Second Edition
August 2018

COOPERATIVE CYBERSECURITY

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

NRECA®
America's Electric Cooperatives

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 for more information on the projects below.

- **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 (DOE).

- ***Essence*** Completed project that successfully developed a cybersecurity technology to detect anomalies in utility network traffic. Funded by the DOE.

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

- **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 DOE.

- **Simba** Project to develop a rapid cybersecurity testing capability using software that can process a year's worth of data in 52 minutes.

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

NRECA Resources (visit Cooperative.com):

- *Guide to Developing a Cybersecurity and Risk Mitigation Plan Toolkit* – a set of tools and resources cooperatives can use to strengthen their security posture.
- *Cybersecurity 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.
- *Business and Technology Update* – 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 DOE. (https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0-0)
- *Cybersecurity Risk Management Process (RMP) Guideline* – guidance from the DOE to incorporate risk-management processes into a new or existing cybersecurity program. (https://www.energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf)
- *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 (https://www.nisc.coop/cybersecurity)
- *Cyber Mutual Assistance (CMA)* – an Electricity Subsector Coordinating Council (ESCC) initiative to develop a pool of industry experts. (http://www.electricitysubsector.org/CMA)
- *Computer Emergency Readiness 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/topics/cybersecurity
- Sign up for Business and Technology Update: https://www.cooperative.com/programs-services/bts/Pages/Technology-Update.aspx
- Contact Cynthia Hsu, NRECA cybersecurity program manager, at Cynthia.Hsu@nreca.coop or the RC3 team at 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 effective 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. This document serves as an update to the August 2017 *RE Magazine* Cybersecurity Insert with a few modifications and updated website links. 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 Senior Vice President for
Business and Technology Strategies

Cynthia Hsu

Cynthia Hsu
NRECA Cybersecurity Program Manager

Bridgette Bourge

Bridgette L. Bourge
NRECA Director, Legislative Affairs

Barry Lawson

Barry Lawson
NRECA Senior Director, Regulatory Affairs

Table of Contents

Cyber Cooperation

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

By Bob Gibson

Photo by Bob Gibson

Attendees at an RC3 Cybersecurity Summit participate in a cybersecurity exercise.

Excerpted version; visit REmagazine.coop for the full article

Tim 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, 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 six Cybersecurity Summits around the country in 2017. More than 150 cooperatives from 33 different states participated in the summits. Five of the summits were hosted by a leading university or national energy lab conducting cybersecurity research. Due to the success of the 2017 Summits, RC3 will hold five more summits in 2018/2019. 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 the 2017 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.

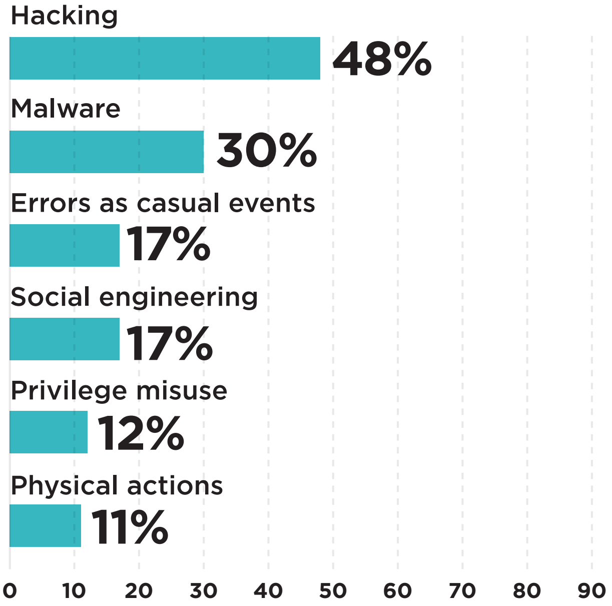
"I've had the luxury of having a very technology-adept board ever since I was hired," he says. "Twelve years ago, they saw that we really needed to make better use of the technology we have and pay attention to it. Having a board that was engaged since the beginning has made my life a lot easier."

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."

What Tactics Do Hackers Use?

Percent of network breaches in 2017 involving:



Source: 2018 Verizon Data Breach Investigations Report
Report: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf

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."

