2019, Issue 3

# The Auditor's Report

## Accounting Standards Update

On August 15, 2019, the Financial Accounting Standards Board (FASB) issued a proposed Accounting Standards Update (ASU) that would grant credit unions and others additional time to implement FASB standards on current expected credit losses (CECL), leases, and hedging.

The proposed ASU describes a new FASB philosophy that extends and simplifies how effective dates for major standards are staggered between larger public companies and all other entities. Those other entities include credit unions. Under this philosophy, a major standard would first be effective for larger public companies. For all other entities, the Board would consider requiring an effective date staggered at least two years later. Generally, it is expected that early application would continue to be permitted for all entities.

The FASB Chairman Russell Golden stated that "Based on what we've learned from our stakeholders, including the Private Company Council and the Small Business Advisory Committee, private companies, not-for-profit organizations, and some small public companies would benefit from additional time to apply major standards. This represents an important shift in the FASB's philosophy around effective dates, one we believe will support better overall implementation of these standards."

Based on that philosophy, the Board proposes to amend the effective dates for CECL, leases, and hedging as follows:

| Standard | SEC Filers | All Other Public Business Entities (PBEs) | Credit Unions |
|---|---|---|---|
| Hedging | January 2019 | January 2019 | January 2021 |
| Leases | January 2019 | January 2019* | January 2021 |
| CECL | January 2020 | January 2023 | January 2023 |

*Also includes Employee Benefit Plans and Not-for-Profit Conduit Bond Obligors that file or furnish financial statements with or to the SEC

The Board invites individuals and organizations to comment on all matters in this proposed Update until September 16, 2019, particularly on the issues and questions below. Comments are requested from those who agree with the proposed guidance as well as from those who do not agree. Comments are most helpful if they identify and clearly explain the issue or question to which they relate. Those who disagree with the proposed guidance are asked to describe their suggested alternatives, supported by specific reasoning. Interested parties may submit comments in one of three ways:

- Using the electronic feedback form available on the FASB website at Exposure Documents Open for Comment.
- Emailing comments to director@fasb.org, File Reference No. 2019-750.
- Sending a letter to "Technical Director, File Reference No. 2019-750, FASB, 401 Merritt 7, PO Box 5116, Norwalk, CT 06856-5116.

All comments received are part of the FASB's public file and are available at www.fasb.org.

**INSIDE THIS ISSUE**

Accounting Standards Update.....1

Employee Awareness and Physical Security.....2

1979 ★ 2019
40 years
Nearman
Maynard • Vallez
Certified Public Accountants
exclusively serving credit unions

**Like what you see? Send an email to news@nearman.com to get The Auditor's Report electronically.**

# Employee Awareness and Physical Security – Protecting Yourself Against Social Engineering

Securing and safeguarding your internal network from external attacks may seem like a never-ending task; however, the attack that may be the most difficult to defend against may very well come not from malware, ransomware, or some other form of electronic payload but from walking, talking and breathing human beings. Unfortunately, it is not enough to have the most up to date firewalls, spam filters, web filters and anti-virus programs. While these programmatic counter-measures are undoubtedly the minimum safeguards you would want in place on your network, they can often be rendered useless or ineffective for someone that is able to gain physical access to your facility.

Social Engineering (the use of deception to manipulate individuals into allowing access to secure areas or divulging confidential information that may be used for fraudulent purposes) can expose an organization to both fraud and reputational risk. Certainly, the acts of network scanning, vulnerability exploitation and privilege escalation are of the utmost importance. However, even the most secure networks can be susceptible to physical attack if the organization's employees are not aware of the proper way to handle unauthorized physical access attempts.

Some of the ways that an organization can be susceptible to physical Social Engineering include:

**"…even the most secure networks can be susceptible to physical attack if the organization's employees are not aware of the proper way to handle unauthorized physical access attempts."**

- **Piggybacking** (following behind) employees in the morning as they arrive and enter the facility;
- **Posing** as a Vendor, Trainer, or other "trusted" 3rd party using forged credentials to coerce an employee to provide access to the facility;
- **Bypassing physical security** mechanisms (loiding a door, which means compromising a lock with a card or other implement, or grabbing a door that hasn't shut all the way after someone has already gone in).

