

# The Iowa County



October 2019

Cybersecurity Month



# MADE FOR THE JOB. YOURS.

The new line of Cat® Wheel Loaders was designed with a new approach that gives you:

- + **MORE MODEL OPTIONS**
- + **MORE STANDARD TECHNOLOGIES**
- + **MORE PRICE POINTS**

For everyday jobs like stockpiling and cleanup, the Cat 950 GC combines high performance with low costs, great fuel efficiency, and easy operation. For tough tasks, the 950M is your versatility champion. Upgraded technology and operator comfort saves you money by boosting accuracy and efficiency. Looking for loaders built to do just what you need? That's what Cat delivers.



## 950 M

NET POWER:	BUCKET CAPACITY:	OPERATING WEIGHT:
230 hp	3.3 – 12.0 yd³	42,357 lb

## 950 GC

NET POWER:	BUCKET CAPACITY:	OPERATING WEIGHT:
202 hp	3.3 – 5.75 yd³	41,174 lb

**LEARN MORE:**  
[www.zieglercat.com/next-gen](http://www.zieglercat.com/next-gen)

**ZIEGLER CAT**

# The Iowa County

October 2019 \* Volume 48, 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 © 2019 Iowa State Association of Counties

<b>Statement of Ownership</b>	4
<b>Feature - Cybersecurity Month</b>	
<b>Application Security</b>	4-5
Anthony Kava	
<b>End User Training</b>	6-7
Scott Meyermann	
<b>Cybersecurity Importance</b>	8-9
Colette Klier	
<b>Cybersecurity Partnerships and Elections</b>	10
Joel Merrick	
<b>OCIO Collaboration with Counties</b>	11
Jesse Martinez	
<b>Ransomware and Cyber Attacks</b>	12
Eric Guth	
<b>Patch Management</b>	13
Joel Rohne	
<b>Mobile Security</b>	14
Nick Ballard	
<b>Employment</b>	15
<b>Miscellaneous</b>	16
<b>Calendar of Events</b>	17



#### 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** Burlin Matthews - Clay County Supervisor  
**1ST VICE PRESIDENT** Carla Becker, Delaware County Auditor  
**2ND VICE PRESIDENT** Richard Crouch, Mills County Supervisor

#### ISAC DIRECTORS

Jean Keller - Bremer County Assessor  
John Werden - Carroll County Attorney  
Russell Wood - Franklin County Community Services  
Matt Cosgrove - Webster Conservation Director  
AJ Mumm - Polk County Emergency Management  
Brad Skinner - Montgomery County Engineer  
Joe Neary - Palo Alto County Environmental Health  
Joel Rohne - Worth County IT  
Kathy Babcock - Chickasaw County Public Health  
Kris Colby - Winnebago County Recorder  
Brian Gardner - Linn County Sheriff  
Gene Meiners - Carroll County Supervisor  
Linda Zuercher, Clayton County Treasurer  
Elizabeth Ledvina - Tama County Veterans Affairs  
Shane Walter - Sioux County Zoning  
Joan McCalmant - Linn County Recorder (Past President)  
Peggy Rice - Humboldt County Auditor (Past President)  
Lonny Pulkrabek - Johnson County Sheriff (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  
Jamie Cashman - Government Relations Manager  
Ashley Clark - IT Support Coordinator  
Tyler Connelly - Network Administrator  
Katie Cook - Office Coordinator  
Kristi Harshbarger - General Counsel  
Molly Hill - Staff Accountant  
Brad Holtan - Finance and Program Services Manager  
Brandi Kanselaar - IT Support Coordinator  
Bailey Krebs - IT Technician  
Beth Manley - Compliance Officer  
Tammy Norman - IPAC Program Manager  
Jacy Ripperger - Marketing Coordinator  
Sue Royce - Administrative Assistant  
Chris Schwebach - Software Developer II  
Jeanine Scott - Information Technology Manager  
Kelsey Sebern - Event Coordinator  
Molly Steffen - Program Support Coordinator  
Jessica Trobaugh - ICACMP Project Manager/Trainer  
Dylan Young - 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@iowacoun-  
ties.org. Subscriptions: \$25 per year.



# Cybersecurity Month

---

## AppSec: Why Our Programs are Vulnerable

My name is Karver, and I'm a hacker. I do digital forensics, investigate cybercrime, and try to improve cybersecurity. I've personally relied on the patronage of the fine taxpayers of Pottawattamie County since 2003. In that time, I've been a party to the unequalled dread of implementing and putting out to pasture dozens of computer applications including ancient software suites long maintained by cloistered practitioners, keepers of lost knowledge, translators of ancient, dead languages; Druids casting spells in COBOL.

Protecting computer programs is a discipline known as Application Security or AppSec, for short. Cybersecurity, in general, is marked by an unhealthy obsession with three primary ingredients called the C.I.A. Triad. (Not that C.I.A.) The triad is a tool to help us remember three dimensions of what was once called Information Security but is now known as Cybersecurity because the prefix 'cyber' is cooler.

The C stands for Confidentiality. It's how we keep secrets, well, secret. We do that with encryption, locks, passwords, and permissions. When people think security, Confidentiality is the concept that immediately springs to mind. We interact with it daily when we type our complicated passphrases, and we know we must use these things to keep sensitive records out of the wrong hands.

I is for Integrity. Integrity ensures that our data are not modified without good reason, or at least without our notice. An example is the plastic seal on a bottle of vitamins. The seal is, in security parlance, tamper evident. You want to be able to tell if someone has changed your account balance in a computer system just as you can tell if an evil doer has replaced your nutritious vitamins with delicious M&Ms.

A means Availability. The art of Availability is keeping your systems online. All the security in the world is pointless if we can't use the things we're trying to secure. Consider a flood. If your servers are submerged your Availability is probably affected. Ideally, you keep backup servers somewhere dry so you can keep doing what you do, and so your systems remain available.

If we do Confidentiality, Integrity, and Availability right we get systems that are secure against intruders, proof against meddling, and reachable. The Platonic form of the triad is a lovely ideal, but it doesn't probe the devilish details that guide the operation of our applications. The minutiae that define systems are vital to securing them against real world threats. To do AppSec we need to look under the hood and remember that attackers will not play by our rules.

Hacking is good. Hackers are good, and we want them working on our side. Hacking is about devising creative tech to solve problems. It's about taking stuff apart, putting it back together, and making it do new, amazing things it was never meant to do. It's writing code and experimenting. It's being curious and caring about what happens inside a system rather than just clicking Next, Next, Finish. So, let's call the criminals 'attackers' instead.

Attackers are a real threat. Local governments nationwide have coped for years with a constant barrage of phishing emails and ransomware infections. These are billion-dollar industries. When a species of crime is this profitable, you can be certain it's here to stay, in one form or another. The answers to these problems are not found in a blinky box or a one-time inoculation. Security is a process.

This is not an endorsement of paranoia. While it's possible, in our globally connected world, that someone at a keyboard in Belarus may individually target an Iowa county, it's almost infinitely more likely that we'll be hit with more mundane and impersonal, yet devastating, automated cyberassaults. There are practical things we can do to protect ourselves against both intentional, pinpoint strikes and garden-variety cybercrime.

