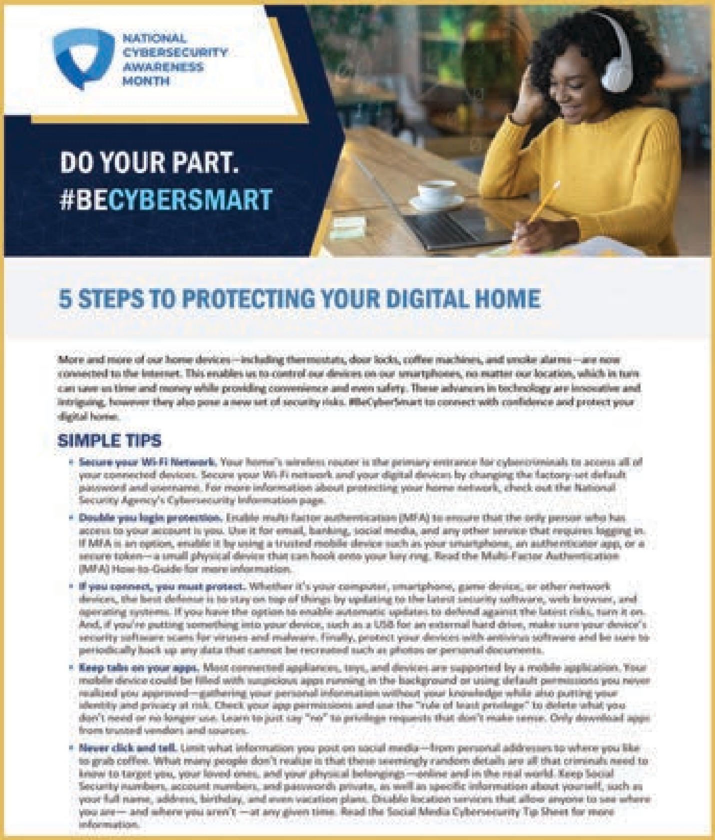
The
Iowa County
magazine


NATIONAL
CYBERSECURITY
AWARENESS
MONTH

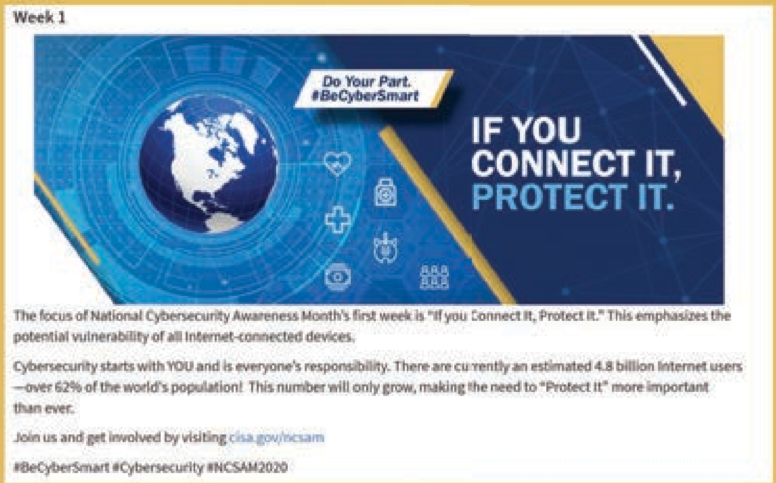
DO YOUR PART.
#BECYBERSMART

5 STEPS TO PROTECTING YOUR DIGITAL HOME

More and more of our home devices—including thermostats, door locks, coffee machines, and smoke alarms—are now connected to the Internet. This enables us to control our devices on our smartphones, no matter our location, which in turn can save us time and money while providing convenience and even safety. These advances in technology are innovative and intriguing, however they also pose a new set of security risks. #BeCyberSmart to connect with confidence and protect your digital home.

SIMPLE TIPS

- **Secure your Wi-Fi Network.** Your home's wireless router is the primary entrance for cybercriminals to access all of your connected devices. Secure your Wi-Fi network and your digital devices by changing the factory-set default password and username. For more information about protecting your home network, check out the National Security Agency's Cybersecurity Information page.
- **Double you login protection.** Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you. Use it for email, banking, social media, and any other service that requires logging in. If MFA is an option, enable it by using a trusted mobile device such as your smartphone, an authenticator app, or a secure token—a small physical device that can hook onto your key ring. Read the Multi-Factor Authentication (MFA) How-to-Guide for more information.
- **If you connect, you must protect.** Whether it's your computer, smartphone, game device, or other network devices, the best defense is to stay on top of things by updating to the latest security software, web browser, and operating systems. If you have the option to enable automatic updates to defend against the latest risks, turn it on. And, if you're putting something into your device, such as a USB for an external hard drive, make sure your device's security software scans for viruses and malware. Finally, protect your devices with antivirus software and be sure to periodically back up any data that cannot be recreated such as photos or personal documents.
- **Keep tabs on your apps.** Most connected appliances, toys, and devices are supported by a mobile application. Your mobile device could be filled with suspicious apps running in the background or using default permissions you never realized you approved—gathering your personal information without your knowledge while also putting your identity and privacy at risk. Check your app permissions and use the "rule of least privilege" to delete what you don't need or no longer use. Learn to just say "no" to privilege requests that don't make sense. Only download apps from trusted vendors and sources.
- **Never click and tell.** Limit what information you post on social media—from personal addresses to where you like to grab coffee. What many people don't realize is that these seemingly random details are all that criminals need to know to target you, your loved ones, and your physical belongings—online and in the real world. Keep Social Security numbers, account numbers, and passwords private, as well as specific information about yourself, such as your full name, address, birthday, and even vacation plans. Disable location services that allow anyone to see where you are— and where you aren't —at any given time. Read the Social Media Cybersecurity Tip Sheet for more information.

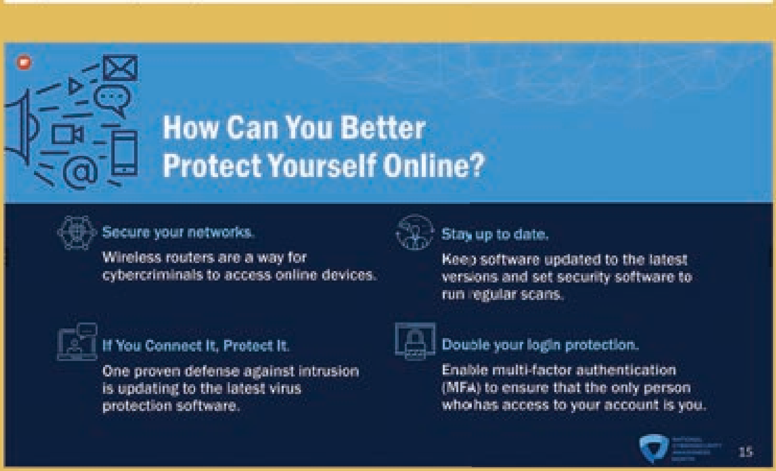

Week 1

The focus of National Cybersecurity Awareness Month's first week is "If you Connect It, Protect It." This emphasizes the potential vulnerability of all Internet-connected devices.

Cybersecurity starts with YOU and is everyone's responsibility. There are currently an estimated 4.8 billion Internet users —over 62% of the world's population! This number will only grow, making the need to "Protect It" more important than ever.

Join us and get involved by visiting cisa.gov/ncsam

#BeCyberSmart #Cybersecurity #NCSAM2020


How Can You Better Protect Yourself Online?

