Cybersecurity Readiness Guide

Whenever our team at PSCU's Solutions Consulting visits a credit union, we go around the table and ask, "What's keeping you up at night?" Lately, the answer has been cybersecurity—or lack thereof.

It may not be much comfort but credit unions aren't the only ones losing sleep: According to PwC's 2018 Annual Global CEO Survey, fears about cyber threats now lead the list of CEO concerns across all industries worldwide. In the U.S. alone, over 63 percent of CEOs describe themselves as "extremely concerned" about cybersecurity, dramatically up from 50 percent in 2017.

What's more, nearly a third of the CEOs surveyed worry that the bad guys might be winning. Over 32 percent expressed "extreme concern" that bad actors had better access to changing technology and skills than they did. That's a serious erosion of confidence from 2013, when only 11 percent of CEOs felt that way.

Creating a Culture of Security

Clearly, credit unions need a strategy to translate their cyber insecurities into a concrete game plan to reduce the risk of exposure to threats. But to be successful, such a plan must take into account the unique fraud climate that credit unions face, the operational and budgetary realities that constrain them, and the highly regulated industry in which they operate.

Fortunately, the Federal Financial Institutions Examination Council (FFIEC), the National Credit Union Administration (NCUA), industry groups like the National Credit Union Information Sharing & Analysis Organization (NCU-ISAO), credit union service organizations (CUSOs) like PSCU and individual credit unions are stepping up to provide their expertise.

Credit unions are uniting as never before to share the innovative strategies, tailored solutions and extensive resources needed to build what Gene Fredriksen, PSCU's Chief Information Security Strategist, calls a "culture of security."

Five Objectives for Cybersecurity Readiness

To share the key developments taking place on the cybersecurity front with our PSCU Owner credit unions, Solutions Consulting has created this Cybersecurity Readiness Guide. Our five objectives in writing it are to:

1. Give you a broad outline of the current cybersecurity threat environment for financial services in general—and credit unions in particular.
2. Provide an overview of the strategic vision for cybersecurity that the NCUA is putting in place to protect your credit union.
3. Outline the key components of the NCUA's threat reduction strategy, including a look at FFIEC's Cybersecurity Assessment Tool (CAT), a variation of which is currently being pilot tested for rollout to credit unions in 2019.
4. Help you identify the gaps in your credit union's current level of cybersecurity readiness.
5. Suggest actions to build your credit union's long-term cyber resilience through education, training, and technology initiatives.

Defining Credit Unions' Cyber Threat Environment

To talk about the current cybersecurity threat environment, it's important to understand just how rapidly our financial lives have gone digital. In fact, as highly regulated as the U.S. financial services industry has been since the 1930s, the FFIEC—the umbrella agency of the Federal Reserve that includes the NCUA—didn't add cybersecurity to its mission until 2013.

What's more, the magnitude of the shift to digital and mobile in just under five years has been seismic: According to Brian Hinze of the NCU-ISAO, 83 percent of today's federally insured credit unions (FICU) now have websites and 73 percent have transactional websites.

That translates to nearly 51 million credit union members with online access to nearly 99 percent of the total FICU system's assets.

The Operational Risks of Underdeveloped Infrastructure

Although the transformation to digital has occurred virtually overnight, the critical infrastructure of the credit union industry—the people, processes and technology—that it relies on to deliver its digital services to members (and compete with larger financial institutions) has not kept up.

The net effect of trying to deliver top-quality, multi-channel member service via an outmoded and/or underfunded infrastructure is that credit unions have created significant cyber risks for themselves on the operational side by trying to do too much with too little—small security staffs, lean budgets and a "come-one-come-all" non-profit mentality.

To quote from the NCU-ISAO website, "As credit unions continue to stretch their resources to serve their members, while at the same time facing increased regulatory scrutiny, they will need trusted security coordination and collaboration to identify, protect, detect, respond, and recover from threats and vulnerabilities."

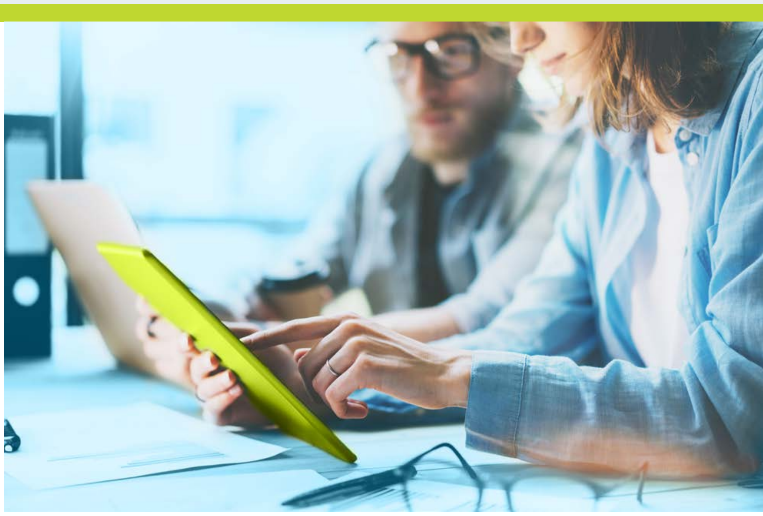
The Ongoing Presence of External Cyber Threats

