

# COOPERATIVE CYBERSECURITY

Are you doing everything you can to  
keep your network safe?



Ransomware explosion [P. 6](#)

HR/cybersecurity connection [P. 9](#)

Keys to the kingdom [P. 10](#)

# Cybersecurity Research at NRECA

NRECA has several cybersecurity research projects under way and offers numerous resources to help members meet their security needs. Visit [Cooperative.com](http://Cooperative.com) for more information on the projects below.



## Research:

- **RC3 (Rural Cooperative Cybersecurity Capabilities Program)** Program to develop tools, resources and training opportunities to improve the cybersecurity and resiliency capabilities of electric cooperatives. Funded by the U.S. Department of Energy.



- **Essence** Recently completed project that successfully developed a cybersecurity technology to detect anomalies in utility network traffic. Funded by the U.S. Department of Energy.



- **GridState** Project to extend and improve the capabilities of *Essence*. Funded by the U.S. Department of Defense.



- **REACT** Research collaboration between NRECA, N-Dimension Solutions, Inc., Milsoft Utility Solutions, and NRTC to integrate *Essence* into commercial products and services. Funded by the U.S. Department of Energy.



- **Simba** Project to develop a rapid cybersecurity testing capability using software that can process a year's worth of data in 52 minutes. Funded by the U.S. Department of Defense as part of the GridState program.



- **MultiSpeak®** Platform to provide online comprehensive interoperability testing and certification and implement cybersecurity extensions for de-risking technology integration.

## NRECA Resources (visit [Cooperative.com](http://Cooperative.com)):

- Guide to Developing a Cyber Security and Risk Mitigation Plan Toolkit – a set of tools and resources cooperatives can use to strengthen their security posture.
- Cyber Security Policy Framework – a collection of cybersecurity policy templates developed in collaboration with the Kentucky Association of Electric Cooperatives.
- RC3 Website – cybersecurity resources developed by the RC3 Program.
- TechUpdate – a twice-monthly email newsletter containing the latest information on technical publications, articles, reports, webinars, and conferences.

## Other Resources:

- Cybersecurity Capability Maturity Model (C2M2) – a self-assessment evaluation tool from the Department of Energy. (<https://www.energy.gov/oe/cyber-security-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity>)
- Cybersecurity Risk Management Process (RMP) Guideline – guidance from the Department of Energy to incorporate risk-management processes into a new

or existing cybersecurity program. (<https://www.energy.gov/oe/downloads/cybersecurity-risk-management-process-rmp-guideline-final-may-2012>)

- Information Security Program Library (ISPL) – cybersecurity template policies, procedures, standards, and forms developed by SEDC. (<https://www.sedata.com/cyber-resilience-initiative-information-security-program-library-ispl-download-request>)
- NISC Cybersecurity Services – a suite of training and network protection resources: [cybersecurity.coop](http://cybersecurity.coop).
- Cyber Mutual Assistance (CMA) – an Electricity Subsector Coordinating Council (ESCC) initiative to develop a pool of industry experts. (<http://www.electricitysubsector.org/CMA>)
- Computer Readiness Emergency Teams (CERT) – teams funded by the Department of Homeland Security to respond to major cyber incidents, analyze threats, and exchange critical cybersecurity information with trusted partners.  
<https://www.us-cert.gov>  
<https://www.ics-cert.us-cert.gov>

## For more information and updates:

- Visit [Cooperative.com/public/bts/cyber-security](http://Cooperative.com/public/bts/cyber-security)
- Sign up for TechUpdate: [TechUpdateSignUpRequest@nreca.coop](mailto:TechUpdateSignUpRequest@nreca.coop)
- Contact Cynthia Hsu, NRECA cybersecurity program manager, at [Cynthia.Hsu@nreca.coop](mailto:Cynthia.Hsu@nreca.coop) or the RC3 team at [CybersecurityRC3@nreca.coop](mailto:CybersecurityRC3@nreca.coop).

# Welcome to the Special Cybersecurity Insert

Digital technologies are allowing electric cooperatives to improve service to members in countless ways. Smart grid communications and remote access or automated control equipment enable more cost-effective, efficient, and safer options to manage our systems.

But greater connectivity comes with a cost.

We are collecting more data and moving it in new and complicated ways. Digital communications, for all their benefits, also create openings for cybercriminals, and our data is an attractive commodity.

As cooperatives ramp up capabilities in the beneficial use of digital technologies, they must also integrate best practices to safeguard consumer data and grid operations from cyberattacks.

To this end, NRECA launched RC3, the Rural Cooperative Cybersecurity Capabilities program, to help distribution cooperatives address the persistent and evolving reality of cyberthreats. One co-op general manager told us, "If you create a strong culture around security, you can prevent 95 percent of the risks of a bad guy getting in." With funding from the U.S. Department of Energy, RC3 is developing tools and resources to help cooperatives build that culture of cybersecurity.

