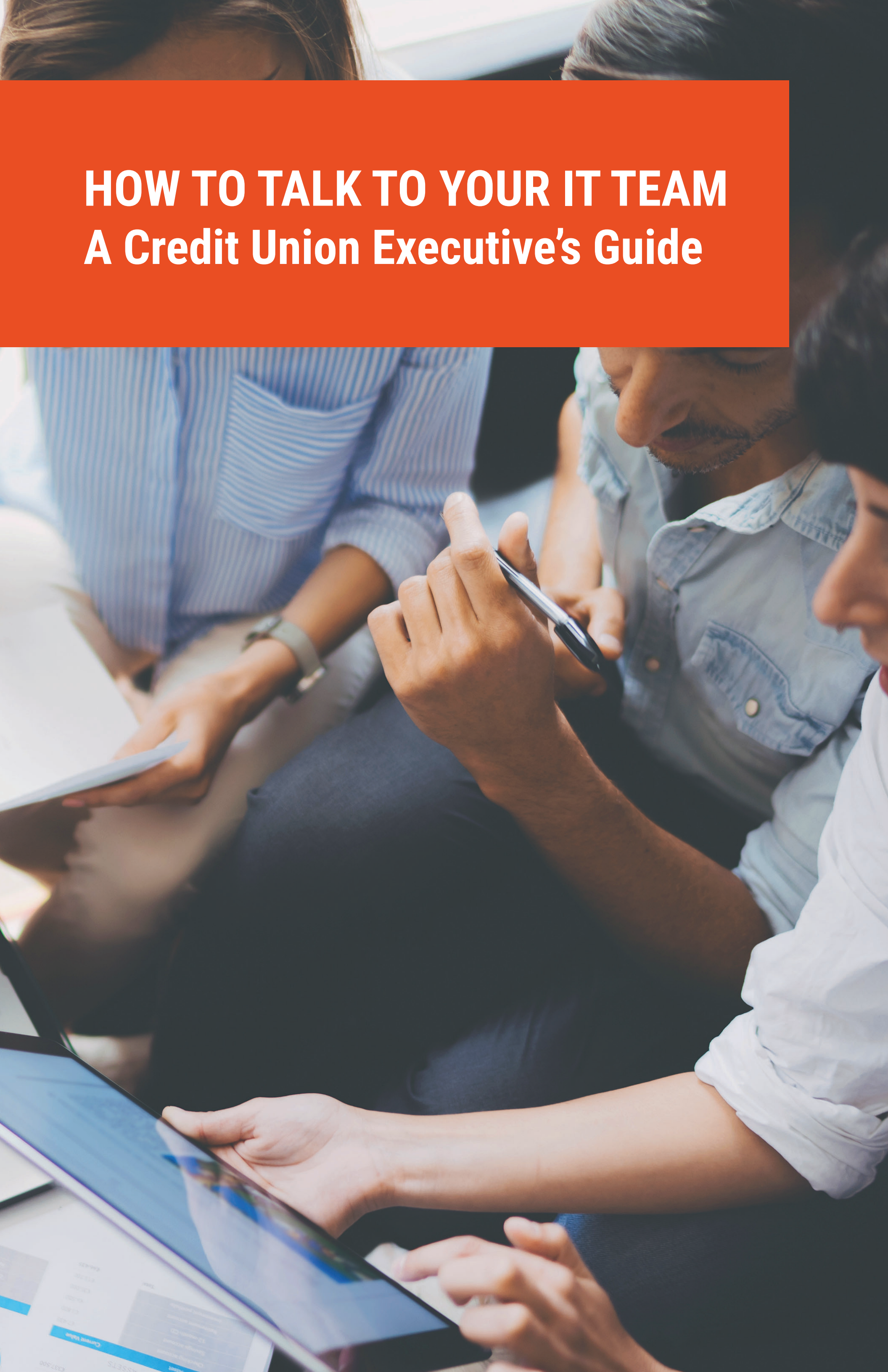
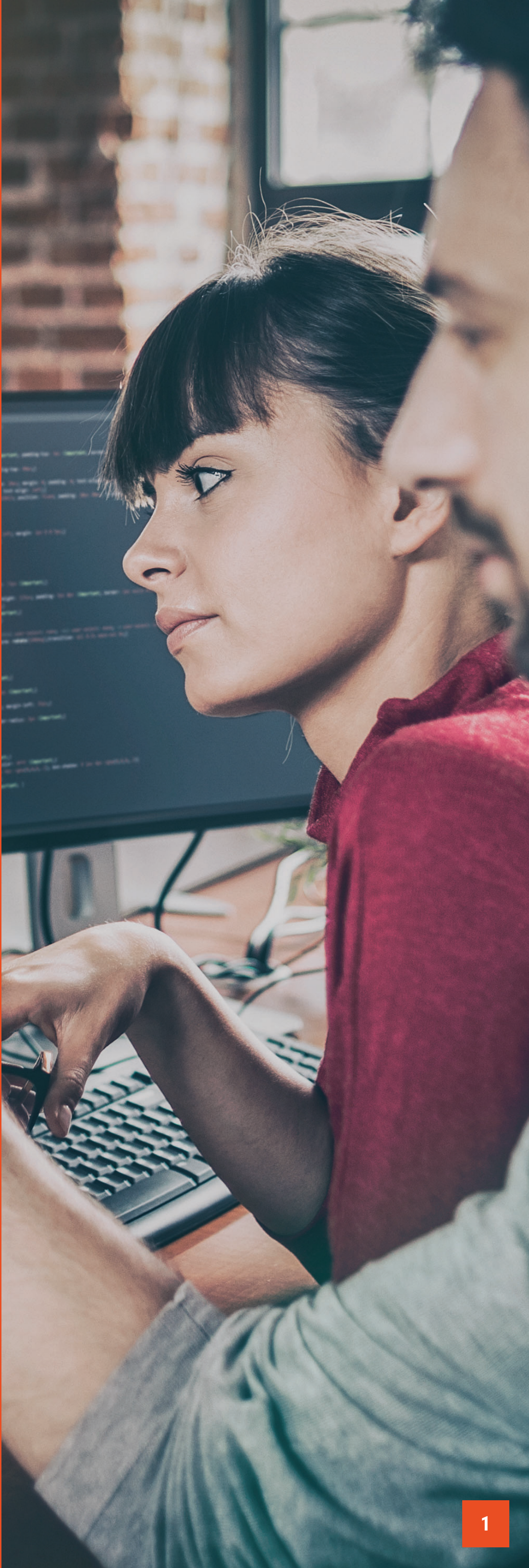
HOW TO TALK TO YOUR IT TEAM
A Credit Union Executive's Guide