Meanwhile, external cyber threats from hackers may have morphed over the years but they haven't gone away. According to Symantec's Internet Security Threat Report – Financial Threats Review 2017, the "good news" is that the most sophisticated cyber criminals have now shifted their focus away from financial services institutions to crypto currency thefts and ransomware.

However, the bad news, according to Tim Segerson, Deputy Director of Examination and Insurance for the NCUA, is that credit unions have now become prime targets for less accomplished hackers. That's because sophisticated hackers are now monetizing their cyber fraud success by selling turnkey "hacking toolkits" on the Dark Web. It's amateur hackers who are buying them and as beginners, they're looking for below-the-radar targets with out-of-date defenses. Many credit unions fit that bill perfectly.

Segerson also points out that it's wishful thinking for credit unions to think that their mission as cooperative financial institutions will somehow exempt them from political attacks, insider attacks, or attacks from disgruntled current or former employees.

In fact, according to Dtex System's 2018 Insider Threat Intelligence Report (registration required), "the clear takeaway is that visibility gaps still allow insiders to jeopardize organizational security through high-risk activity, whether it be due to malicious intent, outside infiltration, or simple human error."



Overview of the FFIEC – NCUA Cybersecurity Strategy

In May 2017, the FFIEC launched its Cybersecurity Assessment Tool (CAT), designed to help financial institutions voluntarily self-assess their risks and "measure their cybersecurity preparedness over time."

The NCUA's Automated Cybersecurity Examination Tool (ACET) mirrors the FFIEC's CAT, but is specifically tailored to help the NCUA assess credit unions' current levels of cyber readiness and benchmark their progress.

With the goal of creating a "repeatable, measurable, and transparent process for assessing the level of cyber preparedness across federally insured institutions," NCUA examiners began working with credit unions with over $1 billion in assets earlier this year to pilot test the ACET on a voluntary basis.

The idea is to work with the largest and most complex credit unions to ensure that the tool will be user friendly and scale properly for smaller credit unions, while at the same time gathering baseline and benchmarking data that will benefit the entire industry when the ACET rolls out more broadly in 2019.

Previewing the FFIEC Cybersecurity Assessment Tool

The FFIEC-NCUA credit union assessment process consists of two parts: evaluating the Inherent Risk Profile and assigning a Cybersecurity Maturity level.

1. Inherent Risk Profile

The Inherent Risk Profile evaluates 39 activities, products or services across five categories to help determine a credit union's overall exposure to risk. For each item, the assessment tool defines and quantifies five possible risk levels, ranging from Least to Minimal to Moderate to Significant to Most.

Table 1: FFIEC Inherent Risk Profile

Activity, Service or Product

Risk Levels

	Risk Levels				
Category: Technologies and Connection Types	LEAST	MINIMAL	MODERATE	SIGNIFICANT	MOST
Total number of internet service provider (ISP) connections (including branch connections)	No connections	**Minimal complexity (1-20 connections)**	Moderate complexity (21 - 100 connections)	Significant complexity (101-200 connections)	Substantial complexity (>200 connections)
Unsecured external connections, number of connections not users (e.g., file transfer prototype (FTP), Telnet, rlogin)	None	**Few instances of unsecured connections (1-5)**	Several instances of unsecured connections (6-10)	Significant instances of unsecured connections (11-25)	Substantial instances of unsecured connections (11->25)

The Inherent Risk Profile categories are:

- Technologies and connection types

Delivery channels

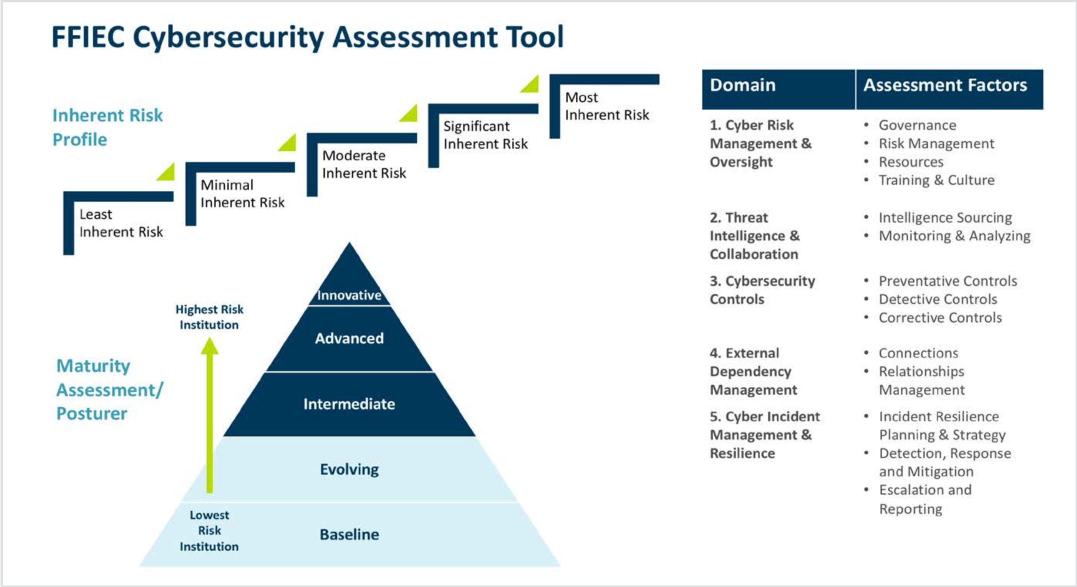
- Online/mobile products and technology services
- Organizational characteristics
- External threats

2. Cybersecurity Maturity

The Cybersecurity Maturity portion of the CAT is designed to help credit unions measure their level of risk and their corresponding controls within five Domains. The five Domains are:

- Cyber Risk Management & Oversight
- Threat Intelligence & Collaboration
- Cybersecurity Controls
- External Dependency Management
- Cyber Incident Management & Resilience

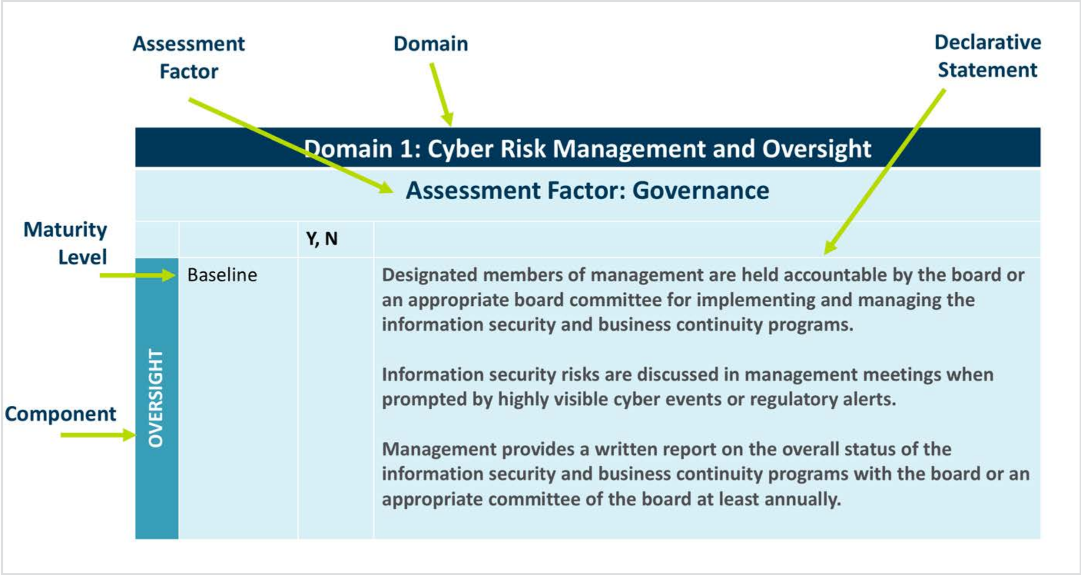
Table 2: Overview of the Cybersecurity Maturity Assessment Process



Domain	Assessment Factors
1. Cyber Risk Management & Oversight	• Governance • Risk Management • Resources • Training & Culture
2. Threat Intelligence & Collaboration	• Intelligence Sourcing • Monitoring & Analyzing
3. Cybersecurity Controls	• Preventative Controls • Detective Controls • Corrective Controls
4. External Dependency Management	• Connections • Relationships Management
5. Cyber Incident Management & Resilience	• Incident Resilience Planning & Strategy • Detection, Response and Mitigation • Escalation and Reporting

Various Components of each Domain are then given a rating from Baseline to Innovative, based on Yes-No answers to various Declarative Statements, which are grouped under the Domain's various Assessment Factors.

