitions, be a guest speaker on the Washington, DC, Federal News Radio, work with multiple ISSA chapters on major security conferences, as well as serve with different boards as the VP of programs in order to attract world-class speakers.

John believes that building a strong connection between experienced security professionals and those new to the field is critical to improving our overall profession. Security experts are passionate about their field, and ISSA brings the experienced security professionals together, giving ISSA the ability to influence and guide the next generation of security expertise.

### Statement of Goals

If elected, John's goals include:

- Promoting projects that generate excitement about the information security field
- Increasing chapter support for conferences and training classes
- Supporting partnerships with schools to promote technical cyber skills

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

Director Candidate

## Alex Grohmann

CISSP, CISA, CISM, CIPT

Alex Grohmann has been a leader in the metro Washington DC/ Northern Virginia information security community for many years and would be honored to continue to serve on the ISSA International board of directors.

Alex has been an active member of the Northern Virginia Chapter (NOVA) since 2003 and the National Capital and Central Maryland Chapters for many years as well. He has served on the NOVA board for over a decade and has held various leadership roles including three terms as president. During Alex's presidency, he created a mentoring program with two local universities and started a Toastmasters chapter.

Mr. Grohmann currently sits on the IT Sector Coordinating Council (IT-SCC), a body designed to help ensure information security concerns are voiced to federal government policy makers. He serves on board of the National Cyberwatch Center (NCC) Information Security Fundamentals Curriculum standards group. He is a board member of Northern Virginia Community College's cybersecurity program advisory committee (2015-present) and a member of the National Institute of Standard's (NIST) National Initiative for Cybersecurity Education (NICE) program (2016-present).

Mr. Grohmann served on the Washington, DC, InfraGard board for four years and is a graduate of the respected FBI Citizens Academy. He is an active STARS mentor to the State of Virginia's cybersecurity accelerator, MACH 37. He frequently speaks at events and has been a guest on the Washington, DC, Federal News Radio multiple times.

During his term as at-large director on the ISSA International board since 2018, he created the regulatory committee, a task force designed to explore and evaluate new and emerging laws and regulations effecting the information security industry.

Mr. Grohmann is an ISSA International Fellow and a 2015 honoree of ISSA's Honor Roll. Mr. Grohmann is an independent security consultant and his clients range from financial services to energy to health care. He has been in technology for over 25 years and information security for the last 17.

### Statement of Goals

Mr. Grohmann's goals, if re-elected include:

- Enhancing communications and information sharing among the chapters
- Creating regional and section working groups of chapter leaders
- Improving chapter resources for items such as membership engagement, management of chapter meeting registration, and board polices and procedures (including the updating of bylaws)

Video link: Click here.

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

JUNE 15 – JULY 3

Director Candidate

## Lee Neely

GMOB, GPEN, GWAPT, GAWN, GPYC, CISSP, CISA, CISM, CRISC

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 cybersecurity courses, and holds several security certifications.

Lee is a current ISSA International board member and past board treasurer. He is a current director for UNCLE Credit Union and holds the CCUB and CCUSC certifications. He is a past president for the (ISC)$^2$ Eastbay Chapter, member of the SANS NewsBites editorial board, SANS analyst, and co-host of Paul's Security Weekly podcast.

### Statement of Goals

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

- Help the board operate effectively, enabling forward progress of strategic initiatives
- Ensure that the board is driving value back to chapters to achieve operational excellence
- Find initiatives to make ISSA the first choice of professional organizations for information security professionals, including relevancy and supporting resources

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

DIrector Candidate

## Michael Rasmussen

GRCP, CCEP, CISSP

Hello! I am Michael Rasmussen, an internationally recognized pundit on governance, risk management, and compliance (GRC). With 27+ years of experience, I help organizations improve risk and compliance processes, design and implement GRC architecture, and select technologies that are effective, efficient, and agile. As a sought-after keynote speaker, author, and advisor I have been referred to as the "Father of GRC" — being the first to define and model GRC in February 2002 as an analyst at Forrester Research.

### Statement of Goals

My goals in serving again on the ISSA International board are to:

- Increase information security's role, presence, and collaboration with other roles such as enterprise/operational risk management, compliance and ethics, legal, and internal audit
- Contribute regular articles to the *ISSA Journal* to assist professionals in communicating and coordinating with other parts of the organization
- Encourage and mentor others in their careers through the Cyber Security Career Lifecycle
- Advocate on behalf of information security professionals to government and standards committees
- Increase partnership with other professional associations
- Assist the international conference in finding and securing sponsors and increase revenue

My time with the ISSA spans my career going back into the 1990s when I founded the ISS Milwaukee Chapter and was the chapter president for several years. I also spent several years on the International board, first as the VP/director of chapter relations, then as VP/director of marketing, and then as the VP/director of standards and public policy. During that time, I contributed to US congressional reports and committees on behalf of the ISSA membership.

Besides my work with the ISSA, I am very involved with other associations in adjacent fields. I am an OCEG Fellow with the Open Compliance & Ethics Group and an Institute of Risk Management Honorary Life Member and global ambassador.

Prior to founding GRC 20/20 Research, I was a vice-president and "Top Analyst" at Forrester Research, Inc. Before Forrester, I led the risk/compliance consulting practice at a professional services firm, and prior to that specific experience managing IT security within commercial organizations. My educational experience consists of a Juris Doctorate in law and a Bachelor of Science in business.

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

JUNE 15 – JULY 3

Director Candidate

## Jimmy Sanders

CISSP, CRISC, CISM

Jimmy Sanders is head of information security at Netflix DVD. Jimmy has spent the better part of two decades securing data and systems from cyber threats and building resilient compliance programs across technology, financial services, and healthcare organizations. At Netflix, he is responsible for managing the security for DVD.com.

In addition to his duties at Netflix, Jimmy has served as the ISSA San Francisco Chapter president since 2014. He also held senior security management roles at organizations that include Samsung, Fiserv, and SAP. He is a Cyber Security Committee advisor for Merritt College and Ohlone College as well as on advisory boards for other colleges and non-profit movements.

Jimmy Sanders maintains the certifications of Certified Information Systems Security Professional (CISSP), Certified in Risk Information and Information Systems Control (CRISC), and Certified Information Systems Manager (CISM). He holds degrees in psychology and behavioral science from San Jose State University.

### Statement of Goals

My goal is to bring enthusiasm, energy, and innovative ideas to the International board.

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

# Ethical Hacking from Vulnerability Scanning to Adversary Emulation

By Jorge Orchilles – ISSA Fellow, South Florida Chapter

PRE-PROFESSIONAL I ISSA ENTRY LEVEL II ISSA MID-CAREER III ISSA

**One continually hears "ethical hacking" or "offensive security" terminology used incorrectly by regulators, customers, etc. This article attempts to clarify the definition so that we can all speak and push the industry to use the correct terminology.**

### Abstract

One continually hears "ethical hacking" or "offensive security" terminology used incorrectly by regulators, customers, etc. This article attempts to clarify the definition so that we can all speak and push the industry to use the correct terminology. These assessments are performed with a common goal: to provide business value. It is key to understand the needs of the regulator or customer before providing an ethical hacking service. We will cover the very basics of ethical hacking through the bleeding edge along with what tools can be used for each: vulnerability scanning, vulnerability assessment, vulnerability management, penetration testing, red team, purple team, and adversary emulation. These ethical hacking assessments rely on people (ethical hackers), process, and technology (tools). Our focus will be on the best tools for each with highlights of processes, frameworks, and methodologies.

## Hacking and ethical hacking

The traditional definition of a hacker is a skilled individual who uses technical knowledge to overcome a problem. Unfortunately, the same dictionary, Merriam-Webster, has another definition of hacker as "a person who illegally gains access to and sometimes tampers with information in a computer system" [4]. For that reason, the information security industry started using the term *ethical hacker* to define someone with these skills that has permission to asses a target system or organization, permission being the keyword that differentiates between ethical and malicious, often called white hat and black hat, respectively. As an industry, we define an ethical hacker as a person who hacks into a computer network in order to test or evaluate its security. The main goal is to provide business value by improving the security of the organization.

There are many assessments an ethical hacker can perform against a target organization. Each has a different definition, goal, process, and tool set. We will cover them in the order most organizations implement them by covering the most basic ethical hacking assessments through the most advanced. This is not a formal maturity model but may be applied as such.

## Vulnerability scanning

Scanning an organization for vulnerabilities with an automated scanner is the simplest of ethical hacking assessments one can perform. Scanners can be configured as blackbox, where they do not log into the target system; whitebox, where the scanner authenticates to the target system with credentials via SMB or SSH; or agent based, where an agent is installed on the target system to call back to the management server.

- **Definition:** Automated (tool-based) scanning against assets (IPs or applications)
- **Goal:** Identify low hanging, known vulnerabilities pre- or post-authentication
- **Effort:** Small, requires tool investment
- **Focus:** Technology vulnerabilities, patches, configuration
- **Frequency:** Weekly to monthly
- **Customer:** System owners and operations teams
- **Process:** Point a network vulnerability scanner at some IPs. Point a web application vulnerability scanner at a website
- **Tools:** Tenable Nessus, Rapid7 InsightVM, Qualys, IBM AppScan, Burp Pro and MicroFocus Fortify WebInspect

There are many tools that perform vulnerability scanning and by far the largest market due to the simplicity and low requirement of skilled ethical hackers to operate the tools. The reports these tools provide are long and use the default risk ratings, which offers low value to business. Blackbox scans are prone to false positives as results are based on signature matching. My favorite is Tenable Nessus as the industry's most popular network vulnerability scanner. On the web application side, I have come to love Burp Pro scanning feature over the more expensive options.

**Ethical Hacker Tools**

| | | |
|---|---|---|
| ATT&CK | CVE | Navigator |
| AttackerKB | VSS | Nessus |
| C2Matrix | Metasploit | SCYTHE |

## Vulnerability assessment

With a vulnerability scan completed, an ethical hacker can validate the vulnerabilities manually to remove false positives and calculate an accurate risk rating. Vulnerabilities are assigned a Common Vulnerabilities and Exposure (CVE) ID and this is generally the starting point from a vulnerability scan result.

- **Definition:** Automated and manual assessment of assets in scope to find security vulnerabilities, which may or may not be used to get in or steal data
- **Goal:** Identify ALL vulnerabilities from assets in scope
- **Effort**: ~30 percent tools based and ~70 percent manual testing
- **Focus:** Assessments are broader and often include explicit policy and procedure reviews
- **Frequency:** Once per year or once per certification of product/version
- **Customer:** System owners, operations, engineers, application stakeholders
- **Process:** Verify each vulnerability identified by the vulnerability scanner
- **Tools:** Client-side tools that connect to the services in scope. For web applications, HTTP proxies such as Burp or OWASP ZAP

In a vulnerability assessment, the ethical hacker must verify the identified vulnerabilities, removing false positives, and calculating the correct risk score. The tools used are based on the service that the scanner deemed to be vulnerable. For example, if FTP is found, an FTP client may be used to verify the service and various configurations that may be vulnerable. For web applications, manual verification is done through HTTP proxies; my favorite is Burp Pro followed closely by OWASP ZAP.

## Vulnerability management

At a high level, your organization should be patching at the same pace that the vendor releases patches. For example, Microsoft has patch Tuesday on the second Tuesday of every month. By the time the second Tuesday of the month comes, you should be fully patched with the patches released the previous month. Oracle does it quarterly. Prioritization then focuses on the real, urgent vulnerabilities that need to be patched at a much faster timeline than the "business as usual" [7]. There are various tools available to prioritize the patching of vulnerabilities.