First, we must accept the shift in our threat landscape in recent decades. Long ago, when some of you were first elected or when public service was merely a gleam in your eye, securing networks meant standing-up a firewall. When you put this all-powerful barrier into place, digital barbarians were kept at bay while you perfected your aqueducts, roads, irrigation, education, and winemaking. This conception, if it ever reflected reality, is dangerously obsolete.



**Anthony "Karver" Kava**  
Tactical Computer Geek  
Pottawattamie County  
Sheriff's Office  
[akava@sheriff.pottcounty-ia.gov](mailto:akava@sheriff.pottcounty-ia.gov)

---



# Cybersecurity Month

---

Firewalls are important, but their job is to segment and control traffic. They can't form the singular defensive fortifications we once believed them to be. The frontier has shifted. To view our networks as castles, with a strong outer wall and moat, is to ignore the fact that besieging criminals are now targeting our endpoints, the PCs. Why spend the effort to breach a firewall when an email with a malicious attachment instantly places you on the inside of a network?

Insider threats are continually underestimated. We still fall victim to the traditional assumption that attackers will launch bombardments from without. We seldom build defense in depth. We don't ensure our networks are tough at each and every layer from the Internet to the employees' PCs. We naïvely assume traffic originating inside our walls is trustworthy.

This paradigm falls apart the moment someone clicks the wrong link. When malware infects a computer on your network, it's no longer your machine. It now belongs to a smooth criminal thousands of miles away. Your outside attacker has become an insider threat. With a foothold in your internal network, the next attacks will be coming from inside the house.

So after we've segmented our networks, automated updates, enabled multi-factor authentication, deployed quantum encryption, and posted deputies in our datacenters, our applications remain our weakest links. They must, naturally, be accessible to our users which makes them vulnerable to attackers who will leverage our own devices against us.

There are many vectors of attack against the special languages, called APIs and SQL, our personal computers use to talk to our servers. For example, a user must authenticate with the server to prove who they are and whether they should be granted access to certain records. If this mechanism is badly engineered an attacker can login without a password or upgrade their access from that of a clerk to that of an administrator.

Some programs are poorly designed. They are written in such a way that every user has direct access to the underlying database. Security is enforced not on the server side, where a big computer can deny access to certain areas, but on the client side where a savvy attacker (or a user who took Databases 101) can manipulate data and circumvent the client's attempts to stop them.

These problems are not hypothetical. Specific vulnerabilities, security weaknesses, including these were found in products sold to Iowa counties. These loopholes have threatened to expose financial information, police reports, and personally identifiable information of employees and citizens.

Who audits our products? Until recently, probably no one. The trouble is that our vendors, who cater to small or medium-sized governments, have little incentive to secure their software. They are not called to account for weaknesses because most of their customers do not have the capacity to look for bugs that could compromise the applications they sell.

A few years ago, we got curious. We began looking for bugs. We're not experts, but we still found glaring flaws by looking under the hood of applications used by hundreds of customers, including many in our own state. We identified problems and reported them to our vendors so they could be addressed.

Shedding light on vulnerabilities carries a superpower. Hackers, as security researchers, have been called the immune system of the Internet. This is because, when a flaw is found and subsequently patched, all users of that software benefit. It's a form of herd immunity. If we all use the same accounting package, and you report a bug that gets fixed, everyone is more secure.

Some vendors are receptive to bug reports. Many, however, get defensive. Weaknesses might be dismissed or take years to fix. Worse yet, a common response is that the developers expect their applications to run in a "secure environment". They disclaim any responsibility because, even if their software is like virtual Swiss cheese, it's your fault if an attacker reaches a workstation to attack it.

So how do we fix this? We need people working in the public interest who will evaluate the security of our products. We need to find flaws, report them, and, most importantly, make software companies responsible for security.

We need to demand better. Our taxpayers deserve this because they not only pay for our apps but will also bear the burden of a breach, in lost data and recovery costs, when an attacker exploits a vulnerability.

There are simple steps we can begin taking today. We can start by writing RFPs with basic security requirements. We can require that vendors audit their software instead of leaving that to the customer. We can demand transparency into our vendors' security practices. We can hack our AppSec. We owe it to our employees and our citizens to try.

# Cybersecurity Month

---

## The Importance of End User Social Engineering Training

With October being Cyber Security Awareness month, it seems appropriate to talk about the subject of social engineering. The weakest link in today's IT environment is the end user. By no means do I mean that in a derogatory sense. Most breaches that happen today start with a phishing attack. A phishing attack is where someone somewhere sends an email to one or several users of an organization in an attempt to get them to respond to an email by either replying to, or clicking on a link that requests they log in to a fake website using their company credentials or asking to provide any personal or financial information. Gone are the days where these phony emails are easy to spot, filled with misspellings or from a Nigerian Prince promising to share his fortune with you if you help him get it out of his country. Phishing emails are getting more sophisticated by the day. Some are so well crafted that they are next to impossible to spot. Phishing is so lucrative that an entire industry's been created for phishing as a service or ransomware as a service. These businesses will do most of the work for a criminal for a fee and are usually located in a foreign country to make prosecution extremely difficult.



**Scott Meyermann**  
Clinton County Network  
Administrator  
[nballard@iowacounties.org](mailto:nballard@iowacounties.org)

---

A social engineering attack is far easier and less time consuming to execute than any other exploit and the likelihood of being caught using this method is close to zero. An attacker doesn't need to spend any time or resources trying to brute force a firewall or run password cracking software on a database of password hashes if he or she can simply send an official looking email to unsuspecting users and just ask them for their credentials.

We can invest in the best perimeter security, antimalware, intrusion detection and prevention systems, and the best log analysis software available, but all of that is useless if the end user willingly gives up their credentials by falling prey to a social engineering email. Once an attacker has valid user credentials it's a trivial task for them to elevate themselves to administrator status and get access to the entire network.

The best defense against a social engineering attack is consistent end user training. One great tool is a phishing simulator. They are easy to set up and provide good information back to the organization. The product can report on who clicked on a link and when, what information they provided, and lots of good information about the PC they were using when they clicked, such as operating system version, browser version, etc.



An initial test run against all users will establish a baseline. Then, conduct a meeting with employees and let them see the results. Use this meeting as a learning opportunity for your users. Explain some of the characteristics of a phishing attempt. For example, a user gets an email to their work email purportedly from Amazon. Have they ordered something from Amazon? Is their work email address connected to their personal Amazon account? (It shouldn't be.) If they still think it may be legit, have them log into their Amazon account from a web browser and check their order status and payments. They could also contact the sender via phone, but not at the phone number listed in the email. They should look up the number another way. Under no circumstances should they reply to or interact with any links in the email itself other than to delete it.

Tell your users that there will be ongoing tests on a regular basis. This will get them in the habit of closely scrutinizing every single email they receive and question its legitimacy. Explain that you're not looking for failure, rather success. If users are aware that regular phishing tests are happening, they'll surely want to pass.

