

The Iowa County

magazine



October 2021
Cybersecurity Month



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 

The Iowa County

October 2021 * Volume 50, 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

Copyright © 2021 Iowa State Association of Counties
USPS Statement of Ownership on Page 13

Cybersecurity Month

Email Safety Anthony Kava	4
Ransomware Joel Rohne	5
Website Vulnerabilities Dylan Young	6
NACo Programs and Services Rita Reynolds	7-9
Cyber Attack Simulation Tim Rahschulte, Rita Reynolds	10-11
CISA Helping Iowa Bolster Defense Chris Judge	12-13
Partnerships and Resources in Iowa Jesse Martinez	14
Elections Cybersecurity Grants Dylan Lynch	15
Cyber Insurance ICAP	16
Calendar of Events	22



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.

ISAC OFFICERS

PRESIDENT Carla Becker, Delaware County Auditor
1ST VICE PRESIDENT Richard Crouch, Mills County Supervisor
2ND VICE PRESIDENT Brian Gardner - Linn County Sheriff
3RD VICE PRESIDENT Kris Colby - Winnebago County Recorder

ISAC DIRECTORS

Jean Keller - Bremer County Assessor
Jennifer Robbins - Wapello County Community Services
Matt Cosgrove - Webster Conservation Director
John Werden - Carroll County Attorney
AJ Mumm - Polk County Emergency Management
Brad Skinner - Appanoose County Engineer
Shane Walter - Sioux County Environmental Health
Joel Rohne - Worth County IT
Brian McDonough - Polk County Planning and Zoning
Kevin Grieme - Woodbury County Public Health
Barry Anderson - Clay County Supervisor
Linda Zuercher - Clayton County Treasurer
Elizabeth Ledvina - Tama County Veterans Affairs
Joan McCalmant - Linn County Recorder (Past President)
Burlin Matthews - Clay County Supervisor (Past President)
Melvyn Houser - Pottawattamie County Auditor
(NACo Board Representative)
Grant Veeder - Black Hawk County Auditor (NACo Board)

ISAC STAFF

William R. Peterson - Executive Director
Nick Ballard - Developer I
Lucas Beenken - Public Policy Specialist
Rachel Bennett - Member Relations Manager
Courtney Biere - Office Support Coordinator
Jamie Cashman - Government Relations Manager
Ashley Clark - IT Project Coordinator
Tyler Connelly - Network Administrator
Katie Cook - Member Support Coordinator
Kristi Harshbarger - General Counsel
Molly Hill - Staff Accountant
Brad Holtan - Finance and Program Services Manager
Brandi Kanselaar - CSN Project Coordinator
Beth Manley - Compliance Officer
Tammy Norman - IPAC Program Manager
Brock Ridders - Software Support Specialist
Jacy Ripperger - Marketing Coordinator
Chris Schwebach - Software Developer II
Kelsey Sebern - Event Coordinator
Molly Steffen - Program Support Coordinator
Jessica Trobaugh - ICACMP Project Manager/Trainer
Elijah Turnow - Law Clerk
Dylan Young - IT Manager/Senior Software Developer

**** 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.

Cybersecurity Month - Email Safety

How Anyone Can Steal Your Email for \$4

Many of us are moving to .gov domains. A .gov name identifies you as a government entity. It also makes it harder for someone to impersonate you because only governments can get a .gov; anyone in the world can buy a .com, .net, .org, or .us name. Plus, and perhaps only for a limited time, it's free.

Earlier this year I did an experiment. Back in January I was on one of those long-lived email threads with lots of people on the CC line. I noticed something odd: one recipient's address had a typo. It ended in pottcounty-ia.org, not pottcounty-ia.gov. Where did those misdirected messages go?

The answer was nowhere. The domain did not exist. But that led to a scary thought: the .org name in question was available for anyone on the Internet to register. There was nothing to stop a criminal with \$15 in their pocket from capturing wayward emails and redirecting misguided web surfers.

This kind of attack – using lookalike and Doppelgänger domains – is called typo squatting. Sleazy online advertisers have done it for years. They buy a name similar to a popular website but misspelled, show some ads, and make a profit. Someone with more malicious motives could do worse.

If our little county was vulnerable to attackers who could silently collect emails and spy on unsuspecting citizens, surely there are bigger places with the same problem. I went looking for them. I wrote code to check for available domains similar to the most populous counties and cities in the United States.

There were a number of tantalizing targets, about three dozen in all. Any jerk with an Internet connection, a little know-how, and a few dollars could impersonate these governments. And there's not much that could be done to stop it once it started. The best defense would be to register these domain names ahead of time to deny good real estate to potential attackers.

A big question remained: would such a scheme actually work? Could a criminal exploit this vulnerability for real, sinister benefit? The experiment answered that question, and the answer was a resounding, "YES!" After registering 36 domains and watching them for three months, these were the results: 2,500 emails received with over 200 documents and 170 photos attached, not to mention 1,300 erroneous web visits each day.

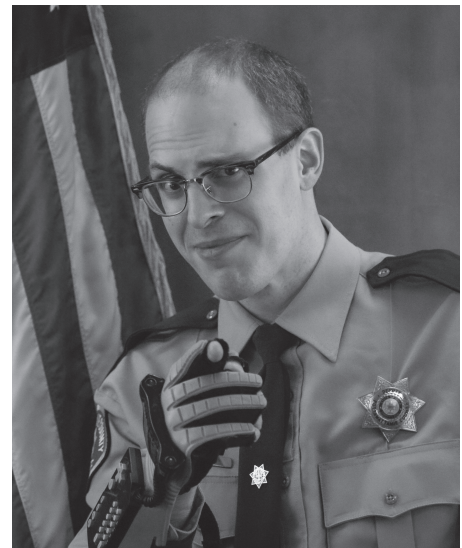
The sort of typo that got me curious in January was affecting local governments nationwide. Citizens, and often employees, mistyped email addresses daily. Long chains of internal communications were being carbon copied out to the Internet, open to receipt by anyone who owned the right lookalike domain. People even sent credit cards numbers and photos of their driver's licenses, social security cards, and birth certificates.

We proved the concept of this attack, but is it happening? The answer is a definite, "Maybe." A lot of government lookalike domains exist. Many are "parked," i.e., registered by someone hoping to flip them like non-virtual real estate to sell at an inflated price. Others are just silently accepting those random emails and web visits.

How do we protect ourselves? The most effective defense is simple: buy lookalike domains. If your county owns them you deny them to scammers. It costs next to nothing; some domains go for about \$4 a year. The best time to buy these domains was before you registered your .gov. The next best time is right now.

I wanted to raise awareness of this easily-overlooked danger. To date, 12 lookalike domains registered for this research have been given to the counties they could have been used to impersonate, and I'm working to transfer the rest. Talks at the Iowa Counties IT ITAG conference in June and the DEF CON 29 Recon Village in August (available on YouTube) have also gotten the word out.

If you want to learn more I've set-up a website to help: <https://impostor.domains>. There's a FAQ and an easy search to run against your own domain names. Try it, then, for your sake and that of your citizens, get your .gov. And don't forget to buy its evil .com and .org twins before someone else does.



Anthony Kava

Hacker

Pottawattamie County

Sheriff's Office

akava@sheriff.pottcounty-ia.gov

Cybersecurity Month - Ransomware

A Parable of Ransomware

Once upon a time, there were two counties in Iowa. The one county was called Proactive and the other county was called Reactive. Iowa has 99 counties, and it was getting tough to come up with good county names.

Proactive was a magical place where the county was very “proactive” in how they approached cybersecurity. All of the county employees were happy, handsome, and always tried to follow good cyber practices whenever they could.

Reactive was a very sad place where the computers crashed all of the time and ran really slowly. They were always “reacting” to all sorts of bad events. A foul beast called Ransomware laid waste to their data. No one could access any of their information and all of the employees spent their time offering “bitcoin” to the Ransomware beast in the desperate hope that they could get their beloved cat pictures restored to them. All of the cats in the pictures were sad as well.

The poor folks of Reactive set out to visit Proactive to see if they could learn how to rid their county of the scourge of Ransomware that had decimated their once great land.