Secure your networks.
Wireless routers are a way for cybercriminals to access online devices.

Stay up to date.
Keep software updated to the latest versions and set security software to run regular scans.

If You Connect It, Protect It.
One proven defense against intrusion is updating to the latest virus protection software.

Double your login protection.
Enable multi-factor authentication (MFA) to ensure that the only person who has access to your account is you.

15

October 2020
Cybersecurity Month
Domestic Violence Awareness Month
No Wait Inside

THE ROAD TO SUCCESS

CAT® COLD PLANERS

With a combination of high efficiency and ease of operation, Cat Cold Planers are built to get the job done. Efficient and powerful performance with simplified controls and integrated technology help you finish the job faster with the milling precision you need.

MODEL	OPERATING WEIGHT	MILLING WIDTH	HORSEPOWER	MAXIMUM MILLING DEPTH
PM620	73,480 lbs.	79.1″	630 hp	13″
PM622	74,737 lbs.	88″	630 hp	13″
PM820	79,653 lbs.	79.1″	800.6 hp	13″
PM822	80,910 lbs.	88″	800.6 hp	13″
PM825	82,673 lbs.	98.6″	800.6 hp	13″

VIEW ALL PAVING MACHINES:
www.zieglercat.com/paving

ZIEGLER CAT

The Iowa County

October 2020 * *Volume 49, Number 10*

The Iowa County: The official magazine of the
Iowa State Association of Counties
5500 Westown Parkway, Suite 190
West Des Moines, IA 50266
515.244.7181 FAX 515.244.6397
www.iowacounties.org
Rachel Bennett, EDITOR

FEATURE - CYBERSECURITY MONTH

ISAC
Iowa State Association of Counties

ISAC's Mission:
To promote effective and responsible county government for the people of Iowa.

ISAC's Vision:
To be the principal, authoritative source of representation, information and services for and about county government in Iowa.

*** The views and opinions expressed in articles authored by anyone other than ISAC staff are those of the authors and do not necessarily reflect the official policy or position of ISAC.*

ISAC members are elected and appointed county officials from all 99 counties. *The Iowa County* (ISSN 0892-3795, USPS 0002-150) is published monthly by the Iowa State Association of Counties, 5500 Westown Parkway, Suite 190, West Des Moines, IA 50266. Periodicals postage paid at Des Moines, IA 50318. POSTMASTER: Send address changes to rbennett@iowacounties.org. Subscriptions: $25 per year.

Domestic Violence Awareness Month

Safe at Home
SECRETARY OF STATE
SERVICE • PARTICIPATION • INTEGRITY

Survivors of assault and violence often live in constant fear. Their days are filled with anxiety, knowing that they may be located by their offender. Many of us know someone who is a victim or survivor of domestic violence. In recognition of Domestic Violence Awareness Month this October, we would like to share a vital resource available in Iowa.

Safe at Home (SAH) is an address confidentiality program for victims and survivors of domestic violence, sexual assault, trafficking, and stalking. The program helps survivors improve their lives by providing a substitute address, mail forwarding, and confidential voter registration and absentee voting.

SAH currently has over 600 participants residing in 61 counties across the state. In 2019, all 99 Iowa counties experienced at least one domestic violence conviction. Domestic violence is present in all types of communities and impacts people regardless of gender, race, social class, career, and family dynamics.

Upon enrollment, each household (includes enrollee and all dependents who live within the same residence) is assigned a legal substitute address. This includes a street address, PO Box, and a unique apartment number. This address becomes the new legal address on record for the participant and can be used whenever an address is needed. Examples include registering a vehicle, obtaining a driver's license or library card, or filling out forms for employment or school records.

When a service requires residency within a district (for example enrolling in school), the office (or agency) may request in writing for SAH to verify that they reside within the district. SAH staff may confirm an individual's involvement in the program.

Mail forwarding is an important component to SAH, as it allows participants the ability to use the substitute address and receive their mail. Mail is sent to the SAH office, repackaged and sent to the participant, which will result in a five to seven-day delay. When sending important, time-sensitive documents to an individual in SAH, please consider this delay and whether there is an alternative method of communication that may be more effective.

SAH also provides confidential voter registration and absentee voting. Voting is a civic activity that many of us participate in without concern of the public record created through voter registration. The June 2020 primary experienced a record number of SAH participants casting their ballot. As the General Election quickly approaches, we hope more participants feel safe and confident enough to cast a ballot.

The powerful impact of SAH was illustrated by the results of a recent survey of current participants. Results show that prior to enrollment in SAH, 54% of respondents never felt safe and 41% felt safe only sometimes. After enrollment 67% of respondents feel safe most of the time and 27% always feel safe.

SAH is a crucial piece of a survivor's safety plan. However, when working with survivors it's imperative to understand it is only one piece of their safety plan. Applicants are also encouraged to contact one of the following agencies to discuss their safety plan and to learn more about available resources: Iowa Coalition Against Domestic Violence - www.icadv.org or 515.244.8028; Iowa Coalition Against Sexual Assault - www.iowacasa.org or 515.244.7424; and Iowa Attorney General's Crime Victim Assistance Division - www.iowaattorneygeneral.gov/for-crime-victims or 515.281.5044.

If you or someone you know would like more information or to fill out an application, visit the SAH website at www.safeathome.gov or call 515.725.SAFE (7233). If you would like materials or a program training for your agency or organization, please contact us. Brochures, removable stickers, palm cards, magnets, and booklets are available free of charge.

For quarterly email updates, sign up for our newsletter at safeathome.iowa.gov. Thank you for all you do to help victims become survivors in the state of Iowa. Every Iowan deserves to be Safe at Home, and together we can make this a reality.

ISAC Endorsed Preferred Vendor Feature

COVID-19 has changed the way we all work and live our day-to-day lives. The new normal has brought a new demand for products and services that weren't necessary a year ago. More specifically, products and services that help counties develop a safe and effective way to continue serving the public through current and future crisis. There's no doubt that the most successful way to minimize risk of any illness is to minimize contact with others. The company No Wait Inside is helping minimize risk to the public and Iowa's essential workers with a software designed specifically to help counties reopen and stay open.

No Wait Inside is a cloud-based technology solution that combines online scheduling, customer communications, contact tracing, and an efficiency dashboard in a simple and intuitive application to allow governments to safely and efficiently offer face-to-face and virtual services to its citizens. No Wait Inside solves a number of problems including the ability to reopen for many services that have not been offered since the beginning of the pandemic and by reducing overall infection risk by eliminating waiting rooms and waiting in line.

NWI
NO WAIT INSIDE

David Waxberg
Account Manager
dwaxberg@nowaitinside.com
515.214.4510

As an organization, ISAC strives to promote companies that are addressing current issues within counties and supporting the efforts of county officials. No Wait Inside offers counties a low-cost and efficient option for safely offering essential services to Iowans. ISAC proudly endorses No Wait Inside, and several Iowa counties use and recommend its services.

"We selected No Wait Inside because our Treasurer's Office was looking for a solution to begin service to the public again. Price and ease of setup/use were the main reasons No Wait Inside was perfect for our situation. We could spin it up very quickly, and it was very easy for both the public and county employees to utilize. Our public health office is looking at using NO Wait Inside for managing immunizations when they start this fall. Overall, a very positive and pain free answer to a question we had been working on since this started." - Joel Rohne, Worth County IT Director.