From there, hold a quarterly meeting or send out an email keeping the users informed of their success rate. They'll soon want to see how close to 100% they can get. Visit users that fail the test and let them know that they may have clicked on something they shouldn't have. Take a copy of the phishing email with you and go over with them what they could've noticed that may have made the email suspect. Make it a positive interaction with the user.

# Cybersecurity Month

Train users to look for one or more of the following characteristics of a potentially malicious email:

- Hover over links to check the true source domain. If it doesn't match the link typed in the email, then it may be malicious.
- If the email has a tone of urgency to act, it may not be legit.
- If the email contains threats or scare tactics, it's probably best to delete it.
- Poor spelling or grammar is another indicator of an attempt to trick the user.
- If the email is unexpected or from someone you don't know, you should contact the sender by other means than any contact information included in the email.
- An offer that seems too good to be true in an email probably is. If your instinct tells you that something is off about it, trust your instinct.

Ask users to contact IT if anything seems funny about a given email. IT should gladly take a look at suspect emails because it takes far less time to prevent a ransomware outbreak or identity theft than to recover from one. Let your users know that you are not looking to trick them or make them fail at something, but that you want them to succeed and need their help in keeping our resources secure. Too often, end users feel they and IT are on opposite sides. That culture needs to change.

Social Engineering goes well beyond Phishing. Ask your users how they're verifying the identity of the person that's calling them on the phone asking for information. Are they verifying the identity of the person sitting in front of them before giving out any private information? Even having information sitting in plain view on a desk or displayed on a monitor can be captured by a cell phone camera.

Management, IT, and end users all need to understand that they all need to be on the same side when it comes to combating cybercrime and social engineering. It takes people, processes, and technology to defend against today's cyber criminals. Inform management of the risks, train your people, put sound identity verification processes in place, and use supported up to date technology. By doing these things, you'll make it difficult for a cyber attacker to pull off a successful social engineering attack against your organization.

Scott Meyermann is a Certified Information Systems Security Professional and serves a Network Administrator for Clinton County. He has 24 years of IT experience, including 19 years in the financial services industry.

## 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: 9/18/2019
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: 09/01/2019
15. A. Total Number of Copies: Average-2,250, Recent Issue- 2,250 B1. Paid/Requested Outside - County Mail Subscriptions Stated on Form 3541: Average-1,938, Recent Issue-1,925 B2. Paid In-County Subscriptions Stated on Form 3541: Average-103 Recent Issue-102  
C. Total Paid and/or Requested pCirculation: Average-2,041, Recent Issue-2,027  
F. Total Distribution: Average-2,041, Recent Issue-2,027  
G. Copies Not Distributed: Average-209, Recent Issue-223  
H. Total Sum: Average-2,250, Recent Issue-2,250  
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 2019 issue of this publication.
17. Signature and Title of Editor, Business Manager or Owner: Rachel E. Bennett, Editor. Date: 9.18.2019



# Cybersecurity Month

---

## Cybersecurity Importance

When Robert Tappan Morris developed a worm in 1988, all he wanted to do was figure out how many computers were on the internet. What started as a curiosity instead turned into the world's first cyber-attack. The program was simple. He designed it to jump from computer to computer without needing help from anyone. As it wove its way through the internet, it kept track of all the devices it encountered and reported the final amount back to Morris. The program worked too well, infecting nearly 10 percent of all devices on the internet at its peak, jamming traffic, and preventing people from talking to each other.

Since Morris' innocent cyber-attack, attacks have drastically grown and are specifically targeting government entities now. Just recently, 23 towns in Texas were hit by a "co-ordinated" ransomware attack that prompted Governor Greg Abbott to order a "Level 2 Escalated Response" which is one step below the highest level of alert, Level 1 or "emergency." This came after state and local ransomware attacks in New York, Louisiana, Maryland and Florida. The majority of cyber-related claims are due to phishing or ransomware according to the Iowa Communities Assurance Pool (ICAP). Cybercrime is expected to reach nearly \$6 trillion in damage by the year 2021. That's the bad news. The good news is an estimated 79% of all cyber-attacks could be prevented by having a good cybersecurity plan.



**Colette Klier**  
IT Risk Control Specialist III  
collette@icapiowa.com

---

Here's a general plan to serve as a starting point that public entities can follow to help reduce your risk on the top ways hackers exploit vulnerabilities. While no plan can provide complete protection, this one will help entities prevent some of the more common ways your network can be attacked.

## Action Plan

What you don't know can hurt you. This is why the first part of protecting your network starts with knowing what's on it. This is what our IT risk control specialist immediately focuses on when they're on-site with a public entity. First, you should document all of your hardware, software, and applications.

- Create a list of all the computers (PCs, laptops, etc.), connected devices (printers, fax machines, etc.), and mobile devices (smartphones, tablets, etc.) that you have on your network. All of these are entry points into your network.
- Document all of the programs that are installed directly on computers and used by everyone.
- Keep a list of all the applications that people use on their tablets, phones, and web applications (Dropbox, Google Drive, etc.).

Once you have all of your hardware, software, and applications documented, you'll want to analyze and examine them for vulnerabilities.

- Locate all unused equipment and completely wipe them. If you plan to use them in the future, store them in a secure location. If not, properly dispose of them. Some attackers scout landfills looking for old hard drives on desktops, laptops, phones, and more. ICAP's IT risk control specialist has seen a lot of unused equipment that's not secured or wiped.
- Go through the list of all of your applications and software. If any of them are no longer being used, they should be thoroughly uninstalled from devices, cloud storage, on premise storage, servers, etc. If you are still using the applications, update them. ICAP's IT risk control specialist has also witnessed a lot of "forgotten" applications and software still installed on devices.
- Ensure the passwords used for accounts are secure. When feasible, each unique account should require a separate and secure password. ICAP's IT risk control specialist has noticed passwords written down unencrypted and not secure, posted on equipment, and never changed.
- Check for applications and programs that serve multiple storage purposes. When you have multiple applications or programs performing the same task, dedicate just one as your main option and the other as your backup option.
- Since we're talking about storage, create a records management plan for your electronic and paper records that includes documented retention schedules. Review them on an annual basis and securely destroy any outdated records utilizing shredders or a third-party shredding company. Secure all paper records remaining.

# Cybersecurity Month

---

Once you've documented all of the hardware, software, and applications on your network and you've removed any old equipment or redundant tools, you'll want to make a plan to lower your cyber security risk by putting these practices in place.

- Update and change your passwords often. If a hacker somehow acquires your password, they'll only have a limited time to use it for criminal purposes before it's changed to a new one. Keep your passwords complex. Use new and different passwords for each account. Don't store them on sticky notes or digital documents. Implement two-factor authentication, where possible.
- Update operating systems, software and firmware (network equipment, cameras, scanners, printers, etc.). Set schedules and reminders for you and the staff. Make them required, if possible.
- Update hardware, when possible (newer chipsets are usually less vulnerable). Older hardware often has more information about its vulnerabilities available to hackers. Older hardware isn't always capable of running most up-to-date software, which increases your security vulnerability.
- Install and maintain a full version of endpoint security for all devices with automated virus signature file updates. Do not use free versions of anti-virus software.

