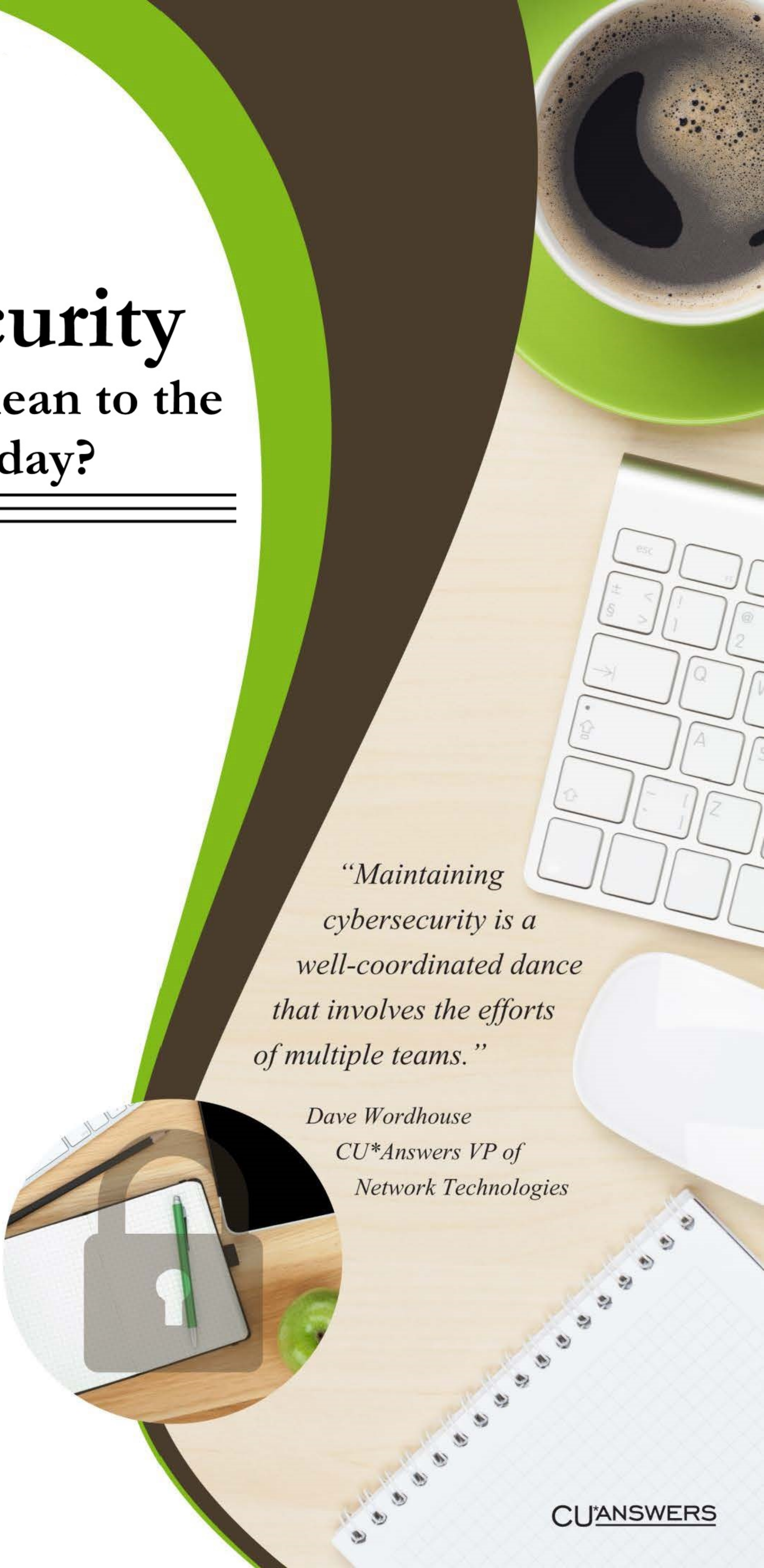
Cybersecurity

What does it mean to the CU industry today?

February 2015



"Maintaining cybersecurity is a well-coordinated dance that involves the efforts of multiple teams."

Dave Wordhouse
*CU*Answers VP of*
Network Technologies

CU*ANSWERS

Decrypting “Cybersecurity”

Randy Karnes, CU*Answers, CEO

Every CEO needs an elevator speech about their organization’s thinking on cybersecurity. It’s no longer enough to say, “That’s for my tech people; I don’t know much about it myself.” That implies you haven’t developed an approach to it, that it has no priority in your strategic thinking.