The good news is that effective cybersecurity at the distribution level does not take a massive financial investment. In this *RE Magazine* Cybersecurity Insert, we pay particular attention to how small- and medium-size distribution systems are meeting cybersecurity challenges. It takes planning and commitment, from the board of directors and from every employee, to make cybersecurity a permanent priority and an essential element in utility operations.

Cooperatives cooperate. It's what we do. And in the following pages, we share key observations, solutions, and successes from several co-op leaders. A critical component of our success as a community to deter and mitigate cyberthreats will be our inclination to share information and collaborate. This is our strength.



Jim Spiers  
NRECA Vice President for  
Business and Technology Strategies



Cynthia Hsu  
NRECA Cybersecurity Program Manager

## Table of Contents

Online Cybersecurity Resources . . .	<b>Page 2</b>	Defense in Depth Steps . . . . .	<b>Page 8</b>
Introduction. . . . .	<b>Page 3</b>	HR and Cybersecurity . . . . .	<b>Page 9</b>
Main Story - Cyber Cooperation . . .	<b>Page 4</b>	Keys to the Kingdom . . . . .	<b>Page 10</b>
Graphic: Ransomware Explosion . . .	<b>Page 6</b>	New Cybersecurity Tool . . . . .	<b>Page 11</b>

# Cyber Cooperation

Co-ops have a secret weapon in the war against network attacks

By Bob Gibson



Attendees at a recent RC3 event participate in a cybersecurity exercise.

Photo by Bob Gibson

*Excerpted version; visit [REmagazine.coop](http://REmagazine.coop) for the full article*

**T**im Lindahl pulled into the parking lot of Wheat Belt Public Power District in Sidney, Nebraska, on a January morning in 2005. He was early for his interview for a manager of information technology position, so he turned off the engine of his pick-up truck, pulled out his laptop, and searched for an internet signal to check emails while he waited.

In 2005, cellular signals were far less ubiquitous than today, even in a town of 6,000 on the panhandle of western Nebraska with an interstate highway close by. But he was in luck; the signal from Wheat Belt's Wi-Fi network was strong – and unsecured.

Lindahl found that not only could he jump onto the internet signal to access his email; he could freely surf inside the utility's network.

"I quickly found the server and several computers, one named 'CFO,' another named 'General Manager,' none of which were password protected," he says. "I realized that [network protection] was not on their minds, as it wasn't for most people at that time."

His discovery provided an opportunity to demonstrate his IT credentials once inside the office.

"I showed them what I had found and gave them some pointers on how to secure that down a little bit," he says. His interviewers "realized that I could have absconded with every single file they ever had and they would have never known I was there in the network."

He got the job.

## RC3

Communication-based technologies are now integrated into every facet of a cooperative's business, and securing those technologies from cyberthreats will help safeguard the financial security and welfare of the co-ops and their members and the integrity of the electric grid. Helping cooperatives build stronger cybersecurity programs is the goal of the Rural Cooperative Cybersecurity Capabilities Program (RC3), launched by NRECA in 2016 with U.S. Department of Energy funding and managed by the association's Business and Technology Strategies (BTS) team.

The program is developing tools, resources, and training opportunities to help co-ops build stronger cyberdefenses and increase their resiliency to cyberattacks like ransomware.

Led by Cynthia Hsu, manager of cybersecurity programs at BTS, the RC3 Program held a series of Cybersecurity Summits around the country this year. More than 100 cooperative members participated in the January, April, and May summits, and each was hosted by a leading university or national energy lab conducting cybersecurity research. At the heart of each one-day event is a peer-to-peer exchange among cooperative employees on the key challenges they face.

## An engaged board

Hsu says one particular message came through loud and clear from summit participants: An engaged board and supportive CEO makes all the difference.

Lindahl, who is now Wheat Belt's general manager, says the foundation for a strong cybersecurity program was in place before he arrived.

"I've had the luxury of having a very technology-adept board ever since I was hired," he says. "Twelve years ago, they saw that we really needed to make better use of the technology we have and pay attention to it. Having a board that was engaged since the beginning has made my life a lot easier."

Brian Heithoff, CEO of High West Energy in Pine Bluff, Wyoming, and an attendee at the first summit, agrees.

"Boards take a lot of pride in being good stewards of the co-op's well-being today and in considering how to innovate for the future," he says. "My board has displayed considerable foresight when it comes to protecting our cyber assets, and I appreciate their leadership."

## Small does not mean safe

"In general, boards easily get the financial and operational risk of something that threatens the co-op's distribution lines," says Heithoff. "They have a harder time gauging the possibility that the co-op's IT system will be hacked."

He says many think, "We're a small utility in the middle of rural America. Why would they target us when they have Citibank and ExxonMobil to go after?"

Mark Hayden, CEO of Missoula Electric Cooperative in Missoula, Montana, is working to correct this misperception.