You'll also want to manage what's happening behind the scenes. This includes keeping track of new installs, the number of users, preparing a safety net, and educating your end users.

- Implement a mandated process for overseeing the installations of new programs and applications. You can do this through software or provide a document that helps guide people. Part of that process should also include documenting on what device and where each program is installed, especially if you have multiple buildings. This will make it easier to maintain a list of all the hardware, software, and applications on your network and make them easier to update later.
- Limit your users. The fewer accounts you have, the fewer opportunities there are for vulnerabilities and attacks. As part of this process, grant administrator access and other rights only to the people who absolutely need it.
- Back everything up. I'll repeat this again. Back. Everything. Up. Ideally, all of your data should be backed up to a secondary source that's separate from your primary source. In the event that your main source is compromised, hacked, breached, or even malfunctions, you'll have a safety net to help get everything back up and running as quickly as possible.
- Employ a cyber-security awareness training program. There are multiple platforms out there. An example would be KnowBe4. It's designed to help you integrate baseline testing using mock attacks, interactive web-based training, and continuous assessment through simulated phishing, vishing, and smishing attacks to build more resilient and secure "human firewalls."

This is a general guide to help you improve your entity's security plan. However, we also know that a lot of entities need help implementing risk control. ICAP has helped implement risk control for public entities ranging from cities under a population of 100 to counties with over a population of 500,000. If you're looking to improve your cyber risk and are an ICAP member, contact us and we'll help set up an IT risk control visit with our IT Risk Control Specialist.



# Cybersecurity Month

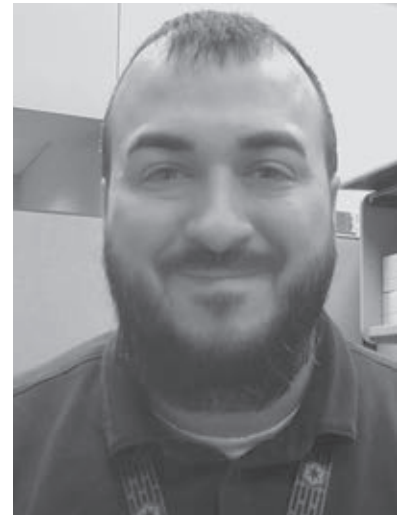
---

## Cybersecurity Partnerships and Elections

According to a report published on August 28, 2019 by the IT security firm Barracuda Networks, almost two-thirds of all publicly-known ransomware attacks that happened in the U.S. in 2019 targeted state or local governments. While some of the most recent headlines came from a collection of mostly small towns and counties in Texas, just before that, it was schools and counties in Louisiana. Not long before those were the higher-profile attacks on Baltimore and Atlanta, costing the cities as much as \$18 million. Unfortunately, we live in a time where everyone, no matter how well-funded, is a target. Which brings up the simple question: “What can we do?”

While this isn’t a problem that’s going away, key partnerships are helping move Iowa in the right direction and working to prevent any of us from being the next big headline. Specifically, partnerships among state agencies, such as state and local groups, like the partnering of OCIO/SOS and the Iowa Counties Information Technology (ICIT) are starting to cover more ground. Additionally, the increased collaboration between the Office of the Chief Information Officer (OCIO) and the Secretary of State’s Office (SOS) has led to large strides in the right direction. Alongside these, partnerships between state and federal agencies like SOS and the Department of Homeland Security (DHS) have been able to provide additional resources and tools across the state. As the rewards of these collaborations continue to come, it reinforces the idea that we all need to work together to help ensure a safer tomorrow.

With the 2020 elections looming, all eyes are beginning to turn towards Iowa. As they do, more scrutiny will fall on our county auditors and the work they tirelessly perform to help ensure our elections run smoothly. To make sure our counties and state can live up to today’s ever-changing threats, a lot of groundwork has already been performed which led to one of our neighbor states voicing their desire to copy the, “Iowa Model” (which was referring to the name given by DHS to the collaboration between counties, SOS, and OCIO to deploy equipment and tools across the state) to boost their security posture. While this has been a great step in the right direction, there remains a lot of work to be done.



**Joel Merrick**  
Secretary of State  
Cybersecurity Services  
Coordinator  
[joel.merrick@sos.iowa.gov](mailto:joel.merrick@sos.iowa.gov)

---



Many of you were able to attend DHS’s National Tabletop the Vote tabletop exercise (TTX) a few months ago, but we would like to make a similar event available for the entire state. A lot of the feedback we received directly from attendees was focused on three areas: location of the exercise; applicability to Iowa’s elections; and a lack of prior incident response planning. Unfortunately, with a nationwide event, a lot of the useful discussion time gets taken up by listening to the problems other states that would impact Iowa very differently. Using knowledge gained from additional TTXs attended by SOS staff and drawing on our strong partnerships, our goal is to be able to provide TTXs that are Iowa focused and more spread out across the state. We are also addressing the remaining issue that was expressed that some counties do not have a cybersecurity incident response plan. This is a major focus for the SOS office. The plan dubbed, “Build-a-Binder,” focuses on assisting counties through the steps of creating a cybersecurity incident response plan and having documentation to turn to in such an event. Once the plans are complete, we will review and test them on an annual basis to ensure they remain strong.

Bio: Joel Merrick is a Cybersecurity Services Coordinator with the Secretary of State. Joel has spent the last four years focusing on information security, two in the banking industry, and two with the State of Iowa. Joel holds several professional certifications including CompTIA’s Secure Infrastructure Specialist, Security+, Network+, Project+, and A+, as well as CIW’s WSA and SDA, and ITIL’s Foundation certification. He is currently studying for a BS in Cybersecurity and Information Assurance at Western Governors University (WGU). He is a father, a husband, a motorcycle enthusiast, a long-time sports fan/former player, and huge fan of many things in the “Nerd” culture.



# Cybersecurity Month

## Cybersecurity Framework and OCIO Information Security Division Collaboration With Counties

Cybersecurity threats to state and local government can come in a variety of categories. Recent headlines have focused on ransomware. Ransomware is a type of malicious software that is engineered to deny access to computer systems or data until a ransom is paid. As cyber attacks become more sophisticated and damaging following a proven cyber defense framework, layering cybersecurity tools, and information sharing is vital to effectively defend computer networks and data.

The Center for Information Security (CIS) has developed a set of the top 20 controls that can be put in place to help mitigate the most common attacks against systems and networks. The CIS controls are developed by a community of experts in cybersecurity. The CIS controls are an effective tool for prioritizing risk-based cybersecurity.

The OCIO (Office of the Chief Information Officer) Information Security Division has developed systems, services, and processes that align with the CIS controls to improve the cybersecurity posture for state of Iowa agencies and counties. Some of the services implemented include security awareness training, vulnerability management, intrusion detection, and anti-malware.

Security awareness training educates the workforce on how to identify different forms of social engineering attacks, such as phishing, phone scams, and impersonation calls. The goal is to empower staff with good cyber defense habits to increase recognition of these exploit attempts.

