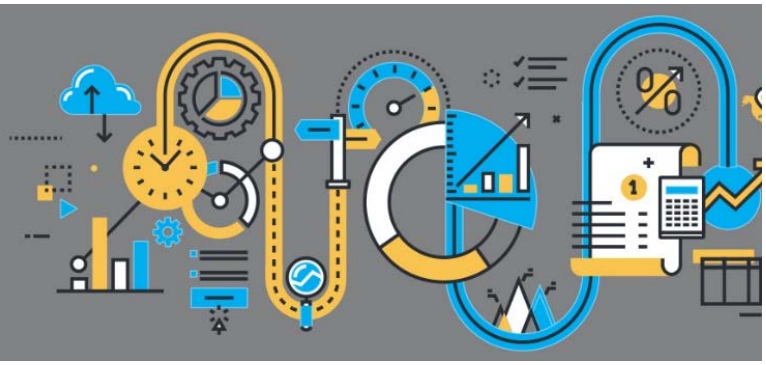
CU ANSWERS
A Credit Union Service Organization

CEO Strategies Week 2016

Scribe Notes



Group 1 | Group 2

Scribe - Julie Gessner

Name	Credit Union
Barbara Harper	Cincinnati Ohio Police Federal Credit Union
Kim Kniola	First Trust Credit Union
Russ Dalke	Northern Colorado Credit Union
Todd Powell	Spokane Firefighters Credit Union
Barbara Bean	Cal Poly Federal Credit Union

Scribe - Liz Winninger

Name	Credit Union
William Burke	Day Air Credit Union
Charles Papenfus	Inland Valley Credit Union
Randy Gailey	Horizon Credit Union (Utah)
Karen Browne	TBA Credit Union
Janet Borer	Members First Credit Union

Group 3 | Group 4

Scribe - Esteban Camargo

Name	Credit Union
Leo Vaulin	CU*South
Steve Kelly	Metrum Community CU
Patrick Post	Mountain River CU
Scott Collins	Xtend
Kim Hall	Tri-Cities CU
Todd Powell	Spokane Firefighters CU
Russ Dalke	Northern Colorado CU

Scribe - Laura Zazakis

Name	Credit Union
Scott McFarland	Honor CU
Greg Smith	CU*NW
Tom Gryp	Notre Dame Federal CU
Adam Johnson	Safe Harbor CU
Carma Peters	Michigan Legacy CU
Karen Browne	TBA CU

Group 5 | Group 6

Scribe - Barbara Cooper | Scribe - Keegan Daniel

Name	Credit Union	Name	Credit Union
Jeff Jorgensen	Sioux Empire	**Linda Bodie**	Element
Michael Abraham	First Financial	**Dean Wilson**	Focus
Vin Cerasuolo	Century Heritage	**Don Mills**	Alpena Alcona
Lindsey Merritt	Jordan CU	**Kevin Ralofsky**	Verve
Kevin Posey	Thinkwise CU	**Dennis Degenhardt**	Glacier Hills
		Jerry Wise	Greensboro

Group 7 | Group 8

Scribe - Marsha Sapino | Scribe - Jim Vilker

Name	Credit Union	Name	Credit Union
Christy Leslie	Bridge CU	**Barb Page**	Kent County
Barb Mills	Calcite CU	**Corrine Coyie**	Advantage
Mark Richter	First United	**Vickie Schmitzer**	Frankenmuth
Kim Bourdo	Service 1 FCU	**Matt Jennings**	Quest
Charles Papenfus	Inland Valley CU	**Janelle Franke**	River
Barbara Bean	Cal Poly FCU	**Randy Gailey**	Horizons
		Steven Janssen	Brewery
		Andy Fogle	Des Moines Police Officers

Group 9

Scribe - Annalyn Hawkes

Name	Credit Union
Mike Brandt	Evergreen CU
Steve Janssen	Brewery CU
Jerry Wise	Greensboro Municipal CU
Jennifer Oliver	South Bay CU
Kris Lewis	Allegan CU
Andy Fogle	Des Moines Police Officers

Group Notes

The following notes are included exactly as taken by table scribes. Scribes were instructed to jot down everything that was discussed at the table, with the idea that reading the notes would be a little bit like eavesdropping on the conversations.