"It's not about being on anyone's radar. The bad guys are throwing out a wide net looking to see who they can snag," he says. "They may not necessarily be targeting Missoula Electric Co-op, but if they find a crack, they'll exploit it."

## Who 'owns' cybersecurity?

Hsu says defining who at a co-op "owns" cybersecurity is an important part of developing a cybersecurity plan.

"Cybersecurity is a risk-management strategy which [belongs to] everybody," says Lindahl. "Yes, cybersecurity is an IT function, but it goes far beyond that. IT just carries out the strategy."

He says at Wheat Belt, cybersecurity is handled much like safety, where everyone is responsible.

"We do monthly security updates for our directors, and we talk about it extensively in our weekly staff meetings," he says. "Can I say with absolute confidence that one of our guys won't get hurt tomorrow? No. But we haven't had anyone injured in 10 years because we've focused on safety. With cybersecurity you can create a good culture, put in the right policies and procedures, the layers of risk protection, and prevent 95 to 98 percent of the intrusions you might otherwise experience."

## Resources for small utilities

RC3 summit attendees expressed a strong desire for resources that are specifically designed for cooperatives and for smaller utilities. As one participant explained, "One of the biggest challenges for small IT staffs is just knowing where to start."

Co-op representatives at the summits also expressed a range of concerns about sharing information. This includes the risk of information about a cybersecurity vulnerability or incident falling into the wrong hands; fear of repercussions if a security breach were revealed; uncertainty about how to differentiate between an actual vulnerability and a benign communication; and lack of clarity on when and where to report an incident.

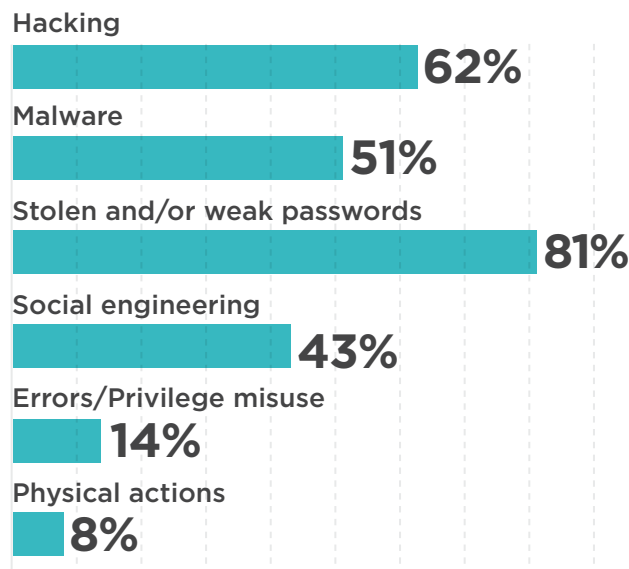
Lindahl says that despite these uncertainties, it's more important than ever for co-ops to find ways to learn from

one another and share ideas and experiences.

"There are certain practices that we won't allow outside our walls just for our protection," he says. "But there are a lot of things that we can share, simple things that everybody can do that won't harm the organization if they get out."

## What Tactics Do Hackers Use?

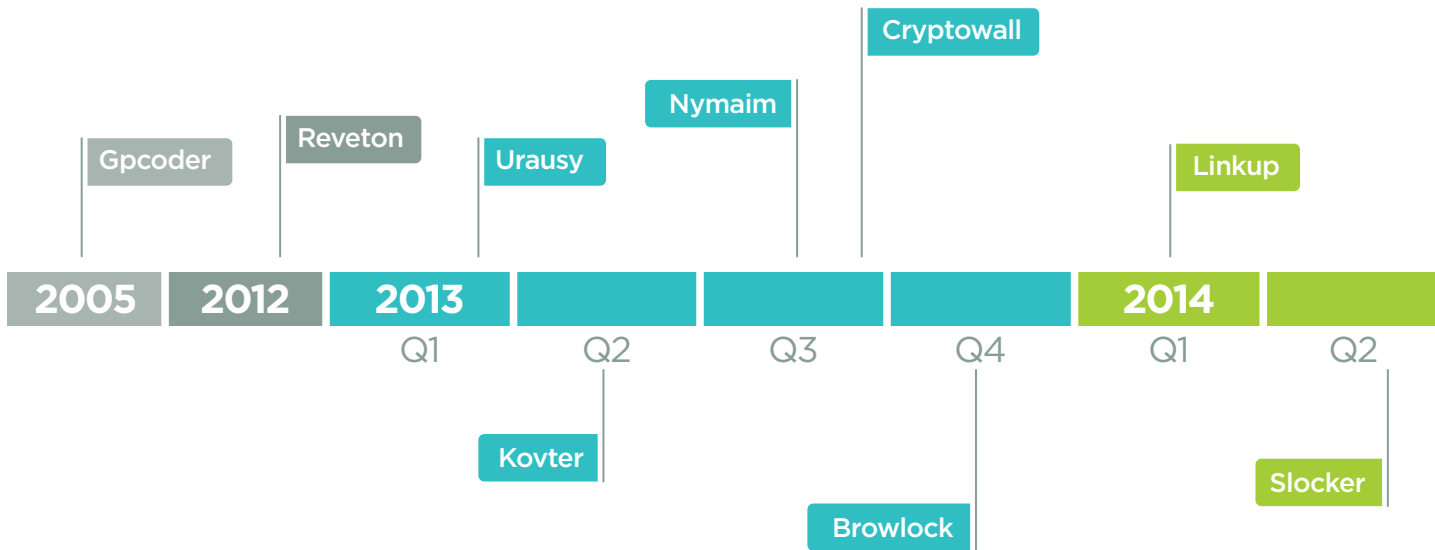
Percent of network breaches in 2016 involving:



Source: 2017 Verizon Data Breach Investigations Report  
Report: <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>

# Ransomware Explosion

Hackers discovered the ease of use and profitability of ransomware in mid-2014, when widespread innovation in ransomware “families” increased from just a handful annually to dozens each year. “The proliferation in ransomware families in 2014 was the beginning of a disturbing trend in cyberattacks that have continued to increase in frequency and sophistication,” says NRECA cybersecurity program manager Cynthia Hsu.



Note: Data on this chart is current through first quarter 2016. Since then, ransomware attacks have increased dramatically. By the end of 2016, 101 new ransomware families were discovered.

Source: Symantec

Report: <https://www.symantec.com/security-center/threat-report>

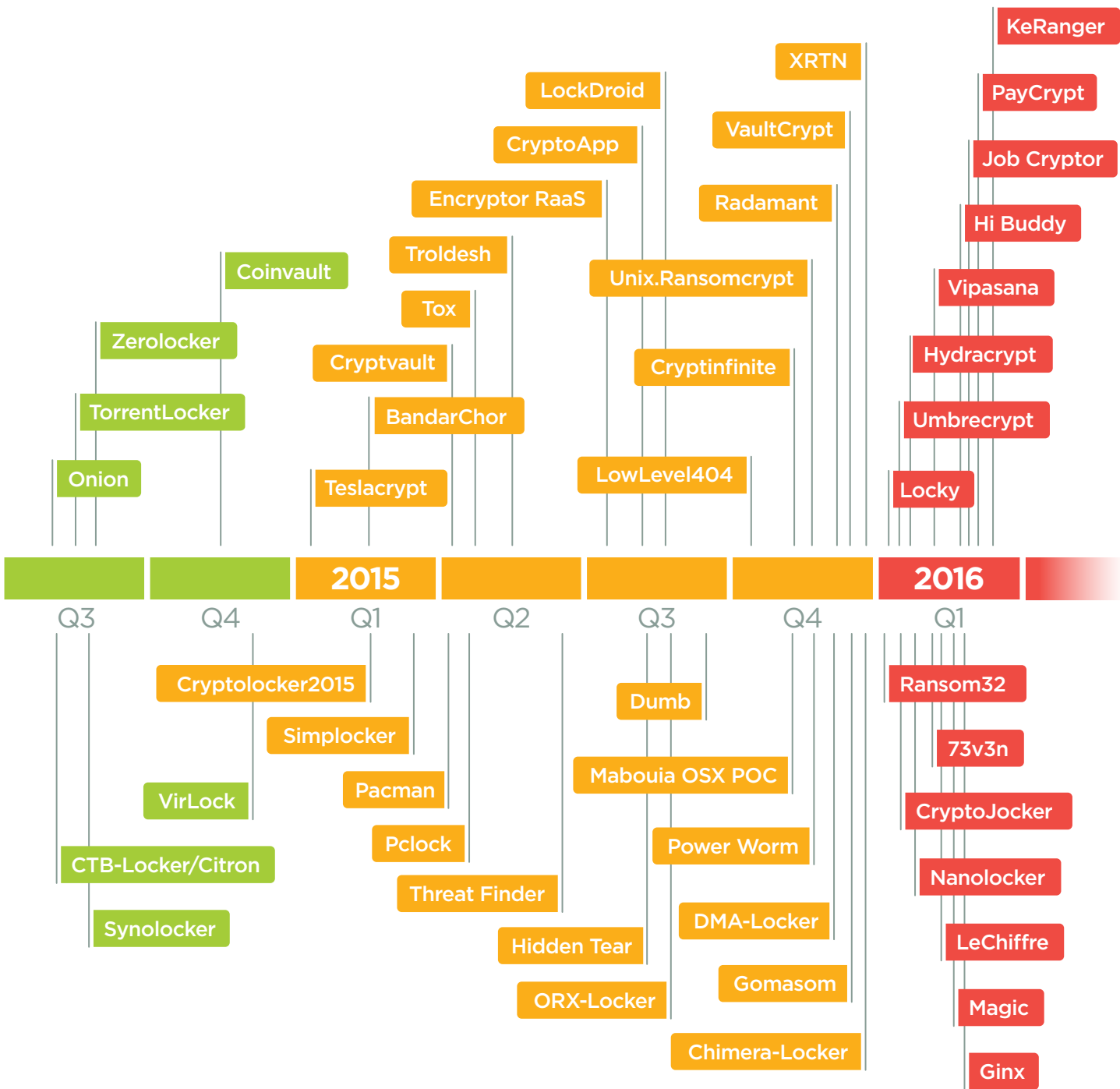
## Passwords: Longer = Better

By Glenn Montgomery and Cynthia Hsu

Attackers can use freely available tools and advanced computing power to break uncomplex passwords in as little as one second, depending on the composition and complexity. Longer passwords are more secure than shorter ones. And passwords that are long and include a combination of numbers, spe-

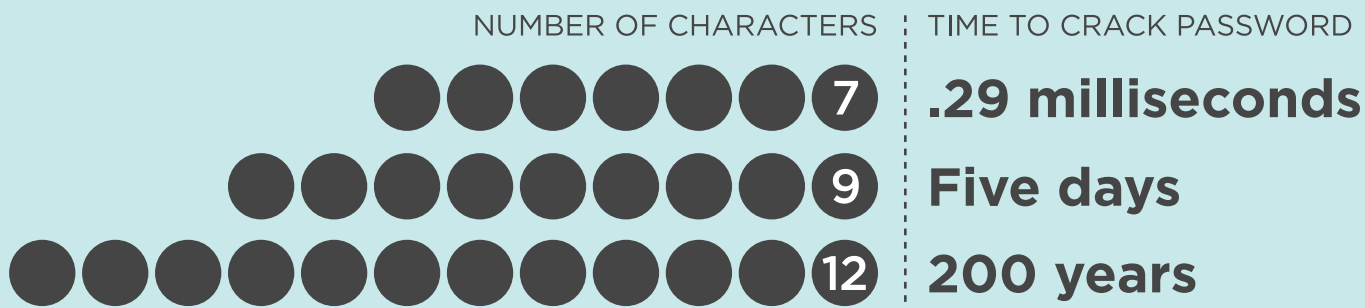
cial characters, and both lowercase and capital letters are even better.

When possible, use mnemonics to remember complex passwords (passphrases), replace letters with numbers, and always use a different password for each account.



## How long should your password be?

The length and complexity of a password has a direct impact on how difficult it would be to crack.



# Defense in Depth: Steps to Build a Strong Cyberdefense Strategy



## Identify

- Understand what sensitive, personal, and critical data, assets, processes, and systems your co-op stores and uses.
- Determine what threats and vulnerabilities your co-op faces.
- Understand what access third-party vendors have to your system.