Hardware and software must be scanned on a regular basis to identify and evaluate the risk of vulnerabilities. A good example of this process is Microsoft Patch Tuesday, the unofficial term used to refer to when Microsoft regularly releases software patches for its software products. In August 2019 Microsoft released patches to fix 93 vulnerabilities. In addition to Microsoft products other software, printers, mobile device, and more will require updates to maintain security.

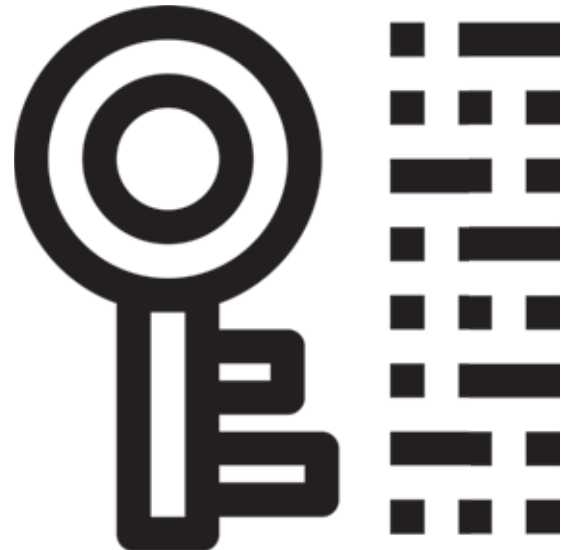
Cyber attackers continuously develop new exploits and attack techniques designed to circumvent network defenses. An intrusion detection system is crucial for network security because it enables detection of unusual or malicious traffic. Unlike a firewall, which sits at the perimeter and acts as a gatekeeper to monitor network traffic and determine if it should be allowed into the network or endpoint at all, an IDS focuses on the traffic that is on the internal network to identify any suspicious or malicious activity. This allows an IDS to detect attacks that manage to slip past the firewall, as well as attacks that originate from within the network.

Designed to attack your systems, devices, and your data, malware moves and evolves quickly. Having a reliable anti-malware solution in place is critical to help detect, stop the movement of, or control the execution of malicious software. Malware is designed to avoid defenses, and attack or disable them. A fast response time can mean the difference between one machine infected or the entire network.

With partnerships that have included Iowa Homeland Security, Iowa Secretary of State, Iowa Counties Information Technology Organization, Iowa State Association of Counties, Iowa National Guard, and Iowa State Association of County Auditors the OCIO Information Security Division has been able to advance the major cybersecurity initiatives mentioned in the article above. Partnerships, collaboration, and information sharing are the key components to a successful cybersecurity program.



**Jesse Martinez**  
OCIO Information Technology  
Specialist  
[jesse.martinez4@iowa.gov](mailto:jesse.martinez4@iowa.gov)



# Cybersecurity Month

---

## Top 5 to Know: Ransomware and Cyber Attacks

1. **Your county is a target.** The bad guys know where you're located, who you do business with, and that you handle millions of dollars on an annual basis. The bad guys want your money, your data, and your reputation.
2. **You are a target.** As a county official YOU are also a target, individually. The bad guys know who you are, what your position is, who your co-workers are, and how your county department functions.
3. **Awareness is essential.** Security awareness training is essential and goes a long ways towards helping keep you and your county safe. Showing leadership by participating in and supporting your IT department's cybersecurity efforts is critical to protecting your organization.
4. **Insurance does not equal security.** Cyber-insurance coverage is very important, but it is a compliment - not an alternative - to making a conscious investment in IT. There is no guarantee data can be recovered after a cyber-attack or other disaster. Insurance cannot replace lost data or lost public confidence.
5. **There is hope.** Despite the doom and gloom of the previous points and the other articles in this magazine, all hope is not lost! The bad guys are constantly on the prowl for "low hanging fruit" - an easy "payday." Many times the "low hanging fruit" turns out to be an organization that hasn't taken a pro-active approach to protecting its computers or training its employees. As the old saying goes, "You don't have to outrun the bear. You just have to run faster than the guy next to you."



**Eric Guth**  
Winnebago County  
IT Director  
[eric.guth@winnebagocountyiowa.gov](mailto:eric.guth@winnebagocountyiowa.gov)

---

So let's keep our counties ahead of that bear by taking cybersecurity and IT investments seriously!

Get in touch with your county IT professional or vendor and discuss practical steps you can take towards creating a safer, more resilient computer environment in your office and county. Specifically discuss your data backups, patch management, and work on developing an Incident Response plan and an IT Disaster Recovery plan.



# Cybersecurity Month

## Patch Management

"Consistent patch management is the first line of defense against being hacked!"

That is the message I want everyone to learn today.

What is Patch Management? And what are we patching?

Think of all of the software programs you have on your computer: Windows, Tyler, Solutions, Vanguard, Microsoft Office, Chrome, Adobe, and the list goes on. Hackers are studying these programs for vulnerabilities or holes that bad people can use to seriously mess up your life. They can use them to steal your information, infect your computer and encrypt your data, and/or infect other computers in your county.

There has been a huge increase for governments being infected and getting their information stolen or held for ransom. Louisiana declared a state of emergency because of the amount of successful attacks they were experiencing. Texas had 23 local governments hit by ransomware in a very well-coordinated attack. It is not a matter of if, but when, and you need to make sure you are doing everything you can to protect your data! Patching is one of those things that you can do.



**Joel Rohne**

Worth County IT Director

joel.rohne@worthcounty.org



Think of software programs like tires on your vehicle. If the tires get holes in them, all of the air leaks out and you cannot get to where you need to go. That is bad! So, if we get holes in our tires, we need to patch them to keep the air in and we can go anywhere we want to go.

The State of Iowa (OCIO) has been providing (for FREE!) a tripwire vulnerability scanner to counties for years. This device scans your networks and gives you a weekly report on what vulnerabilities (holes) you have so you can PATCH them. The OCIO also sends special reports if they see something really bad on your network that should be patched right away. This information is crucial so that you know where your weak spots are, and you can patch them so the bad people cannot use those to ruin your day, week, month, and year. Trust

me...having a cyber-incident is expensive in money, time, and loss of public trust.

If you are paying for a patch management service, this device is a great tool to make sure that the service is doing what it is supposed to do. If you are not paying for a service, make sure that there is somebody tasked with making sure Windows and other applications are being patched and secured on a regular basis.

There are some very common tools for a good cyber security strategy.

1. Backup your data - All the time!
2. Education of employees - You are a target!
3. Identifying and patching vulnerabilities - Keep your software up to date!
4. Password management - Make them difficult and don't reuse.
5. Avoid Phishing and social engineering scams - Be wary of emails and phone calls.

We have just scratched the surface of these topics but there is a treasure trove of great information and resources to help keep us cyber safe. Please reach out to any and/or all of these organizations and they can assist you.