- **Common vulnerability scoring system** (CVSS) – this is the industry standard and every CVE has a CVSS base score calculated and posted to the National Vulnerability Database (NVD) [5] – Ethical hackers should then calculate the temporal and environmental score for their organization
- **Exploit predictability scoring system** – new research presented at Blackhat 2019 to try and determine, through algorithms, the vulnerabilities most likely to be exploited – this is a new working group and work in progress [3]
- **AttackerKB** – new crowdsource, community project by Rapid7 where ethical hackers assess various vulnerabilities and determine attacker value and exploitability – yours truly was a beta tester and this site is now open to the public
- **Tenable vulnerability priority rating** – solution from Tenable for customers of Nessus that rates vulnerabilities based on two components: technical impact and threat [13]
- **Rapid7 real risk score** – solution from Rapid7 for customers of InsightVM that calculates scores based on the likeliness of an attacker exploiting the vulnerability in a real attack [8]
- **FireEye risk rating** – cyber threat intelligence-based rating performed manually by FireEye analysts based on impact and mitigating factors [11]

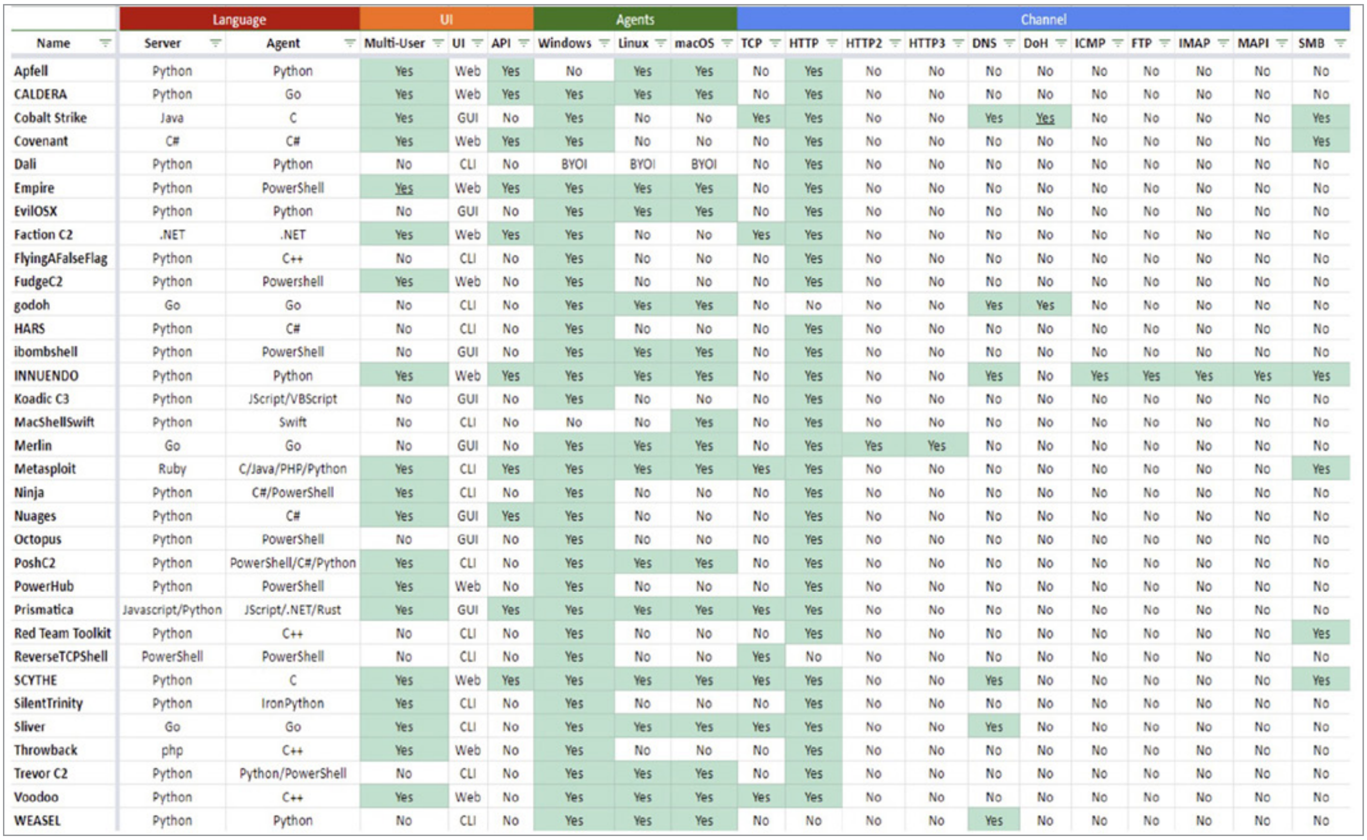
## Penetration testing

Penetration testing goes a step further and exploits the vulnerabilities identified. This is the main differentiator from vulnerability assessment and penetration testing. Penetration testing involves gaining access to the target system through exploitation, further removing false positives, and calculating business risk.

- **Definition:** involves exploiting vulnerabilities under controlled circumstances in a professional, safe manner according to a carefully designed scope and rules of engagement
- **Goal:** Report all exploitable vulnerabilities and calculated business risk
- **Effort:** ~10 percent tools based and ~90 percent manual testing
- **Focus:** Technology and preventive controls
- **Frequency:** ~Once per year
- **Customer:** System owners, operations, engineering, and application stakeholders
- **Process:** Penetration Testing Execution Standard, Open Source Security Testing Methodology Manual, OWASP Testing Guide
- **Tools:** Metasploit, Immunity CANVAS, Core Impact

Penetration testing is mostly manual and requires ethical hackers to find exploits for the identified vulnerabilities so that they may exploited. My favorite tool for exploitation is the tool that has an exploit for the vulnerability I am targeting. When I teach the SANS Penetration Testing course [12], I always comment that if I could only use one tool during a penetration test, it would be Metasploit.

Metasploit has auxiliary modules that allow scanning, fuzzing, and brute forcing, among other items. It has over 1000 exploits already built in but can be used to identify vulnerabilities and create your own exploits. Those exploits need a payload to execute once successful and Metasploit also has many payloads, including the Metasploit interpreter, aka



| | Language | | UI | | | Agents | | | Channel | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Name | Server | Agent | Multi-User | UI | API | Windows | Linux | macOS | TCP | HTTP | HTTP2 | HTTP3 | DNS | DoH | ICMP | FTP | IMAP | MAPI | SMB |
| Apfell | Python | Python | Yes | Web | Yes | No | Yes | Yes | No | Yes | No | No | No | No | No | No | No | No | No |
| CALDERA | Python | Go | Yes | Web | Yes | Yes | Yes | Yes | No | Yes | No | No | No | No | No | No | No | No | No |
| Cobalt Strike | Java | C | Yes | GUI | No | Yes | No | No | Yes | Yes | No | No | Yes | Yes | No | No | No | No | Yes |
| Covenant | C# | C# | Yes | Web | Yes | Yes | No | No | No | Yes | No | No | No | No | No | No | No | No | Yes |
| Dali | Python | Python | No | CLI | No | BYOI | BYOI | BYOI | No | Yes | No | No | No | No | No | No | No | No | No |
| Empire | Python | PowerShell | Yes | Web | Yes | Yes | Yes | Yes | No | Yes | No | No | No | No | No | No | No | No | No |
| EvilOSX | Python | Python | No | GUI | No | Yes | Yes | Yes | No | Yes | No | No | No | No | No | No | No | No | No |
| Faction C2 | .NET | .NET | Yes | Web | Yes | Yes | No | No | Yes | Yes | No | No | No | No | No | No | No | No | No |
| FlyingAFalseFlag | Python | C++ | No | CLI | No | Yes | No | No | No | Yes | No | No | No | No | No | No | No | No | No |
| FudgeC2 | Python | Powershell | Yes | Web | No | Yes | No | No | No | Yes | No | No | No | No | No | No | No | No | No |
| godoh | Go | Go | No | CLI | No | Yes | Yes | Yes | No | No | No | No | Yes | Yes | No | No | No | No | No |
| HARS | Python | C# | No | CLI | No | Yes | No | No | No | Yes | No | No | No | No | No | No | No | No | No |
| ibombshell | Python | PowerShell | No | GUI | No | Yes | Yes | Yes | No | Yes | No | No | No | No | No | No | No | No | No |
| INNUENDO | Python | Python | Yes | Web | Yes | Yes | Yes | Yes | No | Yes | No | No | Yes | No | Yes | Yes | Yes | Yes | Yes |
| Koadic C3 | Python | JScript/VBScript | No | GUI | No | Yes | No | No | No | Yes | No | No | No | No | No | No | No | No | No |
| MacShellSwift | Python | Swift | No | CLI | No | No | No | Yes | No | Yes | No | No | No | No | No | No | No | No | No |
| Merlin | Go | Go | No | GUI | No | Yes | Yes | Yes | No | Yes | Yes | Yes | No | No | No | No | No | No | No |
| Metasploit | Ruby | C/Java/PHP/Python | Yes | CLI | Yes | Yes | Yes | Yes | Yes | Yes | No | No | No | No | No | No | No | No | Yes |
| Ninja | Python | C#/PowerShell | Yes | CLI | No | Yes | No | No | No | Yes | No | No | No | No | No | No | No | No | No |
| Nuages | Python | C# | Yes | GUI | Yes | Yes | No | No | No | Yes | No | No | No | No | No | No | No | No | No |
| Octopus | Python | PowerShell | No | GUI | No | Yes | No | No | No | Yes | No | No | No | No | No | No | No | No | No |
| PoshC2 | Python | PowerShell/C#/Python | Yes | CLI | No | Yes | Yes | Yes | No | Yes | No | No | No | No | No | No | No | No | No |
| PowerHub | Python | PowerShell | Yes | Web | No | Yes | No | No | No | Yes | No | No | No | No | No | No | No | No | No |
| Prismatica | Javascript/Python | JScript/.NET/Rust | Yes | GUI | Yes | Yes | Yes | Yes | Yes | Yes | No | No | No | No | No | No | No | No | No |
| Red Team Toolkit | Python | C++ | No | CLI | No | Yes | No | No | No | Yes | No | No | No | No | No | No | No | No | Yes |
| ReverseTCPShell | PowerShell | PowerShell | No | CLI | No | Yes | No | No | Yes | No | No | No | No | No | No | No | No | No | No |
| SCYTHE | Python | C | Yes | Web | Yes | Yes | Yes | Yes | Yes | Yes | No | No | Yes | No | No | No | No | No | Yes |
| SilentTrinity | Python | IronPython | Yes | CLI | No | Yes | No | No | No | Yes | No | No | No | No | No | No | No | No | No |
| Sliver | Go | Go | Yes | CLI | No | Yes | Yes | Yes | Yes | Yes | No | No | Yes | No | No | No | No | No | No |
| Throwback | php | C++ | Yes | Web | No | Yes | No | No | No | Yes | No | No | No | No | No | No | No | No | No |
| Trevor C2 | Python | Python/PowerShell | No | CLI | No | Yes | Yes | Yes | No | Yes | No | No | No | No | No | No | No | No | No |
| Voodoo | Python | C++ | Yes | Web | No | Yes | Yes | Yes | Yes | Yes | No | No | No | No | No | No | No | No | No |
| WEASEL | Python | Python | No | CLI | No | Yes | Yes | Yes | No | No | No | No | Yes | No | No | No | No | No | No |

**Figure 1 – The C2 Matrix has a list of 40+ command and control frameworks along with their capabilities and features**

Meterpreter. Lastly, Metasploit has post modules for post-exploitation, which make it a favorite. Immunity CANVAS and Core Impact have some but not all the mentioned features.

## Red team

There are many debates on the definition of red team. Red Team Journal published this definition: "the practice of looking at a problem or situation from the perspective of an adversary" [10]. What is not debated is red team origins coming from military [1]. In the commercial sector of information security, red team is an independent group that, from the perspective of a threat or adversary, explores alternative plans and operations to challenge an organization to improve its effectiveness [9]. In information security, red team has a major focus on training and improving people, process, and technology. The only way to do red team wrong is to ignore the blue team. Red team focuses on testing the defenders, detection, and alerting.

- **Definition:** Red team emulates tactics, techniques, and procedures (TTPs) of adversaries to improve the people, processes, and technology in the target environment
- **Goal:** Make blue team better – Train and measure that blue team's detection and response policies, procedures, and technologies are effective
- **Effort:** Manual, some red team automation tools
- **Focus:** Detective controls, testing the defenders
- **Frequency:** Intelligence-led (new exploit, tool, or TTP)
- **Customer:** Blue teams, defenders
- **Process:** A framework for the regulatory use of penetration testing and red teaming in the financial services industry by Global Financial Markets Association [2]
- **Tools:** C2 Matrix, Cobalt Strike

There are so many tools available for emulating TTPs that I co-created an open source and community-driven project called the C2 Matrix. It stands for the Command and Control (C2) Framework Matrix. Command and control is one of the most important tactics in the MITRE ATT&CK matrix as it allows the attacker to interact with the target system and realize their objectives. There are many command and control frameworks available to emulate TTPs and this matrix documents the C2 capabilities, features, and detections for them (see figure 1). Choosing a favorite is difficult as they have different features that may be valuable to test against the target organization. For this reason, the C2 Matrix is my favorite tool as it allows me to choose the best framework to achieve the target business goals. It currently has 45 different C2s documented.

## Purple team

Purple team is a virtual team made up of the red team and the blue team. The blue team are the defenders in an organization entrusted with identifying and remediating attacks, generally associated with security operations center or managed security service provider (MSSP), hunt team, incident response, and digital forensics. The main difference is that a purple team exercise is non-blind, meaning the red team shows the blue team all TTPs performed and the blue team shows red team how they defend.

- **Definition:** A function, or virtual team, where red and blue teams work together to improve the overall security of the organization – Red team does not focus on stealth as they normally would
- **Goal:** Red team emulates adversary TTPs while blue teams watch and improve detection and response policies, procedures, and technologies in real time
- **Effort:** Manual
- **Frequency:** Intelligence-led (new exploit, tool, or TTP)
- **Customer:** Red team and blue team
- **Process:** Like red team process but fully disclosing to purple team
- **Tools:** C2 Matrix, SCYTHE

There are many tools available that simulate TTPs for purple team exercises. I prefer to use the same red team tools and focus the purple team exercise on the process. I did a presentation on performing high-value purple team exercises and provided a list of over 20 tools at the inaugural SANS Purple Team Summit. A post on medium has the video and list of tools [6]. We performed a breach and attack simulation (BAS) vendor shootout and chose to go with SCYTHE as it emulates the TTPs consistently, a very important requirement during purple team exercises.