CONTENTS



OVERVIEW

As a credit union executive, you have a lot on your plate. Ensuring the safety and security of your members and their assets, maintaining your business from an operations standpoint, and taking care of your valuable employees are all keys to the success of your institution. One often-overlooked thing unites all three of these concerns: Technology.

While you may feel you have a handle on your credit union's technology, the intricacies therein make management and maintenance difficult to tackle. It is easy to pass that responsibility off to your IT director; after all, they have the expertise to keep things running. However, instituting regular checks and balances is essential to prevent technological time bombs. In order for your business to succeed, YOU – not just your IT team – have to understand the ins and outs of your network environment.

Developing and maintaining a secure and effective technological strategy has never been more important. According to a recent report by Black Kite, 48% of credit unions have critical cybersecurity vulnerabilities that could lead to an attack, largely due to out-of-date systems. Eighty-six percent had unknowingly leaked employee credentials, all of which now appear on the dark web. Worst of all, direct cyber-attacks could cost a given credit union more than $1 million in damages—and that number multiplies when taking vendor security into consideration. Your members' money, data, and assets are constantly at risk.

Taking control of your technological landscape is critically important, but it does not have to be complicated. In this paper, we will outline several topics to explore with your IT services team, giving you specific questions to spur crucial conversations.

1. BACKUPS

Put simply, backups are saved versions of everything on your computer. Some kinds of backups only save files; other, more comprehensive backups encompass all files and systems on your computer. We recommend a combination of file- and image-based backups, the latter of which copies your entire operating system and all associated data. This ensures a comprehensive restore process should your data ever become corrupted or lost.

Backups are the single most important tool you have. If something goes wrong (loss of data, rogue employee, or a ransomware attack), you need to be able to get your critical files and systems back online ASAP. Many IT departments believe they are getting good backups because the backup system is not reporting a failure. The assumption is that the system must be working if it is not giving an error. Instead, you should be restoring backed up files regularly to know your backups are working. You also want to make sure your backups are happening regularly enough (daily or hourly) to ensure you have relevant data in case of an incident. In the event of ransomware specifically, data must be physically separated from your network in order to protect it from encryption. This is called an "air gap."

TRY ASKING YOUR TEAM:

"Can you provide me a timestamped report of the last good restore from our Active Directory domain controller backup by Friday?"

This should not be difficult for your IT team to produce. If you receive pushback ("I'll get that to you next week," "We don't have backups," etc.), it is a clear sign that something is amiss in your IT department. You may want to ask follow-up questions to diagnose the issue or request a third-party audit of your IT network. The last thing you want is to be caught unprepared in the event of data loss.