When a large group of credit union CEOs were asked some questions about cybersecurity they were stumped. The questions were:

1. How would you explain the top five cybersecurity threats to an organization (CU) today with a single sentence or title as to the threat (most think tools that harvest Identity Theft – but what about just not being able to work until you pay?) – give me your five.

2. Who should they call in the industry to brief a group of CEOs on the real threats and the affordable tactics to minimize them? Is there a recognized vendor?

3. Who should they call to visit and see an organization’s active and well-crafted approach?

4. What are the top 5-10 things a CEO should grasp about cybersecurity today and be able to summarize in a leadership elevator speech?

I asked for various professionals at CU*Answers to provide their perspectives. The answers they’ve provided here are to help you think through the key talking points on cybersecurity and prepare an elevator speech for your board, your member-owners, your examiners, and the market. Are you ready to respond to these questions with your own answers?

Cybersecurity as the CIA Triad

Dave Wordhouse, CU*Answers Network Services, VP Network Technologies

Cybersecurity can be boiled down to a simple concept known as the "CIA Triad":

Confidentiality – only authorized persons have access to data or systems

Integrity – only authorized persons can modify, remove, or introduce data or systems

Availability – authorized persons have timely access to data or systems

There are myriad ways to attack an organization that assault one or more of the Triad concepts:

- A Trojan horse on a PC exfiltrates member data to the attacker. This would be a **Confidentiality** issue because an unauthorized person now has access to information they shouldn't have (implications of ID theft, etc.).

- That same Trojan horse exfiltrates the data so quickly that it fills up the credit union's internet pipe. Now there's also and **Availability** problem that might impact the CU's ability to service members because the internet connection was also the connection to the DP.

- Malware on a PC deletes or alters data on the network (see the recent Sony attack). This is an **Availability** problem, because data is no longer there or usable. It's also an **Integrity** issue because the data isn't whole anymore.

- You get the point

What are the top cybersecurity threats to a credit union today?

- Malware (the stuff is morphing faster than the industry can respond)
  - Trojan horses
  - Back doors
  - Ransomware
  - Virus/worms
  - Etc.

- Employees/staff – uninformed staff performing risky operations
  - Failure to budget for staff training and testing events

- Social engineering – see above – into which I'm lumping phishing, pharming, spear phishing, etc.

- Inadequate network maintenance

  - Inadequate/poorly executed software patching plan
  - Lack of consideration for updating “off the radar” systems and software
  - Incomplete inventory of systems and software used on the network

- Poor network configurations
  - Configurations that don’t follow configuration best practices
  - Lack of third party testing and validation of controls
  - Failure to regularly review existing controls against business requirements
  - Lack of budget to install good controls and tools (note – good tools can be had for not a lot of money)

- Lack of training/understanding of technical controls and limitations

- Users with elevated permissions

Who should the credit union call for training?

There are many good vendors for cybersecurity training, though I’ve not seen much from a “high level briefing” perspective. SANS for more technical (admin) training and KnowBe4 for higher level web based employee training are both good candidates.

What should a CEO grasp about cybersecurity today?

The leader should grasp/seek a program:

- Cybersecurity is a real risk that needs to be managed like any other; it is not a reason to not do business (though risk analysis may shape decisions on what businesses to get into)

- Our cybersecurity program has the full support of executive management

- Our cybersecurity is a coordinated dance, just like any other; involves multiple teams working together: networks, DRBR, compliance, internal audit, management, facilities, etc.

- Our cybersecurity program has a budget line-item priority for investments in training, people-defenses, and technical controls, and is well documented (policy, procedure, strategic technical plans)

- Our cybersecurity program is risk-based – we invest based on identified risks or realized threats, not industry whims or knee-jerk reactions

- Our cybersecurity program is timely – we practice responses; we market regularly to staff (email blasts, training, hallway reminders, etc.)

Cybersecurity is a real risk that needs to be managed like any other; it is not a reason to not do business.

- Our cybersecurity has transparency with senior management and the board and is independently reviewed
- Our cybersecurity program is open to question and being challenged to evolve with the times

Cybersecurity Needs Buy In from the Top Level

Matt Sawtell, CU*Answers Network Services, VP Network Technologies

What are the top cybersecurity threats to a credit union today?

Attacks – this would include malware, spyware, viruses, blastware, ransomware, etc. Attacks result in downtime, data and monetary loss. It would also include things like distributed denial of service (DDoS)/bots, criminals/hackers, etc.