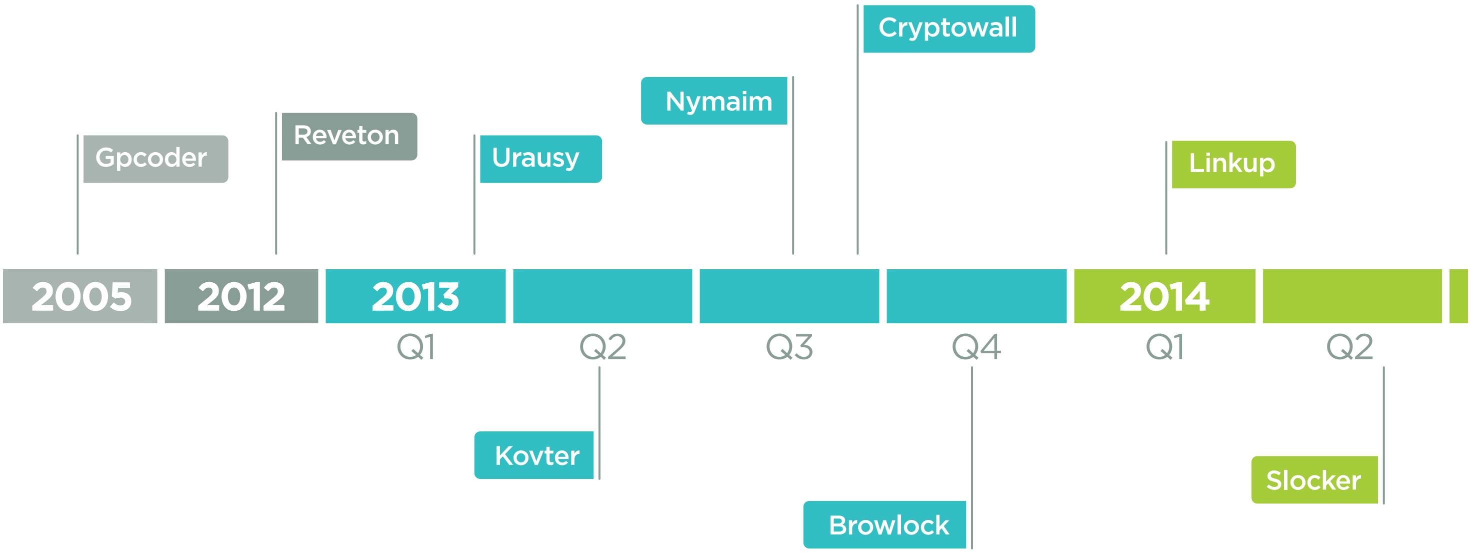
Co-op representatives at the summits also expressed a range of concerns about sharing information. This includes the risk of information about a cybersecurity vulnerability or incident falling into the wrong hands; fear of repercussions if a security breach were revealed; uncertainty about how to differentiate 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."

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.