- Assign responsibility for enforcing cybersecurity policies to a senior manager.



## Protect

- Restrict network access to an employee's specific job requirements.
- Use firewalls to segment your internal network.
- Use two-factor authentication and consider IP whitelisting for sensitive and critical systems.
- Change all default passwords on your computers and operational devices.
- Use long, strong passwords and update passwords every six months.
- Eliminate unnecessary communications between all computers and devices on your network.
- Disable all unnecessary services running on your computers/servers.
- Update and patch operating systems and software on a regular basis.
- Perform regular security awareness training for all employees.



## Detect

- Maintain anti-virus and anti-malware solutions and review firewall rules regularly.
- Perform regular vulnerability assessments, at least once a year.
- Maintain and monitor logs on sensitive and critical systems.
- Consider using an intrusion-detection system to identify anomalous behavior on your network.
- Hold monthly calls with other co-ops on the latest cyberthreats and solutions.



## Respond

- Integrate cybersecurity into incident-response, business-continuity, and crisis-communications plans, and hold practice drills regularly.
- Isolate the impacted computers, devices, and/or systems, and work with professionals to perform forensic analyses.
- If you have cybersecurity insurance, contact your insurance provider for assistance.
- Contact the Electricity Information Sharing and Analysis Center (E-ISAC) if appropriate.
- Consider contacting the Electricity Sector Coordinating Council's Cyber Mutual Assistance (CMA) Program.



## Recover

- Back-up files, store back-ups in locations not connected to your network, and test back-ups regularly.
- Understand your legal obligations with the assistance of counsel.
- Perform a post-incident review, and update policies and procedures as needed.