Disasters – fire, flood, act of god, but also system/equipment failures or communications/vendor downtime. This one is nothing new, but should still be a key consideration – do you know the cost of downtime and therefore, how much your business can sustain?

Employees – they need access to member data to do their jobs, which makes them targets of social engineering and allows the opportunity to intentionally steal/expose data. However employees can also put an institution at risk inadvertently through things like lax workstation controls, weak authentication practices, poorly designed BYOD and lack of general security awareness/training.

There is no single turn-key solution to cybersecurity, but instead requires multiple layers of control to mitigate risk.

Operational Deficiencies – IT systems require a documented and well executed management program. This includes monitoring, patching, logging, alerting and reporting. As the threat landscape changes quickly, without a solid on-going process in place to manage IT assets, what was secure at one point in time can be easily compromised later.

Incident Response – we've all read over the course of the last year how it is likely not a matter of *if*, but *when*. How a business reacts to the threat is key to limiting the exposure. Businesses need to ensure they have a process in place to effectively detect, respond, investigate, recover and follow up when incidents occur.

Who should the credit union call for training?

There is no single recognized vendor, but there are many; it is a key focus for our Advantage CIO group. Look also at educational resources such as SANS, GIAC or ISACA and industry specific ones such as FFIEC and NIST.

Who should CEOs seek out for a well-crafted approach?

I believe the best approach here to be through peer discussion and an effective audit program. It was a key topic of discussion at our first CUSO Technology Users group and many concepts and tactics were discussed; what was working, what wasn't, what the future plans were for the security program, etc.

What should a CEO grasp about cybersecurity today?

An effective cybersecurity program starts at the top level of management and is filtered down through all levels of the business – without top level buy in, the program will fail.

There is no single "turn-key" solution to cybersecurity, but instead it requires multiple layers of controls to mitigate risk. As such, it should be a part of the business's risk management program including identifying risks, assessment, controlling them and then evaluating those controls. As the threats change, the program and processes must change accordingly. Employees are a key component and education and awareness will help a great deal in reducing risk.

Cybersecurity Isn't New

Patrick Sickels, CU*Answers, Internal Auditor

What are the top cybersecurity threats to a credit union today?

(1) **Data Theft (Crime)**. The harvesting of financial or other private data for the purposes of impersonation (identity theft) or crime (fraud); the number one internal threat facing organizations.

(2) **Data Leakage (Privacy)**. The negligent or accidental loss of private data, either through poor externally facing controls (such as misconfiguration on firewalls) or weak internal controls (such as staff members infecting machines through malware).

(3) **DDoS (Denial of Service)**. An attack that renders cyber services unavailable or unusable.

(4) **System Compromise**. Where an attacker is able to access or control a system due to poor security controls (such as default passwords) or through unpatched vulnerabilities (such as POODLE, Heartbleed, and so forth).

(5) **Social Engineering**. Encompasses a wide range of threats designed to swindle a victim into disclosing or providing something of value.

Credit unions should consider working with a major audit firm, or a smaller firm with an excellent reputation for assessment testing.

Who should the credit union call for training?

There is no single recognized vendor. Credit unions should first familiarize themselves with both the FFIEC Guidelines and the NCUA Cybersecurity Resources. Credit unions should also contract with a third party vendor to conduct Internal and External Penetration testing, and Security Assessment testing. Credit unions should consider working with a major audit firm, or a smaller firm with an excellent reputation for assessment testing.

Who should CEOs seek out for a well-crafted approach?

Generally speaking, most organizations are not going to want to disclose details on their cybersecurity defenses because of the risk of accidental disclosure. Also, there is not a one-size fits all approach for organizations. The plus side for credit unions is this approach does not lock the institution into costly security solutions incompatible with the size of the institution and its level of risk.

The State of California has some excellent resources that highlight the key checklists an organization should have when designing its cybersecurity program.

What should a CEO grasp about cybersecurity today?

Cybersecurity is not new. Both the FFIEC and NCUA's approach is closer to "old wine in new bottles" than a fundamental change in the security requirements for credit unions. The advantage to the latest approach is that the FFIEC and NCUA are providing better resources for financial institutions. Credit unions would be wise to directly cite both the FFIEC and NCUA when preparing reports on the security of the institution.

Internal security still remains the biggest risk. Despite all of the vulnerabilities disclosed in the past year, such as Heartbleed, the biggest risk to any organization is closest to home. Executives need to be diligent that their employees are not creating security vulnerabilities through their actions (clicking on links in emails sent by unknown persons) or actively defrauding the organization by harvesting member data undetected.