"No Wait Inside has been a fantastic software solution for Marion County. It has allowed us to successfully open our doors to the public in a safe manner after COVID-19 restrictions. Our constituents really appreciate the ability to now schedule an appointment for services that they previously had to wait in line for, sometimes for hours. We have had several thousand appointments in the No Wait system, and yet it has helped Marion County successfully keep the number of people in our lobbies and waiting areas to a minimum." - Andrew De Haan, Marion County IT Director

Countless precautions have been put in place by county officials, and we commend the efforts of all essential workers during these times. ISAC will continue seeking the support of companies who provide crucial solutions to the challenges counties face.

For more information about No Wait Inside and their efforts to help county offices re-open safely, please visit the ISAC website and watch the No Wait Inside webinar, Re-Opening Your Buildings and Serving Your Residents Safely, https://www.iowacounties.org/2020/08/no-wait-inside/. Please feel free to reach out to David Waxberg, Account Manager at No Wait Inside or visit their website, https://www.nowaitinside.com/, if you have any questions.

FEATURE - Cybersecurity Month

Cybersecuirty: It's Time to Ask the Tough Questions

Anthony Kava
Digital Forensics / Special Deputy
Pottawattamie County Sheriff's Office
akava@sheriff.pottcounty-ia.gov

CYBER INCIDENTS, REAL WORLD EFFECTS

A curious and terrible thing happened last month: a woman died because she didn't make it to the hospital in time. She lived in a country with modern healthcare. Her ambulance was forced to divert to a hospital 20 miles away instead of the the one in town. The delay was deadly, tragic, and avoidable.

She is the first known victim to die as a result of a ransomware attack. Her local hospital couldn't admit patients without computers. Ransomware, malicious software that infects computers, encrypts files, and demands payment to get them back, is a billion dollar industry. It's crime that targets everyone from multi-national corporations to local governments to grandmothers.

This attack on a hospital in Düsseldorf, Germany, provides a vivid illustration of a cybersecurity incident. The hospital wasn't even the perpetrator's intended target. A digital ransom note indicated the criminals meant to extort payment from the university next door. When police informed the fraudsters that they had, in fact, hit a medical facility, the thieves provided the key to decrypt the hospital's files. It was too late, of course, for one patient.

Thirty servers on the hospital's network were infected by way of a vulnerability publicly announced in December 2019. As in most successful cyber attacks, the criminals did not need a flashy, zero-day exploit, i.e., a secret, new flaw for which defenders have had zero days to prepare. The weakness exploited in September could have been fixed with a software update released in January.

The attackers' technique relied on finding a single, unpatched server over six months out-of-date – an eternity in Internet time. Still, it's not unusual for organizations to run unpatched software for years. Windows 7 stopped receiving security updates from Microsoft in January, yet many desktops still rely on it.

The bug in question was found in Citrix remote access software; not that one vendor should be blamed. All programs have bugs, and it doesn't take a software flaw to allow malicious access. The City of Atlanta experienced a ransomware attack that put departments out of business and cost millions to fix because a Microsoft Remote Desktop connection was left open to the Internet. Attackers were able to guess passwords of legitimate users.

WE'LL SECURE IT LATER

COVID-19 has affected everything. Many of us scrambled to enable employees to work from home. We may have done that with remote desktop software so they could use their regular computers from safe locations. Haste isn't compatible with security. When we tell ourselves, "We'll install it today and secure it later," we're almost always lying.

We are building what is known as technical debt. It's the mounting deficit we create when we put-off doing things right. Each new system adds to the tally, and all debts accrue interest. If we aren't baking security into our projects our bill increases. Eventually, we'll have to pay. We'll either fix the outstanding problems at greater cost or suffer a disaster.

You don't have to be a technical wizard to evaluate security. Elected officials can ask hard questions to ensure their county is prepared for the trials and tribulations that so many others have suffered. If questions are dodged, answers seem less than forthright, or you're placated with a string of buzzwords there may be a problem.

Even with the limited details we have about the incident in Germany, we can draw conclusions. The hospital's critical software was outdated. There are good reasons to delay updates, such as the need to properly test them; however, when there's a known security issue there's a responsibility, to the organization, its employees, and, clearly, to the public, to install the patch as soon as possible.

Some things aren't updated because it's believed that a system is too crucial. It can't be down; too much relies on it. There could be side-effects. No one wants the blame if it breaks. These are excuses. If a system is that critical how can we abide not having a redundant backup for it, a procedure to repair it, and a regimen for keeping it secure?

We can work to contain unexpected vulnerabilities. An exploit against a product is only useful if an attacker can reach it. Placing the hospital's vulnerable server directly on the Internet made for an easy work-from-home solution, but it also left the system exposed. An extra step, like using a Virtual Private Network (VPN) with two-factor authentication, would have made the criminals' job exceedingly harder. They might have moved on to an easier target.

Thieves used these failings to gain a digital beachhead, but to infect dozens of servers required lateral movement. The attackers parlayed the initial compromise into multiple compromises. Endpoint Detection and Response (EDR) software (think anti-virus on steroids), automated policies that enforce strong security settings, and firewalls that segment networks can prevent an invader on one computer from catapulting to another.

Disaster Recovery and Continuity of Operations planning also comes to mind. Had anyone asked, "How do we admit patients when the computers are down?" Had there been a tabletop exercise to explore how each part of the business would run? How will we dispatch 911 calls when the lights go out?

After a criminal element has occupied your network, how can you trust it? The crooks have left. How can you know they are gone for good? The short answer is: You can't. You must rebuild everything from scratch. Ask yourself: Could we do this? Would our backups be uncontaminated? How long would it take? What would it cost?

HARD, IMPORTANT QUESTIONS

You have the expertise to ask tough questions. You know how your county works. Technical details are not as important as operational ones. Are our systems kept up to date? Why not? How do we backup our data? Where are our backups? Are they vulnerable? Can we access them in an emergency? Have we tried restoring a backup recently? Have we ever tried rebuilding from scratch? What gaps exist in our security?

In order to update and backup systems, we also have to ask a rudimentary question: How many computers do we own? Inventory is so important it ranks atop the Center for Internet Security's list of Critical Security Controls for Effective Cyber Defense. The first and second controls are inventories of authorized and unauthorized devices and software. You can't secure what you don't know you have.

DUE DILIGENCE OR CONSEQUENCES

We avoid tough questions because we may not like the answers. There's a false security to not knowing; we need to admit how false it is. Finding that your county is deficient doesn't mean heads must roll. It means action is needed. An appropriate response to a disconcerting answer can always be, "What do you need to fix it?"

Avoiding the truth has its own consequences. Even if your county carries a cyber insurance policy it will not pay-out if you haven't done your due diligence. A breach or ransomware infection could leave you out of pocket for a seven-figure expenditure.

Security flaws exist whether you know about them or not. Ignorance does not improve security. It will cost much more in the long-term. Asking questions can at least tell you where you stand. You will know what to fix and where to direct your county's resources for maximum impact.

It's tempting to avoid uncomfortable questions, and it can be tempting to punish messengers bearing bad news. You may already be hearing from them. When an employee or member of the public asks these sort of questions or offers insight into them, you have the opportunity to consider them a source of knowledge you're otherwise being denied. To turn them away is to choose to remain uninformed.

In the end, vulnerabilities exist whether you know about them or not, no matter who exposes them. If you don't find them first the baddies will. Ask tough questions. Someone must.

FEATURE - Cybersecurity Month

Eric Gookin
Chief Operating Officer
Iowa Secretary of State
eric.gookin@sos.iowa.gov

Our Elections Are Secure
The United States and other democracies have many enemies, but despite their efforts there is no evidence that any of them have changed a single vote in any state in any election in the U.S.