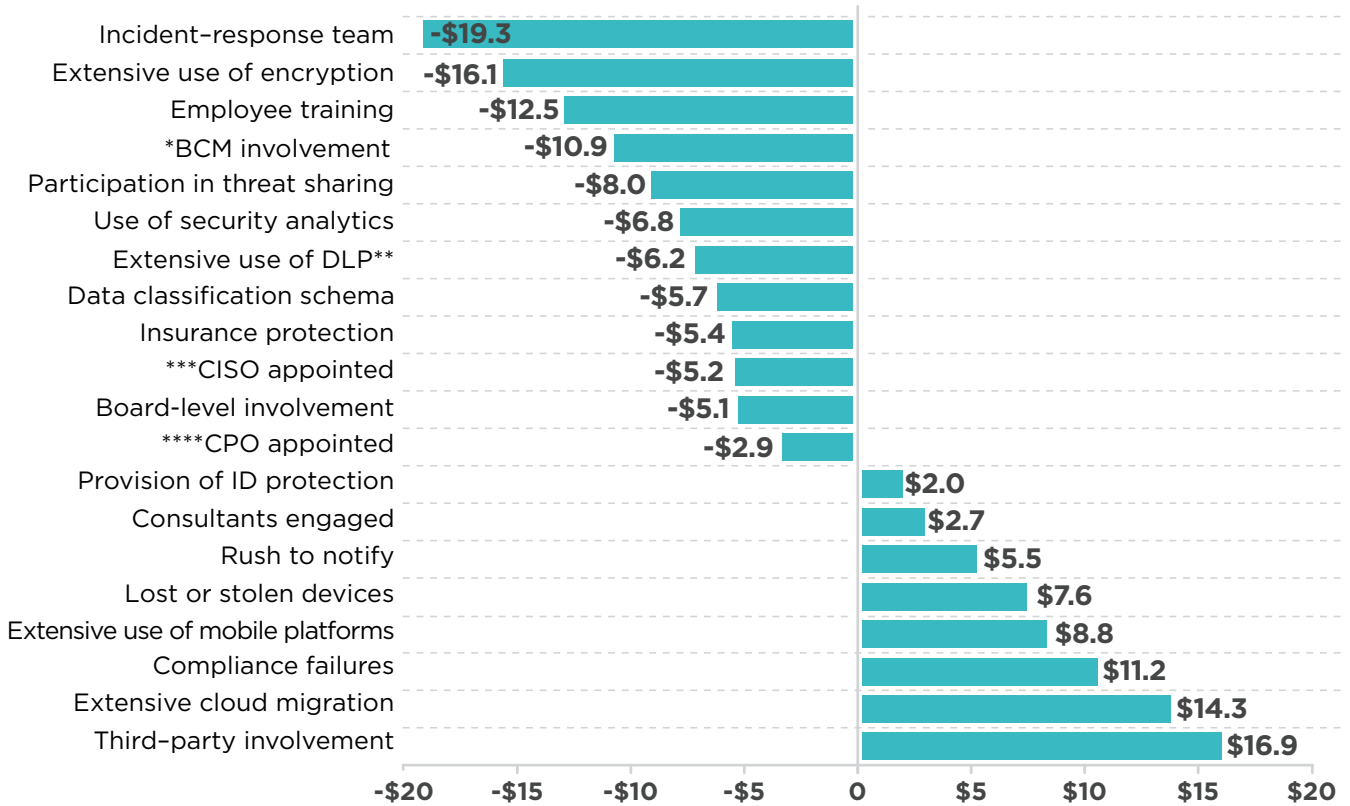
*NOTE: This list does not include all options and is provided as a general resource.*



# Breach Liabilities

A 2017 Ponemon Institute report estimates that the cost of a data breach in the energy sector is \$137 per sensitive or confidential record. Certain actions, however, will have a negative or positive effect on that number. Below are factors that will change that breach liability.

In U.S. Dollars



\* Business continuity management  
 \*\* Data loss prevention  
 \*\*\* Chief information security officer  
 \*\*\*\* Chief privacy officer

Source: Ponemon Institute/IBM Report: <https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03130wwen/SEL03130WWEN.PDF>

## HR's Role in Cybersecurity

By Cynthia Hsu and Bob Gibson

When it comes to creating a culture of cybersecurity within a cooperative, one thing is clear: Changes must be made throughout the organization, not just the IT department.

A natural partner in developing a stronger cybersecurity posture is the human resources team.

After testing a new self-assessment tool as part of NRECA's Rural Cooperative Cybersecurity Capabilities Program (RC3), employees at Laurens Electric Cooperative in Laurens, South Carolina, discovered HR's critical role in cybersecurity.

"I realized as we went through it that there is much more value from a human resources standpoint than I had expected," says Dena Moore, the co-op's human resources coordinator.

After the assessment test, Moore met with IT staff to rewrite job descriptions to include each position's network access needs and create new network security procedures for employees who leave the co-op.

At North Carolina's Electric Cooperatives (NCEC; state-wide), responsibility for security practices has been moved from IT to the supervisory level in each department.

"Rather than being seen as a special function in just one part of the cooperative, this makes cybersecurity a part of the day-to-day work of every employee," says Ajaz Sadiq, NCEC's vice president of grid modernization and technology integration.