## Adversary emulation

An adversary emulation is a cyber threat intelligence-led exercise that can be performed as a red team engagement or a purple team exercise. The main difference is that an adversary with the capability, intent, and opportunity to attack the target organization must be selected. Once selected, it is especially important to understand how the adversary functions and the TTPs they use. With that completed, an adversary emulation plan may be created.

- **Definition:** A type of red team exercise where the red team emulates how an adversary operates, following the same tactics, techniques, and procedures (TTPs), with a specific objective similar to those of realistic threats or adversaries
- **Goal:** Emulate an end-to-end attack against a target organization – Obtain an holistic view of the organization's preparedness for a real, sophisticated attack –Improve overall security in organization
- **Effort:** Mostly all manual except for a couple adversary emulation tools
- **Frequency:** Twice a year or yearly
- **Customer:** Entire organization
- **Process:** MITRE ATT&CK, Unified Cyber Kill Chain
- **Tools:** ATT&CK Navigator, C2 Matrix, SCYTHE

Mapping the adversary TTPs to MITRE ATT&CK is a great start for an adversary emulation and can be performed with MITRE ATT&CK Navigator. With that mapping complete, an adversary emulation plan can be created and emulated by the red team (see figure 2). The red team would use tools that the adversary would use. This was the original use case for creating the C2 Matrix. My favorite tool for doing adversary emulation in a consistent and repeatable fashion is SCYTHE.

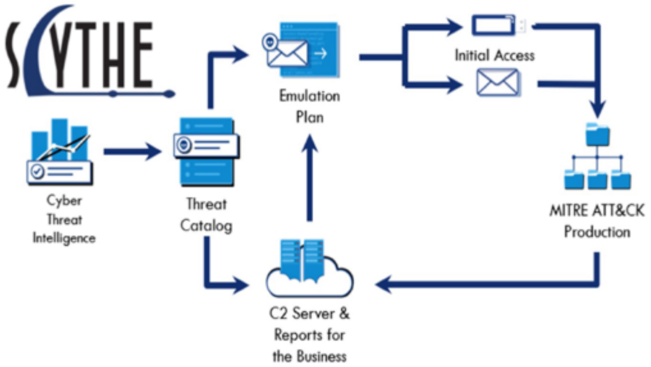


**Figure 2 – SCYTHE leverages cyber threat intelligence to create campaigns that emulate adversaries and map to MITRE AT&CK.**

## Conclusion

It is important that we, as an industry, use the correct terminology. There are differences between these types of assessments, goals, and tools but the focus is to bring business value. Some organizations have matured following similar steps, from vulnerability scanning to adversary emulation, while others are in progress. Like everything in information security, there is no end state. Keep pushing to evolve from CVE to TTP as we all know we will be breached; the question lies in how we will respond. Please feel free to reach out and stay safe.

### References

1. 4n7m4n,"Red Teaming: From the Military to Corporate Information Security Teams," Medium – https://medium.com/@antman1P_30185/red-teaming-from-the-military-to-corporate-information-security-teams-408c040bd87e.
2. GFMA,"GFMA Framework for the Regulatory Use of Penetration Testing in the Financial Services Industry," Global Financial Markets Association – https://www.gfma.org/correspondence/gfma-framework-for-the-regulatory-use-of-penetration-testing-in-the-financial-services-industry/.
3. Jacobs, Jay et al, "Exploit Prediction Scoring System (EPSS)," Arvix – https://arxiv.org/ftp/arxiv/papers/1908/1908.04856.pdf.
4. MW, "Hacker," Merriam-Webster – https://www.merriam-webster.com/dictionary/hacker.
5. NVD NIST, "National Vulnerability Database," NIST – https://nvd.nist.gov/.

6. Orchilles, Jorge. “Purple Team Exercise Tools,” Medium – https://medium.com/@jorgeorchilles/purple-team-exercise-tools-a85187ce341.

7. Orchilles, Jorge. “Vulnerability Management Is Hard! How Do You Prioritize What to Patch? Medium – https://medium.com/@jorgeorchilles/vulnerability-management-is-hard-how-do-you-prioritize-what-to-patch-1fc8e163d740.

8. Rapid7, ”Prioritize Vulnerabilities Like an Attacker,” Rapid7 – https://www.rapid7.com/products/insightvm/features/real-risk-prioritization/.

9. Red Team, “Red Team Development and Operations: Definitions,” Red Team Guide – https://redteam.guide/docs/definition-lexicon/.

10. RTJournal, “Climbing the Red Teaming Ladder,” Red Team Journal – https://redteamjournal.com/blog/2018/11/climbing-the-red-teaming-ladder.

11. Sabel, Cameron and Jared Semrau,“Separating the Signal from the Noise: How Mandiant Intelligence Rates Vulnerabilities — Intelligence for Vulnerability Management, Part Three,” FireEye, April 20, 2020 – https://www.fireeye.com/blog/threat-research/2020/04/how-mandiant-intelligence-rates-vulnerabilities.html.

12. ANS, “SEC560: Network Penetration Testing and Ethical Hacking,” SANS – https://www.sans.org/course/network-penetration-testing-ethical-hacking.

13. Tai, Wei. “What Is VPR and How Is It Different from CVSS?” Tenable – https://www.tenable.com/blog/what-is-vpr-and-how-is-it-different-from-cvss.

### About the Author

*Jorge Orchilles, MS, led the offensive security team in a large financial institution for 10 years; is a SANS Certified Instructor; author of SANS SEC564: Red Team Exercises and Adversary Emulation, co-author of CVSSv3.1 and a threat-led penetration testing framework; C2 Matrix project lead; and 2020 NSI Technologist Fellow. He can be reached at jorge@orchilles.com.*

## Can You Handle a Nation-State Cyber Attack

**Continued from page 10**

curity team at all levels. Hiring skilled workers is notoriously difficult, so they wanted to make sure the team’s skills were constantly improving and second to none. This, too, requires real-world training—the same type of immersive training NATO has created. For businesses, immersive cyber training is new. Experientially, it is a lot more like pilot simulator training than sitting in a classroom. Defenders work in realistic sessions and gain the skills needed to understand how attacks are unfolding and how to execute effective containment activities. The learning experience is called “gamified,” meaning it is interactive and keeps the defender’s attention.

According to Ian Quinn, director, joint operations center and head of global security education, outreach and awareness at Barclays, “As sophisticated attacks unfold, communication and process breakdowns occur because no previous generation training classes can prepare for them. Cyber range blue team exercises are simply the only way to surface and identify critical deficiencies. Immersive cyber skills training is a high-intensity endeavor that quickly uncovers gaps in skills and processes, enhances individual learning and cross-team collaboration, and feeds the data into a system for ongoing learning.”

Barclays’ approach begs the question: Can a company that embraces this operational training approach to cybersecurity stop a nation-state attack? In the end, no one is immune. There will simply never be enough technology to protect desirable targets. But the Barclays team has applied continuous training, assessments, and simulations to confront the most dangerous adversaries. In the process, it has increased their chances of effectively recognizing and taking immediate corrective actions to disrupt and contain them.

### About the Author

*Gordon Lawson is president at RangeForce. He has nearly two decades of experience in the security sector with a focus on SaaS optimization and global enterprise business development. He is a graduate of the US Naval Academy and holds an MBA from George Washington University. He may be reached at gordon@rangeforce.com.*

# Orchestrating Communication Cadence in Hybrid Environments

Continued from page 8

### Managing remotely

Managing hybrid teams involves establishing communications around multiple platforms. Setting a rhythm for preferences of platforms may take some thought. For example, the preference for meeting may be ZOOM or Teams. For back and forth instant messaging (IM), the preference may be Teams, Slack, or similar. For sending attachments and informational directives, email may be preferred. For status of availability, on a call, currently off line, it may be helpful to establish some guidelines rather than "hit and miss" or trial and error using any or all of these.

On the website Remote.co, job posting advertisers mention a range of communication preferences for managing teams.[3] Some have hard and fast rules around response times and promote "core hours" where everyone should be available, and others rely on a platform's user status "being online," looking to see if the person is engaged in a meeting, taking a break, or on a project. Gauging how your team feels is important. Do they feel connected or invisible? Many remote companies say that sharing internal emails to team members for stories of fun or family times works well and scheduling team "social hours" on Teams or Zoom to share binge-watching favorites and other past times while being remote. Seeing others in their work environments and casual clothes creates a spirit of camaraderie, even on ZOOM.

### Hybrid environment

Many companies are now considering a semi-to-permanent hybrid environment of both on-premise and remote teams. Leaders may fear a possible crack in the culture from mixed environments of remote and on premise teams. A hybrid model may even help organizations develop their culture in a more considerate way than they otherwise would, but it will take proactive effort. It is important to address both working arrangements as remote workers may feel isolated as teams go back to work, and teams that go back to work may be uncomfortable in a socially distanced environment after being at home. It is important to have the communication platforms orchestrated for all types of teams. Taking time to establish this will create efficiencies for everyone.

### Hybrid meetings

Where employees once sat side by side in conference rooms or meeting spaces or even traveled to attend quarterly events/conferences, organizations have now re-imagined virtual participation such as joining video or conference calls for team meetings. The pandemic also propelled a surge in "all hands calls," state-of-the-union calls, and weekly virtual team meetings. These attempts have done a great job in keeping everyone connected, displaying transparency, and making the work visible.

In returning to the office, companies will be socially distancing meetings and how employees sit together. Some companies are staffing by percentage where no more than 30 percent of workers are there on the same day. Hybrid meetings will continue to be a mix of where folks are physically located but will stay connected through the orchestration of media platforms.

### Conclusion

During the pandemic and after it is behind us, establishing communication preferences over media platforms will allow our workforce orchestra to play from the same page. For both remote and hybrid cybersecurity teams, these guidelines can set examples and define success for all to follow. During the first half of 2020, we may have learned by "hit and miss," making adjustments on the fly while sheltering in place. But in the latter half of 2020, cybersecurity teams who quickly orchestrate their communications symphony to embrace a hybrid environment will create big gains for the future.

## About the Author

*Dr. Curtis C Campbell is VP of Atlantic Capital Bank in Atlanta, GA, and chapter president of ISSA Chattanooga. She is a cybersecurity author with 25 years experience in information security, compliance, procurements, and third-party risk in the enterprise. Connect with Curtis via curtis@mprotechnologies.com.*

[3] Remote.co. "Can a Remote Friendly Company Have a Healthy Culture?" https://remote.co/qa-leading-remote-companies/can-a-remote-company-have-a-healthy-company-culture.

# Why Top Management Must Now Stop the Drift to Chaos and Disorder

**By Charles Cresson Wood** – ISSA member, San Francisco Chapter **and Perry Carpenter**

**Entropy is a law of nature which specifies that, over time, unless work is undertaken to reverse the trend, things will wind-down, become disorganized, and move into what appears to us to be chaos. This article discusses the need for the new management techniques that must be adopted to reverse the drift into entropy.**

### Abstract

Entropy specifies that over time, unless work is undertaken to reverse the trend, things will wind down, become disorganized, and move into what appears to us to be chaos. The habitual application of old-fashioned management techniques to the information security and privacy area provides an invitation for entropy to proceed in dangerous and ill-advised ways. In this article, we discuss that trend and the need for the new management techniques that must be adopted to reverse the drift into entropy.

## Static approaches don't "cut it" anymore

It's called the second law of thermodynamics—more colloquially it's called *entropy*. In physics terms, if an isolated system is just left to do what it has been doing, it will devolve over time toward chaos and disorder (technically, the lowest energy point or equilibrium). The same principle holds true for our physical bodies—at all times, we are either building strength or allowing atrophy. Switching from physics and kinesiology to information security and privacy, we can see how this same law plays out in the world of government and business. Sometimes the devolution toward entropy is dramatic and sudden, for example, when a hacker owns an organization's systems and uses ransomware to demand millions in bitcoin, bringing internal operations at the victim firm to a halt for months. This is what happened to the City of Baltimore, Maryland [1]. Sometimes the devolution toward chaos and disorder is quiet and drawn-out, as would be the case when Internet-facing systems containing proprietary and/or personal data are no longer patched as they should be. This is what happened at Equifax [4]. In that latter case, hackers were resident within the compromised system for two months, and the case led to the unauthorized release of 147 million personal credit history records, and a settlement with the Federal Trade Commission (FTC) of $425 million.

In days gone past, information security and privacy efforts were thought of as a project, for example, an effort to come into conformity with a particular technical standard like ISO 27000, or a business standard such as the Payment Card Industry Data Security Standard, and/or to come into compliance with a particular law, such as the General Data Protection Regulation. Often, in the minds of top management, these efforts were resentfully undertaken, and often considered both a "necessary evil" and a cost of doing business. For example, management has frequently considered information security and privacy to be a hurdle that needed to be cleared to procure a new piece of business. More recently, management has set aside a line-item budget amount, which is then incurred annually, supposedly to keep things running smoothly. This budget was also often begrudgingly granted because the information security and privacy activities were perceived as making zero contribution to profits, or worse, as a drain on profits.