My confidence in the security of our elections stems from all of the work that our county auditors, our offices, and others have put in over the last four years to learn the new language of cybersecurity, and overlay those protections on the long tradition of physical security measures that have always been in place.

Building on Key Partnerships
The whole of the Elections Community, both in Iowa and nationally, continues to learn about the threats our adversaries pose and act to defend against them. As Secretary of State Paul D. Pate is constantly reminding everyone, "Cybersecurity is a race without a finish line." Iowa is at the front of the pack largely because of the partnerships we have forged with other organizations.

Five years ago, the phrase "Elections Community" referred to state and county election officials and one small federal agency, the Election Assistance Commission (EAC). Now its an alphabet soup of allied local, state, and federal government entities.

It is truly a whole-of-government approach in Iowa, and mentioning any of our partners risks leaving some out. However, especially for this audience, dedicated to good governance at the county level, I think it's important to try to list most of them.

To me the importance of reaching county officials and employees on election cyber security is twofold. First, as the local officials with the most responsibility to implement state law in your communities, every one of you is an important voice in amplifying the confidence that voters need to feel when they vote. Second, many of these (or similar) services are available to you in your offices, paid for by federal or state funds. For those offices that qualify for the services, it is expertise that can be readily available to you without incurring significant costs to hire or develop.

We receive election threat intelligence from the Fusion Center, HSEMD, FBI, and the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC). The intelligence comes in many forms. Frequently, they are technical "indicators of compromise." That is, suspicious network activity or IP addresses that we need to have our technical defenses alert to. However, much of the intelligence is descriptive and provides a (mostly) plain-language overview of threats that the intelligence community has identified as important to distribute throughout the Election Community.

The Election Community receives technical support and guidance from the Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), Iowa's Office of Chief Information Officer, and ICIT. We've worked with ICIT to better understand the IT demands and needs of counties. We've undergone quantitative and qualitative assessments by CISA (and several others) to baseline our security posture.

That information is then leveraged to identify training opportunities for county auditors and staff. People are the front of any cybersecurity defensive line. Most recently we held a series of incident response planning sessions, inviting county auditors, IT, and emergency managers to develop plans in case that a security event does occur. The plans are there to ensure that if an incident does take place, everyone knows how to respond effectively.

The training is critical because at the end of the day, no matter what technical safeguards we put in place, we need humans to be alert to threats and identify any suspicious activities that slip by the technology. We need them to feel comfortable in their ability to report what they've seen. This especially applies if they are the ones who, for instance, open a malicious email, or have their username and password compromised. In order to have that level of comfort, they first need to understand the threats we face and be able to identify issues.

I'll also note that the training goes both ways. Across the United States, elections officials are working to educate our cybersecurity professionals on the intricacies of election administration. All of the people I've been involved with from those other agencies are dedicated to the security of the homeland, and are passionate about protecting elections.

Our office has a different perspective than our counterparts at the local and federal levels. That is to be expected. What we have tried to do since 2016 is to bring those different perspectives together and trailblaze a path to the same goal: accurate, fair, and secure elections. All of the partner agencies listed above have presented to county auditors and staff at some point over the last several years. We will continue to build on those relationships to find those opportunities to continue to build the height of awareness that Iowa's Election Community has to defend our elections. This approach won widespread recognition, and won the National Association of Secretaries of State's 2019 IDEAS Award. You can read more details here: https://www.nass.org/sites/default/files/awards/IA-IDEAS-Award-2019.pdf.

I urge you to explore whether you can utilize the aforementioned agencies to your own office's benefit. If you need help with contacts, I am happy to share that information freely. OCIO in particular has a mission that expressly will support county cybersecurity operations.

Technology Hardening

All of the above are important aspects to the state of elections cybersecurity in Iowa. There is no perfect cybersecurity posture. Because of that, I think it's important to further explain just some of the technological hardening that is possible because of the partnerships mentioned above.

I'll start with a fact that is still not well known outside of the Election Community. Elections in the United States have a natural resilience to tampering because every state is unique in its election laws and technology choices. These decentralized, disparate infrastructures means there is no single point of failure in the system.

Through the partnership with OCIO, malware detection and network intrusion devices have been deployed in county auditors' offices across the state. New efforts led by DHS at the federal level are rolling out similar products to local officials nationwide.

Of course none of that means anything if we don't look for holes in the defense and address them adequately. To that end, we've had SOS systems (including the statewide voter registration database, I-Voters) assessed and penetration tested by a variety of state, federal, and private companies.

By the time this article is in print, our office will be only the second secretary of state office to have a public vulnerability disclosure policy in place. That policy will make it clear to security researchers that their discovery of any weaknesses in SOS defenses will be taken seriously, if disclosed in accordance with the policy. That will enable SOS to learn of vulnerabilities from "good" hackers before "bad" hackers can exploit them.

Key Staff Addition

Earlier this year, we hired Jeff Franklin as our Chief Cyber Officer (CCO). Many of you will know Jeff from his time as state government's long-term Chief Information Security Officer (CISO). Jeff also served as the state's interim-Chief Information Officer (CIO). At the end of his CIO stint, we recruited Jeff to come work for SOS.

As our CCO, Jeff is tasked with helping us to continue to mature Iowa's election's security posture. In his first few weeks, Jeff created a cybersecurity framework for elections that we are in the process of executing. The document is a strategic expression of the projects that will direct election security moving forward and is a hybrid approach based off of several frameworks, including the National Cybersecurity Framework. Jeff's work is itself a partnership between the various SOS teams, as well as county auditors, and IT. The incident response planning sessions were led by him and Heidi Burhans, SOS Director of Elections.

As the state CISO, Jeff was one of the first people we reached out to when it was apparent that we needed to rapidly mature our cybersecurity knowledge and posture several years ago. His guidance was and continues to be invaluable to election security in Iowa.

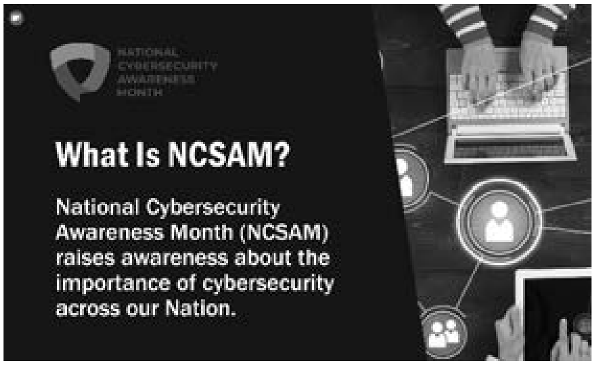
For those reasons above and others I had to leave out due to word count, I am confident in the security of Iowa's elections. We will all continue to defend elections in Iowa to ensure that the outcomes are accurate and secure.

FEATURE - Cybersecurity Month

National Cybersecurity Awareness Month (NCSAM)
"Do Your Part. #BeCyberSmart."

OVERVIEW: Each year, the Center for Internet Security promotes cybersecurity awareness. In its 17th year, this program provides counties with valuable resources that can be used with both employees and citizens to promote cybersecurity awareness.