Table 3: Relationships Between Cybersecurity Maturity Rating Elements



Domain 1: Cyber Risk Management and Oversight

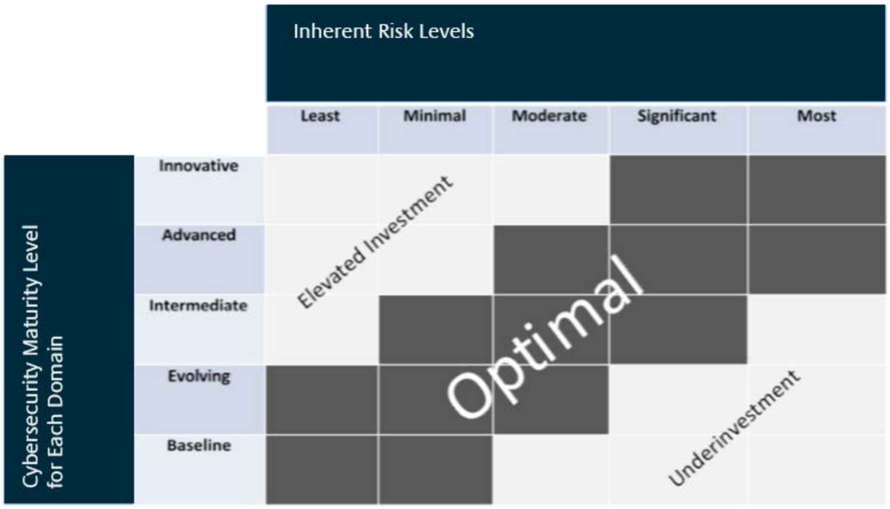
Assessment Factor: Governance

		Y, N	
OVERSIGHT	Baseline		Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs. Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. Management provides a written report on the overall status of the information security and business continuity programs with the board or an appropriate committee of the board at least annually.

As credit unions work through the self-guided assessment tool, it's important for everyone to realize that the NCUA has no expectation that most CUs will—or should—ever score above the Baseline or Evolving levels.

The NCUA's reasoning is that examiners want to encourage credit unions to take an approach to investing for cyber readiness that balances risk and reward. As shown in Table 4 below, the NCUA wants to work with credit unions to optimize their resource deployment to the areas of most significant risk.

Table 4: Optimal CU Risk-Reward Investment – FFIEC Cybersecurity Assesment Tool



Cybersecurity Maturity Level for Each Domain	Inherent Risk Levels: Least	Minimal	Moderate	Significant	Most
Innovative				■	■
Advanced			■	■	■
Intermediate		■	■	■	
Evolving	■	■	■		
Baseline	■	■			

Elevated Investment
Optimal
Underinvestment

Identifying and Closing Your Credit Union's Cybersecurity Gaps

Although the FFIEC has designed a cybersecurity assessment process that is extremely thorough in its basic version (and even contains a number of additional specialty modules that are beyond the scope of our discussion here), the NCUA's big-picture objectives focus not on finding fault with credit unions but on partnering with them to create a culture of resilience and security.

The goal of resilience is based on working with credit unions to give them the expertise and resources they'll need to conduct their operations according to the five key principles outlined below:

1. Growing organizational awareness of cybersecurity from the top down
2. Establishing and enforcing appropriate cybersecurity policies, responsibilities and oversight
3. Creating strong day-to-day cyber- and data-hygiene practices
4. Training and drilling employees on incident response and escalation processes
5. Testing and backing up systems regularly

10 Checklists for Translating the Five Principles to Action

Through its strong partnership with the NCU-ISAO, PSCU heartily endorses and supports the NCUA's approach.

To help your credit union implement the five principles laid out above, Solutions Consulting has summarized guidance from the FFIEC, NCUA, NCU-ISAO, PSCU's own in-house experts in cybersecurity and risk management, and our own supplementary research to create the following series of best practices checklists and informational appendices:

1. Grow organizational awareness of cybersecurity from the top down.

- **Obtain buy-in from your board of directors.** Together with your C-suite, your credit union's board of directors is vitally important to setting your overall cybersecurity priorities and making sure they receive the ongoing technology, workforce, and training investments they require.
  - Engage your board by regularly encouraging them to s**hare their own organizations' cybersecurity strategies and lessons learned.**
  - Establish a **monthly or quarterly cybersecurity reporting process** to keep your board in the loop regarding your credit union's progress with the FFIEC-NCUA assessment tools, how any cybersecurity incidents that may have occurred were handled, technology investments or vendor contracts under consideration, industry trends, cybersecurity challenges your managers are facing, etc.
- **Train your C-suite and IT department in cyber preparedness and disaster response.** Your IT department is the area of your credit union most likely to experience a cataclysmic onetime "meltdown" or "ticking clock" event such as the discovery of malware or a DDoS or ransomware attack.