1. MS-ISAC: <https://www.cisecurity.org/ms-isac/>
2. ICIT: <https://iowacountiesit.org/#!event-list>
3. OCIO: <https://ocio.iowa.gov/>
4. SOS: <https://sos.iowa.gov/>



# Cybersecurity Month

---

## Mobile Security

When it comes to cybersecurity and the latest data breaches everyone tenses up for a moment as they try to remember if they have the latest antivirus program up to date, and if the data on their personal computer is safe and secure. Once the few moments of fear have passed, people will move on with their day worrying about the data on their computer. How come no one seems to be concerned about the data on their phones? An individual's smart phone can contain an amazing amount of personal information, which is why attackers target mobile devices. Attackers can use that information to hack other accounts and gain access to other systems. Mobile security needs to be taken more seriously by users because of the power the information on it can give to a hacker.

Mobile devices contain a vast array of personal information an attacker can use. Smart phones are an integral part of everyday communication and are arguably more common than personal computers. These devices are simply computers that fit in the palm of our hands, and much like personal computers, they store data. A lot of people are unaware just how much personal data can be extracted from their device. Information such as call history, text messages, images, browser history, email, and personal notes are some of the ways an attacker can find valuable information depending on their end goal. The information extracted from a mobile device can be used to target companies, turning what may seem like a small insignificant breach, into something major costing companies millions of dollars in damages.



**Nick Ballard**

ISAC Developer I

[nballard@iowacounties.org](mailto:nballard@iowacounties.org)

---



The personal information on a device can be used to hack other accounts. It is debated that anywhere from 50-80% of users reuse passwords. If someone stores passwords on their phone and they leave it somewhere or someone steals it, the bad guy now has access to their passwords. Now realistically if someone gets a Facebook password it's not going to be the end of the world, but what if that person uses the same password for their email at work? This is a very effective way for attackers to gain access to your county or organization, and users should be considerate of where they store their passwords and how often they are reused. Take a moment to think about how many passwords you use, and how many applications use the same password.

Today, mobile devices are secure in the sense of malicious applications. Unless someone has intentionally modified their device, only apps that have been verified by Google, Apple, and Samsung can be installed on a device through the app store. Users should still be cautious of what permissions a certain application requires. If an application requests special permission on a device, it will prompt the user asking them to accept. Everyone should be cautious of

what permissions they are giving unknown mobile applications because it could allow malicious users to access personal data.

Mobile devices are great pieces of technology and make the process of sharing data across the world as easy as swiping a finger. Users need to be more thoughtful when it comes to securing their device. Steps people should take would be setting a PIN on their device, not an easy one, do not store passwords or other sensitive data in notes, check the permissions applications are requesting, and download a phone tracking app that has the ability to track and/or disable a device. Following these simple steps will help protect users against attacks they can actively defend against. To some people it's just a phone, but to an attacker it can become the keys to the kingdom and the gateway to your company.

# Employment

---

## **County Engineer**

Cass County is seeking applicants for the position of county engineer. Interested parties may obtain an application from the Cass County Auditor's Office or the county website: [www.atlanticiowa.com](http://www.atlanticiowa.com)

Please return the completed application and resume to: Cass County Auditor, 5 West 7<sup>th</sup> Street, Atlantic, IA 50022

This position will remain open until filled. The position requires an Iowa licensed professional engineer. Salary will be in the range of \$90,000 to \$110,000 depending on qualifications and experience. A full benefits package is included. The engineer plans, coordinates, assigns, and supervises all engineering and construction work performed by the county secondary roads department, as well as independent contractors. The engineer also prepares and lets contract documents for projects. The engineer also prepares an annual budget and manages an office staff of three and secondary roads department of about 20 employees. Good communication skills, the ability to establish and maintain an effective working relationship with all county personnel, other government agencies, contractors, vendors, and the general public are essential.

Cass County is a rural county in southwestern Iowa midway between the Omaha and Des Moines metro areas. The population is 14,000 and the county seat is Atlantic.

## **County Engineer**

The Montgomery County Board of Supervisors is accepting resumes for the position of county engineer. Applicants must have an Iowa Professional Engineering License. Registration as a land surveyor in Iowa is preferred, but is not required. Montgomery County, Iowa, with a population of 10,225, is a rural county located in southwest Iowa. The County Seat is the community of Red Oak. The engineering department has approximately 25 employees. The Engineer plans, coordinates, assigns, and supervises all engineering and construction work performed by the county secondary roads department, as well as independent contractors. In addition, the Engineer will prepare and let contract documents for projects, present an annual budget, and a five-year construction program identifying future road improvement projects, and work with union representatives on employment matters. The ability to establish and maintain an effective working relationship with all county personnel, other government agencies, contractors, vendors, and the general public is absolutely essential. Possible salary ranging from \$100,000 - \$115,000 with salary negotiable depending upon experience and qualifications.

Resumes may be sent to: Montgomery County Auditor, 105 E Coolbaugh, PO Box 469, Red Oak, IA 51566 or emailed to [sburke@montgomerycoia.us](mailto:sburke@montgomerycoia.us). Resumes will be accepted until the position is filled.

## **Assistant County Engineer**

Jackson County, Iowa is seeking candidates for an assistant county engineer. Position involves assisting the county engineer in performing professional engineering duties in the surveying, planning, designing, drafting, and inspecting construction and maintenance of all county roads and bridges.

Candidates must have a B.S. in Civil or Structural Engineering; Master's degree and/or Professional Engineer's License a plus but not required. Interested applicants shall have passed the Fundamentals of Engineering exam and possess certifications from Iowa DOT for Aggregate, HMA, and PCC inspections. Candidate must comply with state and federal licensure requirements and/or certifications for bridge inspections. Surveying experience is highly desirable.

Strong communication skills plus computer literacy in AutoCAD, word processing, and spreadsheets is necessary. Must have valid Iowa driver's license and be insurable. Salary negotiable, based on qualifications and experience. Submit cover letter, resume, application (found at [www.co.jackson.ia.us/jobopenings](http://www.co.jackson.ia.us/jobopenings)), and desired salary to: Becki Chapin, Human Resource Administrator, 201 West Platt Street, Maquoketa, IA 52060 or email to [bchapin@co.jackson.ia.us](mailto:bchapin@co.jackson.ia.us)

Applications will be accepted through Friday, November 15, 2019 or until position is filled. Jackson County is an Equal Opportunity Employer.

# Scholarship Opportunity

## IEHA Scholarship

On behalf of the Iowa Environmental Health Association (IEHA), I am writing to share the scholarship opportunity that exists within our organization.

Let me first start by telling you a little about IEHA. We are the Professional Association for Environmental Health specialist in Iowa. We are involved in environmental and public education, reviewing existing and pending environmental health legislation and community service. We are proud to have taken a leading role in the development of groundwater, wastewater management and swimming pool regulations, food service personnel certification programs, and well contractor certifications.