Cybersecurity

When it comes to Cybersecurity everyone has a point of view, but the CEO has to make the call. What are you and your fellow CEOs thinking about as we head into 2017?

- What does cybersecurity mean to you and your spending in 2017-2019? Where are you focusing your efforts, and how will you cover the investment and earn out?
- Guarding member data and understanding how your vendors do it will be a big focus in 2017. What if you needed to pass a SOC 2 exam for your members based on your employees' daily work?

Group 1 Notes

- How are we balancing our internal plans and activities with those we contract with? Answering the questions do we want to do the work or rely on someone else?
- It's always about the conversation on how tight we want to make our network while continuing to do the daily work. How tight do we want to make our network?
- Educating our members just as much or more than our staff. Leveraging education as an investment.
- It is difficult to get ahead and stay ahead. Not necessarily something you can insure your way out of. Placing limitations on workstations, including the number of workstations. Understanding trust and confidence in staff for use of devices.

- Perform an assessment to determine exactly where you're at. What your vulnerabilities are.
- Bring in third party regularly. Surprise audits can determine what the credit union is doing well and what we can do better.
- How can we help members control their own environment? Subscription services that allow members to control their banking experience. Turn off my account so that nobody can perform business. We can do this manually now but how can we place this control in the hands of the consumer so they can do this themselves without having to wait?
- Generations today do not have liability and are just not as careful. How can we put a little bit of the liability back on the consumer?
- Culture shifts – The 'people element' is the scary part. Using safe methods of storing passwords securely.
- VENDORS- Large topic that is hard to wrap our arms around. Vendor management reports are very large. Difficult to find time to sort through all of this information. Give us a summary and teach us how to talk about it to our staff.
- Getting SOC 2 from our vendors can be difficult.
- Hearing from examiners: It's more about the people putting pressure on vendors to provide SOC 2. There has been an evolution in reporting. It's important to anticipate the changes.
- Cyber Security is none of our specialties. We often feel overwhelmed with these types of projects. Trying to do them efficiently, cost effectively, while not overspending.
- FFIEC Exam - Answering the questions as though we have it. Then examine your answers and determine areas that are weak so you can get a plan to get the work done.
- Making the difficult choices on when to transition duties off employees and hire people to help you.

Group 2 Notes

- This is scary, a big concern.
- I am reviewing stuff a lot more than I use to. I am spending more time questioning changes. This also has made me lean on my network services team to help educate me. In addition, I find that I am searching and reading more about security, hacking, regulations, etc. than ever before.
- We are doing more reporting, testing, document processing, etc. than ever before, but I am not sure that it is really helping us, and when the examiners come in it is never enough for them. I don't necessarily feel safer than I did before, but I am doing more than ever before.
- We would love to see Network Services come in and help us understand, educate and assess our risk for us. We aren't just looking for a free risk assessment, we need education on why we are doing these checklists and why we are appeasing the examiners. What are these checklists/examination standards doing to help protect us from risk?
- If we are outsourcing, or even having our own employee manage the risk processes, what if they don't do what they are assigned to do? What if they do the opposite and the bigger we get the more difficult it can be. Dual controls are in place, but is there ever a real protection from hackers?
- HOW MUCH TIME DO YOU SPEND EDUCATING YOUR MEMBERS ON CYBER SECURITY? – Newsletters, emails… not much. One of our biggest concerns is a member actually giving out their own information. Chuck discussed a hack test that a credit union attempted on their own employees. They emailed their employees and told them to enter their user name and password into a site for their new logo gear. It worked! HACKED!

- TBA, Horizon and Day Air are each running test hacking attempts on their own employees. Janet noted how important it is to share that information with the staff to educate them and create awareness.
- Does everyone have filters for outgoing emails? Yes, there are filters, we have filters. If it is sensitive information, encryption has been helpful, but so many of us work on our mobiles and are unable to access some of the encryptions, which alternatively, creates a business stop.
- I don't spend enough time evaluating the cost of not doing anything, or doing less. I would like to put dollar and cents to the cost of compliance.