With both of these just-mentioned management viewpoints, management perceives information security as a static activity, as a stable and readily-delineated activity that can be pigeonholed into the budgeting process and forced to conform to the traditional management approaches used to manage other departments, which for the most part are considerably more stable in nature (such as accounting and finance). The reliance on historical management methods such budgets, project lists, and status reports—many of which have static assumptions behind them—unfortunately isn't working well at all, and management must now get considerably more personally involved.[1] This new approach must be accompanied by the adoption and the deployment of new dynamic management tools in order to support and sustain this expanded level of personal involvement.[2] Overcoming entropy always requires the application of new effort. And that new effort, in the information security and privacy field, now requires the adoption of a host of new, dynamic, learning, and evolving management tools. This article addresses that important shift.

Being more specific to the realm of information security and privacy, static management approaches can be exemplified by traditional contingency plans that provide a backup data center, backup network systems, backup hardware, cut-over procedures, and up-to-date copies of important software, databases, and files. This approach is largely static and passive, just waiting to be used. Sure this traditional approach gets updated annually (at least hopefully it does), but it is not proactive; it does not dynamically identify emerging problems; it does not learn about new attacks as they are happening; and it is not creating new defenses "on the fly" so as to deal with new attacks.

The new proactive, learning, dynamic, and getting-ever-stronger defense approach needs to be leveraging artificial intelligence, big data machine learning, and related tools to not only spot problems before they become losses, but also create defenses before they are required. These new dynamic evolving tools not only protect systems and information without human involvement, but they automatically evaluate their own effectiveness and efficiency and also collect data that can empower humans to better monitor those systems and then decide when, where, how, why, and with whom the systems should be used.

## A crisis-provoked inflection point

Researchers at many health care organizations have been repeatedly urging governments to better prepare for pandemics [7]. As David Quammen indicates in his noteworthy book entitled *Spillover: Animal Infections and the Next Human Pandemic* [5], when the decision-makers in government are not immediately confronted with a problem, they typically cut the budget of those agencies that are charged to look after

## The Open Forum

The Open Forum is a vehicle for individuals to provide opinions or commentaries on infosec ideas, technologies, strategies, legislation, standards, and other topics of interest to the ISSA community. Open Forum articles are not intended for reporting news; they must provide insight, opinion, or commentary to initiate a dialog as to be expected from an editorial. Articles should be around 850 words and include a short bio and photo. Please submit to editor@issa.org. Note that accepted articles may be eligible for CPE credits.

[1] In many cases, this greater level of involvement is not an option; it is required by law. Not only must management be aware of the nature of the work, delegating the work, and properly supervising and governing that work, but there are certain legal duties that cannot be delegated. In this latter category is the legal duty to pay attention to an area where the work carries an inherent risk of serious harm. Since computers and networks are used pervasively these days, that deployment often carries an inherent risk of serious harm (of course, information security and privacy are used to deal with that potential harm). See *Maristany v. Patient Support Servs., Inc.*, 264 A.D.2d 302, 303 (N.Y.S. 1999) while the principal has no duty to control the conduct of third parties, so as to prevent them from harming others, if the principal knew or had reason to believe that the independent contractor was not properly qualified, then liability of the principal may be established; *Bellere v. Gerics*, 304 A.D.2d 687 (N.Y.S. 2003) if the principal knew of the independent contractor's propensity for the conduct that caused an injury, he or she may be held liable.

[2] The need for further personal involvement of the directors and officers of all organizations is in evidence in the National Association of Corporate Directors (NACD) report entitled "2017-2018 Public Company Governance Survey Executive Summary," p. 6. That report indicated that only 37 percent of directors were confident or very confident that their organization was adequately secured against cyber attacks.

essential functions like pandemic identification, prevention, and response. As with pandemics, the out-of-sight/out-of-mind approach that has often been the case with information security and privacy just doesn't work anymore. The "pick up the pieces after the fact" approach doesn't work anymore either. It's time for us to all step up and be considerably more proactive than we have been in the past.[3] The stakes are just now too high for us to believe that the old-fashioned static management approaches are up to effectively doing the work that must now be done.

Collectively, we have reached a most serious crisis-provoked inflection point, where top management and board of directors must get personally involved and also make addressing this area both a priority and on-going part of their jobs. As is the situation with pandemics, the information security and privacy area is clearly not static. Information security and privacy does not simply occur, then get handled, and then allow management to move on. Pandemics, like information security and privacy, must now be addressed all the time; not just in a traditional static rigid fashion, but with a new dynamic rapidly evolving approach. That approach must employ approaches that repeatedly break out of old molds, repeatedly stretch into new domains, and repeatedly reinvent themselves and adapt. For example, we are going to most likely need a contact tracing system based on cell phones so as to enable the rapid identification and successful containment of pathogens that could be the cause of future pandemics.[4]

The serious warnings about something like the current COVID-19 pandemic have been there for a long time, writes Quammen. He indicated that government decision-makers have known that this particular type of fatal virus mutates rapidly, and they have known that these viruses often jump from one species to another. In the same way, management decision makers have long known that information security and privacy is a serious problem, an area that can escalate into a crisis without any advance notice, and an area where crisis might even lead to the demise of the organization. Yet, in many organizations there has been a surprising lack of personal involvement and accountability by the higher-ups. Andy Grove, former CEO of Intel, in his book entitled *Only the Paranoid Survive: How to Exploit the Crisis Points that Challenge Every Company* [3], writes about a time of reckoning when every organization must fundamentally change the way it does business because if it does not, the organization will go out of business. For retail bookstores, such a moment occurred when Amazon.com revolutionized the process of selling books to consumers via the Internet. For most every organization, no matter what industry it is in, such a fundamental "inflection point" is now occurring in the information security and privacy area.

This is an all-hands-on-deck moment, where every person within a company, and that includes temporaries, contractors, consultants, and business partners, must work together in a coordinated and aligned way, so as to not only achieve a satisfactory level of information security and privacy, but to

[3] Further confirming the fact that the "wait until there's a problem, and then we'll deal with it" approach is no longer viable is an important report. This multi-industry analysis was undertaken by a military agency because "cybersecurity" is now a national security issue (actually the term "cybersecurity" is unduly restrictive because it requires that a computer be involved, when the real issue is information security and privacy and what happens to information, no matter what form it's in, and no matter how it's handled). See Air Force Research Laboratory, in Rome, New York, *Economic Analysis of Cyber Security*, July 2006, AFRL-IF-RS-TR-2006-227. This report clearly indicates that the economics no longer allow the primary emphasis to be placed on recovery, correction, and mitigation of damage. Instead, all firms must now move to place the primary emphasis on avoidance, prevention, detection, and similar proactive strategies.

[4] The early detection of a threat, and the containment and suppression of that detected threat, is a demonstrably successful approach that shows up in a wide variety of different environments. Just as it is used in the malware detection and eradication process, so too the human body is designed to approach alien substances in a similar way. Specifically, in the human body, white blood cells are mobilized to destroy unknown foreign substances such as viruses, and a scab is then formed over a wound to allow the injured tissue to repair itself without further infection. For further discussion, see Charles Cresson Wood, "The Human Immune System as an Information Security Reference Model," Computers & Security, vol. 6, 1988, pp. 511-516.

sustain and improve that level going forward. When the Federal Trade Commission fines companies $5 billion for breaking the law for not living up to their information security and privacy obligations (and also threatens to make the CEO personally liable) [2], it is clearly a different ball game. Top management and board of directors need to wake-up, pay attention, and get into action. But what specifically should they be doing?

## Start with a clarification of roles and responsibilities up and down the organization

The topic of roles and responsibilities lies at the center of every effective response to a crisis that we confront. Top management and board of directors cannot ever rationally be expected to govern or manage an appropriate effort to address information security and privacy if they are not first of all clear about the roles and responsibilities of the involved individuals and organizations. As is true for the effective response to pandemics, decision makers must understand the essential jobs to be done, and must then expressly assign those jobs to specific individuals, departments, committees, outsourcing firms, business partners, etc.[5] Only when there is clarity about these essential roles and responsibilities is it possible to detect that certain essential roles and responsibilities are not being performed, at which point appropriate remedial action can be taken. Only when there is clarity about these essential roles and responsibilities is it possible to do meaningful performance reviews, to establish new incentive systems that actually bring about sought-after results, to perform audits to determine whether tasks are being done successfully, and to be assured that all duties that are required by law are in fact being adequately performed.[6]

According to the 2019 IBM/Ponemon "Cost of a Data Breach Report," malicious attacks were not only the most-common root cause of breaches, they were the most costly type of data breach as well. The report indicated that the percentage of successful attacks that were attributable to malicious attacks surged from 21 percent in 2014, to 51 percent in 2019. Our systems are being massively overrun by attackers, and it is not surprising given the clearly evident current involvement of both nation-states and organized crime in the ranks of the attackers. These attackers are using all sorts of new and innovative approaches, such as business email compromise to compromise our systems. This very disturbing rise in malicious attacks should be further support for the declaration of this moment as an inflection point when both top management and board of directors must critically re-think the whole area of information security and privacy, and then adopt a new set of more dynamic and responsive management approaches.

Going back to the most-recent "Cost of a Data Breach Report," we are told that the next most common category of breach is attributable to human error. This conclusion is consistent with the 2014 IBM chief information security officer assessment survey, which pegged human error as an issue in 95 percent of information security incidents they examined. In keeping with the latter study's perspective, if the category of human error were to be defined in a broad way, then all breaches could be ultimately be traced back to some sort of human error: the systems designer at the software vendor who specified the software might have made an error; the programmer at that software vendor might have made an error; the quality control analyst who tested that code might have made an error; the systems administrator who installed the software might have made an error; the operator who uses that software every day might have made an error; the end-user who uses the software for business purposes might have made an error. Unless all the roles and responsibilities in the domain of information security and privacy are clearly understood, documented in job descriptions, committee charters, outsourcing contracts, and similar documents, and unless there is adequate training and awareness to support the performance of the tasks related to those roles and responsibilities, human error, in its broadest sense, will continue to be at the heart of the information security and privacy crisis.

No doubt we can all agree that it is desirable to automate a great deal of information security and privacy work, if that type of automation is in fact feasible from a cost-benefit standpoint. But because information security is still a relatively immature field, much of the work cannot currently be automated. That means that if the work is going to be done, much of it must be done by people. Ultimately, automating this work could eliminate many problems due to distractions, overwork, being sick, failure to communicate, decision-making bias, and similar human failings. But at the present time, far too many people have never been clearly charged with doing certain important jobs, and they have not received adequate training and supervision to support them in doing those jobs either, so it is not surprising that they're just not going to be up to the tasks that must now be performed. Eventually, automating this work can also create an environment where an automated transaction is actually more secure and private than a manual transaction could ever be. With automation, we can also create an environment with far more rigorous quality control and operational orchestration—an environment that markedly reduces the incredible complexity now found with most information security and privacy efforts. But before we can automate, we must clarify and organize. We must clearly specify what the work entails that will be automated, and that brings us back to the jobs to be done (roles and responsibilities), and also to rationalizing and coordinating these jobs to be done.

[5] One place to start the rationalization of roles and responsibilities is to employ what is called a RACI matrix (Responsible, Accountable, Consulted, and Informed). Such a rationalization effort is particularly important because the information security and privacy area is not only multi-disciplinary, but also multi-departmental and in most cases also multi-organizational.

[6] It is alarming that only 56 percent of boards believe that they currently receive the information from management that they need in order to make the proper decisions and perform their oversight role. See the National Association of Corporate Directors (NACD), "2019-2020 Public Company Governance Survey." That about half of board members don't believe they are getting what they need to do their jobs is a further indication that the old-fashioned static ways of managing information security and privacy are not working.

## Even in static traditional business language, it's mobilization time

Any way you characterize the current situation—even if you use traditional accounting and finance language—the traditional static ways for managing and governing information security and privacy must now give way to new and more dynamic approaches. Another analogy to the COVID-19 crisis can be made here. With the pandemic we had a high-stakes low-probability event that failed to get adequate decision-maker support and funding. Since the related systems were not improved, entropy was permitted to proceed, and the drift leading to chaos and disorder continued; the net effect of all that was a disturbingly disorganized, too-little-too-late, and largely ineffective effort to contain the virus. Thus, what was a high-stakes low-probability threat has, as a result of allowing the drift to proceed, now become a high-stakes moderate-probability problem. It has become a moderate-probability problem because we must all deal with the virus going forward in time because recurrences of the virus will continue to pop up again and again throughout our lifetimes [6]. This illustrates that not only must a much more dynamic and responsive approach be adopted, but the fact that if leaders do not adopt such an approach, the results may be irreversible.[7]

Similarly, with information security and privacy, in decades past, we faced a moderate-stakes low-probability breach event. But time passed without sufficient action. And that allowed the drift to proceed, and through that the law of entropy prevailed. Thanks to inadequate funding and inadequate top management and board-level support, what we must now contend with is a high-stakes and moderate-probability breach event. For example, the 2019 IBM/Ponemon "Cost of a Data Breach Report" indicates that average cost of a breach in the United States has now reached $8.19 million. This is up 130 percent over the last 14 years. Similarly, the probability of being hit with a data breach over the next two-year period is now 29.6 percent. In the span of the last six years the probability of being hit with such a breach has increased by 31 percent. We must not allow the drift toward entropy to continue. Continuing to simply employ old-fashioned static management and governance approaches is no longer a viable option. We urgently need to shift the way we address information security and privacy; otherwise data breaches will soon become a high-stakes and high-probability event.