The employees of Proactive were very willing to share the lessons they had learned in their successful fight against the horrid beast, Ransomware.

Here is the cyber decree that all of the employees of Proactive followed and lived by:

1. Thou shalt patch your technology and patch it often. Patching removes the issues in software and hardware that the beast Ransomware uses to get his claws into your data. Sir Jesse Martinez of OCIO can ride to your rescue and let you know what is unpatched.
2. Thou shalt be wary of the scourge of the Phishing attack in all its forms. The beast Ransomware uses Phishing to trick the good people to click on links in emails. Be observant when gazing upon all emails and think mightily before you click.
3. Thou SHALL backup all data and back it up to many places inside and outside the kingdom! Thou SHALL test your backups! How do you know you actually have your data backed up unless you test to make sure? When the Beast Ransomware steals your data (and he shall) you can rest much easier knowing you have outsmarted the monster once again.
4. All the good people of Proactive spent time with the wizards of cyber security (such as Kava the Wise), listening and learning to all the wizards had to say. Proactive knew the value of continuing education when it came to defeating Ransomware.

The simplicity of this decree astounded the good folks of Reactive! They exclaimed!

And the county people of Reactive rejoiced.

Reactive is now a much happier place (even the cats), and a much more handsome place (even the cats) now that they know how to fight the dreaded beast Ransomware.



Joel Rohne

IT/GIS Worth County

joel.rohne@worthcounty.org



We are now at the end of our story, but we must all not forget that the Ransomware beast is always at the door. We must be ever vigilant (that means alert), because the threat is ever changing and always waiting for the slightest opening.

As always, please reach out to any ICIT member if you have any technology discussions or projects that you would like assistance. ICIT is a resource for all counties across the state of Iowa. Start by attending our webinar at 1:00 pm on October 17. Bring your questions, and find out more at www.iowacounties.org.

Cybersecurity Month - Website Vulnerabilities

Common Website Vulnerabilities

As technology continues to surge in today's world, you are probably hearing a lot about cybersecurity and ways to avoid having your systems compromised. You may not even work in the technology field, and it seems day after day you hear about some sort of cyber threat. You may even be tired of hearing from your own IT departments - the same old thing as they tell you to not open suspicious unexpected emails, to not click links in emails from untrusted senders, to never give out your password, and to use different and complex passwords. As these of course are all important, have you ever wondered if these are the only things we should worry about?



Dylan Young

ISAC IT Manager/Senior Software Developer
dyoung@iowacounties.org

Think about all the services and websites that you use on a regular basis. In our world today, there isn't much we do that isn't online. We can purchase merchandise, schedule services, book events, transfer money to and from our banking account, and even access our medical records. With so many services that we use today being available on the web, let's highlight two common ways that cyber criminals use to exploit web applications to gain access to unauthorized data. What exactly are they looking for, and how do they do it?

- 1.) **SQL Injection** First off, what is SQL? Structured Query Language (SQL) is a programming language used to communicate with a database. Most web applications store some sort of information and often use SQL to access that data, which then can be presented through the website. What exactly is SQL injection? Let's say for example you are visiting a website that offers different training courses, and there is a search field for you to find the type of course you are looking for. If you type in "cybersecurity" and click search, this action gets passed to the server, and the server executes a SQL query that looks for all the courses that match "cybersecurity." But what if instead of typing in "cybersecurity" in the search box you tried putting in specific SQL language text to try and intentionally trick the server into executing unintended commands? SQL injection is a way to exploit unsanitized and poorly formed SQL queries on the server side by means of passing SQL statements through input fields or URLs. Success in this can allow potentially any query to be run which could be used to access sensitive information, alter records, delete records, and add records from the systems database.
- 2.) **Cross Site Scripting (XSS)** Cross site scripting (XSS) is when an attacker embeds client-side code (JavaScript) into a web page that then gets executed every time that page is loaded by users. How do they possibly embed code into a website? Let's say for example you are visiting a web forum that allows you to comment on a specific topic. When you type your comment or post in the input field and click save, your post is submitted to the server, stored, and the web page refreshes, which then allows your post to be available for all users to see. What happens if instead of typing your comment, you input JavaScript code? Let's assume that the web application is not sanitizing input or properly handling the way it displays and renders inputted data. If I post some JavaScript code that redirects you to my webpage and this is successfully saved, every user that goes to this forum where my post is will be redirected to my website instead. What's the point of this? In this example this would be more annoying than threatening, but what if I sent you to a malicious site or what if I made my website look exactly like the forum and users couldn't tell the difference between the two? I could prompt users to login on my website, capture their usernames and passwords, and redirect them back to the real website without them being aware. Another common form of an XSS attack is injecting code that sends their session cookies to the attacker's webserver for the attacker to see. If I injected this code into my comment, every time a user loads the forum with my malicious post, I would be capturing each user's session cookies that visited this page without them noticing at all. What is a session cookie? A session cookie is a way for the website to keep track of who you are between the browser and the server. If you are logged in and I get a hold of your session cookie, I could potentially use your cookie and automatically become you without having to know your username and password. I would have access to your account and everything associated with it. This is referred to as session hijacking and is one of the most common goals with cross site scripting.

Cross site scripting and SQL injection are the most common vulnerabilities on websites and are often the most overlooked cyberattacks. As cybercrimes continue to increase and technology continues to change, it is important that we keep ourselves educated in every way our systems could be exposed. People work so hard to protect their systems and networks, but they may overlook or not think about the smaller issues that potentially could be just as catastrophic.

Cybersecurity Month - NACo Services and Programs

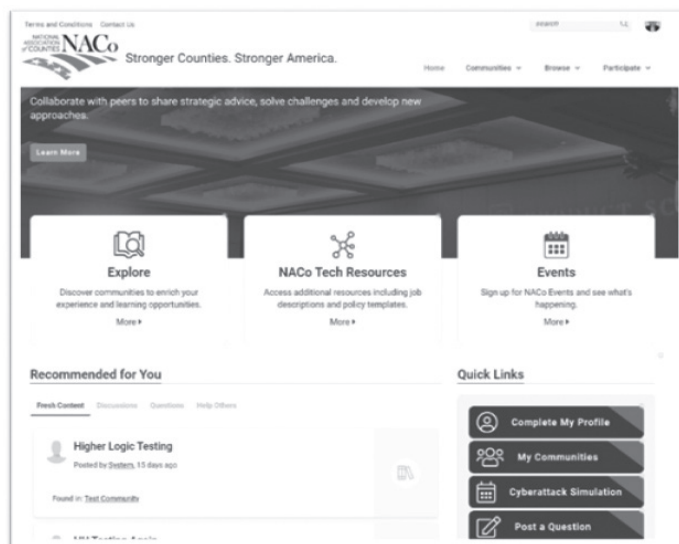
NACo Technology Services and Programs for Counties

The National Association of Counties provides many valuable services and programs for counties across the United States. In recent years, we have worked to create a portfolio of valuable technology resources, services, programs, and education. Highlighted below are the various opportunities that IT Leaders and other county officials and professionals can take advantage of.

NACo TECH XCHANGE

NACo offers a rich discussion platform for county IT Leaders to engage with each other and receive up to date announcements from NACo on evolving technology issues and initiatives. In August, we introduced a new platform that provides even more benefits, including:

- The ability to locate prior conversations;
- The ability to update your personal profile;
- The ability to find other members easily and communicate with them; and
- The ability to set the receipt of Tech Xchange emails to a daily or weekly digest.



In phase two, more features will be added including the ability to join other discussion groups by topic and interest. As of mid-September, we have over 680 county members and are growing.

Also available to those on the NACo Tech Xchange, is a web portal. This site contains a central location for technology resources and a library of policies, job descriptions, RFP's, toolkits, and best practices. For more information on both components of the Tech Xchange and to register, you can visit: <https://www.naco.org/resources/signature-projects/county-tech-xchange>.

COMMITTEES

NACo offers technology related committees in which county members can be involved.