Credit unions should *assume* they will be victims sooner or later and prepare accordingly.

Good governance remains key. A credit union can save itself much pain during examinations by showing that executive leadership is actively aware of the cybersecurity in the organization, and has debated on whether to adopt new security tools or approaches based on the level of risk posed to the organization. This approach will also be very helpful should a credit union ever find itself in litigation as a result of a breach.

Always assess risk. Credit unions should devote time to documenting its cybersecurity risk on no less than an annual basis. A very important, and occasionally overlooked area, is insurance. Is the credit union adequately protected by insurance for the risks the institution is running through its use of technology?

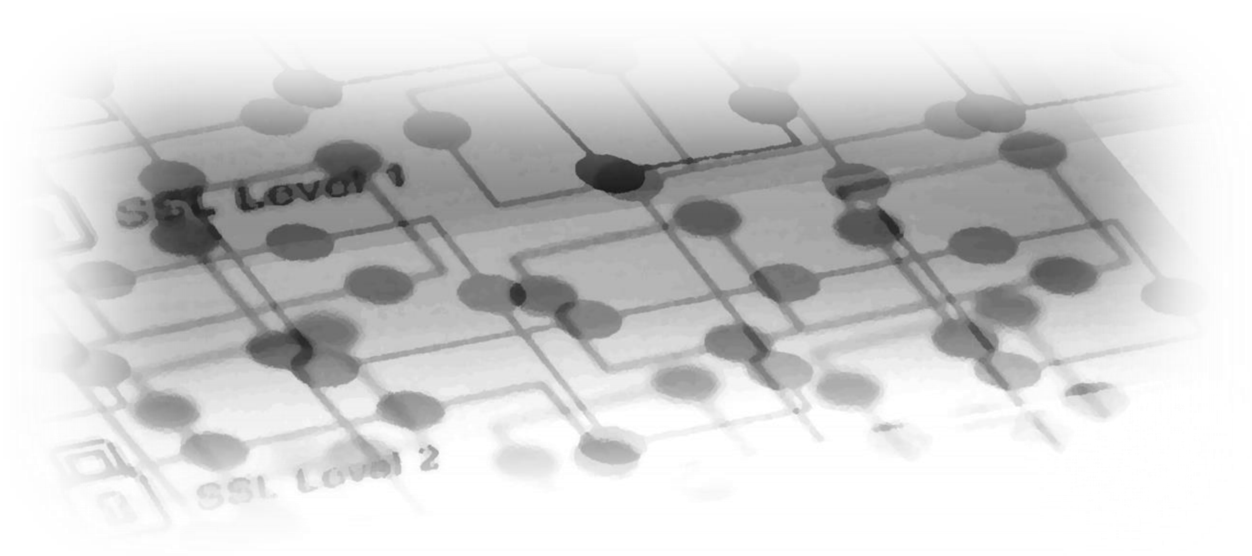
Spending time with the deductibles, coverages, and exclusions of insurance policies is an important if occasionally tedious task.

Educate both staff and members on cybersecurity. Providing education to both staff and members on how to protect themselves against cyber threats is a very efficient way of demonstrating to the world the institution's interest in protecting information and its cybersecurity posture to the world.

Understand state and federal regulations. Compliance should always be the floor where security starts. Does the organization understand its GLBA responsibilities? When does the credit union have to notify members?

Contingency planning. Credit unions should be prepared not only for disaster recovery/business resumption scenarios, but what to do from a public relations and response if a security breach happens at the credit union. Credit unions should *assume* they will be victims sooner or later and prepare accordingly.

The goalposts are always moving. The threats to an organization's security, and the responses needed to counter these threats, will continue to change and evolve. In 2002, few judges or juries were aware of encryption or what it meant to have encryption. In 2015, nearly anyone who works with a computer or even a mobile device has heard of encryption or uses it regularly. Encryption is just an example of a security control that has now become a *de facto* standard with respect to sensitive information. Even if management or the board is not technically savvy, it's important that these leaders have access to people who are and who can provide reasonable explanations of emerging threats and counter measures.



Don't Recreate the Wheel – Update the Pieces

*Jim Vilker, NCCO, CU*Answers, VP Professional Services*

What are the top cybersecurity threats to a credit union today?