## Overcoming Entropy: Embracing a Brave New World of Dynamic Tools

The attackers are now using artificial intelligence and machine learning to attack our systems.[8] We must, likewise, be using dynamic management and governance tools to be able to counter that firepower from our adversaries. For example, our data loss prevention systems must be able to detect, evolve, learn, and reconfigure themselves so as to be able to, in real time, block an exfiltration of sensitive or private data

[7] Irreversibility was the fate of Arthur Andersen, the famous and successful worldwide accounting firm. Andersen did not properly manage the data destruction process associated with its working papers linked to its client, Enron. Working papers that should have been preserved in response to a legal hold order were destroyed. As a result, in 2002, Andersen was charged with and convicted of obstruction of justice in proceedings before the Securities and Exchange Commission (SEC). Even though the conviction was later overturned in a US Supreme Court decision (*Arthur Andersen LLP v. United States*, 544 U.S. 696 (2005)), by that point in time the firm's name had become toxic and it went out of business.

[8] For a discussion about the use of artificial intelligence and machine learning by attackers, see Townsend, Kevin, "DeepPhish Project Shows Malicious AI is Not as Dangerous as Feared," Security Week, December 7, 2018. At the same time, while the posture of information security and privacy is often improved by the use of artificial intelligence and machine learning, this automation is not reducing the need for well-trained personnel. See Ponemon Institute, "Separating the Truths from the Myths of Cybersecurity," June 2018. The fact that we have a "skills crisis" in the information security and privacy field is further indication that roles and responsibilities have not yet been adequately clarified and rationalized, which in turn, as mentioned above, would permit much of the work to be automated.

outside our network. Our intrusion detection systems must be able to catch network-based attacks in real time, before any human could possibly have noticed what was going on, and then proceed according to contingency plans and predetermined scripts (for example immediately shutting down access privileges gained by the attackers, turning on additional logging, notifying certain members of a computer emergency response team, etc.) so that losses are prevented or at least minimized. Our user security awareness and training programs must likewise respond to serious current threats like ransomware and engage users in realistic simulation games and other intriguing life-like interactions so that users can then continue to knowledgeably play the role of first-line defenders of our systems. Similarly, our top management and board members will need to engage in computer-supported realistic simulations of various breach situations so as to be clear not only about what their jobs are, and how to go about making tough decisions, but also to be clear about to whom certain critical tasks will be delegated.

All these new dynamic tools critically depend on a shared understanding of roles and responsibilities in the information security and privacy field. So, here's the critical question: has your organization seriously clarified, rationalized, and documented these roles and responsibilities? If not, now is the time. The attackers won't wait. They are coming for you. And at all times, your organization is either building strength or it is allowing atrophy and entropy.

In terms of where to go from here, we suggest that readers go back over the roles and responsibilities defined in their organizations, as they relate to information security and privacy, and then reassess those assignments in light of the many significant changes recently taking place in the information security and privacy field. Ask yourself whether new tools, techniques, and/or methodologies should be expressly reflected in these roles and responsibilities. Ask yourself whether new organizational structures, new communications structures, and/or new reporting relationships are now in order. Also ask yourself whether critical tasks and activities have been expressly assigned to individuals, committees, projects, departments, and/or third parties. And then consider whether this arrangement of roles and responsibilities actually adjusts and evolves, whether it dynamically adapts, whether it learns over time, and whether it includes mechanisms to proactively deal with problems before they become disasters.

### References

1. Duncan, Ian, "Baltimore Estimates Cost of Ransomware Attack at $18.2 Million as Government Begins to Restore Email Accounts," The Baltimore Sun, May 29, 2019 – https://www.baltimoresun.com/maryland/baltimore-city/bs-md-ci-ransomware-email-20190529-story.html.
2. Fair, Leslie, "FTC's $5 Billion Facebook Settlement: Record-breaking and History-making," Federal Trade Commission business blog, July 24, 2019 – https://www.consumer.ftc.gov/blog/2019/07/what-ftc-facebook-settlement-means-consumers.
3. Grove, Andy, *Only the Paranoid Survive: How to Exploit the Crisis Points that Challenge Every Company,* Random House (2010)
4. Newman, Lily Hay, "Equifax Officially Has No Excuse: A patch That Would Have Prevented the Devastating Equifax Breach Had Been Available for Months," Wired, September 14, 2017 – https://www.wired.com/story/equifax-breach-no-excuse/.
5. Quammen, David, "Spillover: Animal Infections and the Next Human Pandemic," Norton & Company (2012).
6. Resnick, Brian, "How 1oes the Coronavirus Outbreak End? Government's 1ailure to Contain the Virus Means That It May Be Here to Stay," Vox, March 7, 2020 – https://www.vox.com/science-and-health/2020/3/6/21161234/coronavirus-covid-19-science-outbreak-ends-endemic-vaccine.
7. Staples, Jeffrey, "The Science: How a Human Pandemic Could Start," Harvard Business Review, Mary 2006 – https://hbr.org/2006/05/preparing-for-a-pandemic.

## About the Authors

*Charles Cresson Wood, Esq., JD, MBA, MSE, CISM, CISSP, CISA, CGEIT, CIPP/US, is a management consultant and independent compliance auditor specializing in information security and privacy. He has 40+ years of experience in the information security and privacy field and can be reached via dutiesaudit.com.*

*Perry Carpenter, MSIA, CCISO, CCMT, is chief evangelist and strategy officer at KnowBe4, an information security and privacy awareness and training firm. Prior to that position, he led security awareness, security culture management, and anti-phishing behavior management research at Gartner. He can be reached via knowbe4.*

# Sophisticated Tools Alone Cannot Prevent Advanced Persistent Threats: What's Next?

By **Srinivasulu Vuggumudi** – ISSA member, Silicon Valley Chapter **and Yong Wang**

**This article introduces different groups of cybersecurity tools, discusses challenges with them, identifies the possible reasons why they are not enough to defend against advanced persistent threats, and discusses the research in progress to complement existing cybersecurity tools.**

## Abstract

Advanced persistent threats (APTs) are executed by nation-state sponsored agents or cybercriminals. APTs are prolonged and targeted cyber attacks where cybercriminals use multiple vectors and entry points to navigate around defenses to breach into enterprise networks and evade detection for months. They present a challenge for organizations because of their complexity, duration, and undetectability. Enterprises need a toolbox of basic-to-bleeding-edge tools to set up multi-layered defense against APTs. This article introduces different groups of cybersecurity tools, discusses challenges with them, identifies the possible reasons why they are not enough to defend against APTs, and discusses the research in progress to complement existing cybersecurity tools.

The United States Air Force coined the phrase advanced persistent threat (APT) in 2006 [1]. The goal of APT attackers is to steal data and intellectual property. APTs occupy news headlines often because of the potential damage they can cause regarding reputation, data (both consumer and corporate), and intellectual property. The infamous cyber attack on credit rating agency Equifax in February 2017 is still in people's minds. The US Department of Justice confirmed that a team of hackers from the Chinese military was behind the attack on Equifax, in which personally identifiable information (PII) of over 147.9 million people was stolen [14]. Recently, computer security firm Eset reported that a cyber attack on San Francisco International Airport (SFO) was carried out by state-sponsored Russian hackers in March 2020. The airport revealed that some users of its websites (SFOConnect.com and SFOConstruction.com) may have had their logins stolen. APTs are a looming threat to enterprises both large and small. Several vaunted enterprises like Google, RSA, DuPont, Walt Disney, Johnson & Johnson, Morgan Stanley, Sony, General Electric, etc. were victims of APTs [5].

NIST defines APT as an adversary equipped with advanced technical expertise and extraordinary resources to create opportunities to achieve its objectives utilizing all possible attack vectors [11]. Richard Bejtlich, a well-known cybersecurity expert, explains what APT stands for [1]:

- **Advanced:** Attackers are highly skilled in hacking tools and techniques. They start their intrusion efforts by exploiting well-known vulnerabilities. They can up their game, research new vulnerabilities, and develop custom exploits if the initial intrusion efforts are not successful.
- **Persistent:** Attackers are focused on the target and set to accomplish a mission. They are not hit-and-run attackers but remain in victim's network, evading detection for a prolonged period. Persistent does not necessarily mean that the attackers constantly perform malicious activities in the victim's network. The attackers perform minimum activity needed to execute their objectives and avoid detection.
- **Threat:** The adversary is not simply a piece of malicious code. The attackers are organized, funded, and motivated, and their successful intrusion attempts result in potential damage to the organization's finances and reputation.

APTs are clearly distinct from hit-and-run hacking events because APTs have the following distinct characteristics: customized, persistent, organized, funded, sophisticated (advanced tools and techniques), and timeliness. The following sections present the cyber kill chain, tools to prevent APTs, discussions about the effectiveness of tools, and an outline of research in progress as the conclusion.

## Cyber kill chain

*Kill chain*, a term originated in the military, defines a series of steps an adversary follows to attack a target. In 2011, Lockheed Martin developed the cyber kill chain framework, identifying what adversaries must complete to achieve their objectives [10]. By understanding the cyber kill chain framework, defenders are better prepared to identify and stop attackers at each stage. The closer to the beginning of the chain, the better the attack can be stopped. Moreover, the more stages at which defenders can intercept the attackers, the higher the chances of detecting and terminating the attacks. This means defenders should be equipped with tools to detect and prevent APTs in all stages of the cyber kill chain.

There are seven stages in Lockheed Martin's cyber kill chain:

1. Reconnaissance
2. Weaponization
3. Delivery
4. Exploitation
5. Installation
6. Command & Control
7. Action on Objectives

### Reconnaissance

In the reconnaissance stage, adversaries begin with a target organization, gather information about the target, and look for vulnerabilities. Information gathering activities can be passive or active. In the active mode, adversaries run scanning and finger printing tools against an organization's systems deployed in the demilitarized zone (DMZ) to uncover ports that are vulnerable to exploitation and find out the technology stacks of the systems. Adversaries can also identify security systems that are in place such as firewalls, intrusion prevention systems, and authentication mechanisms. In the passive mode, adversaries gather information about the organization and its employees using the publicly available databases and social media networks.

### Weaponization

During the weaponization stage, adversaries develop customized malware that exploits vulnerabilities discovered during the reconnaissance stage.

### Delivery

During the delivery stage, adversaries transmit the custom-developed malware to the victim's systems for exploitation. Spear-phishing attacks targeting internal employees of the organization is the most common method to transmit malware into the organization's internal systems [18]. Ninety percent of APT groups use spear phishing as an effective way to deliver malware into a company's internal network [13].

### Exploitation

In the exploitation stage, the delivered malware begins executing on the target's system(s). The goal at this stage is to gain access to additional systems in the target's network and gain access to superuser or admin accounts. Adversaries monitor unencrypted network traffic inside the network to steal login credentials, search for vulnerable internal systems running on older versions of software, try escalating user privileges on the systems where they already have access, and use the vulnerabilities discovered during the reconnaissance stage.

### Installation

At the installation stage, the already delivered malware downloads additional components to create a persistent backdoor or other ingress accessible to the adversary outside the victim's network for an extended period.

### Command and control

In the command and control stage, adversaries establish a command channel to the victim's systems or network to remotely manipulate the victim. At this stage adversaries are

| CYBER KILL CHAIN STAGE | TYPES OF TOOLS | DESCRIPTION OF TOOLS |
|---|---|---|
| **Reconnaissance** | Firewall, web analytics tools | Firewalls are the first layer of defense against APT attacks because they play the role of controlling network visibility and enforcing security policies. Firewalls segment an organization's network into zones, controlling inbound and outbound traffic between network zones and network zones to the Internet by enforcing security policies set by the organization. Configuration of firewalls is very important to prevent APTs. Firewalls must be configured accurately and intelligently to analyze and block any network traffic that signals APTs.<br>Web servers are public-facing assets of organizations. Web analytics tools provide the ability to correlate logging events based on time and user activity. Abnormal user activities like intelligence gathering on the website, repeatedly entering invalid inputs, etc. indicate intention to breach. |
| **Weaponization** | Network intrusion detection system (NIDS) | NIDS tools monitor network-based traffic and activity. They detect malicious activities by examining network activity logs and packets moving across the network. NIDS tools use anomaly-based and signature-based detection techniques to analyze log files for malicious activities. |
| **Delivery** | Anti-malware/end point detection and response (EDR), secure email gateway | Anti-malware protection and endpoint detection and response tools identify, prevent, and react to malware delivery or installation on an endpoint by APT actors.<br>Secure email gateways (SEGs) scan both outbound and inbound email for malicious content. SEGs offer protection against virus and malware, which are normally delivered via malicious messages and attachments. |
| **Exploitation** | Host-based intrusion detection system (HIDS), patch management system | HIDS tools monitor logs for suspicious activities and report to the device administrators. HIDS tools use anomaly-based and signature-based detection techniques to analyze log files for unusual behaviors.<br>A patch management system (PMS) can automate the patching of operating systems and applications running on endpoints and servers. PMS continuously identify vulnerable operating systems and applications and apply security patches by leveraging verified vulnerability intelligence. PMS tools can prioritize patch application based on criticality of vulnerabilities. |
| **Installation** | HIDS, anti-malware/ EDR | HIDS<br>Anti-malware/EDR |
| **Command & Control** | NIDS, Firewall | NIDS, Firewall |
| **Actions on Objectives** | Data loss/leak prevention (DLP) | DLP tools monitor data movement in and out of the network. The objective of DLP solutions is to detect and prevent data breaches, exfiltration (abnormal outbound data transfer), and unwanted destruction of sensitive data. |

Table 1 – Cyber kill chain tools

capable to move deeper into the network, exfiltrate data, and conduct destructive operations like denial of service (DoS) or distributed denial of service (DDoS).