We are excited to announce that we started a scholarship program in 2016. The details are as follows:

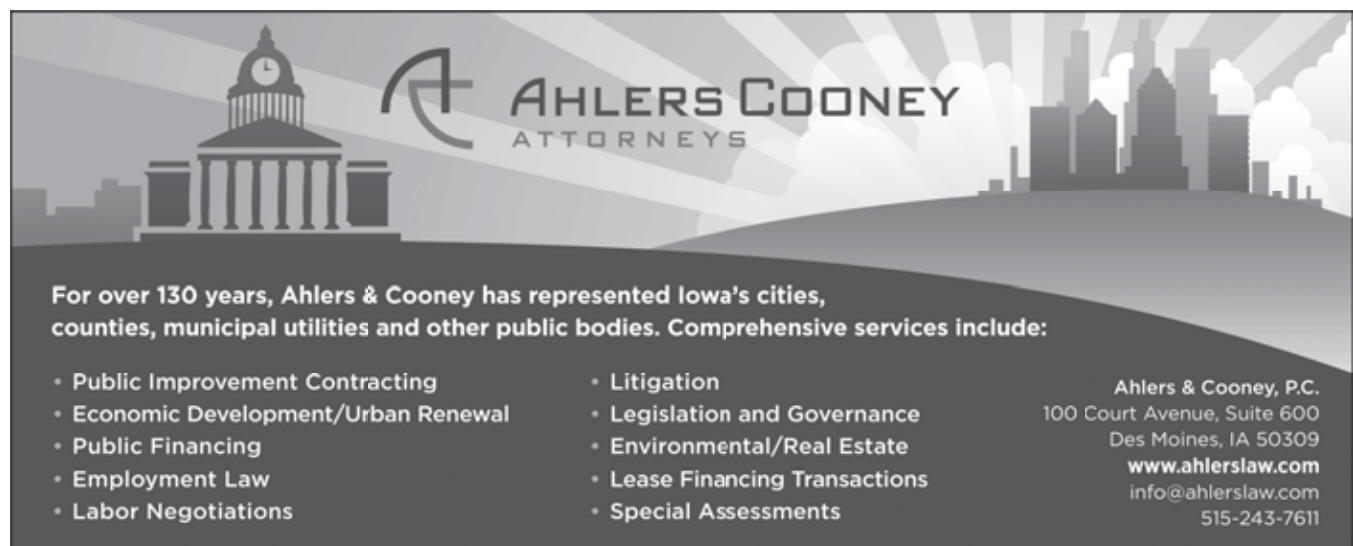
- \$500 for the school year, scholarship may be renewed one time if student is in good academic standing (2.0 GPA or above) with their respective college.
- Scholarship monies will be paid directly to the college or university.
- The selection committee shall consist of five IEHA members. The committee shall award the scholarship and the decision of the committee shall be final.
- IEHA reserves the right to verify any information on the application.
- Scholarship recipients will be notified in March 2020 and will be recognized at the IEHA business meeting during the Iowa Governor's Conference on Public Health in April 2020.

To be eligible for this scholarship, recipients must be:

- A resident of the state of Iowa.
- A high school senior OR a non-traditional student returning to college in the state of Iowa.
- Currently a full-time student at any college, university, or community college in the state of Iowa.
- Recipient must be majoring in environmental health or a related field.

To apply for the scholarship, please follow this application process:

- Download the scholarship application, <http://www.ieha.net/College-scholarship>. Please complete the application and submit it with all required documents to the address on the bottom of the application. This application cannot be submitted on-line at this time.
- Include three letters of recommendation from three individuals that are not family members (i.e. teachers, high school guidance counselors, employers, minister, family friends, etc.)
- Enclose an official high school transcript.
- Enclose an essay – approximately 250 words (one typed page, font size 11 or 12) explaining your career plans and goals.
- Applications must be postmarked by February 1, 2020.



**AHLERS COONEY**  
ATTORNEYS

**For over 130 years, Ahlers & Cooney has represented Iowa's cities, counties, municipal utilities and other public bodies. Comprehensive services include:**

• Public Improvement Contracting	• Litigation
• Economic Development/Urban Renewal	• Legislation and Governance
• Public Financing	• Environmental/Real Estate
• Employment Law	• Lease Financing Transactions
• Labor Negotiations	• Special Assessments

**Ahlers & Cooney, P.C.**  
100 Court Avenue, Suite 600  
Des Moines, IA 50309  
[www.ahlerslaw.com](http://www.ahlerslaw.com)  
[info@ahlerslaw.com](mailto:info@ahlerslaw.com)  
515-243-7611





### Website Development for Iowa Counties

Brian McMillin, President  
[brian@neapolitanlabs.com](mailto:brian@neapolitanlabs.com)  
(515) 999-5221

[neapolitanlabs.com](http://neapolitanlabs.com)



## Engineering Solutions Across Iowa

Our engineers and scientists work in Iowa and across the Upper Midwest building professional relationships to complete successful projects.

**stream restoration | rural drainage | \*dam mitigation  
watershed planning | urban stormwater**

\*More than 90 dam projects completed  
throughout the Upper Midwest



West Des Moines | 515.401.1471 | [www.houstoneng.com](http://www.houstoneng.com)

# 2019 calendar

## October

- 2 ISAC County Budgeting and Property Tax Seminar (Gateway Hotel and Conference Center, Ames)
- 6-9 Assessors Fall Conference (Airport Holiday Inn, Des Moines)

## November

- 20-21 ISAC Board of Directors Meeting (ISAC Office)

## December

- 8-10 ISSDA Winter School (Airport Holiday Inn, Des Moines)
- 11-13 2019 Iowa County Engineers Conference (Veterans Memorial Community Choice Credit Union Convention Center, Des Moines)

## January 2020

- 15-16 ISAC University (Sheraton West Des Moines)
- 30 Statewide Supervisors Meeting (Embassy Suites Downtown Des Moines)

## March 2020

- Feb 29-Mar 3 NACo Legislative Conference (Washington Hilton, Washington, D.C.)
- 12-13 ISAC Spring Conference (Veterans Memorial Community Choice Credit Union Convention Center, Des Moines)

## June 2020

- 24 ISAC Scholarship Golf Fundraiser (Toad Valley Golf Course, Pleasant Hill)

## July 2020

- 17-20 NACo Annual Conference (Orange County, Florida)

## August 2020

- 26-28 ISAC Annual Conference (Veterans Memorial Community Choice Credit Union Convention Center, 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](mailto:ksebern@iowacounties.org).

## 2019 ISAC Preferred Vendors

### Endorsed Elite Preferred Vendors

County Risk Management Services, Inc.  
representing ICAP and IMWCA  
Kingston Life and Health

### 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  
Election Systems & Software  
Henry M. Adkins and Son  
Hopkins & Huebner, P.C.

ISG  
MidAmerican Energy  
Northland Securities, Inc.  
Schneider Geospatial  
Thinix  
Tyler Technologies

### Endorsed Gold Preferred Vendors

Wellmark Blue Cross Blue Shield of  
Iowa

### Gold Preferred Vendor

Ahlers & Cooney, P.C.  
Cost Advisory Services, Inc.  
Delta Dental  
DEVNET, Inc.  
Dorsey & Whitney LLP  
Forecast5 Analytics  
Houston Engineering Inc.  
InfoTech, Inc.