- The NACo Technology and Telecommunication (T&T) Policy Steering Committee covers all matters pertaining to telecommunications and technology policy, including, but not limited to the county role as a telecommunications regulator, service provider, and consumer, cable services technology and implementation, information technology development and implementation, information technology innovation, e-governance, and geo-spatial.
- The IT Standing is comprised of county IT leaders and elected officials that have a more in-depth interest in technology. This committee interacts with federal agencies like CISA (a part of Homeland Security) and provides subject matter expertise to the T&T committee.
 - The IT Advisory Council is the newest subcommittee under the IT Standing Committee. Its purpose is to provide input to, and help develop and vet, the various technology program offerings provided by NACo.
 - The Geospatial subcommittee is comprised of county professionals including GIS Directors, Assessors, Planning Directors, as well as elected officials with an interest in promoting GIS. The GIS subcommittee serves as subject matter experts to support IT Standing and T&T.

These committees have regular virtual meetings and hold in person meetings at the NACo Legislative Conferences and Annual Conference. You can learn more about NACo technology including the committees and application process by visiting NACo's website at <https://www.naco.org/topics/telecommunications-technology>

Continues on page 8-9.

NACo Services and Programs Continued...

EVENTS

Cyber Attack Simulations: Throughout 2021, NACo has partnered with the High-Performance Leadership Academy to offer quarterly Cyberattack simulations. The goal of these exercises is to provide a structured forum for counties to test their continuity and response to various types of cyber simulations. Cyberattack scenarios that have been offered include ransomware, pandemic, third-party provider, and IoT (internet of things). The week-long activity involves a daily 30-minute webinar, as well as homework for county attendees. IT, county administrators, continuity directors, and HR directors are encouraged to participate. The next scenario will focus on insider threat. To read more flip to page 10, and register your team at <https://www.naco.org/naco-cyberattack-simulation>.

Webinars: Also available through NACo are monthly technology webinars. The topics covered include cyber, improving your county infrastructure, data governance, broadband, citizen engagement through social media, and strategies for implementing technology. The most recent webinar is an excellent overview of the importance of multi-factor authentication, which (every county should be implementing). Visit <https://www.naco.org/events/practical-path-mfa-%E2%80%93-how-secure-every-single-account-one-step-time> to watch “A Practical Path to MFA – How to Secure Every Single Account, One Step at a Time”.

"Cybersecurity is such an important topic. I believe that we stand a much better chance at collective improvement if we're all working together. The simulations provided by NACo and the PDA Leadership Academy significantly contribute to that cause."

CIO Forums and IT Summits: County IT leaders and elected officials can learn a great deal on technology priorities and stay up to date on technology innovation by attending the NACo CIO Forum and IT Summit. The all-day event generally precedes the NACo Legislative and Annual Conferences and consists of panels, fireside chats, and other interactive presentations containing relevant content provided by knowledgeable speakers from national entities, county members, and industry experts. Save the date of February 11, 2022 and visit <https://www.naco.org/events/conferences> for up-to-date information. Prior CIO Forum recordings are available at <https://www.naco.org/education-events#on-demand> and filter using “Telecommunications and Technology.”

CYBER

Cyber Priorities and Best Practices: NACo recently released a Cyber Priorities and Best Practices publication, which can be found at <https://www.naco.org/cyberpriorities>. This new publication highlights the importance of cyber and can serve as a resource for counties in strengthening cyber defenses. This three-page summary was developed with input and information gathered from county CIO and IT director leadership, national resources such as the Multi-State Information Sharing and Analysis Center (MS-ISAC), and cybersecurity and Infrastructure Security Agency (CISA), Tech Xchange surveys and discussions, as well as interaction with other national associations, including the National Association of State CIOs (NASCIO).

October Cyber Awareness Month

Cyber Security Awareness Month is just around the corner – CISA has released a nice toolkit that can be used during the month of October for counties to educate employees as well as citizens on the importance of cyber security. These templates will not only save you time, but also help promote cyber hygiene. Another great resource to share during October is the CISA web resources on Ransomware. <https://www.cisa.gov/stopransomware>.

Member Quote:

I just want to say that I appreciate the way that NACo handled the priorities and best practices document. I have had some anxiety about a best practices document being 'weaponized' to support federal mandates. I think you did a great job of framing this so that it characterizes both the practices and the challenges that counties are struggling with in the chase to implement such practices.

NCSR: NACo supports and encourages all counties to Sign up for the National Cyber Security Review. The NCSR is an online and in-depth survey that county IT can complete. NCSR is a no-cost, anonymous, annual self-assessment designed to measure gaps and capabilities of your cybersecurity programs. It is based on the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) and evaluates cybersecurity maturity across the nation while providing actionable feedback and metrics directly to individual respondents. You can use the results to prioritize your cyber defense improvements. More information and registration for new users is open at cisecurity.org/ms-isac/services/ncsr/

Continues on page 9.

NACo Services and Programs Cont...

Cyber Program and Product Offerings: Cybersecurity Collaborative: Government agencies across the nation are being challenged to change their approach to cybersecurity to defend their organizations and citizen data. As a government leader, where do you go to learn from other security leaders to solve your challenges? Cybersecurity Collaborative can elevate your cybersecurity teams by providing a forum to share experiences and insights, access CISA-approved tools, and collaborate to solve their problems in real-time. Visit <https://www.naco.org/resources/cost-saving-tools/cybersecurity-collaborative> for more information.

NuHarbor Security powered by Tenable and Splunk: NACo has formed a partnership with industry leading cybersecurity providers, NuHarbor Security, Splunk, and Tenable, to provide a comprehensive strategy to counties' Information Security Program. This program maximizes the cost and operational efficiency of leading-edge software solutions, the efficiency of county resource utilization, and will uphold the highest cybersecurity standards. Visit [NuHarbor Security powered by Tenable and Splunk \(naco.org\)](https://www.naco.org/resources/cost-saving-tools/nuharbor-security) for more information.

For further information on any of the NACo services and programs, you can contact Rita Reynolds, NACo CIO, at reynolds@naco.org.

On behalf of Chief
Technology Officer
Rita Reynolds and
the NACo team,
THANK YOU!

NACo SCHOLARSHIP FOR \$795

100% OFF

**ENTERPRISE CYBERSECURITY
CYBERATTACK SIMULATION**

Please accept this scholarship for your participation in the NACo CIO Forum. Email moderator@pdaleadership.com to redeem your scholarship and RSVP today.



For more information email
moderator@pdaleadership.com



Cybersecurity Month - Cyber Attack Simulation

Cybersecurity: A Better Way to Test Readiness than Experiencing Reality

Let's face it, when it comes to some realities it is best to not experience them at all. No one wants to experience a fire in their home or a devastating earthquake, tornado, tsunami, or pandemic. Similarly, no one wants their privacy stolen or the critical assets of their organization threatened. While we would like to avoid risks altogether, we know that they are part of reality; and while nothing tests our readiness quite like reality, we will perform better if we properly prepare.

So, we prepare accordingly. We use risk management protocols to protect and defend against a variety of risks. An example of this is the auto-shutoff switches to our electrical breakers in our homes that prevent a surge in electricity that could cause a fire. We use seat belts to prevent injury from an auto accident. We also use incident response and recovery plans when risks do become reality. Conducting fire drills in schools, offices, and our homes help to prepare us if there is a fire and where we need to respond quickly to protect ourselves and others. We use documented playbooks and manuals sometimes when responding and recovering from a risk-turned-reality because emotions and anxieties can cloud judgement and impair decision making during the chaos of a crisis. It is for similar reasons that we have cyber simulations; we prepare for a reality that we hope never occurs. We prepare because we know the occurrence is very possible, and perhaps, very probable in today's world.

Our understanding of the probability of a cyber risk occurring is similarly high. We know that it is common practice to talk about an inevitable hack, phishing attack, data ransom, or even network sabotage. We also know from security officers, risk managers, and administrators in our community that counties, government agencies, and organizations are not as prepared as they would like to be for the cyberattacks threatening their operations, stakeholders, critical assets, and overall brand. For a variety of reasons (budget, staffing), counties lack fully tested incident response procedures and fully detailed operationalized playbooks ready for use to mitigate cyber threats and to adequately respond to attacks before they become a crisis. Consider the following list of threats. Are you prepared?