### Actions on objectives

At this stage the adversaries are equipped with hands-on keyboard access to the victim's systems to execute actions to achieve their objectives. The adversaries devise methods to avoid detection by the victim's monitoring/alerting systems while performing their intended actions. The actions are generally data exfiltration, modification, and destruction.

## APT prevention and detection tools

Table 1 provides the most important tools used at various stages of cyber kill chain to stop APT attacks. The functionalities of the tools are provided at a high level to get understanding and are well known in the information security community. Security information and event management (SIEM) and security orchestration, automation, and response (SOAR) tools are not included in this table. Both tools process data from all stages of the cyber kill chain. In addition, they are relatively new compared to the other tools mentioned in table 1. Thus, SIEM and SOAR tools are covered more in the discussion section.

## Challenges with popular security tools

There are a wide variety of tools to detect and prevent APTs at all stages of cyber kill chain offered by several vendors. According to Radicati, the market for APT protection solutions is expected to grow from $4.3 billion in 2019 to over

$9.4 billion by 2023 [17]. According to FireEye, the global median dwell time (the number of days an attacker is present on the victim's network before detection) decreased year after year: 101 days in 2017, 78 days in 2018, and 56 days in 2019 [4][9]. The decreasing trend of dwell time reflects progress in technology and an increase in ransomware and cryptominer attacks, which are detected more quickly. Tools show improvement regarding dwell time, but APT attacks are still rising [8]. "Global data from 2018 found that 64 percent of all FireEye-managed detection and response customers who were previously Mandiant incident response clients were targeted again in the past 19 months by the same or similarly motivated attack group" [4].

It is difficult to detect APTs in early stages of cyber kill chain. Many APT attackers use customized malware exploiting zero-day vulnerabilities in target's systems. The more advanced the tools to detect and prevent are, the more advanced and skilled adversaries are. This is an ongoing race between defenders and adversaries where adversaries are gaining the upper hand. There are protocols to follow for a vendor to develop and release a tool into market, but adversaries can build and use tools without any obstructions. Tools developed by vendors to detect and prevent APTs are general in nature to cater to a wider market, though they are meant to apply at a specific stage of cyber kill chain. Adversaries gain upper hand because tools developed by them are customized for specific targets.

LOOKING AHEAD

Journal Themes

**July: Security vs Privacy Tug of War**

Despite the evolution and maturity of cybersecurity, threats to privacy are increasing, leading companies to continually look for more effective ways to protect personal information. Information privacy is an intertwined relationship between collecting, protecting, and sharing data, technology, and the expectation that our privacy is protected. Every data breach, engagement with social media, search history, and smart appliance reveals that our control over privacy has weakened even though privacy rights have grown stronger. What privacy challenges have you faced in your organization?

**August: Disruptive Technologies**

The word *disruptive* can sometimes make people uncomfortable because it means change, and change makes most people uncomfortable. Disruptive technology is an even bigger change because it changes current technology and modifies business, markets, and unchanging networks. This type of technology is innovative and advances our society and even our lives. The ISSA Journal is looking for information on experiences with what is considered disruptive technology and if it has impacted the author's life, or what does the author see as the next disruptive technology and how it can change all of our lives.

**SUBMIT ARTICLES TO EDITOR@ISSA.ORG.**

Off-the-shelf solutions for individual servers or endpoints and network protection are hopelessly outclassed by cyber attackers. Since cyber attackers possess advanced technical skills, they devise new techniques to bypass anti-malware software, sandboxes, and intrusion detection/prevention systems [13]. "Advances in attacker sophistication have not been matched by similar defensive advances. The concept of keeping the internal, trusted network separated from the external, untrusted one (i.e., boundary protection) has become obsolete. The use of blacklists or signatures for attack detection is practically useless against sophisticated attackers. The security industry, having spent decades developing security products such as anti-malware solutions and intrusion detection/prevention systems refuse to admit the shortcomings of these products" [19]. Employees are the first line of defense for any organization. Therefore, they need have to security education, and a sober understanding of the protection systems in place to secure their key assets.

## Challenges with new and advanced security tools

Security information and event management (SIEM) and security orchestration, automation and response (SOAR) tools have been used in security operations centers (SOCs). Both SIEM and SOAR tools are considered advanced tools for cybersecurity operations; however, SOAR tools are not as common as SIEM tools. SIEM solutions collect and analyze events in system logs: logs from firewalls, intrusion detection/prevention systems, network appliances, database servers, application servers, etc. SIEM tools analyze that data to catch abnormal behavior indicating potential cyber attacks. SIEM tools are equipped with analytics and machine learning capabilities. They check for event patterns and correlate event information between devices for any anomalous activity and issue an alert when necessary.

SIEM tools are not created to unify people, processes, and technologies within a security operations center. "While the SIEM detects the potential security incidents and triggers the alerts, a SOAR solution then takes these alerts to the next level, responding to them, triaging the data and taking remediation steps where necessary" [3]. SOAR tools add value to SOCs as they automate and orchestrate time-consuming, manual tasks including opening a ticket in a tracking system, such as Jira, without requiring any human intervention. Using SOAR tools SecOps team can automate incident response work flows.

SIEM and SOAR tools are advanced-level cybersecurity tools and do appear to have potential to detect APTs, but there are challenges. "SIEM tools provide a central place to collect events and alerts but can be expensive, resource intensive, and customers report that it is often difficult to resolve problems with SIEM data" [12]. Most of them will reflect the following as major issues with adoption and operations of SIEM products [16]:

1. Initial adoption takes time because of necessary coordination with various stakeholders within the IT organization
2. Time-to-value realization is very high
3. Correlation of events is difficult to achieve, leading to a high number of false positives
4. SIEMs are very high maintenance products
5. Out-of-the-box reports from SIEM products are mostly useless and require quite a bit of work to get meaningful reports
6. Operational costs outweigh the benefits

SOAR tools are not popular yet. According to Gartner, "By year-end 2022, 30 percent of organizations with a security team larger than five people will leverage SOAR tools in their security operations, up from less than five percent today" [2]. SOAR tools are still evolving and reliance on them for APT detection is not there yet. Charles Herring, chief technology officer at Witfoo, says "If you do not have the critical/basic controls in place, it makes no sense to do advanced controls like SOAR" [7].

Though SIEM and SOAR tools are advanced, there are implementation challenges to make the tools effective. Jurgen Kutscher, executive vice president of service delivery at FireEye, says "FireEye Mandiant has seen organizations largely improving their level of cybersecurity sophistication, but combatting the latest threats is still a huge challenge for them" [9]. The projection for APT protection solutions is expected to grow, but organizations are not looking for the missing pieces of the puzzle in the game of defending against APTs. With the heavy focus on tools to prevent APT attacks, non-technical attack vectors like insider threat and social engineering are not given much needed attention. The *Verizon 2019 Data Breach Investigations Report* states that 34 percent of all breaches in 2018 were caused by internal actors [18]. In 2018, 60 percent of breach investigations can attribute successful social engineering as the conduit to initial point of entry [6].

## Proposals to complement security tools

Committed implementation of a cybersecurity framework and an effective method of testing defenses are the missing pieces in the puzzle to defend against APTs.

### Simple cybersecurity framework

According to Tenable strategist Cris Thomas, cybersecurity frameworks help organizations to create a solid baseline for measuring security effectiveness and to meet compliance requirements. Implementation of security frameworks can be challenging without the tools, talent, and support from executive leadership. A study conducted by Tenable and the Center for Internet Security, found that 95 percent of organizations face significant challenges when implementing leading cybersecurity frameworks [15]. The same study reports the top five impediments to cybersecurity framework implementation as follows:

1. Lack of trained staff
2. Lack of necessary tools to automate controls
3. Lack of budget
4. Lack of appropriate tools to audit continuous effectiveness of controls
5. Lack of integration among tools

Because of the implementation challenges of cybersecurity frameworks, most organizations implement a cybersecurity framework just enough to satisfy auditing requirements.

Cybersecurity frameworks like NIST and COBIT are comprehensive. To make adoption of cybersecurity framework easier, it can start with a framework that is simple and easy to implement. Once adoption of a simple framework is accomplished, a solid baseline for measuring security effectiveness will be in place and adopting a comprehensive framework like NIST becomes just an enhancement.

### Convergent testing

Defense-in-depth (DiD) or multi-layered defense is a common strategy organizations use to defend themselves from cyber threats. DiD means security controls (technical and administrative) are put in place at the application, endpoint (host), and network levels. Organizations implement multiple security controls at different levels of DiD architecture to defend their security posture, but all security controls are not tested simultaneously. We did not find any method or framework that is designed to test defense-in-depth security strategy in our literature review. To fill in the gap to test DiD, we introduce a new testing strategy called *convergent testing*—testing all defenses of the security posture of an organization at all layers as a single effort. The major advantage of convergent testing is to verify whether the security controls work in coordination with one another or not. In addition, convergent testing verifies if a security control fails at one level, whether the related security control in the next level can defend or not. One example of convergent testing is simulating data exfiltration activity. When data exfiltration is simulated, administrative controls, DLP solution, firewall, NIDS, HIDS, and SIEM are tested. Testing independently does not give much value compared to simultaneous testing of all controls in the exfiltration path.

## Mindlessly Following "Best Practices"

Continued from page 7

to who it really was since we can track it back. However, a good clue was lost, which was how to determine which user was used to connect. If the hacker was sophisticated, I would expect him to mask his IP address. The company spent, literally, a year putting in the new check out system, not to mention thousands of dollars. The result, at the end of the day, the security was worse than before.

Yes, the company now can say they have two-factor authentication, but looking at it as a hacker, the company made breaching their servers and getting away clean much easier.

### About the Author

*Stephen Kirby is an attorney based in Washington State and the managing director of an IT consulting firm. As an attorney Mr. Kirby has focused on the impact of law and regulation on the behavior of companies and individuals and the law around hacking, security research, and privacy. He may be reached at kirby@kirbylawoffice.com.*

Convergent testing covers the missing gap left by penetration testing (pentesting), blue teaming, and red teaming. Red teams (offensive security professionals) are external entities specializing in attacking systems and breaking into defenses. Blue teams (defensive security professionals) are internal security teams responsible for setting up and maintaining defenses against cyber threats. Blue teaming is tasked with setting up defenses, but not necessarily testing the coordination among security controls. Red teaming is more about measuring the business impact of the vulnerabilities, whereas penetration testing is about finding and exploiting vulnerabilities. Penetration testing's focus is very narrow, limited to an application or a network. Red teaming is too broad; the main objective of red teaming is to test and strengthen the organization's ability to detect and respond to advanced cyber attacks and demonstrate the insufficiency of response procedures or security controls. Red teamers may not know all the security controls available at various levels of defense. The goal of convergent testing is to get the value of red teaming with minimal budget of time and money. Convergent testing can be accomplished by the internal security team. In the corporate world, different stakeholders are responsible for different security defenses. Thus, testing all defenses at a single point of time requires challenging coordination, but is necessary. Blue teams should adopt convergent testing to ensure identification of coordination gaps among security controls.

### Conclusion

In this article we presented an overview of APTs, the cyber kill chain, tools used at various stages of the kill chain, and the current state of effectiveness of cybersecurity tools. Organizations are improving their cybersecurity sophistication, but APTs are still a huge challenge. Our literature review reveals that technologically sophisticated organizations are not immune to APTs. Criminals long ago figured out how to bypass antivirus software, sandboxes, and intrusion detection/prevention systems. Advanced security operation tools like SIEM and SOAR have their challenges, which make them ineffective to detect APTs. It is time for organizations to recognize that allocating heavy budgets to acquire cybersecurity tools is not enough and identify what else can be done to enhance defenses against APTs. We hypothesize that relying on tools for cybersecurity without implementing a framework and a methodology to test defense in depth provides organizations a false sense of security.

As part of our research study, we are conducting an anonymous survey of cybersecurity professionals. The survey questions are about existing administrative and technical controls placed at their organizations as security defenses. We convert the survey responses to key risk indicators (KRIs). KRIs are measures such as numbers, counts, percentages, etc. Key risk indicators are metrics used by organizations to find out early signals of increasing risk exposures in various areas of the enterprise. The survey results will help our research study in three ways:

1. Identify the need for the framework to be proposed
2. Identify what exactly needs to be included in the framework
3. Identify the missing methodology to test DiD architecture

Our research outcome should help organizations by complementing cybersecurity tools in defense against APTs.