Look to your HR department for other cybersecurity input, like recruiting security-minded staff and developing cyber training programs.

# Limit the Damage

Not everyone should have the 'keys to the kingdom'

By Bob Gibson

Cybersecurity professionals agree that no organization can be 100 percent secure 100 percent of the time. The question is, how do you thwart cybercriminals most of the time, and how do you limit the damage if they do get in?

The answer: layers.

One of the primary values of your computer network is the ability for employees to access resources across the network. Not surprisingly, this is also one of its greatest security weaknesses. The risks are compounded if co-ops don't actively limit access to their most critical data and systems.

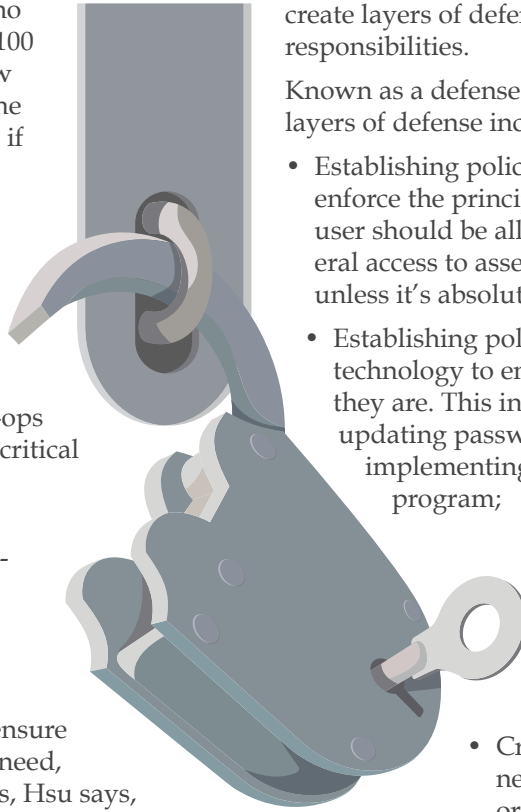
"If everyone has the 'keys to the kingdom,' then every access point to the network becomes a liability," says Cynthia Hsu, NRECA's cybersecurity program manager.

Experts recommend a combination of people, processes, and technologies to ensure that employees can reach the data they need, but only the data they need. The process, Hsu says, begins by determining what is valuable, where it's located on the network, and how it's accessed. Then decide who should be able to get to these assets, and

create layers of defenses to limit access based on job responsibilities.

Known as a defense-in-depth strategy, possible layers of defense include:

- Establishing policies and using technology to enforce the principle of "least privilege;" no user should be allowed administrative or general access to assets and systems on the network unless it's absolutely needed to perform their job;
- Establishing policies, training staff, and using technology to ensure someone is who they say they are. This includes using strong passwords, updating passwords at least annually, and implementing a two-factor authentication program;
- Using technology to limit unnecessary communications between desktops, laptops, mobile devices, printers, routers, servers, workstations, and other devices;
- Creating separations in your network using internal firewalls or demilitarized zones (DMZs) between critical systems/assets and less-critical systems/assets;



## Life Cycle of a Cyberattack

From the time a cybercriminal identifies a potential vulnerability until the end of a criminal mission, a cyberattack goes through a series of definable steps. Certain defenses can be used to prevent movement from one phase to the next, and a successful defense-in-depth strategy will ensure the cybercriminal never reaches the final step.



- Using technology to detect threats and filter incoming files to prevent them from reaching end users;
- Regularly patching computers, network equipment, and substation devices and equipment.

Hsu says deploying strong network defense techniques can be disruptive, particularly if employees aren't supportive of policy changes that limit their access to the internet or certain files or drives. They may question

why they're no longer allowed to download software directly, or why they have to install security systems onto their mobile phones.

"Ultimately, it's a question of convenience vs. security," says Edward VanHoose, general manager of Clay Electric Cooperative. "How much convenience do we need versus how much security are we willing to give up?"

## Taking Stock

### A new tool to assess your co-op's cybersecurity posture

By Bob Gibson

How robust are your cooperative's cybersecurity defenses? It's a question that can be hard to answer, particularly for smaller utilities.

There are many tools that can help assess an organization's cybersecurity posture, but "the biggest need we have is for a cybersecurity guide that is scaled to utilities of our size," says Mark Hayden, CEO of Missoula Electric Cooperative, a Montana co-op that serves about 14,500 meters.

To fill this gap, NRECA's Rural Cooperative Cybersecurity Capabilities (RC3) Program is developing a self-assessment tool specifically designed for small- and mid-sized utilities with few or no IT employees.