Pro Tip: Don't tell your IT team you're doing this! Create a custom Word or Excel file and drop it into a network location that should be backed up. After you believe a backup has been run, delete the file, and request a restoration of it. If they cannot produce it, that indicates the system is not being backed up or the frequency is not high enough.

Advanced Questions to Ask:

- ✓ What backup solution do we use?
- ✓ Do we backup to a local server/appliance
or to a cloud hosting location?
- ✓ Are our backups file-based or image-based?

2. MONITORING

Consistent, proactive network monitoring is essential in any technological environment. This practice ensures that systems are working as they should from the inside; that is, no network interruptions or server failures compromise the integrity of your systems. All businesses - especially credit unions - should have plans in place to both detect and respond to outages.

Failure to monitor your systems proactively could result in costly network downtime, leaving you unable to service your members. On top of that, downtime makes it near impossible for your other employees to complete necessary work, resulting in lost productivity and, as a consequence, lost money. Make sure you have a plan in place before an outage occurs to mitigate any negative effects.

TRY ASKING YOUR TEAM:

"If our Internet Service Provider (ISP) fails in the middle of the night, who is responsible for ensuring service is restored?"

Your IT team should have 24/7 network monitoring in place, making this answer easy. They may show you a schedule of on-call team members or refer you to an outside vendor. If they cannot (at minimum!) walk you through a proven step-by-step process for remediation, it is time for you to step in and request an immediate plan of action.

Pro Tip: An outage like the one described above should be treated like an emergency. You may want to review your IT policy/vendor contracts to determine what emergency response time falls within your SLA, or service level agreement. We recommend a one-hour response to all emergencies, especially time bombs like this one.

Advanced Questions to Ask:

- ✓ Who monitors the space on our server's drives? How often are they audited to ensure they will not fail?
- ✓ When exactly is help desk support available?
- ✓ Do I have access to a U.S.-based team of engineers 24/7?

3. MAINTENANCE

As is the case with monitoring, maintenance is an essential proactive measure that keeps your IT systems running consistently. Your team should be performing maintenance on a regular schedule. Otherwise, your network may become vulnerable to breaches. We recommend weekly maintenance on each of your machines to keep them secure and up to date. Server maintenance is also key, though for the sake of minimizing downtime, we recommend a monthly cadence.

During your regular maintenance window, each machine on your network should undergo the following:

- ✓ Security patch installation
- ✓ Driver updates
- ✓ Hard drive defragging (which improves performance)
- ✓ Software updates
- ✓ Error scan on all hard drives

These essential maintenance tasks not only keep your network secure, but also ensure optimal performance on all devices, leading to fewer tech-related interruptions during the workday.

TRY ASKING YOUR TEAM:

"Can you provide a detailed, dated report of what occurred during our last maintenance window? In addition, what critical patches are missing from our server(s)?"

If your team struggles with these questions, it is likely an indication that maintenance is not being performed on a regular schedule. IT works best—and safest—when your team is proactive, not reactive. If your team only evaluates the security and performance of your devices/network when something goes wrong, it is time for you to re-evaluate their approach.

Pro Tip: While on-premises Microsoft Exchange servers (i.e., the servers that control email, calendaring, and scheduling) used to be the gold standard for businesses, vulnerabilities have been detected that now leave them susceptible to cybersecurity breaches. Check with your team to see whether this affects your credit union. If an Exchange server is still part of your network environment, you may want to consider transitioning to a cloud-based solution like Microsoft 365. This solution eliminates the need for an on-premises appliance.

Advanced Questions to Ask:

- ✓ What Microsoft build number is on our workstations? Are all devices still supported by Microsoft?
- ✓ Is our hardware still within warranty? What is our cadence for replacement?
- ✓ What antivirus solution do we use? How often are scans completed?

4. CYBERSECURITY

Cybersecurity has recently become a more pressing topic for all businesses, but especially those within the financial sector. High-profile hacks like the Colonial Pipeline cyber attack have highlighted the devastating effects of breaches. Perhaps most importantly, the NCUA requires that certain actions be taken to prevent against and respond to cybersecurity events. In order to continue providing your members with the services they need, both proactive planning and detailed remediation processes are absolutely necessary. Failure to complete these tasks will almost certainly cost you your members' trust.

Though technical solutions are key when combating cyberattacks, one of the most important things you can do to prevent malicious users from gaining access to your network is to train your employees on proper cybersecurity practices. Does your team know how to spot a phishing email? Do they use complex passwords? Do they understand how to use multi-factor authentication (MFA) to better secure their accounts? Your IT team should invest in educational resources for your entire team and develop foolproof security policies that affect everyone, not just the people who manage your technology. That said, you also need to make sure that your network perimeter is secure from the outside in.