  In those events, time is of the essence, so everyone from your C-suite to departmental managers to staff members must know what to do and how execute based on clear directives and a pre-existing chain of command.
  - Build an **incident response and escalation process**, both within your credit union and including escalation to the US Computer Emergency Response Team (US-CERT).
  - Have **contact information** handy and know who to call and when to call them, including backup contacts.
  - Participate in **cybersecurity drills and simulations** that focus both on responding to an incident in real time and handling the aftermath of an incident.

    For example, during work on this Cybersecurity Readiness Guide, a member of our Solutions Consulting team participated in a live cyberattack simulation and webinar sponsored by the Harvard Business Review.

    Entitled "What Would You Do During a Cyberattack?" the exercise was conducted by Rob Austin, professor of Information Systems at Ivey Business School at the University of Western

Ontario in Canada. Following the simulation, Professor Austin shared a protocol for managing a cyber event in real time, as well as his best practices for post-incident external communication.

Before and during the event:

- Be prepared. Have everyone's office and mobile phone contact information at your fingertips.
- Always keep your group's discussions calm and rational.
- Don't fixate on initial hypotheses. Be open to new interpretations as the situation evolves.
- Preserve the diagnosis environment. RESIST the temptation to shut down your systems because that will destroy the forensic footprints of the attack.
- Keep diagnosis and response in the right order. Don't jump to conclusions.
- Every action you take should be deliberate. Never take action just to be doing something.
- Draw on your team's reserves. Bring all hands on-deck. Don't leave anyone's input out because it's not their shift, it's their day off, or they're on vacation.
- Avoid distractions. Unless another task is relevant to the crisis at hand, put it aside.
- Keep track of what you know or don't know at any given moment using written notes. Keeping a running log of the incident is vital, not only for post-incident debriefing and learning but for reporting the incident to regulators and avoiding possible lawsuits.

In your external communications following the event:

- Keep your statements truthful.
- Avoid scary words like "suffered an attack."
- Don't speculate or say more than you have to.
- Don't invite follow-up, e.g., "we'll be holding a press briefing tomorrow at 1 p.m."
- Don't challenge the hackers by announcing that your defenses thwarted their attack.

2. Develop a robust backup regime.

The NCUA estimates that a whopping 50 percent or more of cyber incidents could be stopped simply by applying the patches necessary to keep system and application software up-to-date.

- **Patch your system software.**
  - Turn on automatic updates and/or install all software security fixes as soon as they are issued — but always within 48 hours.
- **Patch your application software,** e.g., Flash, web browsers, Microsoft Office, Java, and PDF viewers.
  - Turn on **automatic updates**.
  - Enforce **vendor service agreements**. DO NOT let vendors drag their feet on issuing and delivering patches. Insist on receiving updates and patches no later than every 30 – 50 days.
  - Require **third-party verification** by getting an independent party to confirm that your credit union has actually requested a change or ordered a new service or product.
- **Perform daily backups** of important new or changed data, software, and configuration settings.

- **Retain multiple generations of software.**
  - Retain prior versions for at least three months.
  - Disconnect your stored versions.
  - Test restoration initially, annually, and when IT infrastructure changes.

3. Limit access to your IT environment

The Australian Signal Division (Australia's version of our NSA) Cyber Security Centre has taken a global leadership role in issuing what it calls its Essential Eight strategies for protecting your information security environment.

The ASD believes that implementing the strategies below, in addition to the backup strategies discussed above, will stop or mitigate up to 85 percent of cyber threats.

- **"White list"** approved/trusted programs to prevent execution of unapproved/malicious programs including .exe, DLL (dynamic link library), scripts, e.g., Windows Script Host, PowerShell, HTML applications (HTAs), and installers.
- **Harden your user applications as targets.** Configure your web browsers to block Flash (ideally uninstall it), ads, and Java on the internet. Disable unneeded features in Microsoft Office, e.g., object linking and embedding (OLE), web browsers, and PDF viewers.
- **Block macros from the internet in your Microsoft Office settings** and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
- **Restrict administrative privileges** to operating systems and applications based on user duties.
  - Regularly revalidate the need for privileges.
  - Don't use privileged accounts for reading email and web browsing.
- **Require multi-factor authentication.**
  - For virtual private networks (VPNs), remote desktop access (RDP), secure shell servers (SSH), and other remote access
  - For all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.
- Create so-called "air gaps" to **physically isolate your credit union's secure networks** from its unsecured networks (such as publicly available internet access or unsecured LANs).
- Ensure that your telecommunications and ethernet **cables carry the proper CAT-ratings** to withstand power surges and other attacks.