There are likely many risks on this list that you feel highly confident about addressing if faced in reality. There are likely many as well that you are not very sure about your abilities to face effectively and that you may not even recognize. Finally, there are likely many others that you know for sure that you are not prepared to face with any level of confidence.

In a recent cyber simulation we engaged in, 48% of participants said they have nothing in place to protect, defend, respond, and recover from a ransomware attack. Another 20% in the study said they had a defense defined, but it has not been tested. No one in the study felt highly prepared in their readiness to experience such a cyberattack.

Collaboration is key to success when facing any of these risks. It is for this reason that the NACo County Tech Xchange and the Professional Development Academy have partnered to offer quarterly cyberattack simulations for leaders (<https://www.naco.org/naco-cyberattack-simulation>) – collaborating with one another in a highly facilitated, online program to increase readiness to address the riskiest of risks.

The overriding objective of any cyber simulation is to assess current risk management capabilities among individuals, teams, and key stakeholders. Most simulations assess how well that team of people can detect, defend, respond, and recover from a cyberattack. In addition to people, a well-planned simulation can also highlight readiness of planned processes and use of risk management technologies. In short, the purpose of a simulation is to assess current preparedness to develop action steps that will help close gaps from current state of readiness to a future ready state. That is exactly what these simulations accomplish.



Tim Rahschulte
CEO, Professional Development Academy
www.naco.org/cyberskills



Rita Reynolds
CIO, NACo
rreynolds@naco.org

Continues on page 11.

Cyber Attack Simulation Cont...

The objectives of each simulation are to:

1. Provide a certified test of incident management plans and associated cybersecurity and risk management playbook details aimed to detect, defend, respond, and recover from a cyber risk;
2. Baseline current cybersecurity and risk management work capabilities relative to a cyber risk;
3. Strengthen the leadership skills of incident managers leading the company through risk planning and incident resolution;
4. Improve the quality of the incident management plans and playbook details based on participant engagement in assessments, peer reviews, and best practice benchmarking; and
5. Develop immediate action improvement plans to strengthen people, process, and technical security controls.

We encourage county leaders to participate in our quarterly sessions – which are held online and facilitated by expert practitioners; and engagement is 100% FREE! Learn more and enroll today at <https://www.naco.org/naco-cyberattack-simulation>.

Tim Rahschulte is the CEO of the Professional Development Academy and chief architect of the NACo High Performance Leadership Program (www.naco.org/cyberskills). Rita Reynolds is the CIO of the National Association of Counties.

A WORLD OF THREATS		
Website defacements	Obtain data left undeleted in cloud	Delete or modify data on public site
Malware-directed internal spying	Blocks access to information system	Computing critical data
Phishing attack	Counterfeit website	Obtain unauthorized access
Compromise mission-critical information	Cause disclosure of sensitive information	Compromise key suppliers' design, manufacturing, or distribution
Network sniffers intercept communications	Exploits weak or no encryption of information	Obtain sensitive data from publicly-available sources
Counterfeit certificates	Malware via email	Wireless jamming
Multi-staged attacks (e.g. hopping)	Malware via removable media	Denial of Service (Dos) attack
Internal and external attack (mixing physical and cyber methods)	Dumpster diving (written passwords left exposed)	Distributed Denial of Services (DDoS) attack
Tampered hardware in supply chain	Software collect network traffic data	Physical attack (e.g. bombing)
Fire	Flood	Hurricane
Earthquake	Pandemic	Tornadoes
Zero-day attack	Data scavenging attacks in the cloud	Exploit vulnerabilities in mobile
Wireless sniffers collect data inside facilities (e.g. key cards)	Physical attack on supporting infrastructure (e.g. cut power)	Subverted individuals placed into organization
Exploit split tunneling (e.g. entering network through laptop on public and secure system simultaneously)	Man-in-the-Middle attack (e.g. third party secretly joins a two-way online engagement)	Exploit multi-tendency in cloud (e.g. observes organizational processes, acquire info, or interfere)
Login/password guessing attack	Hijack IT sessions	Ransomware
Attack timed with critical organizational operation	Malware directs transmission of sensitive information	Third-party violations to policy or procedure accessing information
IoT/SCADA compromises	Insider threat	Software releases with malicious code

Cybersecurity Month - CISA Helping Iowa

CISA and Cybersecurity: Helping Iowa Bolster Defense

People are often surprised to learn that the U.S. Cybersecurity and Infrastructure Security Agency (CISA) has field advisors working in each state, but CISA leadership understand the importance of having security professionals ingrained in the community, working together with area businesses, governments, and community leaders. I was born and raised in Iowa, and it is an honor to be working for CISA in my home state. The relationships I can build by being here go a long way toward keeping Iowans safe and secure, which is very rewarding.

Theodore Roosevelt once said, “nobody cares how much you know until they know how much you care.” CISA’s Regional Director Phil Kirk lives by this mantra, and he instills that sentiment into all his staff.

At the core, this quote means that people appreciate advice from those they know have their best interests at heart. I believe this, and I tend to listen to people who care about others and who seek out opportunities to help those around them.

That is a large portion of what I do every day. As CISA’s Protective Security Advisor (PSA) for the state of Iowa, I proactively seek out opportunities to support stakeholders in protecting Iowa’s critical infrastructure, people, and soft targets. It’s a rewarding job, and others like me are working across the country to help bolster security efforts in every corner of the U.S. and American territories. CISA is our nation’s risk advisor, and there is a lot of risk that needs to be addressed.



Chris Judge

CISA Protective Security Advisor,
Iowa District
christopher.judge@cisa.dhs.gov

Each CISA Region consists of a cadre of security professionals. This group of regional personnel manage incident response operations, critical infrastructure analysis, and strategic outreach to critical infrastructure partners. There are PSAs in a similar role to mine, Chemical Security Inspectors (CSIs), Cyber Security Advisors (CSAs), Emergency Communications Coordinators (ECCs), and many other staff all working together to coordinate critical protection and security missions across the region.

CISA’s staff reinforces our national capacity to defend against cyber incidents, and we work alongside other federal, state, and local agencies to provide cybersecurity tools, incident response services, and assessment capabilities to safeguard the thousands of commercial and ‘.gov’ networks.



Chris Judge, CISA Protective Security Advisor Iowa District, discusses ways to better protect election infrastructure and personnel with the National Election Infrastructure Subsector Coordinating Council during the 2021 National Association of Secretaries of State Conference held in Des Moines, Iowa, August 2021.

Our world is becoming increasingly digitized, the volume, variety, and velocity of data is growing exponentially. While this digital revolution has progressed humanity immensely, as the world gains more platforms, data points, and devices, there are also increasingly more points of failure, and a growing vector for threat actors. In a recent speech to cybersecurity professionals in Las Vegas, CISA Director Jen Easterly stated that there are currently 1.8 billion websites. There is now a cyber-attack roughly every 40 seconds, and one in 10 of those 1.8 billion websites leads you to malware. She also stated that damages from cybercrime are costing the world trillions of dollars, and ransomware has become a scourge affecting every American.

Continues on page 13.

CISA Helping Iowa Cont...

Recent cyber incidents have targeted elementary schools, hospitals, local municipalities, state government offices, pipelines, and meatpacking plants. Every organization – big and small – is at risk.

This was particularly concerning in the health care sector last year when several stressed ICUs, at maximum capacity due to the COVID-19 pandemic, were then struck with ransomware. Every day, threat actors are weaponizing our data and the vulnerabilities of our networks to threaten the confidentiality, integrity, and availability of our information, our privacy, our identity, our critical infrastructure, and our way of life. We must unite to deter these threat actors and prevent these unnecessary attacks.

This is what CISA's staff strive to protect. CISA's new website www.StopRansomware.gov is full of information and resources designed to help organizations and individuals prevent ransomware attacks that can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services. There are tips and best practices listed on this website that can be implemented by organizations today. The time to start reducing risk to future cyber attack is now.