TRY ASKING YOUR TEAM:

"What router solution do we use? How is it configured?"

Perimeter routers are nested between your external firewall and the Internet at large. These routers therefore manage how inbound and outbound internet traffic flow to/from your devices. The cyber-protection offered by routers varies depending on the type of hardware you use. Safer, more sophisticated routers contain intrusion prevention and intrusion detection systems. The former detects known threats, while the latter monitors activity to ensure safety. We highly recommend having both of these solutions in place. To maintain your workforce's flexibility, you will also want to make sure you have access to a virtual private network (VPN), which masks your Internet traffic so that people outside of your network cannot view your activity.

Pro Tip: Another solution you may want to deploy is Domain Name System (DNS) protection. A DNS guides your traffic on the Internet, looking up any given site and returning its IP address. Errant clicks could land you or your team members at an Internet location designed to remotely install ransomware or other malicious programs. DNS protection gives your credit union the ability to block suspicious activity and sites. This protection is different from that which your router provides, but it can be extremely valuable, especially when dealing with personal financial information.

Advanced Questions to Ask:

- ✓ What endpoint security solution do we use?
- ✓ What is our step-by-step ransomware remediation process?
- ✓ Where is our current network diagram?
- ✓ Who has access to its critical components (e.g., router, domain controller, etc.)?

5. BUSINESS CONTINUITY

Particularly in the wake of COVID-19, credit unions must take seriously the need for a comprehensive, nimble business continuity plan (BCP). 2020 proved that disasters can easily be right around the corner. Your size, constituency, and physical location should inform the likelihood of certain incidents; it is your job to determine which threats are most pressing and how, in the event that they are realized, your credit union will bounce back from adversity.

According to a study by ViClarity, 8 out of 10 credit unions with BCPs were unable to perform critical functions when COVID-19 started. Worse, only 78% of credit unions had BCPs, even though BCPs are required by the NCUA. These statistics point to a startling reality: A vast majority of credit unions are unprepared for disaster. Specifically, your IT team should be well aware of looming cybersecurity threats and the actions needed to return to normal working conditions should the worst occur.

TRY ASKING YOUR TEAM:

“May I see a copy of our BCP? Has it been updated since the pandemic?”

Several things should be included in their response. First, your team should have a copy of your BCP somewhere other than your physical office. This way, in case of a disaster that affects your location(s), you can quickly and safely enact your plan as it is written. Your BCP should also contain contact information for all your vendors and employees, including internal/external communication protocol. This section should be detailed and include multiple forms of contact (What if your email server is destroyed? Do you have a phone tree?). Other key components include risk assessment, continuation of critical business functions, plan activation/deactivation procedures, alternate facility options, and insurance considerations. Each of your team members should have a clear directive in the case of an emergency. If your BCP has not been updated since COVID-19, you need to assess it as soon as possible.

Pro Tip: 2020 taught us that remote working and member engagement solutions are an absolute necessity. To this end, make sure that your team is well-versed in mobile banking, online problem resolution, and the mobility of your phone system. Ask yourself and your IT team: Is your app sufficiently user friendly? Are online solutions available to members should your physical location become compromised? Is your phone system accessible from your team members’ home offices?

Advanced Questions to Ask:

- ✓ What cybersecurity training are we providing to our members?
- ✓ What is our proactive communication strategy in the event of a service interruption?
- ✓ Have we received BCP feedback from any recent audits? Who is responsible for correcting errors?

CONCLUSION

Backups, monitoring, maintenance, cybersecurity, and business continuity are all essential components of your credit union. It is easy to pass responsibility for these matters off to your IT team. However, without your involvement, it is entirely possible for vital issues to be overlooked. Again, proactive measures like the ones outlined above prevent time bombs from manifesting and leaving ruin in their wake.

If you have any doubts about the integrity of your IT systems, team, or strategy, third-party vendors like Dynamic Edge can help. We can audit your network from a neutral perspective, scanning for vulnerabilities and offering alternative solutions where necessary. We happily work with a number of IT teams across the nation to offer extra protection and strategic planning to credit union networks. We customize our offerings based on your credit union's needs, tailoring our suggestions to meet your business goals. For more information on Dynamic Edge, visit our website at www.dynedge.com.

DYNAMIC EDGE
BEYOND **TECH** SUPPORT

855.461.9050 / www.dynedge.com

DYNAMIC EDGE

BEYOND TECH SUPPORT