4. Implement policies and train your back-office and branch employees to follow them.

Your back-office and branch employees are proud to work at your credit union and very much want to be proactive and helpful. But that eagerness can work against them in terms of cybersecurity. That's where education and policies come in:

- Make it clear that well-meaning haste can have negative consequences. Encourage your employees to slow down and **think before they click.**
- Show your employees **concrete examples of spear phishing emails** and let them practice exercising the proper amount of caution using simulations of real-world situations.
- Teach **proper spam quarantine techniques.**
- Develop a **"buddy system" that provides trained supervision,** so employees know where to go for help or a second opinion before they click.

- **Insist on strong passwords**
  - Incorporate upper and lowercase characters, numbers and special characters, perhaps as a strong passphrase.
  - Change passwords at a maximum of every 90 days
  - Never share passwords.
  - Never hide passwords "in plain sight" on Post-Its or under mouse pads for delivery people or visitors to see.
- Create **clear policies that limit use of personal cloud file sharing solutions** and company social media accounts — and monitor for violations.
- **Limit or prohibit personal business** conducted on company computers and monitor for compliance.
- Be aware that **insiders can and do pose threats for cyberattacks and fraud.**
  - Watch for suspicious behaviors such as an unusual rate of copying/moving files to a local machine or a different server.
  - A user using the **Tor browser to access the Dark Web.**
  - Any unusual use of **incognito or private browsing mode.**
  - Any attempts to **disable or tamper with security controls.**

5. Harden your call center as a target.

Your credit union's call center is more often associated with social engineering fraud than cyber threats but hardening access to your IVR digital account access and website should be part of your overall strategy to reduce cyber threats.

And remember that unlike your credit union's other employees, your call center agents work on the front lines of cybersecurity and fraud threats on every call of every shift on every day.

Every interaction with a confused or upset member could be a social engineering gambit. So, unless you've hired retirees from S.E.A.L Team Six, understanding that no employee can possibly maintain a 24/7/365 level of readiness will be key to creating the policies and training structure that will allow your credit union to practice an empathetic approach within a firm cybersecurity structure.

PSCU's recent white paper, "Fighting Fraud in Your Call Center: Get Tough With These Timely Solutions" makes a number of additional call center recommendations, but those below are particularly relevant within the overall context of maintaining cybersecurity within a people-centric organization.

These recommendations can be used to familiarize all of your employees with the risks of multi-channel fraud threats, as well as the devious new social engineering techniques that hackers and fraudsters are using use to gain control of accounts.

- Teach your agents the **various social engineering techniques** (e.g., anger, feigned travel emergencies, hard-to-understand accents, etc.) that fraudsters might try to use on them. (See Appendix A.)
- Let your agents and other employees take the lead in **role playing**. Have them brainstorm social engineering techniques and have them practice trying to fool each other.
- Make your call center and branch employees **especially aware of how fraudsters will use the threat of service complaints to intimidate** them.

  - Arm your agents with scripts that give them ways to make graceful excuses when their sixth sense tells them not to comply with unreasonable or suspicious account demands.
  - Empower your employees to trust their guts.
- **Re-evaluate your need for certain "boilerplate" questions** such as "How satisfied are you with the service you have received today?" and "Is there anything else I can help you with today?" They may sound friendly but they're invitations to fraud.
- Revise your scripts to **incorporate proactive dispute mediation and persuasion techniques** from the growing field of behavioral economics, as discussed in the Harvard Business Review article, "How Call Centers Use Behavioral Economics to Sway Customers." Such techniques will be beneficial, not only in fighting fraud but in elevating member service in general.
- Identify and train specific agents in your call center who will be responsible for handling and **resolving high-risk or suspicious calls.** Teach your front-line agents when and how to escalate calls and what to say.
- Improve the **security of your knowledge-based authentication.**
  - Add to or replace traditional knowledge-based verification questions that rely on publicly available information like birthday, Zip Code or mother's maiden name with dynamic knowledge-based verification protocols.
  - These should vary randomly and should ask the caller to provide private, account-specific information that couldn't be accessed through the IVR system.
- Move to **registered mobile phones** that enable your credit union to send secure push notifications.

6. Create Information Loss Prevention Policies.

Management guru Peter Drucker famously noted that "You can't manage what you can't measure." CIO translation: if you don't know what sensitive information your credit union has and where it's supposed to be, you cannot possibly know if something is digitally amiss (or just plain missing).