Finally, October is Cybersecurity Awareness Month, which, now in its 18th year, aims to raise awareness about the importance of cybersecurity across our nation. Cybersecurity Awareness Month is a collaborative effort between government and industry with a goal to ensure all Americans have the resources they need to be safer and more secure online. In support of this effort, CISA is holding a Cyber Awareness webinar at 10:00 am on Tuesday, October 12. We will focus on issues and concerns related to Iowa, and the greater region, and we will provide a platform for partners to connect with one another; engage with local, state, and federal agencies; and share solutions and best practices to challenges faced in this unique environment. Register for the free webinar at www.bit.ly/3DnBOPU.

No organization can confront today's security challenges alone, and no organization that partners with CISA should ever have to.

United States Postal Service: Statement of Ownership, Management and Circulation

1. Publication Title: The Iowa County magazine
2. Publication Number: 0892-3795
3. Filing Date: 9/29/2021
4. Issue Frequency: Monthly
5. Number of Issues Published Annually: 12
6. Annual Subscription Price: \$25
7. Complete Mailing Address of Known Office of Publication: 5500 Westown Parkway, Suite 190, West Des Moines, IA 50266
Polk Co. Contact Person: Rachel E Bennett
Telephone: 515.244.7181
8. Complete Mailing Address of Headquarters or General Business Office of Publisher: Iowa State Association of Counties, 5500 Westown Parkway, Suite 190, West Des Moines, IA 50266
9. Full Names and Complete Mailing Addresses of Publisher, Editor, and Managing Editor: Publisher- Iowa State Association of Counties, 5500 Westown Parkway, Suite 190, West Des Moines, IA 50266. Editor- Rachel E. Bennett, Iowa State Association of Counties, 5500 Westown Parkway, Suite 190, West Des Moines, IA 50266
10. Owner: Full Name- Iowa State Association of Counties. Complete Mailing Address- 5500 Westown Parkway, Suite 190, West Des Moines, IA 50266
12. Tax Status: Has Not Changed During Preceding 12 Months
13. Publication Title: The Iowa County magazine
14. Issue Date of Circulation Data Below: 9/01/2021
15. A. Total Number of Copies: Average-2,100, Recent Issue-2,100 B1. Paid/Requested Outside - County Mail Subscriptions Stated on Form 3541: Average-1,869, Recent Issue-1,864 B2. Paid In-County Subscriptions Stated on Form 3541: Average-94 Recent Issue-77
C. Total Paid and/or Requested pCirculation: Average-1,963, Recent Issue-1,941
F. Total Distribution: Average-1,963 Recent Issue-1,941
G. Copies Not Distributed: Average-137, Recent Issue-159
H. Total Sum: Average-2,100, Recent Issue-2,100
I. Percent Paid and/or Requested Circulation: Average-100%, Recent Issue-100%
16. Publication Statement of Ownership: Publication Required. Will be printed in the October 2021 issue of this publication.
17. Signature and Title of Editor, Business Manager or Owner: Rachel E. Bennett, Editor. Date: 9.29.2021

Cybersecurity Month - Partnerships in Iowa

Leveraging Partnerships and Available Resources in Cybersecurity

By leveraging funding available from the Department of Homeland Security, a strong partnership between the Office of the Chief Information Officer (OCIO) and Iowa counties was formed, directly resulting in improvement of the overall cybersecurity posture for Iowa counties through intrusion detection system (IDS), vulnerability scanning, endpoint detection and response, security awareness training, and phishing tests. The OCIO Security Operations Center (SOC) continuously monitors the aforementioned tools and communicates any alerts or suspicious activity back to the impacted county providing assistance to ensure maximum coverage and optimal usage of these services.

Early on, OCIO knew that the implementation of additional services needed to protect all 99 counties from cyber attacks was not going to be an easy task. The individual requirements of each county had to be taken into consideration as a plan was being developed, which took time, constant collaboration, communication, and trust to ensure the successful execution of this plan.

The OCIO Information Security Division (ISD) continues to support and refresh the cybersecurity services available. Censys is a new service that helps discover an organizations' unknown internet assets, inventories those assets, and then identifies the risks that should be remediated. The goal is to reduce your organization's Internet attack surface. If you have any questions about OCIO ISD services your county is participating in or would like more information, please email soc@iowa.gov.

Part of the overall plan was to help implement an Identity and Access Management (IAM) program that can protect user credentials with features like Single Sign-On (SSO) and Multi-factor Authentication (MFA). Cyber threat actors can take advantage of compromised account credentials by gaining access to confidential information or spreading malware. OCIO is currently implementing Okta as an IAM solution for state agencies and is available as a service to counties from OCIO. For information regarding cost, features, and implementation of Okta, please contact government.services@iowa.gov.

Counties are also encouraged to become members of the Multi-State Information Sharing and Analysis Center (MS-ISAC). MS-ISAC has been a valuable source of cybersecurity information and services for many years. Including Malicious Domain Blocking and Reporting (MDBR), a DNS filtering system. MDBR blocks users from accessing harmful websites that could cause malware infections, ransomware, or other dangerous cyber attacks and is being offered to U.S. state, local, tribal, and territorial (SLTT) government MS-ISAC members at no charge. For details contact info@msisac.org.

As the issues we face in cybersecurity evolve, OCIO will strive to inform, discuss, and promote resources that a county can leverage as we all continue our mission to protect the systems and information that we use daily. We will expand the partnership with Iowa counties in an effort to make cybersecurity advancements and provide the needed protections while displaying value to the citizens of the state of Iowa.



Jesse Martinez

Office of the Chief Information
Officer (OCIO)

ocio.iowa.gov

ISAC Legislative Priorities Online Voting Open October 11 through 11:59 pm on October 22!

ISAC voting members will have the opportunity to vote on the 2022 ISAC Legislative Priorities in October. Voting members are the elected officials or appointed department heads of ISAC's 16 affiliates. We will be sending an email to all members on October 11 that will include a link to vote via Survey Monkey. Voting members will authorize their right to vote, vote on policy statements as a package, vote on objectives individually, and recommend up to five objectives or policy statements for ISAC's top priorities. During its meeting on November 9, the ISAC Board of Directors will ratify the member vote on policy statements and objectives, and it will set the top priorities. To aid in the Board's decision, board members will receive three top priority recommendations: 1. Member Vote; 2. ISAC Legislative Policy Committee; and 3. ISAC staff.

If you have any questions or would like to receive a PDF or hard copy of the ballot, please contact Rachel Bennet, 515.369.7010 or rbennett@iowacounties.org.

Cybersecurity Month - Elections Cybersecurity Grant

Elections Cybersecurity Grants for County Auditors

Elections cybersecurity is a continual operation, so too is the funding necessary for cybersecurity. Recognizing the need to support local election cybersecurity efforts, Secretary Pate pledged \$1 million to county auditors in February of 2021. The funds come to Iowa through the Help America Vote Act (HAVA), a federal grant program.

Through the Secretary of State's office, each county auditor in Iowa is able to receive \$10,000 in HAVA security funds to address technology gaps and improve the cybersecurity of elections in Iowa counties. This is a great opportunity for county auditors, and other vested offices, to bolster the elections cybersecurity posture of their county. Below you can find more information about the grants as well as some frequently asked questions.

Frequently Asked Questions:

Who can apply for the grant? Because the grant specifically addresses elections technology gaps and cybersecurity improvements, county auditors should apply for the grant.

How do I apply for the grant? You will need to submit a grant agreement to the Secretary of State's office. The agreement requires you to attest that the funds will be spent in accordance with HAVA and will require a countersignature from the chair of your board of supervisors.

What is the deadline for applying for the grant? This grant is available until the end of the current fiscal year, June 30, 2022.

What if I don't need all \$10,000? You may ask to receive less than \$10,000, but we certainly encourage you to use as much of the funds as possible. However, once you have made one request for a grant, you cannot make a second request even if you did not request all the funds the first time.