## References

1. Betlich, Richard. 2010. "What APT Is (And What It Isn't)," Information Security – http://viewer.media.bitpipe.com/1152629439_931/1279750495_63/0710_ISM_updated_072010.pdf.
2. Demisto. 2019. "Gartner Releases 2019 Market Guide for Security Orchestration, Automation, and Response (SOAR)," Demisto – https://blog.demisto.com/gartner-releases-2019-market-guide-for-soar.
3. DFLabs. 2019. "The Difference between SIEM and SOAR (Why Do I Need SOAR, If I Have SIEM?)," DFLabs – https://www.dflabs.com/resources/blog/the-difference-between-siem-and-soar-why-do-i-need-soar-if-i-have-siem/.
4. Fireeye. 2019. "FireEye 2019 Mandiant M-Trends Report Finds Organizations across the Globe Are Faster to Identify Attacker Activity Compared to Previous Year," FireEye – https://investors.fireeye.com/news-releases/news-release-details/fireeye-2019-mandiant-m-trends-report-finds-organizations-across.
5. Grimes, Roger A. 2011. "Prepare for Advanced Persistent Threats, or Risk Being the next RSA," CSO Online – https://www.csoonline.com/article/2623889/prepare-for-advanced-persistent-threats--or-risk-being-the-next-rsa.html.
6. Help Net Security. 2019. "Cybercriminals Are Becoming More Methodical and Adaptive," Help Net Security – https://www.helpnetsecurity.com/2019/04/26/cybercriminals-becoming-methodical/.
7. Herring, Charles. 2020. "An Ounce of Prevention Is Worth a Pound of SOAR." Charles Herring's Blog – https://charlesherring.com/blog/ounce-prevention-worth-pound-soar#.XqabA2hKiUl.
8. Jacobs, Peter. 2019. "Dwell Time Is Down, APTs Are on the Rise, and Other Cyberattack Trends You Need to Know." Government Technology Insider – https://governmenttechnologyinsider.com/dwell-time-is-down-apts-are-on-the-rise-and-other-cyberattack-trends-you-need-to-know/#.XsDSGmhKiUk.
9. Kovacs, Eduard. 2020. "FireEye Spotted Over 500 New Malware Families in 2019," SecurityWeek – https://www.securityweek.com/fireeye-spotted-over-500-new-malware-families-2019.
10. Lockheed Martin. 2019. "Gaining the Advantage. Applying Cyber Kill Chain Methodology to Network Defense," Lockheed Martin – https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/Gaining_the_Advantage_Cyber_Kill_Chain.pdf.
11. NIST. 2013. "NIST Special Publication 800-53: Security and Privacy Controls for Federal Information Systems and Organizations," NIST – https://doi.org/10.6028/NIST.SP.800-53Ar4.
12. Petters, Jeff. 2020. "What Is SIEM? A Beginner's Guide," Veronis – https://www.varonis.com/blog/what-is-siem/.
13. Positive Technologies. 2019. "Hack at All Costs Putting a Price on APT Attacks," Positive Technologies – https://www.ptsecurity.com/ww-en/analytics/advanced-persistent-threat-apt-attack-cost-report/.
14. Sass, Rami. 2020. "The Equifax Saga: It Could Happen Again. Don't Let It." InfoSecurity Magazine – https://www.infosecurity-magazine.com/opinions/equifax-could-happen-again/.
15. Seals, Tara. 2013. "Organizations Struggle with Implementing Security Frameworks," InfoSecurity Magazine – https://www.infosecurity-magazine.com/news/organizations-struggle-security/.
16. Shukla, Rajeev. 2019. "Most SIEM Products Fail. And, So Does Threat Monitoring !" Peerlyst – https://www.peerlyst.com/posts/most-siem-products-fail-and-so-does-threat-monitoring-rajeev-shukla.
17. The Radicati Group Inc. 2019. "Advanced Persistent Threat (APT) Protection-Market Quadrant 2019," The Radicati Group Inc. – https://docs.broadcom.com/doc/apt-protection-market-quadrant-2019-en.
18. Verizon. 2019. "2019 Data Breach Investigations Report," Verizon – https://enterprise.verizon.com/resources/reports/2019-data-breach-investigations-report.pdf.
19. Virvilis-Kollitiris, Nikolaos. 2015. "Detecting Advanced Persistent Threats through Deception Techniques" – https://www.infosec.aueb.gr/Publications/Virvilis-Kollitiris%20Dissertation%20Text.pdf.

## About the Authors

*Srinivasulu (Srini) Vuggumudi, CISSP, CEH, CCSK, AWS-CCP, PMP, Network+, is a senior security engineer at Malwarebytes Inc. and is a PhD student at Dakota State University, Madison, SD. Srini's research interests are advanced persistent threats and application security. He can be reached at srini.vuggumudi@gmail.com.*

*Yong Wang is an associate research professor in the Beacom College of Computer and Cyber Sciences at Dakota State University. He received his PhD degree in computer science from the University of Nebraska-Lincoln in 2007. His research focuses on security and privacy issues in wireless networks, mobile devices, cloud, and Internet of things. He can be reached at yong.wang@dsu.edu.*

# 14

# Python Programming: Processing NVD Data

By Constantinos Doskas – ISSA Senior Member, Northern Virginia Chapter

**This article continues our discussion on database programming by exploring methods of downloading data from websites, loading them on databases, and analyzing them. In past articles we had an overview of NVD database data and the data was downloaded in local storage. In this article we will be loading some of the data on a table and present ways of creating visualizations from it.**

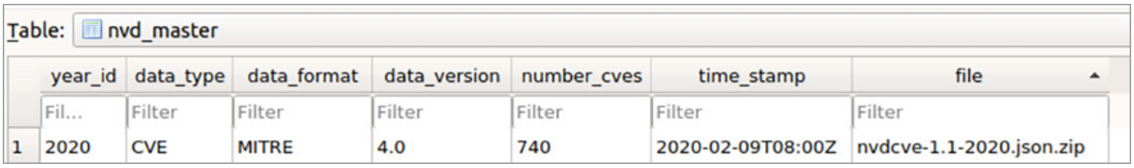


Table: nvd_master

| | year_id | data_type | data_format | data_version | number_cves | time_stamp | file |
|---|---|---|---|---|---|---|---|
| | Fil... | Filter | Filter | Filter | Filter | Filter | Filter |
| 1 | 2020 | CVE | MITRE | 4.0 | 740 | 2020-02-09T08:00Z | nvdcve-1.1-2020.json.zip |

Figure 1 – nvd_master table

## The scenario of this article

So far, in previous articles, we downloaded the NVD database in the form of zipped JSON files. Then we decompressed the files and processed them creating a database with one table whose purpose is to give us a general description of the data contained in each JSON file. We named the table *nvd_master*. Each row of that table contains data from one of the files, see figure 1.

Having completed that step, we will add a table that provides us with CVE summary data. This table will be useful to those who want to know what vulnerabilities exist up to this point, and how they are categorized by weakness, exploitability, and impact. The table will be part of a relational system of tables.

## Creating the second table

Before we create the table we must decide what type of data we will include. Let's look up the available data. Examining the top of each JSON record, we find the CVE ID and data related to the problem category. We will be using the CVE_ID as a primary key on most tables.

```
"cve":{
   "data_type": "CVE",
   "data_format": "MITRE",
   "data_version": "4.0",
   "CVE_data_meta": {
   "ID": "CVE-2020-0001",
   "ASSIGNER": "cve@mitre.org"
   },
   "problemtype": {
       "problemtype_data": [
            {
                "description": [
            {
                "lang": "en",
                "value": "CWE-269"
            }
       ]
   }
   ]
},
```

Note that CWE stands for Common Weakness Enumeration, and it is used as a baseline in handling software and hardware security weaknesses (see cwe.mitre.org). We will then include the CVE ID and the CWE ID in our record. In a near future we will incorporate more CWE data in the database.

After the *problem type* directory there is another directory with valuable information. This is the *impact* directory. Let's include in this second table the impact data that is in numeric form.

```
"impact": {
   "baseMetricV3": {
    "cvssV3": {
        "version": "3.1",
        "vectorString":"CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/
    C:H/I:H/A:H",
        "attackVector": "LOCAL",
        "attackComplexity": "LOW",
        "privilegesRequired": "LOW",
        "userInteraction": "NONE",
        "scope": "UNCHANGED",
        "confidentialityImpact": "HIGH",
        "integrityImpact": "HIGH",
        "availabilityImpact": "HIGH",
        "baseScore": 7.8,
        "baseSeverity": "HIGH"
    },
    "exploitabilityScore": 1.8,
    "impactScore": 5.9
   },
   "baseMetricV2": {
    "cvssV2": {
        "version": "2.0",
        "vectorString": "AV:L/AC:L/Au:N/C:C/I:C/A:C",
        "accessVector": "LOCAL",
        "accessComplexity": "LOW",
        "authentication": "NONE",
        "confidentialityImpact": "COMPLETE",
        "integrityImpact": "COMPLETE",
        "availabilityImpact": "COMPLETE",
        "baseScore": 7.2
    },
    "severity": "HIGH",
    "exploitabilityScore": 3.9,
    "impactScore": 10.0,
    "acInsufInfo": false,
    "obtainAllPrivilege": false,
    "obtainUserPrivilege": false,
    "obtainOtherPrivilege": false,
    "userInteractionRequired": false
    }
},
```

The above data is a sample of the data contained in the impact directory. The highlighted fields are the fields that we will add to our table. Note that some of the data fields that we are not including in this table contain valuable information for pentesters and the person who prepares the final vulnerability report. We will include these fields in another table in the future.

Now we have the list of fields to add on the table. While processing the file we may encounter CVE records that do not have all the expected data. We must then construct our program in a way that it can handle missing data. Therefore, lack of data should cause a NULL value to be inserted in the corresponding database field.

Let's assume that every time we run this program we recreate the table. Our database is *nvd_data.db* and it is the same as in the last article. The new table name is *nvd_cve_summary.* We must include the following modules in the program:

```
import zipfile
import os
import json
import sqlite3
```

The JSON files that we downloaded last month are still in the CVE_FILES directory. The program will access these files one by one as we have previously done. The files will be decompressed and their data loaded in a Python directory using the same methodology that we used before. You could find that information by reading the previous articles.

Programmers prefer to write a skeleton of the code before it is developed. That skeleton is called pseudocode and it is written using a simple notation in plain English. Let's create a simple skeleton of our code using pseudocode.

We will start with a function which we will name *obtain_cve_summary_data().* This function will take three arguments. The first argument is a Python directory of all the data of a JSON CVE directory. The second argument is the current year and the third argument is a Boolean variable called *verbose.* Note that Boolean values are just True or False. The *verbose* argument will enable or disable printing of progress statements while the data is processed.

Here is the pseudocode:

```
def obtain_cve_summary_data(cveItemsDir,year,verbose):
  Extract and store the CVE ID from the data – note
      that this will never be NULL
  Extract the CWE ID and store it if present,
      otherwise store NULL
  Extract base metrics version 2 and store them – if
      not present store NULL
  Extract base metrics version 3 and store them – if
      not present store NULL
  Return the stored values to the calling program
```

That was easy right? Now lets develop the pseudocode of the main program:

```
Open the database nvd_data.db
If the table nvd_cve_summary exists, remove it
Create an empty nvd_cve_summary table
Get a list of the files in CVE_FILES/ directory
Process the files – one by one
  Decompress the file
  Place the data of the file in a Python directory
  Get the keys of the above Python directory
  While not all keys are processed do
      process the next key
      If the key is "items" process it's data
          call obtain_cve_summary_data() passing the
      value of the "items" key to it
          Insert in a row of the table the data which
      returns from the function
          else go back to the while statement
      go back to the while statement
  When finish processing all files save the table in
      the database
  Close the database
```