- Begin with **information mapping.**
- Designate a working group to take inventory of the sensitive information your credit union has, where it is stored, who owns it and who has what permissions to use it.
- Bear in mind that it's far easier to map the information before a theft than after, when **investigators will be breathing down your neck.** In that event, your credit union will be expected to identify what information may have been compromised and working from an incomplete or informal list will only lengthen the time before affected members can be notified.
- **Encrypt sensitive information** and investigate the use of data-loss prevention systems if you don't have one. Develop departmental protocols for changing default configurations and passwords frequently but on a staggered schedule.
- **Develop dedicated security roles** but don't isolate the security department so far from the rest of your credit union that member-facing employees who "see something" don't know how or to whom to "say something." **Ensure that your Information Security group has visibility across the organization.**

- Create and adhere to a **data retention policy** for compliance purposes but be aggressive in purging data that is no longer needed. Remember, it's a lot easier to defend a smaller, more concentrated territory than a larger, more dispersed one.

7. Educate your members and make them your partners.

Your members are the most important variable in your cybersecurity and fraud prevention equation because your credit union exists to serve them and cannot exist without them.

Without their trust, you don't have a sustainable business, but that doesn't mean you should treat them as innocents who must be kept in the dark about the cybersecurity challenges your credit union faces. After all, your members are facing cybersecurity challenges on a lesser scale in their own personal lives.

Explaining why policies that might seem restrictive are actually for your members' protection and educating them about phishing, call spoofing, and strong passwords can easily become a value-added service your credit union provides.

- Use wait time PSAs, online education, statement inserts, branch education, etc. to educate your members about what your credit union is doing to protect them and prevent fraud.
- Encourage your members to be vigilant about creating strong passwords, setting fraud alerts, and safeguarding access to their computers and mobile phones.
- Bring the managers of your member-facing departments together with representatives from your credit union's marketing, risk management, and IT departments to discuss the thought leadership behind the classic Harvard Business Review article, "Stop Trying to Delight Your Customers."

Not every recommendation will be right for your credit union, but you may realize that you have been stressing some member service ideas that are at odds with today's stepped-up awareness of cybersecurity.

8. Manage your vendors.

In today's world of data analytics and digital marketing, working with third-party vendors has become so commonplace that it's easy to forget that other companies may not take data protection as seriously as your credit union does.

It becomes vital to put vendor governance and oversight policies into place to mitigate the risks of data theft or contamination when your data leaves your premises.

- At minimum, your credit union must know **which vendors have what data.**
- Don't send your data off-premises without a **clear agreement on how a vendor will protect it** while it's in their custody.
- PSCU has designed its own Vendor Governance and Oversight program to meet the regulatory and compliance requirements of the CFBP and NCUA. The program earned selection as a finalist for the prestigious T.E.N. Information Security Project of the Year Award in 2015.

  T.E.N. is a national technology and security executive networking organization, and this award acknowledged the PSCU Vendor Governance and Oversight Program's achievement in appropriately identifying, assessing, and mitigating third-party risk throughout the organization.

- PSCU's program has formalized its third-party onboarding process, created a novel third-party provider risk scorecard, and tied those scores to an ongoing oversight program that features online vendor credentials and dashboards to facilitate executive-level risk reporting.

9. Think before you outsource.

It goes without saying that not all outsourcing agreements are created equal, but your credit union may not have realized how very complex it can be to integrate the process into your overall cybersecurity efforts.

The FFIEC "Outsourcing Technology Booklet" provides a thorough and invaluable guide. Here are just a few factors it covers:

- Board responsibilities
- Creating service provider RFPs
- How to perform due diligence
- Contract issues
- Pricing and bundling
- Ongoing monitoring of service agreements
- Controlling the environment of the service provider
- Business continuity planning and anticipating potential changes due to external environment
- Building in procedures to safeguard information security
- Outsourcing to foreign service providers

10. Choose a CUSO that prioritizes cybersecurity and fraud protection. Choose PSCU.

In all that we do, from our transaction processing to our call centers to our industry-leading information security, risk management and anti-fraud solutions, PSCU prioritizes your cybersecurity and that of your members.

Through our partnership with the NCU-ISAO, our close working relationship with the NCUA, and our cutting-edge in-house thought leadership and educational resources, we stand committed to easing your fears about cybersecurity and fraud.

Let's work as partners in the months and years ahead to keep this Cybersecurity Readiness Guide current and implement its teaching and suggestions.

That way, when Solutions Consulting next visits your credit union and you tell us our work put you to sleep, we'll know to take it as the highest form of praise!

Appendix A: Glossary of Cybersecurity Terms

Cybersecurity: In general, cybersecurity refers to the people, processes and technology your credit union uses to protect the integrity of its digital infrastructure — its networks, hardware, data, programs, software, website, APIs, social media accounts, etc. from attack, damage or unauthorized access.