Can I do X with the grant funds? It would be impossible to list all the ways to spend the funds. However, possible options include:

- Mitigating issues discovered during vulnerability scanning
- Purchasing hardware or software to protect your network or computers
- Hiring a vendor to assist in mitigating or understanding your threat reports
- Covering expenses related to Dot Gov that are not reimbursable by the Secretary of State
- Meeting the new elections cybersecurity administrative rules
- Other and similar cybersecurity expenditures

The grant funds can also be used on physical security measures related to elections cybersecurity, like new security doors for your voting equipment storage area.

Looking for guidance on how to use the funds? Since this is a federal grant program, it's important to highlight that whether a particular purchase qualifies would come down to what a federal auditor might say yes or no to. With that being said:

The U.S. Election Assistance Commission has quite an extensive FAQ page on the HAVA grants (<https://www.eac.gov/payments-and-grants/grants-faqs>). They even provide some examples and explanations to common questions they receive on possible fund uses. Generally speaking, a proposed expenditure should fulfill the standards of "necessary, reasonable, and allocable."



Dylan Lynch

Elections Cybersecurity Specialist
Office of the Iowa Secretary
of State
sos.iowa.gov

Continues on page 17.

Cybersecurity Month - Cyber Insurance

Cyber Insurance Environment

If you're an ICAP member, you've likely heard us talk about "cyber" over the past few months. We've hosted multiple events on the topic; undertaken an arduous cyber application process; and provided multiple market updates in our attempts to ensure member representatives have been informed of the changing cyber insurance market.

If you participate in the Pool, you know cyber coverage has been on our minds. The insurance landscape is changing. The market is hardening, and the cyber insurance industry is reeling. When you start to dig into things, it becomes very easy to understand why.

AM Best, a credit rating provider, recently reported "the prospects for the cyber insurance market are grim." In a June 2021 report, the agency stated the percentage increase in [cyber] claims is outpacing that of premiums.

Take a look at the US Department of Justice chart shown at right (**Internet Crime Complaint Center IC3*); this chart depicts actual monetary damages caused by cybercrime for the period dated 2001-2020. The year-over-year growth in related damages, especially since 2018, is staggering.

Estimates indicate cybercrime will cost the world \$6 trillion this year, and \$10.5 trillion annually by 2025. For a point of reference, cybercrime damages totaled \$3 trillion in 2015.

At present, cyberattacks are the fastest growing crime in the US. Our collective reliance on technology, coupled with the unique circumstances of the pandemic, has caused organizations and individuals alike to be more susceptible to cyberattack, which are increasing in both severity and frequency.

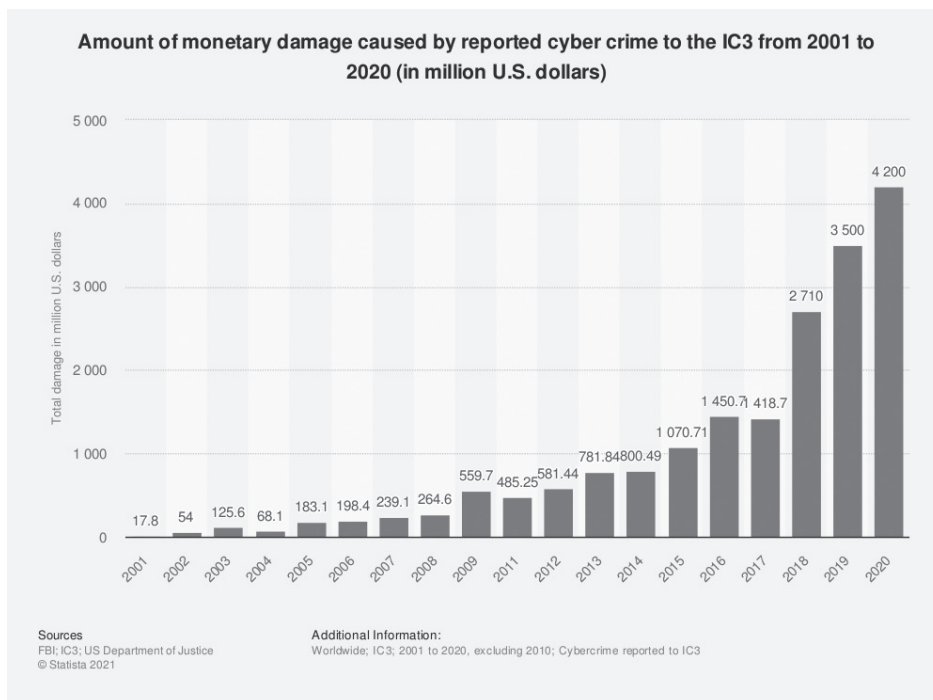
ABC News reports malicious emails are up 600% due to the pandemic (Fortinet reports 1 in every 6,000 emails contains a suspicious URL), and Varonis, an independent data security platform, suggests ransomware attacks jumped 148% in the first month of the pandemic alone.

These are scary statistics, and they get worse, because public entities are being targeted by such crimes. A 2021 Data Breach Investigations Report by Verizon indicated "Almost one in five breaches in 2019 involved the targeting of public sector organizations."



Iowa Communities Assurance Pool

www.icapiowa.com



Continues on page 17.

Elections Cybersecurity Grant Cont...

Another, more technical resource, and possible source for inspiration, is the National Institute of Standards and Technology's (NIST) draft Cybersecurity Framework Election Infrastructure Profile (NISTIR 8310). The profile defines specific practices, provides details for implementing cybersecurity best practices, and is intended to support cybersecurity decision making. Consult with your IT staff or IT provider to determine what may be the best use of the funds.

Can the funds be used for a project that is not 100% elections related? Grant funds can only be used to cover elections-related expenses. If elections expenses or upgrades are part of a larger project, the funds can only cover the percent of costs related to elections.

For example, if your county wants to improve the locks and security system on each of the four doors to your office building, and the elections office only uses one of those doors as their entrance. The grant could only cover the cost of 25% of the project, e.g. one door out of the four.

What are the reporting requirements? The Secretary of State will be sending out a reporting link later this year to all counties that have utilized the grant. The grant is subject to audit by the federal government, and recipients should follow guidelines for expenditure and recordkeeping as required by the U.S. Election Assistance Commission.

For more details about this Cybersecurity Grant, specific questions about the program, fund uses, or for a copy of the grant agreement, please email cyber@sos.iowa.gov.

Cyber Insurance Cont...

There are a number of factors contributing to this, and they boil down to three main considerations:

1. Local governments do not have the funds to replace technological infrastructure and related IT items.
2. The majority of local and state government employees lack training as relates to cyber attack prevention (less than 40% are trained in ransomware attack prevention).
3. Many municipal representatives believe they aren't as "at risk" of cybercrime as larger, for-profit organizations.

Local governments now face increased scrutiny when it comes to cyber insurance. Coverage providers are looking at public entities as an increased risk and requiring a significant amount of nuanced, heavily detailed underwriting information before they will even entertain providing cover. As a result, it is becoming increasingly more difficult for counties and local governmental agencies to secure adequate levels of cyber coverage at prices they can afford.

As we stated earlier, providers are paying out more in cyber-related claims than they are collecting in cyber coverage premiums. This jeopardizes the profitability of the industry and suggests that we should expect to see pricing for cyber coverage increase as we move into 2022. It also suggests, pricing aside, that public and private organizations alike may face an uphill battle when it comes to securing cyber coverage. That is, of course, unless one can present itself as a favorable risk to a provider.

Fortunately, there are things your county can do to help with this. Every public entity should have measures in place to help mitigate the risk of a cyber attack. ICAP's IT Risk Control Team recommends every county:

- Develop an incident response plan;
- Monitor for security incidents;
- Develop relevant policies (and train to them!);
- Establish data backup protocol;
- Maintain a records retention schedule;
- Know the difference between an incident and a breach, and have reporting measures in place; and
- Outline steps to be taken in the event of a breach.

While these recommendations are general in nature, they are relevant to every single Iowa county. They are also a great jumping off point for reviewing any security measures your county already has in place. If ever there is a time to do this, the time is now!

CHECK IT OUT!

THE IOWA STATE ASSOCIATION OF COUNTIES WEBSITE HAS AN ALL NEW LOOK!