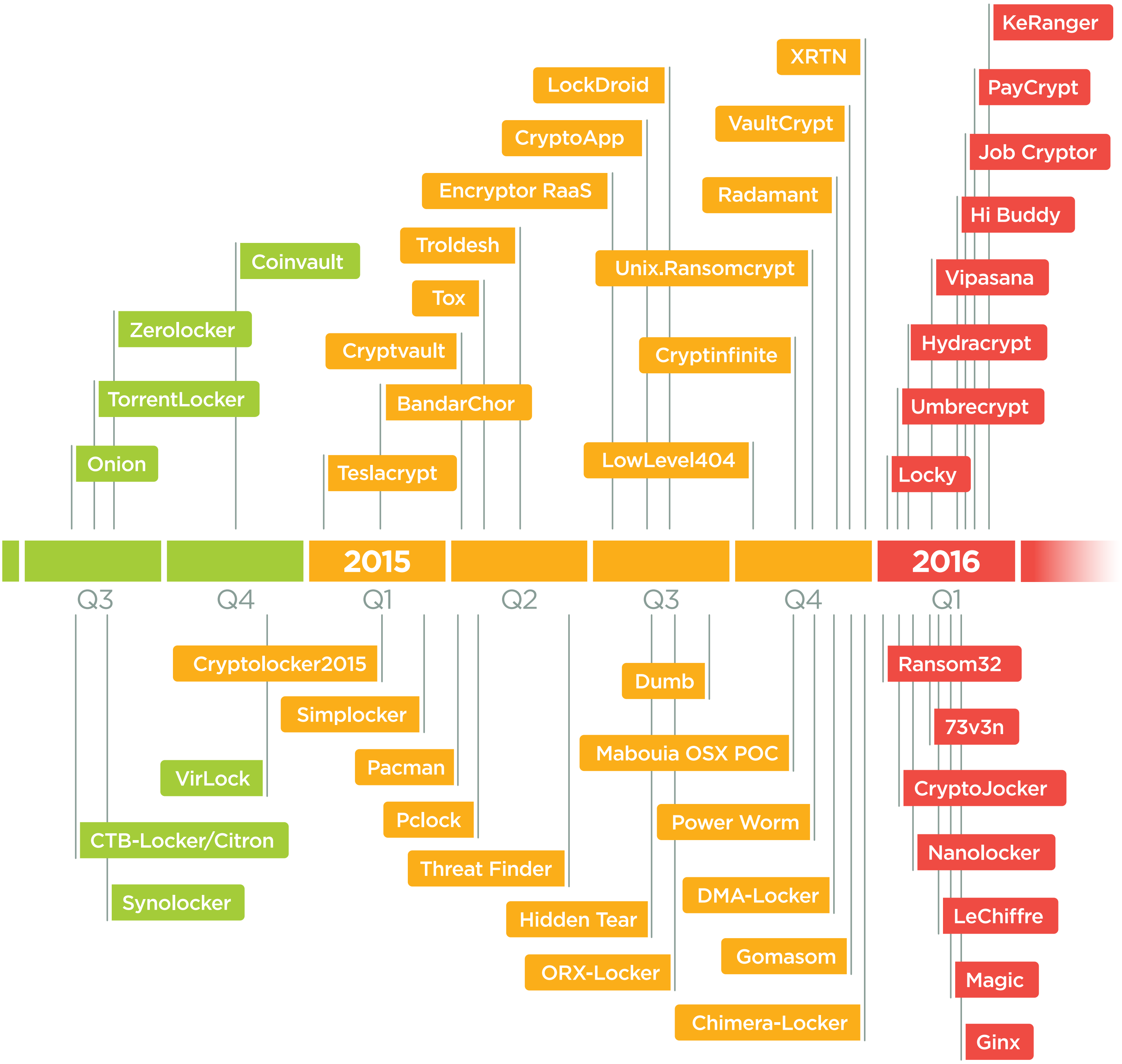
Source: Symantec
Report: https://www.symantec.com/content/dam/symantec/docs/security-center/archives/istr-16-april-volume-21-en.pdf

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, special 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.

NUMBER OF CHARACTERS	TIME TO CRACK PASSWORD
●●●●●● 7	**.29 milliseconds**
●●●●●●●● 9	**Five days**
●●●●●●●●●●● 12	**200 years**

Source: BetterBuys

Defense in Depth: Considerations for Building a Strong Cyber Defense Strategy

Identify

- Understand and control what sensitive, personal, and critical data, assets, processes, and systems your co-op stores and uses.
- Identify mission critical systems that cannot be exposed to either the internet or the enterprise network.
- 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.
- Physically segregate mission critical systems from both the enterprise network and the internet.
- Use multi-factor authentication and consider IP whitelisting for sensitive and critical systems.
- Change all default passwords on your computers and operational devices.
- Use long (12 character or more), 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.
- Patch mission critical systems with only OEM supplied updates. DO NOT patch mission critical systems with generic OS patches.
- 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.
- Use 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