Although cyberattack methods are constantly evolving, some well-known hacker tactics are:

- **Malware:** Short for "malicious software," malware uses files or code to provide an attacker with remote control of an infected computer. Viruses, worms, Trojans, rootkits, botnets and spyware are all forms of malware.
- Ransomware: Ransomware uses malware to take control of valuable internal information and hold it for ransom. First, attackers compromise and take control of a system or device, then prevent access to the system and demand a ransom and return full service once it is paid.
- **Phishing:** Phishing uses fraudulent emails disguised as legitimate communications to trick the recipient into clicking a link, opening an attachment or directly answering. Phishing attacks are typically aimed at getting the user to provide sensitive information such as a password to enter the system directly or to introduce spyware such as keystroke loggers to capture the information more covertly.
- **Distributed Denial of Service:** DDoS attacks use a large-scale network of botnets to take a target company offline by flooding its server (or that of its cloud provider) with bogus traffic designed to overwhelm its system.
- Access to the Dark Web, a subset of unindexed websites that require the Tor (which stands for "The Onion Router") browser to reach. Tor directs internet traffic through a worldwide network of free, volunteer relay links (known as web proxies) to conceal a user's location.

Sites on the Dark Web sell criminal content such as stolen information and access to premium malware and many change web addresses often to minimize exposure to law enforcement.

Interesting fact: Onion routing was originally developed by the U.S. Naval Research Laboratory to protect U.S. intelligence communications in the early days of the internet.

- **Social engineering** refers to hackers' and fraudsters' use of psychological techniques to manipulate people (such as branch personnel and call center agents) into performing actions or divulging confidential information that give bad actors confidential account information or system access.

Although hackers and fraudsters have proven to be endlessly creative in devising new schemes (particularly in perpetrating call center fraud), almost all social engineering attacks employ one of the six principles contained in Cialdini's theory of influence. Build employee awareness of tactics like these:

- **Reciprocity:** "Give me the email for your boss so I can write and tell him how helpful you've been today."
- **Congruence with self-image:** "I'm normally such a nice, helpful person. So, if I think this member is being a jerk, it must be me, not him."

- **Conformity/social proof:** "Oh, I'm such an idiot! I get locked out of my account all the time! Last time, Katie, I think her name was, told me just to ask for a temporary password next time. Can you give me one?"
- **Authority:** "Young lady, my car dealership happens to be one of your credit union's biggest accounts. Please don't waste my time asking me these questions."
- **Liking:** "You sound much too young to have grandchildren! You do? Me, too! Tell me the names of yours …"
- **Perceived scarcity:** "I'm here in the airport and racing to catch a plane home and your ATM just ate my card. Please help me, and can you please hurry?"

Appendix B: Additional Links, Reading and Resources

Credit Union Industry Resources:

- FFIEC Cybersecurity General Observations
- FFIEC Cybersecurity Assessment Tool
- NCUA Cybersecurity Resource Center
- Tim Segerson, NCUA, segerson@ncua.gov, (703) 518-6397
- NCU-ISAO website
- Brian Hinze, NCU-ISAO, Brian.hinze@ncuisao.org, (813) 431-1221 NAFCU blog

Government Security Organizations:

- US-CERT
- Defense Cyber Crime Center (DC3)
- DHS Cyber Resources
- Forum for Incident Response and Security Teams (FIRST)
- Homeland Open Security Technology (HOST)
- International Telecommunications Union, Cybersecurity Gateway (link is external)
- National Council of ISACs (Information Security Analysis Centers)
- National Cybersecurity and Communications Integration Center (NCCIC)
- Organization of American States, Cyber Security Program
- Organization of Economic Cooperation and Development, Information Security and Privacy

Cyber Threat Mitigation Resources:

- Australian Signals Directorate Essential Eight
- CERT Coordination Center at Carnegie-Mellon University
- SANS Institute Center for Internet Security Critical Security Controls (detailed infographic and chart)
- NSA top 10 Information Assurance Mitigation Strategies (very technical with some very advanced suggestions not contained elsewhere in this guide)
- FCC guide to creating a small business cybersecurity guide
- DHS Small Business Resources page

Further Reading from PSCU and CUES:

- Gene Fredriksen, "Fostering a Culture of Security," Forbes, June 5, 2018.
- Gene Fredriksen, Blocking and Tackling in the New Age of Security (speaking at Insecurity Conference 2017) Dark Matter, December 1, 2017.
- Gene Fredriksen, Author page at CUInsight (links to five articles)
- CUES Cybersecurity archive (articles by