Group 3 Notes

- At our last exam, we (Metrum) received a memo stating that every vendor needs a SOC 2 who holds member information. I asked to get a difference in price between a SOC 1 and 2, and to discuss whether it's worth having the CUSO get.
- Credit unions who have in in-house processing system should probably get a SOC 2.
- In the end, the commissioner who proposed this took a higher level job and now regulators have backed off this new requirement. But in Colorado, some vendors have already broken down and acquired one.
- Steve doesn't take any of the suggestions the regulators suggest for minimizing employee risk with respect to breaches.
- One of the main reasons Steve switched from in-house to SaaS was to point to the security improvements by having that aspect managed by somebody else.
- Site-Four has allowed CU*South and (CU*NorthWest to collaborate on an SSAE-16; reducing costs for both service providers by bringing it under a single data center name. Right now it works because examiners just use it to check a box off.
- Since there's not a lot of prescription to audits, credit unions don't necessarily need to create heavily involved rules; do something and document it.
- Kim mitigates employee risk by using Office 365 for work email; Kim is the only person able to access email outside of the office.
- Patrick comes from a banking background where security was a big focus. Coming to the credit union space 5 weeks ago; he was startled by the lax nature the credit union took security. He immediately put more stringent rules to prevent risk.
- Trusting employees still carries some element of risk; regardless of longevity at the CU. Patrick had a BSA officer caught committing fraud.
- "One little mistake can happen and it triggers an (over)reaction."
- Leo gave an example of a statement issue at 2 credit unions in which members received the wrong statements. 1 credit union took it in stride, but the other wanted to change all account numbers. How do you not only curb overreactions to mistakes while also improving processes to prevent these types of mistakes?
- Tri-Cities has a documented process for managing compromised card situations; that might be the best defense. Having the knowledge and a plan for responding to typical security breaches.
- Steve has stopped doing reissues for cards on compromised card situations opting to take a wait and see approach to whether there's an actual risk for the credit union.

Group 4 Notes

- **Scott McFarland** - Not enough money to fix it. Trying to be proactive…Is there a way to test? First you educate your staff. When you educate, you teach them how to do it. Some are targeting CU's and board members of CU. How do you respond and what is the response plan?

- Test for social engineering, offer of money
- Proactively prepare for SOC 2 Audit Standards
- **Carma Peters** – Watchful Waiting – Limit debit cards when there is a breach, but lower limits. Internal controls…communication to staff after it happens. Missed warning signs. Post mortem needs to be better.
- Do you know areas where you have the greatest losses?
- **Tom Gryp** – Hard to get your arms around something, when you don't know, until you know. Can't solve it by overspending. The advantage we have is that we are small. A sophisticated hacker may not waste their time on a small CU.
- Isn't this the perfect business for Audit Link or someone that is already in the CUSO? Use aggregate best practices of everyone, do as much as we can with lowest possible cost.
- If you've had a breach and shut it down, how long do you wait before you turn it back on?
- **Greg Smith** - Most exploits occur from outside. Advantage to being small is less people to watch. CU*NW uses same approach as CU*A. Then as collaborative partners we have to worry about each other. Policies and procedures need to align. One part is keeping the thief out, other is knowing the thief has been there and tracking them once they leave. Statistically it will happen to you at some point. Response policy is key – shut it down quickly. Assess first; close the gate. Needs to be a balance in the response.
- Detection, scope, response, and assessment. Fix before you can bring it back.
- Need more exercises for awareness. Need to do more test exercises. Do you hire a firm to test the employees and offer $1,000 to see if they will breach security?
- Focus on education, so that there is a learned response. Talk with CU's about how we test these things
- Members push back on strong passwords, etc. Market to member – you expose other members if your security settings/features are weak. Testing is to protect the CU. Talk about the investment you are making.
- **Pushing Advantage CIO** – perform a threat assessment. Participate in a self-insured program as a CUSO. Have a panel to determine best practices everyone will abide by. Very interesting collaborative idea.
- We can manage the network for the CU, then have someone else perform the audit or vice versa.
- SOC 2 (cost is almost double vs SOC 1)
- Regulators will tell CU's it's a requirement, when it's actually a "recommendation"

Group 5 Notes

- Michael: Participates in the CUA Networks Client Tech Users Group that answers to strict exams and audit requirements. Dave Wordhouse gave very good examples of breaches and review how new types of devices are being used to hack, such as baby monitors. His credit union also offers ID Shield to their members, where ID Shied does the work. They are impressed with ID Shield's service.
- Lindsey: Brought up the exposure through employee email
- Jeff: His credit union has been doing cyber security for quite some time, just now calling it that.
- Creating a budget line for this expense is important in the planning for risk mitigation.
- Explored with the table if they offer outside vendor presentations or collaborate products like 'Lifelock".
- Considering asking for SOC 2 exam from vendors that manager your members' data.