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

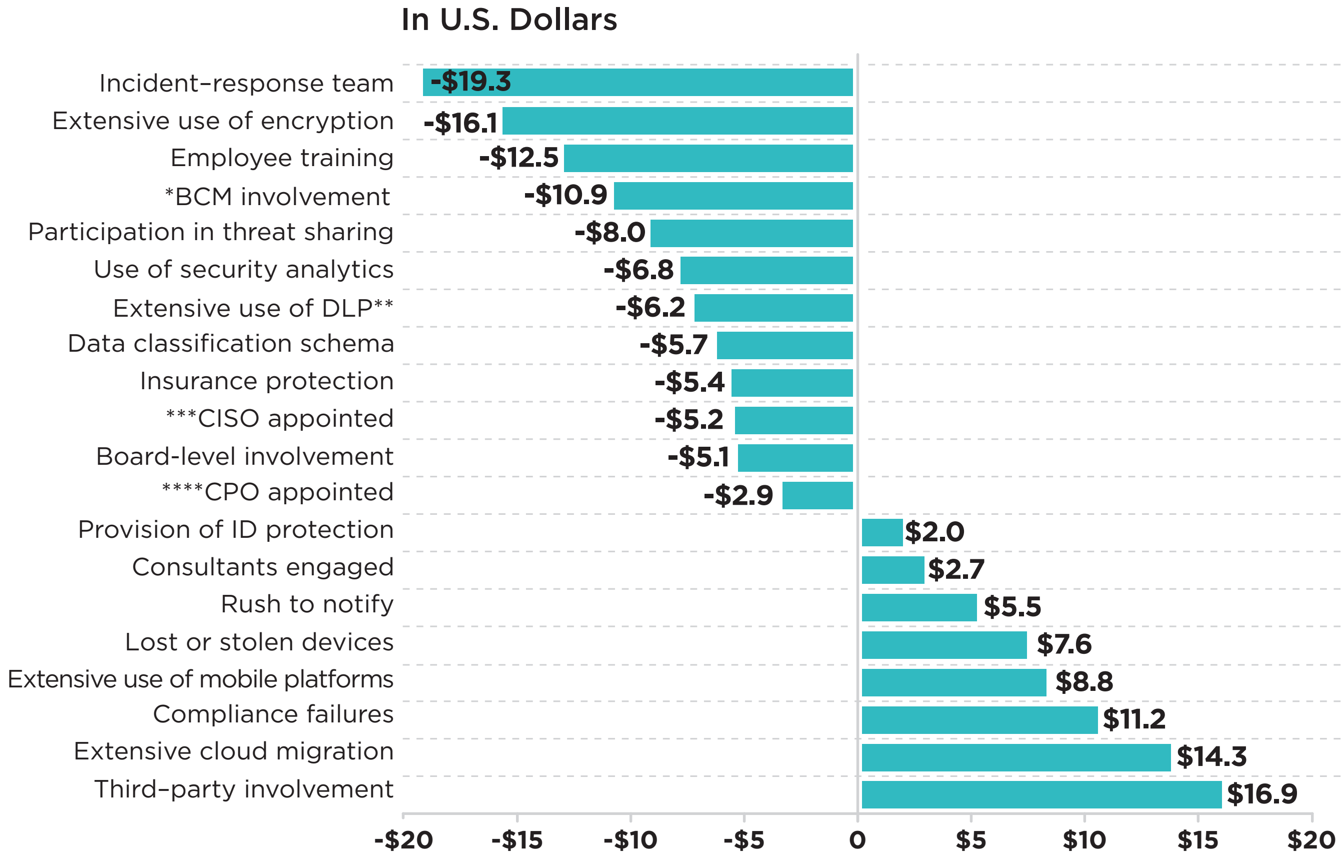
Recover

- Back-up files daily, store back-ups in locations not connected to your network, and test back-ups regularly.
- Employ a "generational" back-up strategy.
- Perform a post-incident review, and update policies and procedures as needed.

NOTE: This list is not exhaustive, so it does not include all options and considerations and resources. The notes above are merely considerations. Each electric cooperative has unique circumstances, and this document is provided as a general resource, among others, for their consideration.

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 can change that breach liability.



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

Source: Ponemon Institute/IBM Report: https://www.ibm.com/security/infographics/data-breach/

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 self-assessment, 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 (NCEMC; statewide), 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’

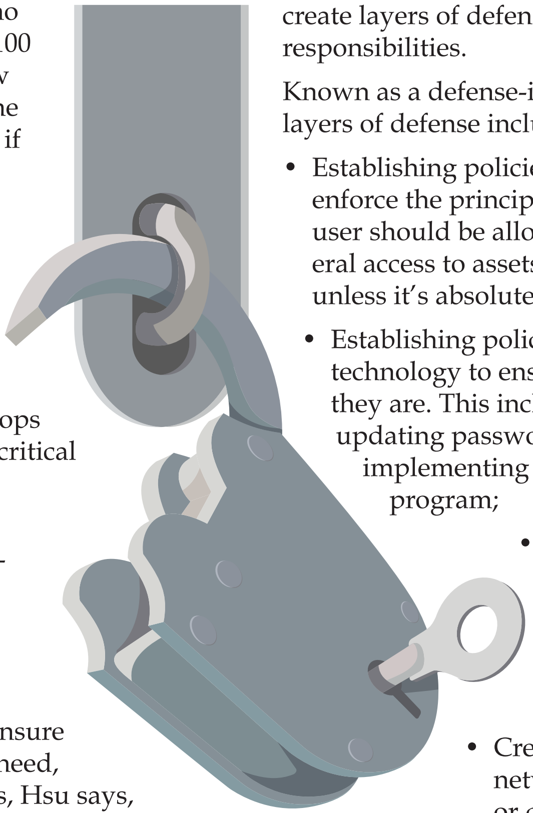
By Bob Gibson

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.