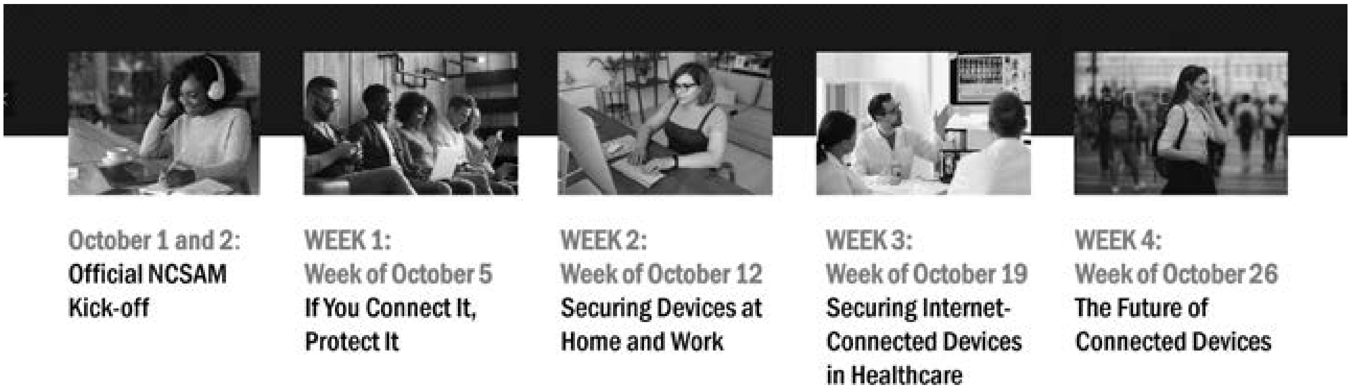
This year, NCSAM will be emphasizing "If You Connect It, Protect It." Throughout October, CISA and NCSA will focus on the following areas in promotions and outreach. See the schedule below.


NATIONAL CYBERSECURITY AWARENESS MONTH

What Is NCSAM?

National Cybersecurity Awareness Month (NCSAM) raises awareness about the importance of cybersecurity across our Nation.

Rita Reynolds
NACo Chief Technology Officer
rreynolds@naco.org



October 1 and 2:
Official NCSAM Kick-off

WEEK 1:
Week of October 5
If You Connect It, Protect It

WEEK 2:
Week of October 12
Securing Devices at Home and Work

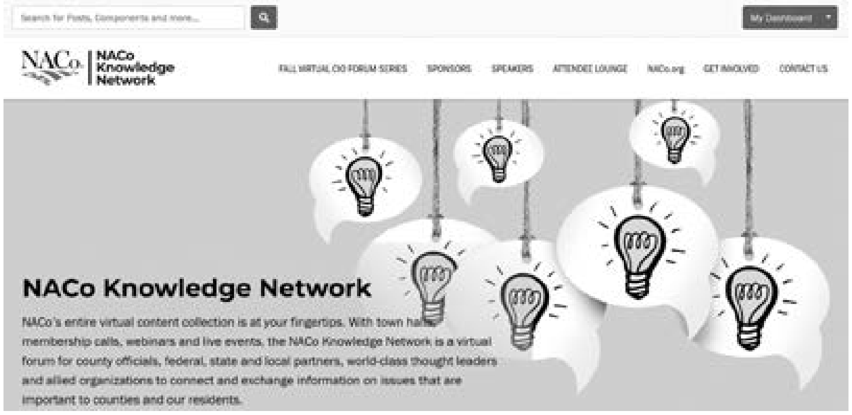
WEEK 3:
Week of October 19
Securing Internet-Connected Devices in Healthcare

WEEK 4:
Week of October 26
The Future of Connected Devices

FREE RESOURCES! On their website are valuable resources in the following areas (see visual examples of these resources on the cover):

Tipsheets on identity theft, online privacy, phishing, passwords, social media, and more.
An excellent educational PowerPoint.
Sample social media posts and graphics for each week.

ADDITIONAL RESOURCES
National Cyber Security Awareness Month and CISA
NACo County Tech Exchange
NACo Virtual Fall CIO Forum Series: October Theme Cybersecurity (delivered on the new NACo Knowledge Network Platform)



NACo Knowledge Network

NACo's entire virtual content collection is at your fingertips. With town halls, membership calls, webinars and live events, the NACo Knowledge Network is a virtual forum for county officials, federal, state and local partners, world-class thought leaders and allied organizations to connect and exchange information on issues that are important to counties and our residents.

FEATURE - Cybersecurity Month

Cybersecurity Collaborative

In our current remote work environment, the susceptibility of a cyberattack has increased with users being exposed to new vulnerabilities that threaten the critical work counties conduct daily. Due to the dynamic nature of cybersecurity, the technology we use is not an exclusive component that requires consistent updating and knowledge development. We must also prioritize the education and awareness of essential personnel within an organization of the best practices to increase cybersecurity readiness and risk mitigation.

Brandon Natsuhara
Operations Manager, NACo FSC
bnatsuhara@naco.org

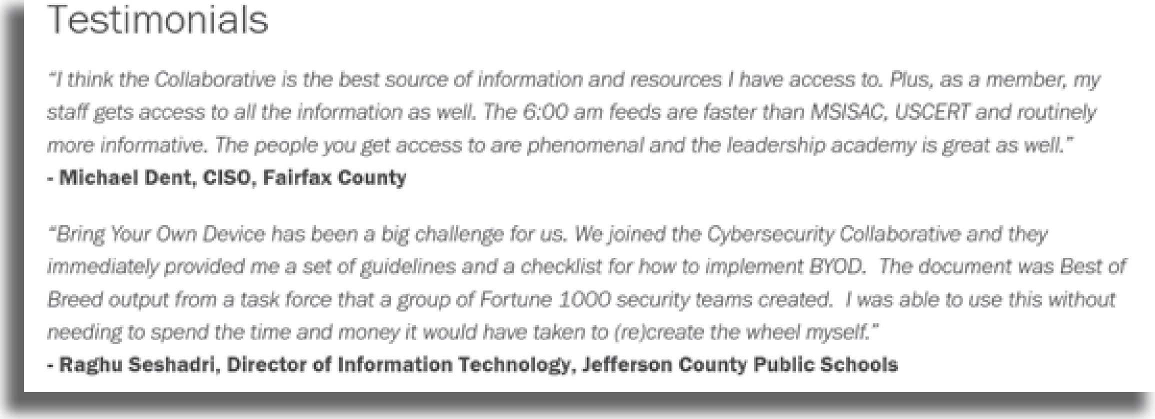
The Cybersecurity Leadership Academy (more on page 12) and the Cybersecurity Collaborative (CSC) are some of NACo's latest initiatives that equip leaders with the necessary knowledge and expertise to proactively strengthen America's counties to better defend and protect themselves, their communities, and our economy from cyberattacks.

CSC specifically is a mission-based membership organization that helps cybersecurity leaders be more successful. The Collaborative facilitates trusted peer-to-peer collaboration, networking, and knowledge sharing to strengthen our members. CSC's core values are providing strategic and technical insights to defend our organizations against our adversaries; professional development in cybersecurity; and mission-oriented advocacy and engagement to advance the cybersecurity industry.

Benefits of the Cybersecurity Collaborative include:

- Daily Security News Alerts arriving in your mailbox by 6:30 AM
- Task Forces and SWAT Teams
- Resource Library of industry leading best practices
- Access to membership – direct communication with industry leading chief information security officers (CISOs)

Counties are already benefitting!



Testimonials

"I think the Collaborative is the best source of information and resources I have access to. Plus, as a member, my staff gets access to all the information as well. The 6:00 am feeds are faster than MSISAC, USCERT and routinely more informative. The people you get access to are phenomenal and the leadership academy is great as well."

- Michael Dent, CISO, Fairfax County

"Bring Your Own Device has been a big challenge for us. We joined the Cybersecurity Collaborative and they immediately provided me a set of guidelines and a checklist for how to implement BYOD. The document was Best of Breed output from a task force that a group of Fortune 1000 security teams created. I was able to use this without needing to spend the time and money it would have taken to (re)create the wheel myself."