The tool, which is in field testing at cooperatives around

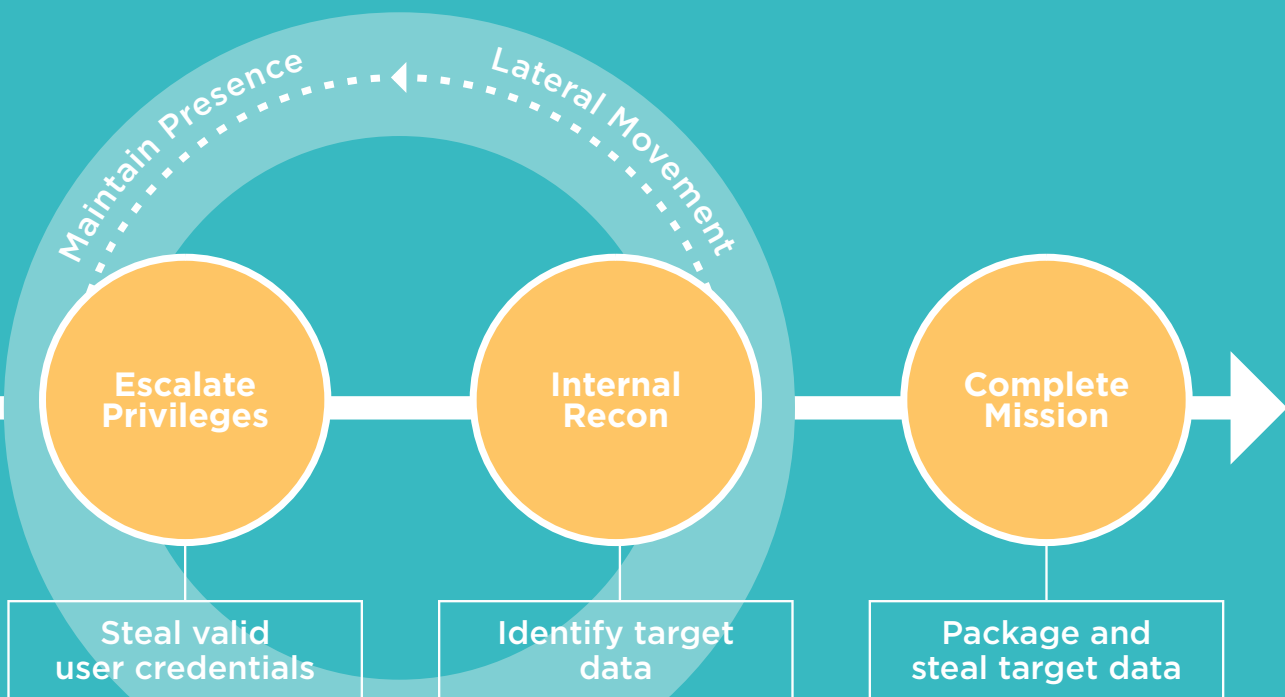
the country, is designed to be a cross-departmental team exercise. The process walks the organization through a series of questions about their cyber capabilities and practices, and assigns a ranking based on the maturity of the utility's program.

"The cross-department engagement was awesome," says Kirk Garrett, vice president of safety and loss control at Laurens Electric Cooperative in South Carolina, one of the field test participants.

"It absolutely made sense for the non-IT people to be there," agreed Matt Stanley, vice president of finance and accounting at Laurens Electric.

"Going through the self-assessment will give co-ops a baseline for their current capabilities, identify priorities for improvement, and help them document their progress over time," says Cynthia Hsu, NRECA's cybersecurity program manager and head of the RC3 project.

The RC3 team will make changes to the tool based on recommendations from the field tests, and a final version is scheduled to be released to all cooperatives in 2018.



Credit: FireEye Report: <https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html>

# RC3 Cybersecurity Summits

NRECA is building a strong network of collaborators in cybersecurity through the RC3 Cybersecurity Summit series. We thank our partners for the first four summits.



---

The Electricity Information Sharing and Analysis Center (E-ISAC) is an ongoing collaborator with the RC3 Cybersecurity Summit series. The E-ISAC gathers and analyzes security information, coordinates incident management, and communicates mitigation strategies with stakeholders within the electricity industry. Cooperatives can join the E-ISAC for free at <https://www.eisac.com/>



---

## Comments by RC3 Summit Attendees ...

- “Very timely and important topic!”      “I learned a lot.”      “Relationship building was great.”  
“Very relevant to our needs at this point in time.”      “Great eye opener!”  
“Valuable knowing we are not alone or unique in the challenges we face.”

---

## More summits to come...

NRECA will be offering additional Cybersecurity Summits. Visit the RC3 page on Cooperative.com for announcements of future summits, and sign-up for TechUpdate (TechUpdateSignUpRequest@nreca.coop) to stay informed of our latest RC3 Program offerings.



The RC3 Program, Cybersecurity Summit series, and this publication are supported by the Department of Energy, Office of Electricity Delivery and Energy Reliability, under Award Number DE-OE0000807.

This material is based upon work supported by the Department of Energy National Technology Laboratory under Award Number(s) DE-OE0000807.

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.