- Sioux Empire uses an ATM Network owned by a bank, called *Advantage Network.* Jeff was the first client to ask for SOC 2 exam report with no result. The bank has the SOC2 exam, not the ATM Network. Now more clients are asking and they are looking at how to provide this.
- The biggest risk can come from employees.
- Lindsey credit union has developed policies regarding employee behavior and requires the employee to read and sign.
- Jeff – Sioux Empire sends 2 'fake' emails per day which asks the employee to 'click' on a link. The employees are aware of this testing. They also use knowbefore.com – which provides online education on phishing and other types of breaches.
- The summary for the team is that they need to understanding the level of risk, and review current expenses for any cybersecurity offerings, then budget a more realistic and efficient use of their funds.

Group 6 Notes

- Counting number of days for survival until we get hacked (DD)
    - How do we prevent this? Hackers are getting more serious and determined.
- Ransomware was a real-life experience for my credit union (DW)
    - Has anyone reviewed the dark net?
- It is going to happen (DM)
    - Take a deep breath
- Don't click on questionable links, or open materials that appear suspicious (LB)
    - If there is any question, don't do it
    - This is a constant verbal reminder passed on to my team at meetings and any occasion where warranted
- We hired a third party firm (KR)
    - They posed as vendors, and were able to access numerous branches
    - The "Big Red Button" didn't even work
    - Published results internally followed by an intense amount of training
    - Quarterly DR/BR tests ran by internal IT team
    - We will operate/train knowing how to avoid getting hacked
- Credit unions have a natural tendency to want to help (DD)
    - How do we continue to have a helpful mindset and not be become gullible to fake information/hackers
    - Malware is possible through simple google search
    - Outside of control for key vendors
- Has email/web access been taken away from employees who do not require it (DD)?
- We have blocked various websites (DW)
    - But there are loopholes/spoofed websites that allow staff to get where they want anyways (Facebook, for example)
- What is unique with backups (DM)?
    - We perform replication every 4 hours through the CU*Answers Network Services team (DW)
- How much do we spend when employees are the greatest threat (DD)?
- We need to show we are not negligent (DW)
- We need to train on spoofs/emails (KR)
- Do Apple products help (DD)?
    - We separate our networks for specific employees that have access to private data (LB)

- What do cloud options (Office 365) bring to the table (DD)?
- Should we provide tablets/devices for email/surfing that employees can use (outside of private network)? (LB)
- We are our own worst enemy when we listen to staff in order to make tasks/jobs easier
    - Sending data/non-masking when working with third parties?
- We need to have a strategy for what staff can download (KR)
- We need to identify the risks that we cannot eliminate (DW)
- There is no easy answer (DD)
- Should we have the 'Show me where the Regulation…" attitude?
- Employees are all adults (LB)

Group 7 Notes

- First United
    - State chartered – smaller CU. Seems like their efforts are not enough. Examiners want "I told you so" moments. They constantly set you up.
    - Castleguard is the vendor they use to audit them
    - Malware can sit on your system from 6 months to 6 years
    - Invoices to accounts payable that have a link to pay a bill (that has already been paid)
    - Constantly have to train and remind staff
    - What about the employees that are actually trying to steal money?
    - Castleguard will test for 'What If's'. Data disaster recovery plans. The CU will write a scenario and test the CU (like a fire drill for data).
    - FFIEC Website. Use the cyber security checklist
- Calcite
    - Having the same issues. Partner with vendors to have the right controls to combat this issue. Their weakest area is their employees (social engineering tests). Huge eye opener. They even trained.
    - Document their controls. They require certain number of characters.
    - Auditors argued that their GOLD password wasn't enough. Examiners said that it is fine but document that you accept the risk.
    - How do you remind regularly?
    - Write up employees. Seems harsh but necessary
    - Good policies and practices. Who do you call if something happens?
- Service 1
    - Have not had any testing. No IT exam yet this year. But still wants to get proper processes in place.
- Bridge
    - They have had employees fail as well. Looking into vendors that will do the email tests.
    - Have used Castleguard as well but now have to hire BKD (in addition to Castleguard because they hit different areas)
    - Never know that we are being hacked
    - Every company has either been hacked or doesn't know they have been hacked
    - We send monthly reminders but have failed every social engineering test we have done
    - The con artists are very good.
    - Clean desk policies
    - CUA and Shared branching, for example, how could you possibly control security?
    - No way to guarantee prevention