- Raghu Seshadri, Director of Information Technology, Jefferson County Public Schools

If you would like to sign up for more information and/or schedule a demo of the platform, please fill out this form here. Also, please do not hesitate to reach out to me directly if you have any questions.

FEATURE - Cybersecurity Month

Rita Reynolds
NACo Chief Technology Officer
rreynolds@naco.org

NACo Cybersecurity Leadership Academy
In our current remote work environment, the susceptibility of a cyberattack has significantly increased with users being exposed to new vulnerabilities that threaten the critical work counties conduct daily. At the same time, the dynamic nature of cybersecurity makes it more imperative that county IT leaders continue to increase their knowledge around both cybersecurity as well as leadership skills.

To that end, NACo had the foresight to partner with the High Performance Leadership Academy in 2018 to bring two core courses to NACo members, The High Performance Leadership Academy and the Cybersecurity Leadership Academy. While in my former role as CIO for the County Commissioners Association of Pennsylvania, I had the privilege of completing the Cybersecurity Leadership Academy. I can say it was one of the top online education experiences I have been a part of.

What makes this offering stand out! The NACo Cybersecurity Leadership program has been designed and developed in collaboration with CISO, CIOs, other executives and thought leaders including General Colin Powell, Dr. Marshall Goldsmith, and many more. This 12-week online facilitated program is a comprehensive, whole solution to help leaders improve. Content focuses on the most important leadership capabilities and skills which will enable cyber leaders, risk managers, and others responsible for business continuity to be more effective in their roles, enable greater team performance, and deliver higher levels of business value.

From my personal experience, let me share three benefits to taking this course. First is the access and structure. This online offering is spread out over 12 weeks, with short daily readings the first three days in the week, followed by a small group discussion on Thursday, and then a one-hour cohort presentation on Friday. By having specific assignments, it was much easier to stay up to date on the course.

Second is the content. Topics include the following, along with a combination of proven theory, action learning, and practical application that is immediately valuable.

- The Security Leader Mindset
- The Art of Security Intelligence
- Balancing Security and Innovation
- Security Change Management
- Positive Leadership in Security
- Collaboration and Negotiation
- Security Communication
- Relationship Management
- Security and the Network of Things
- Your Changing Role in Security
- Performance Coaching in Security

One of the learnings that I took away from the course, was how to get to “yes”, even when the immediate answer appears to be no. I learned there is almost always a way to get to “yes”; sometimes it is “not now” or “how about we look at the problem or issue another way”. I also was reminded of the importance of relationship building. While technology knowledge is vital, relationships with other departments is critical. Suggestions include spending time with department directors and other senior level leaders and getting to know their business, their pain points, and their innovative ideas!

Third is the networking. I found that being partnered in a smaller breakout group of about 10 individuals of similar roles, I was able to network with other county CIOs and IT Directors across the United States. Sharing insight and similar experiences, made us all feel very comfortable with each other! As the weeks progressed, that foundation was pivotal in our diving into the material and discussing how to apply it.

Let me share with you a few quotes from others that have taken the course:

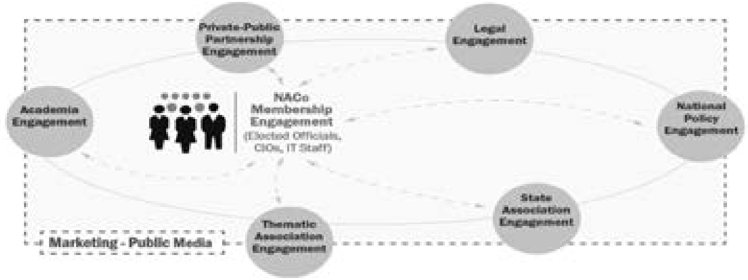
> “Incredible results! I don’t know if unprecedented is too strong a word – I don’t think so!" CIO, University of Pennsylvania
>
> “Each week the course provided skills that could be applied immediately. I worked the weekend so I could use the material on Monday.”
>
> “Like a mini-Masters course on effective cybersecurity leadership! Highly recommended!”

In closing, for any county that has not participated in either of the leadership programs, there are NACo scholarship funds available for the first county participant. To learn more about the program, you can visit the NACo Resource Page (www.naco.org/cyberskills).

NACo Tech Xchange

In late 2019, NACo embarked on creating a Technology Blueprint. The goal was to craft a new organizational technology vision that supports the overall NACo mission and to meet the growing and diverse needs of county IT leadership and their teams.

With the input from a broad range of county IT and state association IT leadership, a blueprint was developed. The group developed a vision and mission, which are focused on promoting access to secure, resilient, and innovative county technologies through collaboration and cost-effective solutions.


Private-Public Partnership Engagement
Legal Engagement
Academia Engagement
NACo Membership Engagement (Elected Officials, CIOs, IT Staff)
National Policy Engagement
State Association Engagement
Thematic Association Engagement
Marketing - Public Media

To that end, seven pillars were identified (see image), with the most important being the NACo Member Engagement.

Under member engagement, one of the goals for 2020 was to create an online opportunity for county IT leadership to engage with each other. That online portal is called the NACo County Tech Xchange.

The NACo County Tech Xchange is an online portal designed to connect county CIOs, IT Directors, CISOs, and other county IT leadership. This portal provides valuable resources in a central location that counties can use to improve their overall technology infrastructure.

What's in it for you and your county?

- A rich community of interaction with other county IT professionals
- An online library of technology policies, job descriptions, request for proposals, best practices, as well as toolkits
- Monthly IT newsletters
- Technology webinars presented by speakers from the federal, state, local, and corporate communities
- Valuable external resources that county IT staff can leverage to improve their county IT infrastructure
- Surveys garnering county feedback on technology opportunities such as technology software and services aggregate agreements

Testimonials

- This is the type of information that we have been missing. - Mark Curtis, IT Director, Stevens County, Washington
- Great opportunity here to interconnect all of the Counties across the US to the resources we need access to! - Phillip Walter, MS, Chief Information Officer, Adams County, Pennsylvania
- I really love the way the Tech Xchange is coming along. Good work! - Christopher Nchopa-Ayafor, CIO, Tarrant County, Texas

For more information go to https://www.naco.org/resources/signature-projects/county-tech-xchange or contact Rita D Reynolds, NACo CTO (rreynolds@naco.org) to sign up for this valuable resource.

FEATURE - Cybersecurity Month

Nick Ballard
Software Developer
nballard@iowacounties.org

You are the Target

People do not believe they can fall victim to a cyber-attack, they believe that it will not happen to them. An important thing to remember about hackers is they do not discriminate. Anyone they can get information from becomes their target. The easier of a target you are, the more likely you will become a victim. Here are steps you can take to prevent yourself from becoming a victim, such as keeping your software up-to-date, running an antivirus program, using strong and unique passwords for different accounts, and not downloading untrusted files.

Keeping software up-to-date with the latest patches will help protect your data. Hackers are constantly testing common applications that people use every day, trying to find vulnerabilities. When hackers can successfully find vulnerabilities, they are able to use the vulnerability to get access to your computer or use it to get complete control of it. When updates are available, it is not always just for adding a new feature. Updates are also used to increase performance and efficiency of applications, and to patch know security issues that an attacker could use to take over your machine. Keeping your computer, and the applications on them, up-to-date will help protect your computer from cyber criminals.