ITC Midwest, LLC  
Matt Parrott/ElectionSource  
Neapolitan Labs  
Purple Wave Auction, Inc.  
Speer Financial, Inc.  
The Sidwell Company  
Wells Fargo  
Ziegler CAT

### Silver Preferred Vendors

Clifton Larson Allen, LLP  
Cott Systems, Inc.  
Nyhart

### Endorsed Preferred Vendors

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

**FOR ALL YOUR  
ELECTION NEEDS**

Contact Your Election Sales Representative  
**DANI DUNHAM, C.E.R.V.**  
800-728-4621 EXT. 3427 | DDUNHAM@MATTPARROTT.COM

MATT PARROTT ElectionSource DOMINION VOTING  
A Stony Hill Company

**CONNECTED COMMUNITIES  
ARE COLLABORATIVE COMMUNITIES**



Tyler's software for Iowa counties can help you build a collaborative community. See our ideas take flight at [tylertech.com/connectedcommunities](http://tylertech.com/connectedcommunities).

**tyler** technologies  
Engineering people who serve the public.



**The Leading Solution  
for Infrastructure Construction  
Management**

— **APPIA** —

- Real-Time Project Collaboration
- Comprehensive Daily Reporting
- Efficient Payment Management

Learn more at [infotechfl.com](http://infotechfl.com) InfoTech



Developing  
Solutions,  
Delivering  
Results.  
**Sidwell** GIS done right.

**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](http://www.purplewave.com)

**DEVNET**



**DEVNET EDGE IOWA SOLUTIONS**

Devnet's integrated Edge software and Cloud Edge solution works together with your current information to bring you an agile and efficient workflow.

Cloud Edge  
Data & Analytics  
Mobile & Tablets  
Network Management  
Performance & Uptime  
Security

[info@devnetinc.com](http://info@devnetinc.com) | 800-4-DEVNET | [www.devnetinc.com](http://www.devnetinc.com)

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



## 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



## Simplify Your Cash Management & Focus On Managing Your Budget

*Building your trust by effectively managing your entire banking relationship.*



Member  
**FDIC** [bankcsb.com](http://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](mailto:cedwards@bankcsb.com)



**Mark Rathbun**  
SVP Business Development  
515-249-4236  
[mrathbun@bankcsb.com](mailto:mrathbun@bankcsb.com)



## THE IPAIT DIFFERENCE... Since 1987



Knowledge.

We have long been honored to serve the investment, liquidity, and cash management needs of Iowa's public agencies.

We know how important it is to understand your needs and offer peace of mind through money market and fixed-term investments.

Safety ~ Liquidity ~ Yield



Iowa Public Agency Investment Trust | (800) 872-4024 | [www.ipait.org](http://www.ipait.org)

Call us today to let us know how we can serve you!

Sponsored by ISAC

Investment Advisory Services provided by Miles Capital, Inc.

**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](http://www.hhlawpc.com)



# ROOTED IN IOWA COUNTIES

Architecture + Engineering + Environmental + Planning

ISGInc.com



6903 Vista Drive  
West Des Moines, IA 50266  
[www.northlandsecurities.com](http://www.northlandsecurities.com)  
515-657-4675  
Member FINRA and SIPC  
Registered With SEC and MSRB

Helping Iowa counties  
manage debt and plan for the  
future in changing times

Competitive Bonds 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



Jeff Heil  
[jheil@northlandsecurities.com](mailto:jheil@northlandsecurities.com)  
641-750-5720



Michael Hart  
[mhart@northlandsecurities.com](mailto:mhart@northlandsecurities.com)  
515-657-4683



Heidi Kuhl  
[hkuhl@northlandsecurities.com](mailto:hkuhl@northlandsecurities.com)  
515-657-4684

RC 18-72 / MUNI 18-58



## Experience the ES&S Difference

Election Systems & Software is the most experienced provider of total election solutions. For more than 40 years, ES&S has remained true to our vision,

**"maintain voter confidence and enhance the voting experience."**

Providing our customers with trusted, quality and timely election services and products is our purpose, our promise and our passion.

Learn more about our mission by visiting our website:

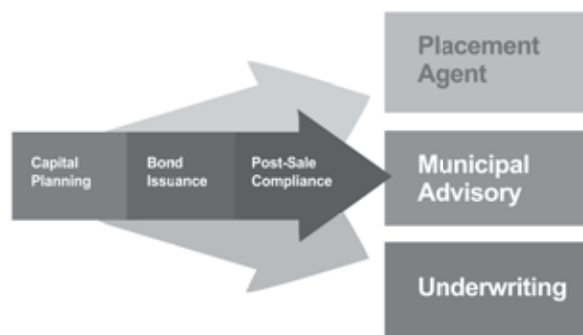
**essvote.com**



## FINANCING SOLUTIONS FOR MUNICIPAL INFRASTRUCTURE



### Project Finance: Planning Through Maturity



**D|A DAVIDSON**

FIXED INCOME CAPITAL MARKETS  
D.A. Davidson & Co. member SIPC and FINRA

#### 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

#### Aaron H. Smith

Associate Vice President  
(515) 471-2720  
ASmith@dadco.com

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



# You're missing out...

if your county hasn't taken advantage of these resources from ICAP

## The ICAP Grant

**\$1,000 for loss control and/or risk management items...every year!**

## Law Enforcement Policies & Training Grant

**A limited-time grant opportunity for agencies that implement a law enforcement policy and training program. \$1,500 minimum grant, amount varies by number of officers.**

**Learn more at  
[www.icapiowa.com](http://www.icapiowa.com)**

**COUNTY RISK  
MANAGEMENT SERVICES, INC.**

*representing*



## Let Us Help Manage Your Electronic Poll Book Systems.

### Did You Know?

Our Thinix ONE™ solution allows us to provide management, updates, and support for **Precinct Atlas** and other Windows-based e-poll book systems – reducing cost and complexity to ensure a smooth election.

We help to ensure your e-poll books remain compliant with state regulations for encryption, authentication, and updates. Give us a call at 888-484-4649 for a no-obligation consultation.



**Thinix ONE™**  
E-Poll Book Security & Management

**[Thinix.com/Auditors](http://Thinix.com/Auditors)**

# EMPLOYEE BENEFITS CONSULTING

- ISAC Association Health & Dental Plans
- Exclusive ISAC Life & Disability Trust
- Voluntary ISAC Worksite Benefits
- Leveraged Resources
- Claims Experience Discounts
- Wellbeing Rewards & Discounts
- Customized County Contracts
- Healthcare Analytics
- Actuarial Modeling
- Human Resources and Benefits Technology
- Dedicated Service and Support Team



Kingston Life and Health

phone: 515-223-1114 fax: 515-223-9994

1755 Westlakes Parkway, West Des Moines, Iowa 50266

web: [www.kingstonlifeandhealth.com](http://www.kingstonlifeandhealth.com)

email: [timothyj@kingstonlifeandhealth.com](mailto:timothyj@kingstonlifeandhealth.com)



**KINGSTON**  
LIFE & HEALTH