Here are three security recommendations for 2019 from Heather McCalman, credit union council manager at the Financial Services Information and Analysis Center.

Recommendation 1: Credit unions should do everything they can to secure and lockdown the Internet of Things (IoT).

IoT devices are getting more prolific and not going away. With the IoT comes a wide range of known and unknown vulnerabilities. Threat actors know the vulnerabilities that IoT devices contain better than the users do. IoT devices then become a backdoor with a very faulty lock. If the lock is easily broken, the IoT device can be used to breach the internal network of the credit union. This is an easy fix and a breach hazard that can be addressed.

Senior management needs to mandate that the Information Technology (IT) and Information Security (IS) departments are involved in the entire purchase and implementation process of every IoT device to help determine the safest device and maintain it.

From there, IoT best security practices should be followed:

- Change the default password on the device;
- Add the device to the hardware management program;
- Consider setting a private virtual local area network for IoT devices alone that is segmented from the rest of the network; and
- Periodically check for updates or upgrades to the firmware and operating system of the device.

The hard part is getting all departments across the credit union to let the IT and IS departments know when they've purchased and connected a device. A network access control system will help lock down open data ports and alert when unapproved devices have been connected.

Recommendation 2: Credit unions should practice incident response plans, business continuity plans and disaster recovery plans.

The language in security has shifted from "if" to "when" an organization will suffer an incident. It has shown time and time again that organizations who practice their response plans are the ones who come out on the other side of a breach or disaster with minimal fiscal, operational or reputational damage.

Exercising a plan can be as simple as a walkthrough, where teams openly discuss a potential scenario and how they will react. Exercising a plan can also be more hands-on, where specific departments or processes are stopped to practice the workaround, recovery or other backup plan. These types of exercises should involve *all* stakeholders in the organization. IT and IS of course, but also operations, marketing/communications and member services. All departments will be affected and involved when an incident occurs. For instance, if the news of a data breach at a credit union reaches the public and a member asks a teller about the incident, will the frontline staff know what to say, to prevent further reputational damage and not spread fear, uncertainty and doubt?

It's good to put network defenders (IT and IS staff) in an environment where they can practice what they will do. Many times, organizations train and exercise all departments, including IT, but the technical side of a potential incident remains largely theoretical. It's good to send IT and IS staff to practice against current threat scenarios, like a ransomware or business email compromise campaign.

FS-ISAC offers cyber-range exercises specifically for financial services staff to practice their hands-on capabilities against current threats. This type of hands-on exercising builds muscle memory that becomes knowledge. That knowledge becomes innovative thinking in the time of an incident.

Recommendation 3: Credit unions should encourage their cybersecurity staff to communicate and cooperate with other institutions' staff to share operational knowledge and threat intelligence.

Credit unions support the financial lives of their members and the financial ecosystem of the local groups, communities, cities and states they serve. This same cooperative spirit enables credit union IS departments to better protect and secure the assets of the institution and its members. The motivation of cybersecurity staff at credit unions and community banks should be to prepare for, prevent, detect and defend against cyberattacks because cyberattacks aren't going to stop and they aren't going to discriminate.

The next logical question is, "How do other credit unions and institutions do this?" The answer to that question can range from simple, easy and basic to complex, intricate and holistic. However, maybe the first question shouldn't be about how this is done but more about ***who to ask***. The safe answer is to ask other credit union and community banks' cybersecurity staff. They can relate operational knowledge of what works and what doesn't work, the pros and cons of certain solutions, how to overcome internal or external hurdles and the perceptions of their programs and solutions.

With the help of FS-ISAC and threat intelligence sharing, these credit union and community bank cybersecurity personnel:

- Shared technical information so other financial institutions could defend against WannaCry when it was spreading;
- Offered the technical information to assist with the global interruption of the Citadel, Ramnit, ZeuS and GameOver ZeuS banking trojans; and
- Communicated information about ATM skimmers allowing other local institutions to find and remove them from their ATMs.

This is only a snapshot of how sharing technical threat intelligence enables small and mid-sized institutions to secure their members and institutional assets from attacks.

In the communities that FS-ISAC serves, basic information like policies, procedures and best practices are shared between community institution members. Very knowledgeable, technical analysts answer questions and share information with not as technically-sophisticated network defenders as well. FS-ISAC recently started another sharing community for fraud departments at institutions to share generic, non-attributable information and create obstacles for fraudsters who target local communities.

An information sharing community:

- Needs to be a trusted community, where participants are vetted and agree to protect the information shared according to a security level protocol;
- The strength of the information sharing community relies on the participants to share the intelligence they are seeing as well as receive the intelligence shared by others;

- Is a two-way street that benefits all participants;
- Protects institutions and consumers alike; and
- Should be a trusted leader in the space with a proven record of protecting the information being shared.