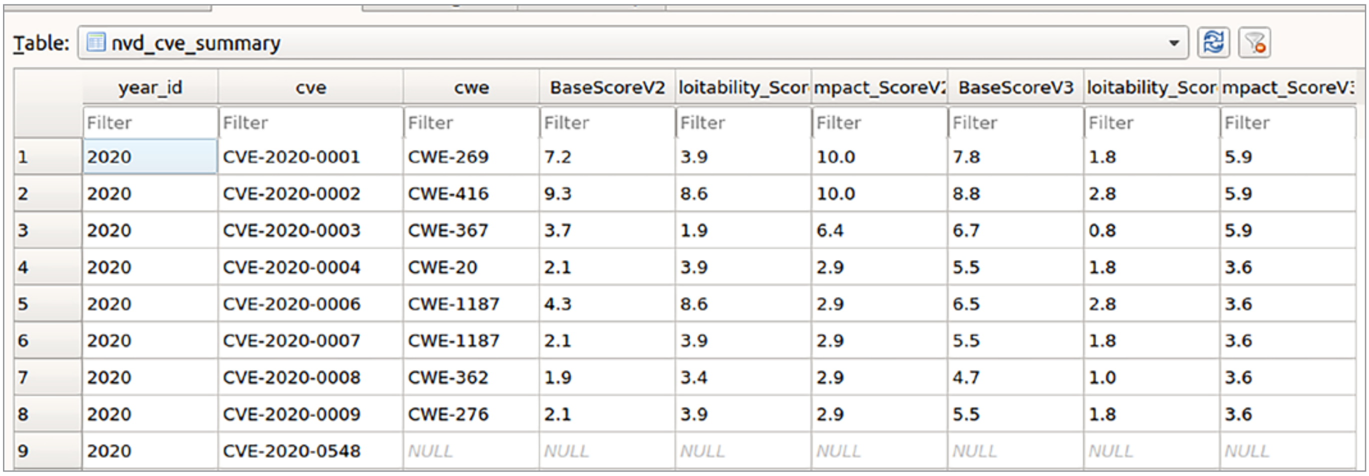


Table: nvd_cve_summary

| | year_id | cve | cwe | BaseScoreV2 | loitability_Scor | mpact_ScoreV: | BaseScoreV3 | loitability_Scor | mpact_ScoreV: |
|---|---|---|---|---|---|---|---|---|---|
| | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter | Filter |
| 1 | 2020 | CVE-2020-0001 | CWE-269 | 7.2 | 3.9 | 10.0 | 7.8 | 1.8 | 5.9 |
| 2 | 2020 | CVE-2020-0002 | CWE-416 | 9.3 | 8.6 | 10.0 | 8.8 | 2.8 | 5.9 |
| 3 | 2020 | CVE-2020-0003 | CWE-367 | 3.7 | 1.9 | 6.4 | 6.7 | 0.8 | 5.9 |
| 4 | 2020 | CVE-2020-0004 | CWE-20 | 2.1 | 3.9 | 2.9 | 5.5 | 1.8 | 3.6 |
| 5 | 2020 | CVE-2020-0006 | CWE-1187 | 4.3 | 8.6 | 2.9 | 6.5 | 2.8 | 3.6 |
| 6 | 2020 | CVE-2020-0007 | CWE-1187 | 2.1 | 3.9 | 2.9 | 5.5 | 1.8 | 3.6 |
| 7 | 2020 | CVE-2020-0008 | CWE-362 | 1.9 | 3.4 | 2.9 | 4.7 | 1.0 | 3.6 |
| 8 | 2020 | CVE-2020-0009 | CWE-276 | 2.1 | 3.9 | 2.9 | 5.5 | 1.8 | 3.6 |
| 9 | 2020 | CVE-2020-0548 | NULL | NULL | NULL | NULL | NULL | NULL | NULL |

**Figure 2 – Table nvd_cve_summary**

The code, once completed, creates the table in figure 2.

Having completed the above task, we start analyzing the data which is on the table.

I developed a couple of programs to demonstrate what can be done with the data. The name of the first program is **cwe_analysis_a.py**. There are a couple of functions in the program that are doing some pre-processing to verify if the database and the table exist. We will not present this part of the program in the article but all the code will be available to download.

We must import the following libraries:

```
import sqlite3
import matplotlib.pyplot as plt
import numpy as np
import sys
import os

dbase=sqlite3.connect('nvd_data.db')
mydbCursor=dbase.cursor()
the_year='2019'
mydbCursor.execute("SELECT cwe, count(cve) AS cves\
   FROM nvd_cve_summary\
   Where cwe IS NOT NULL AND\
   year_id IS '"+the_year+"'\
   GROUP BY cwe\
   ORDER BY cves DESC")

data=mydbCursor.fetchall()
if len(data) == 0:
   print('No records returned. Program terminates.')
   sys.exit() # -- Note: this statement will cause the
    program to terminate
else:
   print("Records returned ", len(data))
print_tabledata(data)
```

The above code counts the number of CVE per CWE. Note that a CWE indicates the category of weakness and it is more general than the CVE. Therefore, there will be one or more CVEs per CWE.

Let's see the top five CWEs that the program identified for Year 2019:

```
Pre-processing ok - Proceeding
Records returned 145
CWE-79      1486
CWE-20      1363
CWE-119     1036
CWE-200     939
CWE-284     672
…
```

As you can see in the above listing CWE-79 has 1486 CVEs associated with it. If you want to learn what are the category descriptions and detail explanation of the above CWEs, you may visit the website mitre.org or google for CWE ID. Here is a short explanation of them.

```
CWE-79 "Command Injection"
CWE-20 "Improper Input Validation"
CWE-119 "Memory Corruption" which indicates that a
   program is writing outside of the allocated buffer.
CWE-200 "Exposure of Sensitive Information to an
   Unauthorized Actor"
CWE-284 "Improper Access Control"
```

Next is an example of creating a bar graph of CVE/CWE. For clarity we are going to restrict the output of the SQL statement to CWEs with more than 400 identified CVEs under them. We will process data for the year 2019

The name of the program is **cwe_analysis_b.py**.

```
dbase=sqlite3.connect('nvd_data.db')
mydbCursor=dbase.cursor()
the_year='2019'
mydbCursor.execute("SELECT cwe, count(cve) AS cves\
   FROM nvd_cve_summary\
   Where cwe IS NOT NULL AND\
    year_id IS '"+the_year+"'\
   GROUP BY cwe\
   HAVING cves > 400\
   ORDER BY cves DESC")

data=mydbCursor.fetchall()
if len(data) == 0:
   print('No records returned. Program terminates.')
   sys.exit() # -- Note: this statement will cause the
    program to terminate
cwe, cve_cnt= zip(*data)

width=0.5 # -- width of each generated bar
plt.bar(cwe,cve_
    cnt,width,align='edge',color=(0.9,0.3,0.1,0.8),\
   label='Vulnerabilities')
plt.xlabel('Figure 3. Common Weakness
    Enumerations',color='Blue')
plt.ylabel('CVE Count',color='Blue')
plt.title('Year '+the_year+' CVE count per CWE ',\
   fontsize=15,loc='center',color='green')
plt.legend(loc='upper right')
plt.show()
```

The output of the program is figure 3.

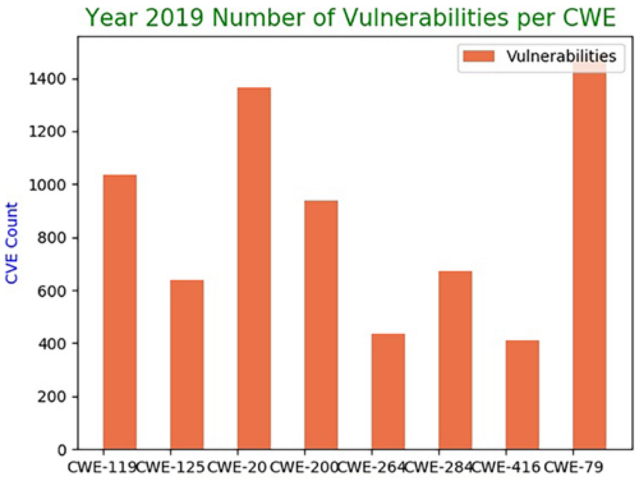


**Figure 3 – Common weakness enumerations**

Some security analysts may have an interest to find out how a certain type of weakness appears through the years. In this case the table may be used to create a graph of the number of vulnerabilities found per year for the specific weakness. We just need to modify the SQL statement to pull the right data and adjust the labels of the graph. Let's say that we want to see data related to CWE-284. The code listed in **cwe_analysis_c.py**.

```
dbase=sqlite3.connect('nvd_data.db')
mydbCursor=dbase.cursor()
the_year='2019'
mydbCursor.execute("SELECT year_id, count(cwe) AS cwe_
    count\
   FROM nvd_cve_summary\
   Where cwe IS NOT NULL AND cwe ='CWE-284'\
   GROUP BY year_id\
   ORDER BY year_id")

data=mydbCursor.fetchall()

year, cwe_cnt= zip(*data)
print(cwe_cnt)
print(year)
plt.plot(year,cwe_cnt,'darkslateblue',label='CVE')

# -- Create x axis labels and color them
plt.xlabel('Figure 4. Improper Access
    Control',color='Blue')
plt.ylabel('CVE Count',color='Blue')
plt.title('YEARLY CVE count for CWE-284',\
   fontsize=15,loc='center',color='green')
plt.legend(loc='upper right')
plt.savefig('Figure 4. Improper Access Control CVEs per
    year.jpg')
plt.show()
```

The output of the program (figure 4) shows an increase of improper access control vulnerabilities between 2015–2016 and again after 2018.

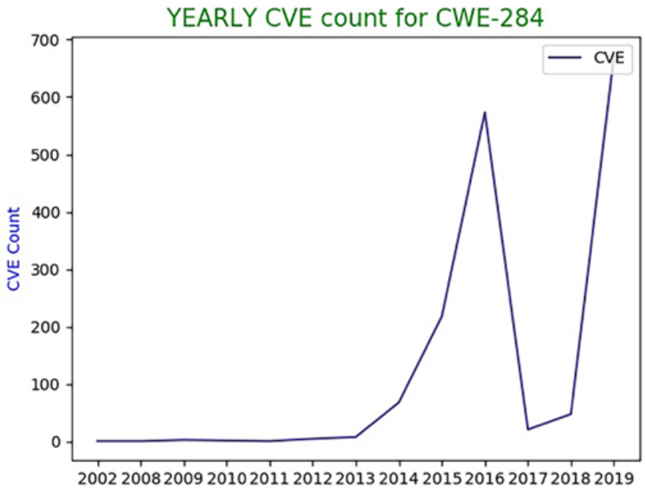


**Figure 4 – Improper access control**

Let's have another analysis example using the version 2 scores that came with the JSON data. If we want to see what was the exploitability that relates to CVEs in the CWE-284 category, we may modify our code as in **cwe_analysis_d.py**.

```
the_year='2019'
mydbCursor.execute("SELECT cve, Exploitability_ScoreV2\
   FROM nvd_cve_summary\
   Where cwe ='CWE-284' AND\
   year_id IS '"+the_year+"' AND\
   Exploitability_ScoreV2 is not NULL\
   ORDER BY cve")

data=mydbCursor.fetchall()

cve, exploitability= zip(*data)
print(cve)
print(exploitability)
xtick_location = np.arange(len(cve))
width=0.1
```

```
plt.bar(xtick_
   location,exploitability,width,align='edge',\
   color=(0.9,0.3,0.1,0.8),\
   label='Exploitability')
plt.xlabel('Figure 5. Improper Access
   Control',color='Blue',fontsize=13)
plt.ylabel('Exploitability Score
   V2',color='Blue',fontsize=13)
```

## Thoughts on Disasters, Planning, and Training

Continued from page 9

lives. If and when something major happens, you will be a part of the infrastructure necessary for the response to be effective. You'll be part of the solution, rather than part of the problem.

Now go wash your hands. And then call your local emergency management agency and volunteer.

### About the Author

*Rob Slade is so* ***fever****ishly excited about* ***cough****ing up this column that he can practically* ***smell*** *it. (Well, no. He can't.) More information than anyone would wish to know about him is available at https://twitter.com/rslade. It is next to impossible to get him to take "bio" writing seriously (especially with his death so imminent), but you can try at isc2@outlook.com.*

```
plt.title('Year '+the_year+' Improper Access Control
   Exploitability',\
   fontsize=15,loc='center',color='green')
plt.legend(loc='upper right')
plt.savefig('Figure 5. Improper Access Exploitability
   '+the_year+'.jpg')
plt.show()
```

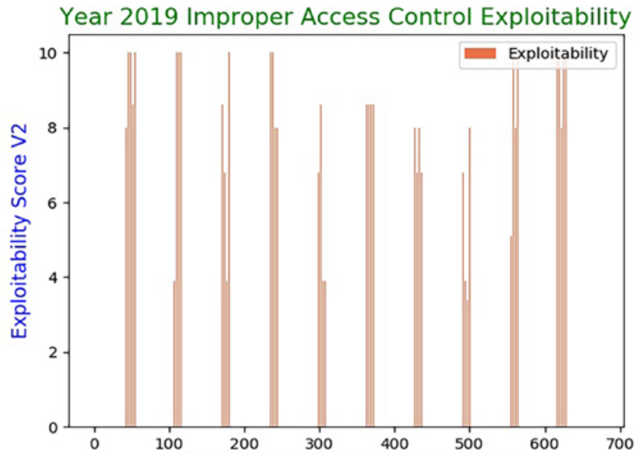


**Figure 5 – Improper access control**

The rest of the metrics could be graphed in the same way.

### Review and conclusion

This article is part of a series of articles that aim in helping cybersecurity professionals understand how information is acquired, organized, stored, and processed. The topic of the current article is how data from the NVD website may be loaded on SQL tables and analyzed. The article explained how programmers are using pseudocode as a way of planning programming steps before the actual code is written. Then, the correlation of CWE and CVE was discussed and a few methods of analysis were presented. In the next article we will be discussing how additional data may be extracted and utilized.

I hope that you enjoyed the article and will find ways to apply the presented concepts to your daily tasks. I am moving slowly on these concepts, giving you time to run the code and experiment. ISSA International makes the code available on its website.

You are always welcome to email me with any questions you may have. I wish you well and will be pleased to "see" you through the next article.

### About the Author

*Constantinos Doskas is head of the IT and Security Department of Olympus. He has been in-volved in information systems management and development for over 30 years. He is currently involved in mentoring graduate students and ISSA members in Northern Virginia. He may be reached at cdoskas@ofdcorp.com.*