🔍 www.iowacounties.org

UPDATED FEATURES:

SIMPLE NAVIGATION FROM THE ISAC HOME PAGE

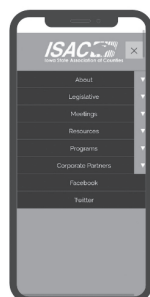
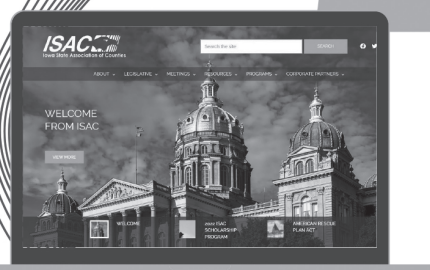
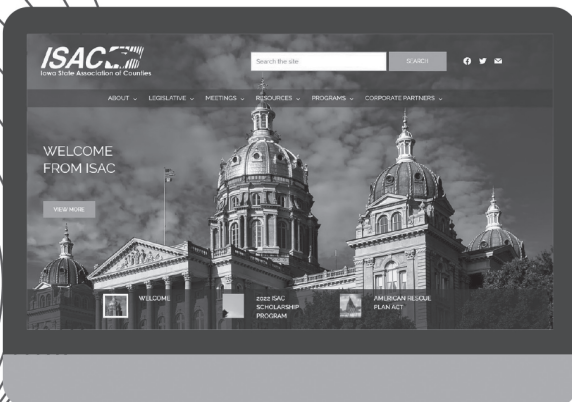
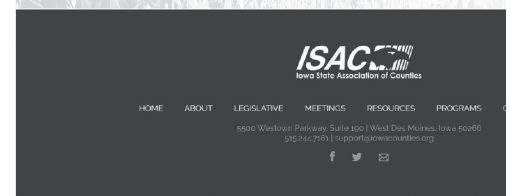
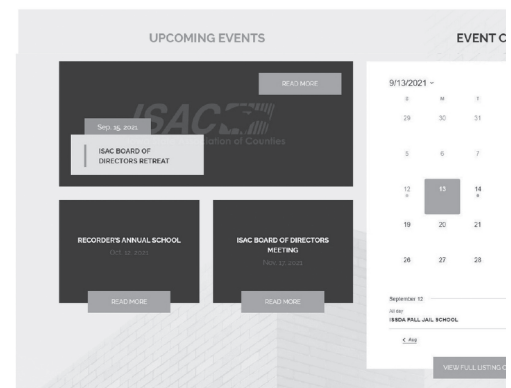
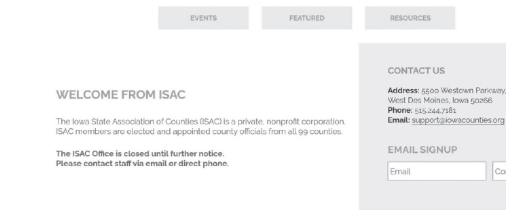
LONG SCROLLING PAGE VIEWS

EASIER ACCESS TO EVENT INFORMATION

SELF-UPLOAD FORMS FOR BID NOTICES AND CLASSIFIED ADS



OPTIMIZED FOR
VIEWING ON
ALL DEVICES!





The IPAIT Advantage

Comprehensive Investment Solutions
designed for Safety, Liquidity and Yield

IPAIT Board Representatives:

Craig Anderson - Plymouth County Supervisor

Jarret Hell - Marshall County Treasurer

Dan Zomermaand - Sioux County Treasurer

Contact Paul Kruse: (515) 554-1555 | toll-free (800) 269-2363 | pkruse@pmanetwork.com

Sponsors:



Investment Advisor/
Administrator/Marketer:



©2020 PMA Securities, LLC. All rights reserved.

Visit www.ipait.org

Take a look!

ANY permit

ANY department

 **GeoPermits™**

UNLIMITED users

UNLIMITED workflows

GeoPermits.com | 515-509-2121



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!



**THANK
YOU!**



Thank you to our generous sponsors of the ISAC Friends of the Education Foundation program. The ISAC Education Foundation is proud to offer scholarships to the children of county officials and county employees.

**WELLS
FARGO**

**COUNTY RISK
MANAGEMENT SERVICES, INC.**
representing

ICAP **IMWCA**



Group Benefit Partners

US★Imaging

Interested in supporting the ISAC Education Foundation?
Contact Jacy Ripperger at jripperger@iowacounties.org



A Cornerstone for Revitalization + Resiliency

Connecting communities to water resources and recreation.



Healthy Eyes. Healthy Smile.
Healthy You!



deltadentalia.com

2021-2022 Calendar

October 2021

- 10-13 Assessors Fall School
(Airport Holiday Inn, Des Moines)
- 12-14 Recorders Annual School
(Dubuque)
- 27 ICTS Advisory Meeting
(Virtual)
- 28-29 Treasurers Leadership Conference
(Emmetsburg)

November 2021

- 9 ISAC Board of Directors Meeting
(Virtual)
- 17-19 ISACA Conference
(TBD)

December 2021

- 5-8 ISSDA Winter School
(Holiday Inn Des Moines Airport)
- 15-17 ICEA Conference
(Veterans Memorial Community Choice Credit
Union Convention Center, Des Moines)

2022

- January 19-20 ISAC University (West Des Moines)
- February 12-16 NACo Legislative Conference (Washington, D.C.)
- March 9 ISAC County Day at the Capitol (Des Moines)
- March 10-11 ISAC Spring Conference (Des Moines)
- July 21-24 NACo Annual Conference (Adams County, CO)
- August 24-26 ISAC Annual Conference (Des Moines)
- October 9-12 Assessors Fall School (Des Moines)

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.

2021 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

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
InfoTech, Inc.
ISG
Neapolitan Labs
Purple Wave Auction, Inc.
Speer Financial, Inc.
Tyler Technologies

Wells Fargo
Wellmark Blue Cross Blue Shield of
Iowa
Vanguard Appraisals, Inc.
Ziegler CAT

Silver Preferred Vendors

FirstNet
Iowa Roadside Management
Murphy Tower Service
Sidwell

Endorsed Preferred Vendors

National Association of Counties
(NACo)
Nationwide Retirement Solutions
Omnia Partners
Professional Development Academy

Simplify Your Cash Management & Focus On Managing Your Budget

Building your trust by effectively managing your entire banking relationship.

csb
community state bank

Member
FDIC bankcsb.com

The Community State Bank Treasury Management Team offers the solutions you need to increase the efficiency of your day-to-day operations and maximize your profitability.

- Liquidity Management
- Receivables Management
- Payables Management
- Risk & Fraud Management
- Information Reporting
- Merchant Processing Solutions
- Business Credit Card Services

Expertise in:

- Association Financial Services
- Government & Public Funds



Crystal Edwards
VP Portfolio Management Officer
515-350-3448
cedwards@bankcsb.com



Mark Rathbun
SVP Business Development
515-249-4236
mrathbun@bankcsb.com

HOPKINS & HUEBNER, P.C.
ATTORNEYS AT LAW
Des Moines - Adel - Quad Cities

Experienced legal counsel for Iowa's counties, cities, and other local government entities.

877-ASK-ATTY
877-275-2889

www.hhlawpc.com

purplewave.com

GOVERNMENT AUCTIONS



purple wave
auction®

- We market your equipment online and in your community.
- We sell your equipment to the highest bidder

866.608.9283 | www.purplewave.com

CONNECTED COMMUNITIES
ARE DATA-DRIVEN COMMUNITIES



Utilize real-time data to drive important decisions for Iowa counties. Learn what's possible at tylertech.com/erp.

tyler
technologies


infotech.

Struggling with FHWA compliance?

Learn more at
infotechinc.com/appia

Appia® helps teams meet state and federal reporting requirements with reports, change orders, certifications, and more tracked and stored in a secure online database.