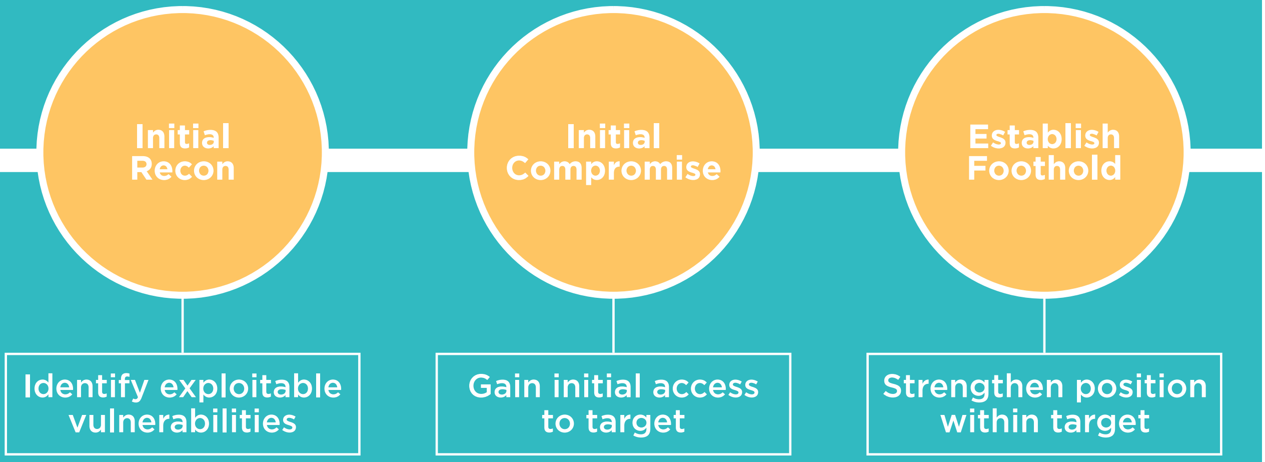
Experts recommend a combination of people, processes, and technologies to ensure that employees can reach the data they need, but only the data they need. The process, Hsu says, begins by determining what is valuable, where it’s located on the network, and how it’s accessed. Then decide who should be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



Initial Recon

Identify exploitable vulnerabilities

Initial Compromise

Gain initial access to target

Establish Foothold

Strengthen position within target

- 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 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 developed a self-assessment tool specifically designed for small- and mid-sized utilities with few or no IT employees.

