Credit Union MAGAZINE
Credit Union National Association

MAY 2019

Measure cybersecurity readiness

Boards must understand cyberpolicy, technology in play

JENNIFER PLAGER

Board members are tasked with ensuring the credit union complies with rules and regulations designed to protect members' data and privacy. But how involved in the credit union's cybersecurity program does the board need to be?

"The fearful phrase is the board is effectively responsible for everything," says David Reed, attorney, consultant, and trainer with Reed and Jolly PLLC.

"The board is the top of the decisional food chain. They don't have to be experts in cyberthreats and the defenses that are available, but the board is responsible for the direction and control of the credit union," he says.

That means the board must be aware of the rules, regulations, and laws that affect the credit union, and ensure the credit union takes the appropriate steps to comply with these rules and maintain adequate security measures, Reed says in a CUNA News Podcast interview about the board's role in cybersecurity.

The board also should delegate tasks such as security audits or other reviews to experts within the credit union.

"Even though the ultimate responsibility is the board's,

> **I WOULD CAUTION THE BOARD THAT EVEN THOUGH THEY'RE NOT HANDS ON, THEY NEED TO HAVE THE TOOLS IN FRONT OF THEM.**
>
> **David Reed**

and that can't be delegated, the actual tasks can be delegated," Reed says.

An outside auditor or the credit union's supervisory committee should perform audits that examine applicable rules and regulations, and how the credit union addresses them, Reed suggests. The resulting reports should be reviewed to gauge cybersecurity readiness and identify what changes need to be made.

Among the reports the board should review:

- **Regulatory** examination findings.
- **Supervisory** committee audits.
- **Specialized** information technology (IT) audits.

"I would caution the board that even though they're not hands on, they need to have the tools in front of them," Reed says.

Even if these reports indicate the credit union is performing satisfactorily regarding cybersecurity efforts, the board should not assume there's nothing else the credit union needs to do.

"It's often said with any security that you're only as strong as your weakest link," says Reed, who uses social engineering as an example.

This is a concept where fraudsters try to trick employees into providing secure information, such as passwords or account details, by clicking on a malicious link or giving account information over the phone.

In addition to implementing policies and providing staff training, Reed says it's important for the board to request periodic audits to ensure employees practice the behaviors they've learned through training.

Have a tester—usually a third party or a member of your IT staff—send an unannounced email with a link or make a phone call seeking information. See how many employees click on the link or give information to the caller.

"They need to see whether or not those trainings, reminders, policies, and procedures are in fact working," Reed says. "When those are done, the results should be given to the board. If everything is working great, then the board is given a double thumbs up."

If things have gone awry, Reed says the board will know changes have to be made to the information security program or employees will need to undergo additional training.

"The board needs to have a dashboard of information so it has a reasonable assurance the data is safe and the credit union is complying with all of the different laws, rules, and regulations," Reed says.

The board also should be familiar with the credit union's operations, technology, and data security policy. This will allow the board to view the applicable information, understand potential problem areas, and identify where changes need to be made.

"Know the doors and windows of your credit union that members and data come in and out of," Reed says. "You need to understand how those operations work."

Reed also says board members need to understand the technology members use—whether they use online banking, mobile banking, remote deposit capture, or prefer to complete their transactions within the branch.

"Even if a board member doesn't use that technology, they need to understand the basics of it and how many of their members are using it, and then they need to make sure they're following all of the laws, rules, and regulations for each of those technologies," Reed says.

Gaining a greater understanding of credit union operations and the technologies behind it, Reed says, will allow the board to understand and appreciate the importance of cybersecurity. He says it's an issue and process that is manageable, but requires the board to carry out its due diligence.

"The board simply needs to understand how it's deploying its own resources," Reed says. "Make sure you're your own quality assurance."

Steps to safeguard member information

A comprehensive written information security program includes administrative, technical, and physical safeguards appropriate to the credit union's size and complexity, and the nature and scope of its activities.

The board should coordinate all elements of the information security program throughout the institution.

According to Valerie Y. Moss, CUNA's senior director of compliance analysis, an information security program should be designed to:

›**Ensure** the security and confidentiality of member information.
›**Protect** against any anticipated threats or hazards to the security or integrity of such information.
›**Protect** against unauthorized access to or use of information that could harm or inconvenience any member.
›**Ensure** the proper disposal of member information and other consumer information.

Key elements of developing and implementing a member information security program involve:

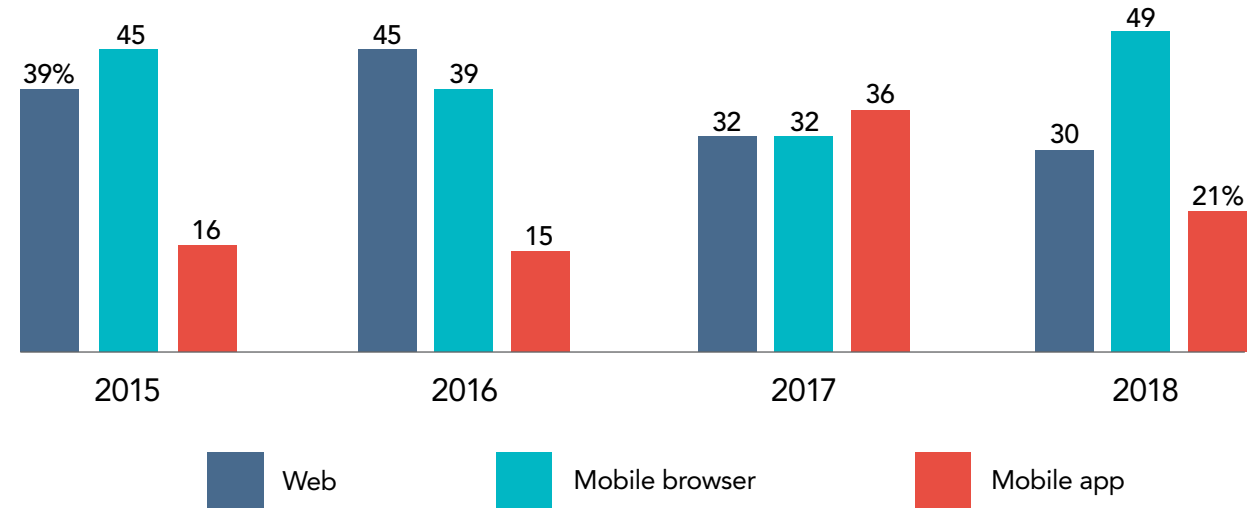
›**Identifying** the services provided and systems used.
›**Identifying** the risks and threats associated with each system and service.
›**Determining** the likelihood that identified risks or threats could occur.
›**Identifying** and evaluating various methodologies to mitigate risks or threats.
›**Developing** policies and procedures to address risks or threats.
›**Monitoring** and adjusting policies and procedures.
›**Overseeing** service provider arrangements.
›**Reviewing** policies and procedures at least annually.
›**Training** staff to implement the program.

Management or other appropriate staff members should report to the board or a board committee at least annually. The report should describe the overall status of the information security program and the credit union's compliance with rules and regulations.

The report should also cover issues such as risk assessment and control decisions, service provider arrangements, testing results, any security breaches or violations and management's response, and recommendations for changes in the information security program.

Fraud and mobile channels

Mobile applications and mobile browser transactions make up nearly three-quarters of fraud transactions, according to the RSA Quarterly Fraud Report. There is a growing preference among fraudsters to initiate unauthorized transactions through mobile applications.



Source: RSA Quarterly Fraud Report Q4 2018

CUNA continues to call for national data security standard

No set of national data security standards currently exists, but there's push from CUNA and other financial services industry groups calling on policymakers to create a national data security framework.

CUNA has sent letter to various committees—including the Senate Committee on Commerce, Science, and Transportation and the House Energy and Commerce Committee—advocating support for the creation of new federal protections on data.

"Taking a narrow view that this debate is about Facebook, Amazon, and Google would be a grave mistake," CUNA President/CEO Jim Nussle states in a letter to the Senate Committee on Commerce, Science, and Transportation.

"There is no way for Congress to provide consumers with the data privacy they need without enacting robust data security standards that are preemptive of state law and apply to everyone."

> **THERE IS AN URGENT NEED FOR CONGRESS TO ACT TO SET A FEDERAL DATA PRIVACY STANDARD**
>
> **Jim Nussle**

CUNA believes any new privacy law and/or data security requirements should:

›**Cover** both privacy and data security.

›**Cover** all companies that collect, use, or share personal data.

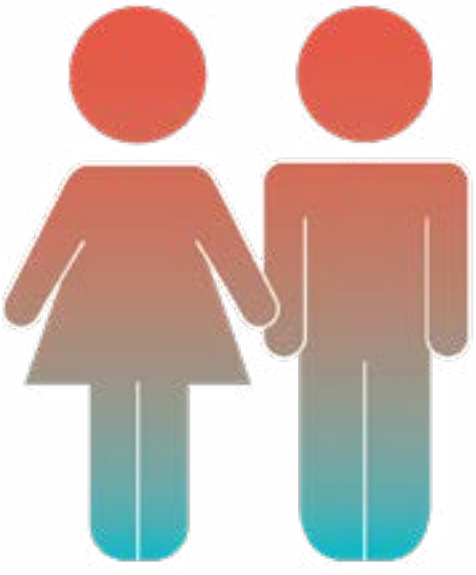
›**Be based** on protection of data to prevent from theft and misuse. Disclosure after the fact is important, but it's not a substitute for adequate protection.

›**Provide** the mechanisms to address the harms that result from privacy and security violations, including data breaches. Individuals and companies should be afforded a private right of action, and regulators should be able to act against entities that violate the law.

›**Preempt** state law to simplify compliance and create equal expectation and protection for all consumers, with a goal to create a national standard for all to follow.

"There is an urgent need for Congress to act to set a federal data privacy standard," Nussle says.

The letter also indicates that data privacy is a national security issue because there have been more than 10,000 data breaches in the U.S. since 2005, compromising nearly 12 billion consumer records.



43%

of credit union members **expect** their institution to reduce their exposure and quickly fix the situation if their data is **compromised.**

Source: General Global Assistance

TRAINING: Look for insights from your credit union professionals who are attending the CUNA Cybersecurity Conference with NASCUS June10-12 in Austin, Texas. cuna.org/cyber. Prepare yourself at the CUNA Roundtable for Board Leadership Oct. 19-20 in Phoenix. cuna.org/boardroundtable.