Installing a trusted antivirus software can stop an attack in progress on your computer. Antivirus programs are built to defend against malicious programs, but certain antiviruses can detect and prevent malicious activity. An antivirus program can monitor and identify certain functions within the operating system that are commonly used by malware and hackers. If an attacker already has access to your computer, it is likely you will not notice. The benefits of running an antivirus software is that it can help prevent an attacker from getting initial access, and possibly detect and stop them if they already have access.

Create strong and unique passwords for each website and application you use. Passwords are still one of the biggest causes of cybersecurity breaches to this day. Weak passwords can be easily guessed by an attacker using a script. A good rule of thumb is to use at least a 10-digit alphanumeric password with a mix of uppercase and lowercase letters, and to avoid using words or phrases. Creating unique passwords for each website you use will also help protect you. Take a moment and think about how many of your accounts online use the same password. Reusing passwords is dangerous because if a hacker can get your password from one of the many websites you use, they could get access to all your other accounts too. It is recommended to use a secure password manager to create and manage strong and unique passwords for all your accounts.

Being conscious of the files you download can help prevent you from becoming a victim. One of the most common ways a hacker gains access to a computer is from the user running a malicious file generated by the attacker. The attacker can distribute these files by sending them to you over email or a messaging app like skype, or by uploading it to a website with a flashy popup trying to get you to 'Download Now!'. Once a malicious file is run on a computer, the attacker will have full control. So be conscious of the files you receive over email, or a messaging service, from someone you do not know, and be conscious of downloading files from a website that you are not familiar with to help prevent you from becoming the next victim to a cyber-attack.

There are a lot of different ways a hacker could get access to your data. By following the steps mentioned, you could stop an attack and protect yourself. Hackers rely on out of date applications, no antivirus, weak and reused passwords, and distributing malicious files to gain access to a computer, and harvest the information found on it. Be conscious of how you are protecting yourself from an attack because remember, you are the target.

FEATURE - Cybersecurity Month

Beth Manley
Compliance Officer
bmanley@iowacounties.org

HIPAA Security Risk Analysis
The Health Insurance Portability and Accountability Act (HIPAA) Security Rule requires covered entities, and business associates of covered entities, to conduct a risk analysis. Covered entities are health plans, health care clearinghouses, and certain health care providers. Business associates are entities or people who create, receive, maintain, or transmit protected health information (PHI) on behalf of a covered entity. Even if HIPAA does not apply to your entity, it is still a good idea to conduct a security risk analysis to identify potential security risks so you can implement measures to prevent unwanted security attacks.

What is a security risk analysis?
According to 45 CFR 164.308(a)(1)(ii)(A), a risk analysis is required and states you must "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate." Once a risk analysis has been completed, the next step is to manage the identified risks, but that's another topic and isn't discussed in this article.

The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is responsible for issuing guidance on the Security Rule and often works with other departments to help covered entities understand and comply with the Security Rule. The National Institute of Standards and Technology (NIST) is one of those departments. Specific to the Security Rule, NIST issues publications about cybersecurity standards and best practices to enhance organizations' ability to address current and future computer and information security challenges. NIST's Special Publication (SP) 800 series presents information about computer security and is often referenced when OCR issues guidance on the Security Rule. NIST SP 800-30 is specific to conducting risk assessments.

HIPAA does not define every term used in the Security Rule. The security risk analysis requires you to identify risks and vulnerabilities to electronic PHI but fails to define risk or vulnerability. OCR has identified a few definitions from NIST SP 800-30 that can be used for context but should not be used inconsistently with the terms used in the Security Rule. Here are some definitions that might help you understand what a risk analysis is:

- **Vulnerability** "[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy."

- **Risk** "The net mission impact considering (1) the probability that a particular [threat] will exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur...[R]isks arise from legal liability or mission loss due to — 1. Unauthorized (malicious or accidental) disclosure, modification, or destruction of information, 2. Unintentional errors and omissions, 3. IT disruptions due to natural or man- made disasters, [and/or] 4. Failure to exercise due care and diligence in the implementation and operation of the IT system."

- **Threat** "[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability."

Continues on page 16.

Cybersecurity Month - HIPAA Continued

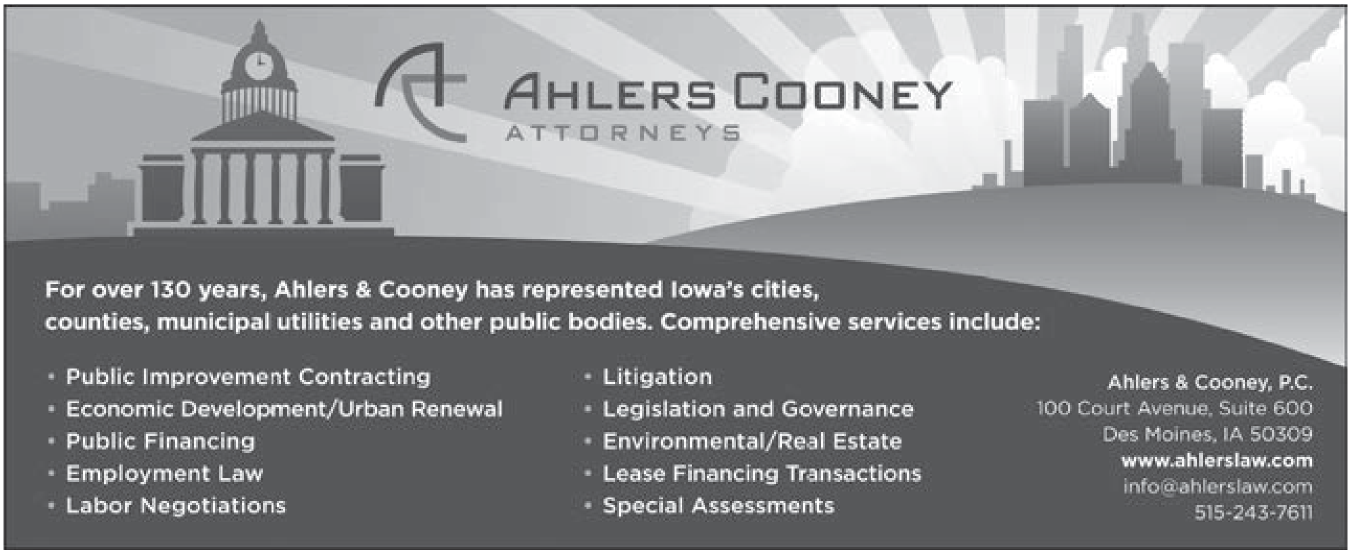
How often should I conduct a security risk analysis?
HIPAA does not have set requirements for how often a risk analysis should be performed. A risk analysis should be an ongoing process and updated as needed. Some covered entities update their risk analysis on a set schedule, like every one to three years, and some update as their environment changes, whether those be external (new cyberthreats) or internal changes (updated systems or work environment). If you haven't already done so, now would be a good time to update your risk analysis if your work environment changed as a result of the current pandemic (i.e. employees working from home).

Are there tools that can help me?
There are multiple tools that can help you perform a risk analysis and comply with other parts of HIPAA. Guidance on numerous topics can be found on the HHS website, including general guidance on performing a risk analysis and answers to specific questions. OCR also created a tool to help covered entities conduct a risk analysis. The tool is free to use and was updated last year.