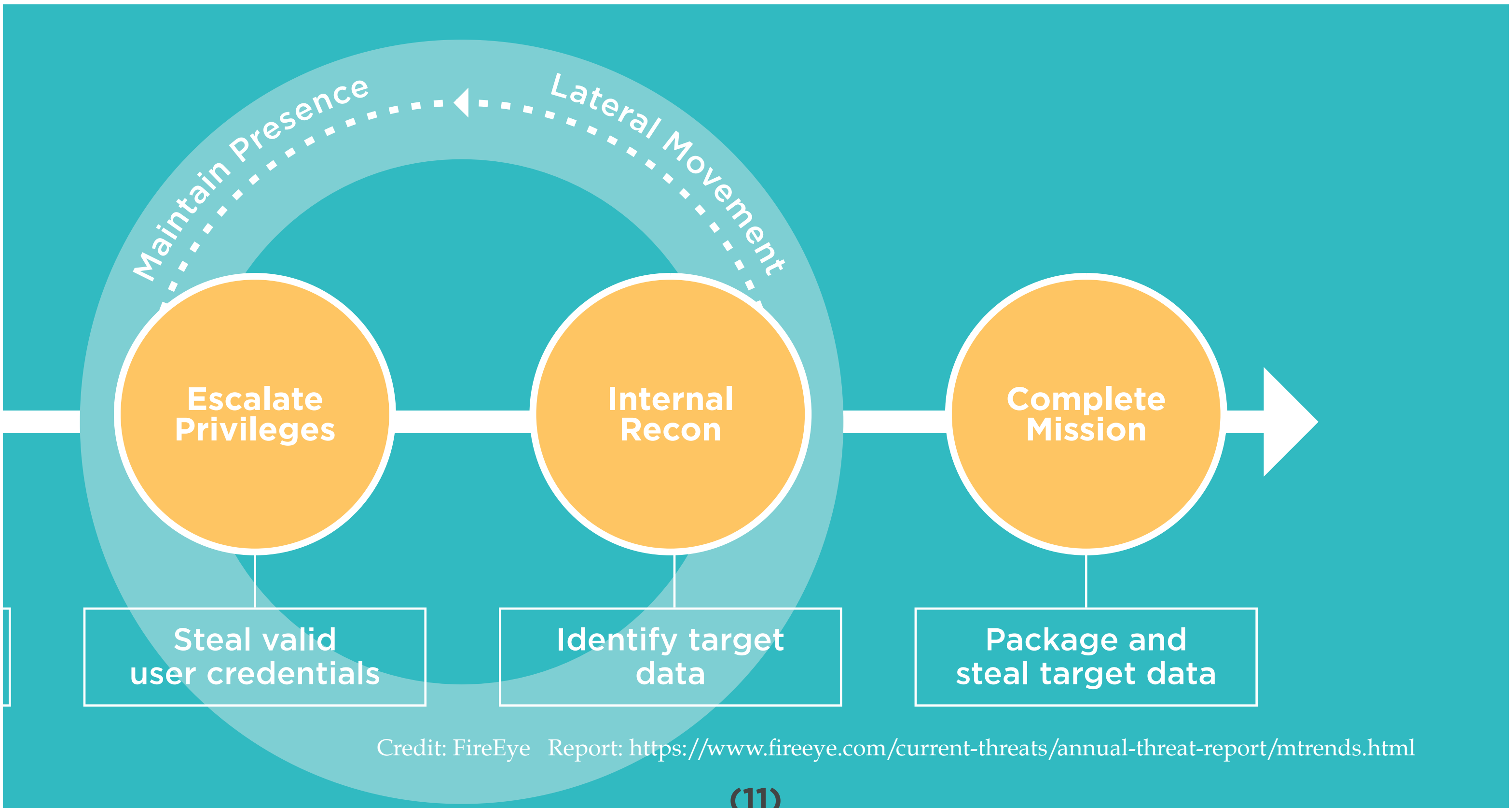
The tool, which is in field testing at cooperatives around the country, is designed to be a cross-departmental team exercise. The process walks the organization through a series of questions about their cyber capabilities and practices, and assigns a ranking based on the maturity of the utility's program.

"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 program.

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



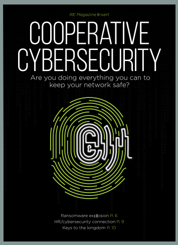
Credit: FireEye Report: https://www.fireeye.com/current-threats/annual-threat-report/mtrends.html

NRECA’s Rural Cooperative Cybersecurity Capabilities Program (RC3)*

RC3

$7.5 million received from the U.S. Department of Energy in 2016 for RC3, a 3-year program to work with cooperatives’ as they improve their cyber and physical security.

200+ leadership staff at 36 co-ops received cybersecurity training in 2017 and helped build an RC3 Self-Assessment toolkit.



RE Magazine Insert

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

22,000 copies of RE Magazine’s supplement and articles on cybersecurity distributed to members.

194 staff from 152 electric co-ops received cybersecurity awareness training at six RC3 Cybersecurity Summits in 2017.

40 co-ops are helping each other and the broader co-op community learn cybersecurity skills through the RC3 SANS Voucher Training Program.

More than 100 co-op staff who participated in the RC3 Self-Assessment Research Program said it will help their co-op improve its cybersecurity capabilities.

One co-op network, with NRECA’s leadership, fostering a culture of cybersecurity.

*RC3 is starting the final year of this 3-year effort.

NRECA® America’s Electric Cooperatives

U.S. DEPARTMENT OF ENERGY

August 2018

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

This report 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.