AN IOWA COMPANY
SERVING
IOWA COUNTIES



**FOR COST ALLOCATION SERVICES AND
FINANCIAL MANAGEMENT SERVICES**

**Contact Jeff Lorenz (515)-238-7989
or Roger Stirler (515) 250-2687**

INNOVATIVE RECORDS MANAGEMENT FOR OVER 130 YEARS



Donald Beussink, Account Executive
c) 319.621.3059 | e) dbeussink@cottsystems.com
cottsystems.com

neapolitanlabs

Website Development
for Iowa Counties

Brian McMillin, President
brian@neapolitanlabs.com
(515) 999-5221
neapolitanlabs.com



Vanguard Appraisals, Inc.

For All Your Assessment Services



- Consultation
- Appraisals
- Software
- Web Sites

1-800-736-8625 www.camavision.com

DORSEY
always ahead

WE ARE A PROUD SUPPORTER OF ISAC AND IOWA COUNTIES.

Dorsey's attorneys provide specialized legal services to Iowa counties, including financing, economic development, public health, privacy laws and litigation.

Dorsey & Whitney LLP
801 Grand, Suite #4100
Des Moines, IA 50309
(515) 283-1000



dorsey.com



6903 Vista Drive
West Des Moines, IA 50266
www.northlandsecurities.com
515-657-4675
Member FINRA and SIPC
Registered with SEC and MSRB



- *Competitive Bond Sales*
- *Debt Refinancing*
- *Property Tax Impact Analysis*
- *Tax Increment Financing*
- *Financial Management Plans*
- *Bond Underwriting*
- *Continuing Disclosure*
- *Bank Private Placement*
- *Referendum Assistance*
- *Capital Improvement Plans*
- *Equipment Financing*

NORTHLAND'S IOWA TEAM

- *Commitment to integrity*
- *Creative solutions to complex issues*
- *Engaged team approach*
- *Customized financial planning models*
- *Staff with depth and experience*



Heidi Kuhl
Director
hkuhl@northlandsecurities.com
515-657-4684

Jeff Heil
Managing Director
jheil@northlandsecurities.com
641-750-5720



Chip Schultz
Managing Director
cschultz@northlandsecurities.com
515-657-4688



RC 20-403; Muni 20-274 10/20

Henry M. Adkins and Son, Inc. (Adkins) was founded in 1939 by Henry Merritt Adkins and has maintained representation in the county government field for over 75 years. In 2011, Adkins became a business partner with Unisyn Voting Solutions, selling and supporting Unisyn voting system products. Our staff has over 100 years of experience in conducting elections and providing quality products and exemplary service to our clients.



- **Full Service Election Provider**
- **Unisyn Voting Solutions voting equipment**
- **Tenex Electronic Poll Books**
- **Tenex Election Night Reporting**
- **EasyVote Election Management Software**



Keeping People Safe One Appointment at a Time

NO WAIT INSIDE

David Waxberg, Account Manager

dwaxberg@nowaitinside.com

517-214-4510

www.nowaitinside.com

Financing Solutions for Municipal Infrastructure



Project Finance: Planning Through Maturity

Capital
Planning



Bond
Issuance



Post-Sale
Compliance

Scott Stevenson, Managing Director
(515) 471-2721 | SStevenson@dadco.com

Michael Maloney, Senior Vice President
(515) 471-2723 | MMaloney@dadco.com

Nathan Summers, Vice President
(515) 471-2722 | NSummers@dadco.com

Full Service Platform:

- Placement Agent
- Underwriter
- Municipal Advisory



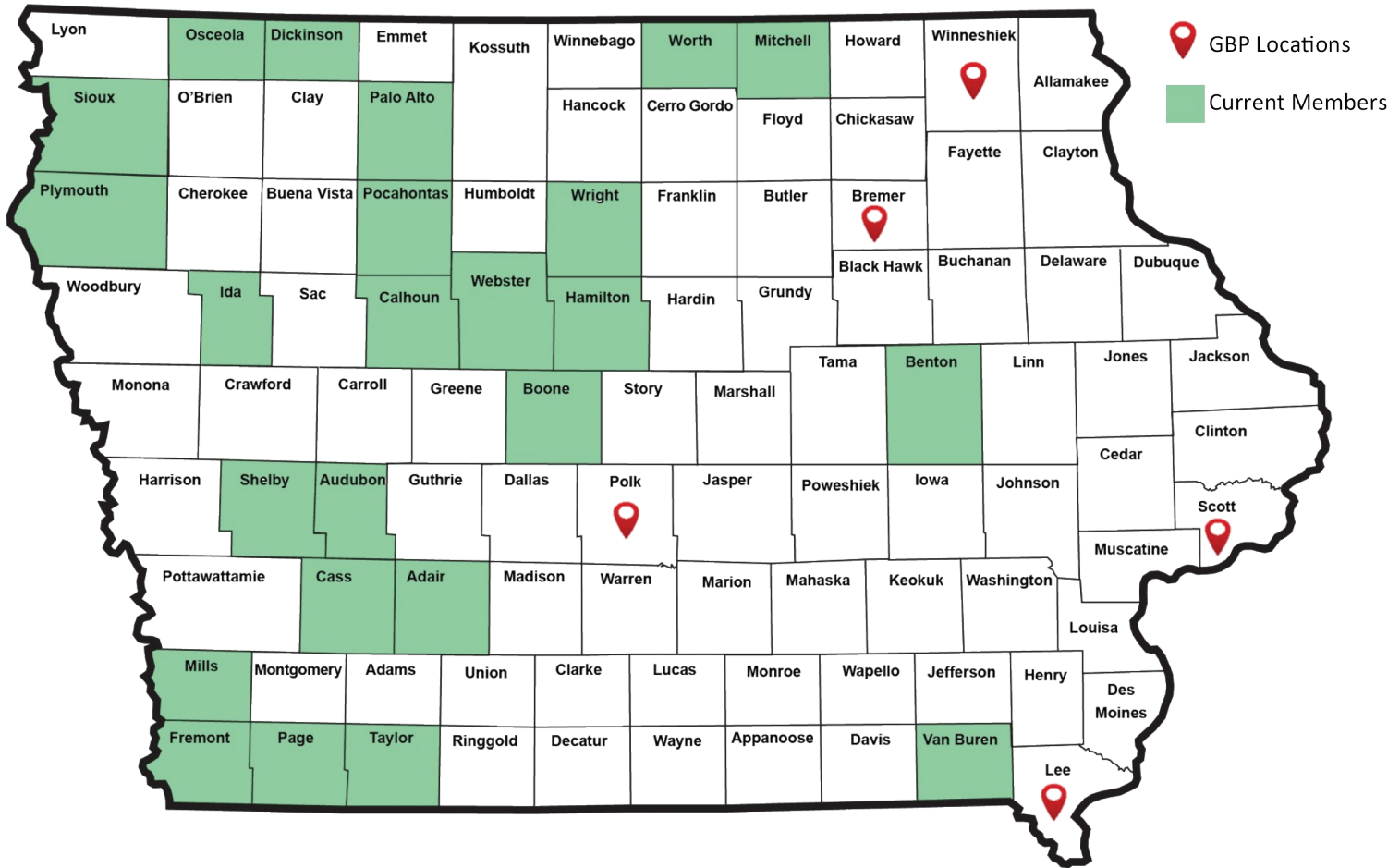
D | A | DAVIDSON

FIXED INCOME CAPITAL MARKETS

D.A. Davidson & Co. member SIPC and FINRA

515 East Locust St., Suite 200 | Des Moines, IA | (515) 471-2700 | (800) 642-5082 | dadavidson.com

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

Check out this member resource, available 24/7

IMWCA Learn online training

With Courses Like:

- Managing Stress in Uncertain Times
- Cybersecurity: Data Privacy and Safe Computing
- Media Training: Crafting Your Message & Preparing for the Interview
- Defensive Driving
- Dealing with Conflict

COUNTY RISK
MANAGEMENT SERVICES, INC.

representing



IMWCA

See the whole list at www.imwca.org/training/learn/



crmsia.com | icapiowa.com | imwca.org



A WHOLE LIBRARY

of e-resources at your fingertips.

Details at www.icapiowa.com



COUNTY RISK
MANAGEMENT SERVICES, INC.

representing



IMWCA

crmsia.com | icapiowa.com | imwca.org