OCR guidance on the Security Rule: https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

Security Risk Assessment Tool: https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool

Another resource for Iowa counties and MH/DS regions is the ISAC HIPAA Program. For a small yearly fee, the ISAC HIPAA Program provides basic consultation, assistance and training on general HIPAA topics and issues. Feel free to reach out to me if you have any questions and find out more here: https://www.iowacounties.org/member-resources/legal/hipaa-information-for-counties/



2020 calendar and Future Dates

October

1	ISAC Board of Directors Retreat (Virtual)
4-7	ISAA Assessors Fall School (Airport Holiday Inn, Des Moines)
13-15	Recorders Annual School (Hotel Julien, Dubuque)
21-23	Treasurers Leadership Meeting (Wild Rose Casino, Jefferson)

November

18-19	ISAC Board of Directors Meeting (ISAC Office)

December

2-4	Iowa Engineers Conference (Veterans Memorial Community Choice Credit Union Convention Center, Des Moines)
6-9	ISSDA Winter School (Holiday Inn Des Moines Airport)

FUTURE DATES

January 13-14, 2021	ISAC New County Officer's School
January 28, 2021	Statewide Supervisor's Meeting
March 11-12, 2021	ISAC Spring Conference
August 25-27, 2021	ISAC Annual Conference

If you have any questions about the meetings listed above or would like to add an affiliate meeting to the ISAC calendar, please contact Kelsey Sebern at ksebern@iowacounties.org.

2020 ISAC Preferred Vendors

Endorsed Elite Preferred Vendors
County Risk Management Services, Inc. representing ICAP and IMWCA
Group Benefit Partners

Elite Preferred Vendor
IP Pathways

Endorsed Platinum Preferred Vendor
Iowa Public Agency Investment Trust (IPAIT)

Platinum Preferred Vendors
Community State Bank
D.A. Davidson Companies
Henry M. Adkins and Son
Hopkins & Huebner, P.C.
MidAmerican Energy
Northland Securities, Inc.
Schneider Geospatial
Sturgis
Tyler Technologies

Endorsed Gold Preferred Vendor
No Wait Inside LLC

Gold Preferred Vendor
Ahlers & Cooney, P.C.
Cost Advisory Services, Inc.
Cott Systems
Delta Dental
Dorsey & Whitney LLP
EagleView
Forecast5 Analytics
InfoTech, Inc.
ISG
Neapolitan Labs
Purple Wave Auction, Inc.
Speer Financial, Inc.
TechShare
Wells Fargo
Ziegler CAT
Vanguard Appraisals, Inc.
Wellmark Blue Cross Blue Shield of Iowa

Silver Preferred Vendors
FirstNet
Houston Engineering Inc.
Iowa Roadside Management
ITC Midwest, LLC
Nyhart
Thinix, a division of RDI

Endorsed Preferred Vendors
National Association of Counties (NACo)
Nationwide Retirement Solutions
Omnia Partners

Contact Speer today:

Maggie Burger, Sr. Vice President

mburger@speerfinancial.com

Helping Counties Navigate:

- Bond Issues
- Debt Planning
- TIF Projects
- Continuing Disclosure
- Debt Refinancing

MAKE

Speer Financial, Inc.

Your Municipal Advisor TODAY!

County Risk Management Services, Inc.

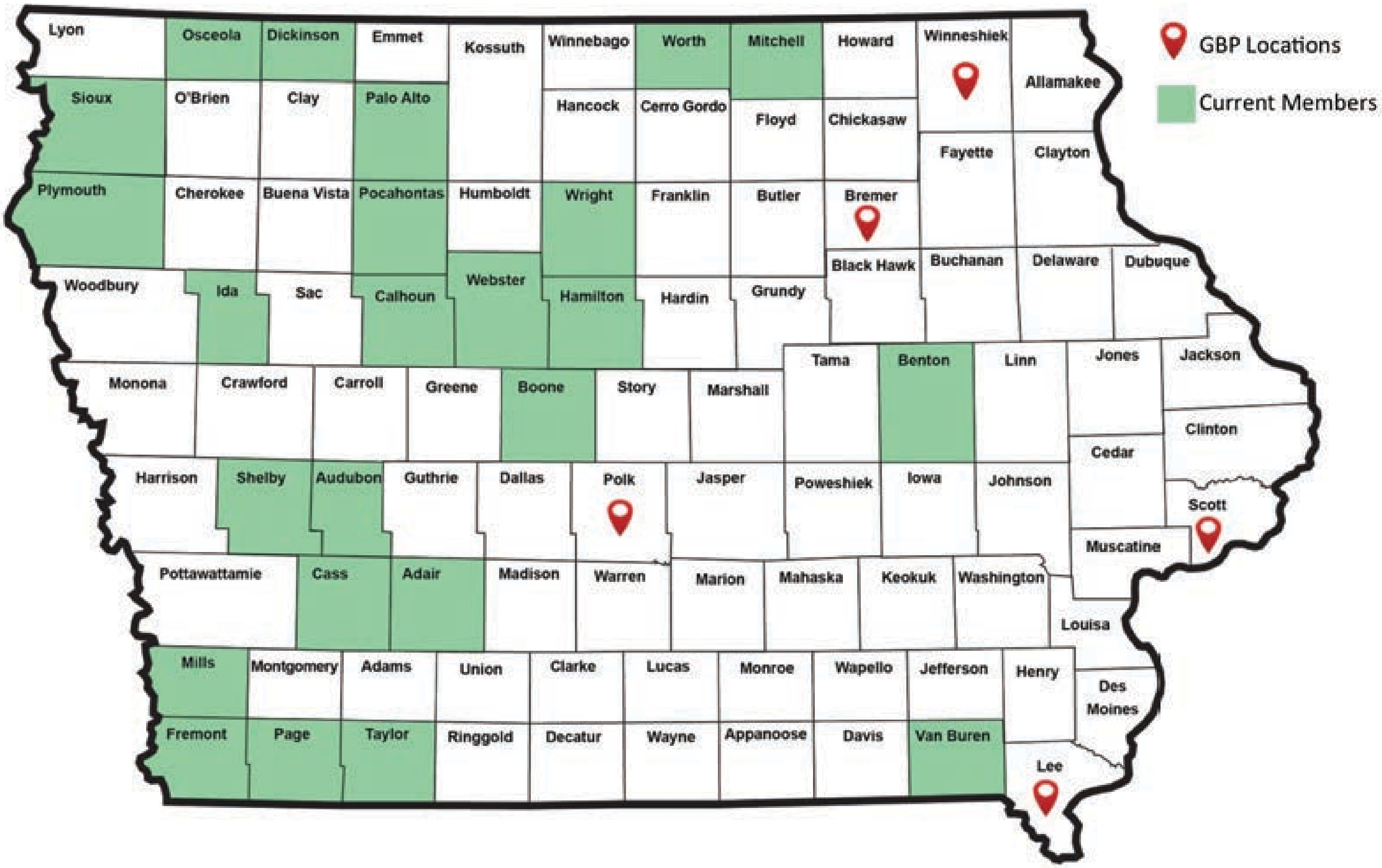
representing

Providing PROPERTY, CASUALTY & WORKERS' COMPENSATION coverage for counties in Iowa.

We're here to serve you!

Programs endorsed by ISAC www.crmsia.com www.icapiowa.com www.imwca.org

ISAC Group Benefits Program



Partnering with Counties across Iowa

- Medical, Dental & Vision Programs
- Online enrollment platform
- Consolidated billing provided
- GBP service & support
- Wellness Program with incentives
- Employee Assistance Program
- HR & Compliance resources
- Third Party Administrator services

Group Benefit Partners

www.gbp-ins.com | 12337 Stratford Drive, Clive, IA 50325 | 515-493-0802