Group 8 Notes

- IT department is the only group that one CEO doesn't know what they are doing.
- One credit union now talks about what is happening internally. Based upon what happened at Clarkston
- Another credit union spoke about how many passwords and how they are saved. Janelle spoke about using keypass, and encrypted site to save passwords.
- Another uses Keeper which also can be used on a mobile device
- There is never enough security in one opinion and if they are going to get in they will get in
- EMV chip is already absolute with their own token generator in Europe
- knowb4.com to test staff on opening e-mails and educate staff on security. Credit union has all zip files go directly to CIO to test before opening
- did not feel that there is so much coming at you that we will never be ahead of the curve and it is a risk of doing business. Control what you can
- Having a good plan and response is the best thing we can do
- One credit union spoke about a potential hack at Coop
- Knowing how to react was a theme
- Understanding what is exposed was a common
- Matt was reading "cyberwar" by Richard A Clarke and Robert K Knake
- One is spending on risk assessments and audits more than anything else
- One was looking at foreign traffic hitting their website and was surprised to see what countries
- Soc2 group felt that the credit union is ultimately responsible regardless of where the breach was. Merchant responsibility needs attention
- Spend on attorney fees relative to hacks is going up

Group 9 Notes

General Discussion

- CU*Answers manages our firewall, local company manages network & IT issues. There's actually an audit you can do in CU*BASE where you can verify who has downloaded files. This one's important to keep track of. I've heard people talk about locking down USB Ports. (Andy)
- You can shut (USB Ports) down for things that have storage. Symantec has that ability on both the enterprise and cloud version. You want to be on the cloud version because there's no override on the enterprise version. (Mike)
    - We collaborate through the network. I've got debit card risk, loan risk, online application risk. So I have everything with the network because they're going to be the experts while helping manage the cost. I think there's a responsibility in our network to do this well. (Andy)
- I looked at our Disaster Recovery Plan to see what was in it. It was older so we are re-evaluating and updating it. We're looking at who has access to what, when, etc. Also are looking at penetration testing & some other similar testing.
- CU*Answers manages all our networks, but I think it's important to be looking at who's testing me internally and what my staff are doing. It's scary to think about staff being the weak link with passwords of '123'.
- So, we are also working with another small CU who's going through the same evaluation process. We're saying 'let's collaborate on this kind of thing' and 'why aren't we more forward thinking on this kind of stuff?' (Kris)

- I'm in the same spot (on evaluating the DR plan). Some things we currently do for testing are: PEN testing, Social Media testing, weekly network scans, also CU*A will have passwords to access all those reports. I switched over my networks to CU*BASE. I once talked to an individual who had someone hold her server at ransom. She called CU*A and they came in and took care within 4 hours. And of course, we do have some education with the staff because that's so important. (Steve)
- You want to have an era of training and build the culture to keep employees engaged. (Jennifer)
    - One of the things we worked on was getting employees to tell them when something was goofy. Had to change the culture so they felt that they could tell me if something looked strange or if they did something. (Mike)

Future Spending

Insurance

- That's what you need – the catastrophic coverage. If you're going to insure for all the small things there's no point.
- I also just increased my insurance premiums because we were paying so much that I had to say yes there's a risk of it happening, but I also need to have some income coming in without it all going out to paying insurance.
- I always say no give me the highest deductible possible.