There does not seem to be a strong correlation between success rates of physical security attacks and the size of the credit union. One would think that a small credit union with less than 10 or so employees would be hard to infiltrate due to the fact that the employees most likely all know each other. This turned out not to be the case for a small credit union where during a recent engagement, CastleGarde was able to walk in behind an employee arriving for work, make their way to a conference room and plug in a laptop to a network connection. The same also happens with larger credit unions. While they may often have better and more intensive physical access controls, these organizations often have so many employees that you can pose as just about anyone, from an auditor to a trainer, to a new employee and often find yourself provided access to places that should have been prohibited. In another case, a large credit union fell for an imposter who was able to use a forged badge identifying himself as an employee of a document shredding vendor. He was able to use the badge to obtain a vendor vest and an ID card that gave him access to the entire building (a very large building) including the data center!

At the end of the day, it's often the case unfortunately that your employees are the weakest link in your securing your facility. You can have a plethora of expensive network safeguards, but if you allow a single person access to "employee only" areas of your facility, there will be numerous opportunities for data compromise or internal network access. Credit union employees are trained provide excellent member service in everything they do. It's that welcoming attitude that can often lead to success when it comes to gaining elevated access to a facility. It is not suggested that employees be rude or non-welcoming but instead ensuring that you impress upon all of your employees that you can't always judge a

*Continued on page 3*

## ABOUT US

Since 1979, Nearman, Maynard, Vallez, CPAs has provided auditing and consulting services exclusively to credit unions throughout the United States. Our dedication to the credit union industry has given us the unique ability to provide exceptional service at a reasonable price. Our primary objective is to assist our clients in accomplishing their goals through our experience, service, and commitment. If your Supervisory/Audit Committee, Management, or Board of Directors is interested in obtaining information on the subjects in this issue or about our many services, call or email us today.



1979 ★ 2019
40 years
Nearman
Maynard • Vallez
Certified Public Accountants
exclusively serving credit unions

Website: www.nearman.com

E-mail: info@nearman.com

Toll-free: 800.288.0293

*Continued from page 2*

book by its cover. Employees need to be able to evaluate every situation independently and if something doesn't seem or feel right or they do not have enough information to make a split second decision, they should never feel sorry for making someone wait outside, requiring someone go to a main entrance instead of an employee entrance, or for simply telling someone "sorry, I don't know who you are and I can't let you in". One way to drive home this point to your employees would be to ask them "If this were someone trying to gain access to your home, would you allow them in or would you make them wait outside until you could verify that they were who they said they were?"

Testing or training against Social Engineering techniques can be difficult. It requires purposefully trying to deceive people and put them in compromising situations. As much as people dislike this type of testing, they would dislike it much more if they ever found out that their organization was infiltrated in this way by a real attacker. The likelihood of this type of attack may not be as high as the likelihood of a phishing attempt or malware attack, but the danger is present and unfortunately the type of person that would be bold enough to initiate this sort of action likely would have no qualms escalating any situation to stress levels much higher than would occur as part of this form of testing. Simulating can allow the option to back off when a situation may be escalating too far, an actual attacker would not. It's for that reason alone that you must make it a priority to ensure employees are trained in the importance of identifying unknown persons as well as how to handle these types of situations. Unlike software where you can patch a security weakness, you can't "patch" people. But, with repetition and an emphasis on situational awareness, you can train them to be more diligent, more perceptive and better prepared to deal with these specific types of physical security risks.

*Aaron Tank, CISA, CISSP, CRISC, VP Information Security Service*
*Castlegarde, Inc.*

**CastleGarde is an acknowledged expert provider of credit union information security-based assessments and regulatory compliance program services currently providing services to over 300 credit unions nationally and internationally. CastleGarde specializes the area of Information Security policy, technology assessment and the physical aspects addressing the controls, access, management, and safeguarding of member information as defined by NCUA Reg. 748 Appendix A and B. CastleGarde provides information security policy and procedure reviews, external penetration testing as well as onsite vulnerability assessments including physical security reviews to measure the overall effectiveness of your information security controls and related programs. Other services include the performance of General Controls Reviews and a full turnkey offering in Business Continuity Planning.*