From a CEO's perspective I would boil cybersecurity down by its risk components including:

- **Reputation risk…** Where the credit union has been breached by one of the methods listed in Dave's list and exposed member data to the wrong people
- **Transaction risk…** Where the threat yielded enough information that funds could be extracted from accounts
- **Compliance risk…** Where the breach was so great that the credit union was sited under GLBA and subsequently performed remediation
- **Strategic risk…** Where the breach or attack was so grave that it actually forced the institution to change direction on a major goal
- **Legal risk…** Credit union is actually taken to court for disclosure of non-public member information that caused loss.
- **Regulatory risk…** Increased scrutiny of the credit union's infrastructure and processed by examiners based upon the breach

Even if management or the board is not technically savvy, it's important that these leaders have access to people who are.

Who should the credit union call for training?

I would start with the FSISAC (Financial Services Information Sharing and Analysis Center)/or MSISAC (Multi State Information and Analysis Center). The FSISAC is actually is the one mention in the FFIEC guidelines on cybersecurity and much can be gleaned from this site including training. The link to the training site for the MSISAC is https://msisac.cisecurity.org/resources/videos/free-training.cfm

Also, NCUA has compiled a site with multiple links to best practice, related laws, opinion letters, and links to NIST and the FSICAC: http://www.ncua.gov/Resources/Pages/cyber-security-resources.aspx. This site could be used by internal staff to teach others as it is very well laid out and should become something of a go to when a CEO asks their internal staff on the nuances of cybersecurity.

Who should CEOs seek out for a well-crafted approach?

Again, the financial institutions that participate with the FSISAC and their IT experts would be one place to look. That group has been taking this seriously for much longer than the recent attention being drawn to the problem. My understanding is that Brian Vitale at Notre Dame Federal Credit Union has spoken at their events in the past and is an active member. If I were a CEO I would ask my Head of IT if there are any local credit union discussions revolving around this topic and go from there.

Cyber criminals are financial institution agnostic.

What should a CEO grasp about cybersecurity today?

This is the hard one as the expectation is that CEOs have grasp far beyond what was expected in the past. Also, CEOs need to take to heart the fact that their credit union is just as vulnerable as BofA to an attack. Cyber criminals are financial institution agnostic. Much of what you will find below comes from the FFIEC compilation of the 500 or so cybersecurity exams federal agencies did last year. So here are the catch words that I would understand in my elevator speech.

- *We fully understand how we are connected to the outside world and the related risks associated with them and are constantly evaluating the evolving threat vectors and environments.*
- *We routinely discuss the cybersecurity threats and potential internal vulnerabilities with the senior team and BOD and provide them with reports outlining the evaluation of the inherent risks and remediation of known threats.*
- *It has become an important factor when evaluating and making decisions on new services and we hold ourselves accountable for understanding what decisions could bring on additional risk.*
- *We have a robust training program for staff, management, and Board of Directors. This training is required annually.*
- *It has become part of our Head of IT's job description to get involved in as many organizations to keep up to speed on cybersecurity. This has since become a part of their annual performance evaluation.*
- *On a routine basis we review our internal controls relative to our preventative, detective, and corrective controls as it relates to our critical information (as defined and documented). We require that risk identified in our detective systems are remediated and become part of reports to the Board.*
- *We review our connections to third parties and perform due diligence upon those post inherent risk to our network and critical member data. We have included their responsibilities in response plan.*

…get involved in as many organizations as possible to keep up to speed on cybersecurity.

- *We have a well-documented plan to respond to an attack including communication to members, law enforcement, third parties, and regulators and have incorporated the potential scenarios into are DR/BR plan.*

Finally it is important to understand that cybersecurity is in some ways just a new catch phrase for information security, disaster recovery, and business resumption but with a new twist. That twist comes from the growing number of attack vectors our networked world has created and we do business in. In a sense do not recreate the wheel, just understand what pieces need to be updated.

About CU*Answers, Inc.

CU*Answers offers expertise in implementing technical solutions to operational needs, and is a leader in helping credit unions form strategic alliances and partnerships. CU*Answers provides a wide variety of services for credit unions including its flagship CU*BASE® processing system (online and in-house) and Internet development services featuring **It's Me 247** online and mobile banking. Additional services include web development, network design and security, and image check processing. Founded 40+ years ago, CU*Answers is a 100% credit union-owned cooperative CUSO providing services to credit unions representing over 1.7 million members and $15.7 billion in credit union assets. For more information, visit www.cuanswers.com.

CU*Answers, Inc.
6000 28th Street SE
Grand Rapids, MI 49546
tel :: 800 327 3478
www.cuanswers.com

CU*Answers, Inc.
6000 28th Street SE
Grand Rapids, MI 49546
tel : 800.327.3478
www.cuanswers.com