Guarding Member Data

Mobile Devices

- There is literally no way to protect against it all. It doesn't have to be a thumb drive. I could sit here and take pictures of member data with my phone. (Kris)
- Talk about not taking your laptop home – what would be the purpose of restricting that? I don't see a problem with it as long as we have training on what the risks and such can be. (Jennifer)
- I tell my staff they have to go offline if they need to use their phones. (Kris)
- If they want to send a text during the day, ok. But I just don't want them on the phone when a member walks in. (Andy)
    - If you don't allow them to use it during the day they will anyways and then it's just a friction point. (Mike)
    - It's culture, it's an appendage. It can be a service piece. If you want an employee to go deeper with one-on-one service, they need to have all the tools. (Jennifer)
- We have iPads that our employees use in the branches, what does everyone do to keep those secure? (Kris)
- Track iPads by only having 1 in each location. (Jennifer)
- We just have one branch so we keep it in a safe & consistent spot, it always stays there.
- And do you have an option to burn it if it does leave? (Mike)
    - Verizon, if I buy iPads through them I can just shut them off if I need to. (Kris)
    - But what's on it? We're not using them in branch for more than just internet and a few other things. (Jennifer)

Receipts, paper, what's everyone doing there? Shredding?

- Do you have your printers locked down? What I understand is that hackers can go in the backdoor of the printer system and get into the network or get documents off the printer hard drive in some cases. (Steve)

- How many reports do you have printed and where are they sitting at? (Security companies) will come in and do a walkthrough and look for passwords. What are your employees doing with all this info? (Jerry)

Encrypted Emails/eDocuments

- I had the discussion with my staff after cybersecurity conference. I told my staff even if you get an email from a trusted source like CU*A asking you to download something – DON'T. My biggest concern is they're clicking something they shouldn't. (Kris)
- I think they'll even do that kind of testing. Send an email to try and catch someone doing it. Trace does dumpster diving too.
    - And all this can be a budget issue. It's all on what you want to spend. Is there always enough? I doubt it. And examiners will always want you to do more.
- We have an application for our mail filter which has the encryption ability. We also have a rule set up with social security number detection, etc. (Mike)
- We just signed up with eDoc for loan documents and closing (Kris). It's awesome. We are closing way more loans (Andy). Agreed. We use it too (Steve). Members love it (Kris).
- I've gone to CU*Answers for my email service. This allows me to use a way to send encrypted emails. (Steve)

Currently using CU*A Network Services?

- Most of the group is a yes. One uses 3rd party for network & security.
- We also use CU*Answers AuditLink team so they document anything that's been downloaded and that helps me see what's happening. BSA audits, Dormant activity, wire transfers, download reports, etc. (Jerry)
- When you have small staff it's hard to say "who's going to do that". With AuditLink it's so easy, as I just get a daily report. (Jerry)

Do you like having a separate IT?

- No. There are parts that are great. We were their first client and their service level is off the charts. Very available. That's the good side, but as we discuss the needs that we have for reporting, they're not capable of that. This next year I have to consider going to CU*Answers Network Services just to get it standardized. Right now, the reports are coming from all over the place.

Summary

What is everyone doing?

1) Most have CU*Answers network services
    a. Consolidation of the network management is cost-effective for most
    b. Standardization of reports is really helpful
    c. Case Study – A friend had their server held hostage – CU*A resolved in 4 hours.
2) AuditLink via CU*Answers (daily BSA, download reports, etc)
3) PEN testing
4) Locking down USB ports (hot topic in Wisconsin right now)
5) Weekly network scans (CU*A network)
6) Passwords to access reports (CU*A can set up)
7) Paper records – walk-throughs to look for sensitive data lying around office on paper
8) Password management – Outlook Secure & password safes
9) Social Media testing

10) Ensure CAMS reports are being reviewed
11) New vendor due diligence
12) Encrypted email
13) Lockdown printers (also never let leased copiers leave without wiping their internal hard drives)
14) Anyone walking in that's not an employee has to sign in
15) Set firewall to restrict certain communication out of ports
16) Mobile devices are allowed – 1) They are culturally appendages, & 2) Employees need these tools for deeper member support
17) Collaborating with fellow CU going through same internal DR review

Needs – Several CUs are currently re-doing:

- Re-doing disaster recovery plans
- Network security plans
- Education of staff (sometimes they're trained to be so helpful that they may just let someone in before realizing what they've done)