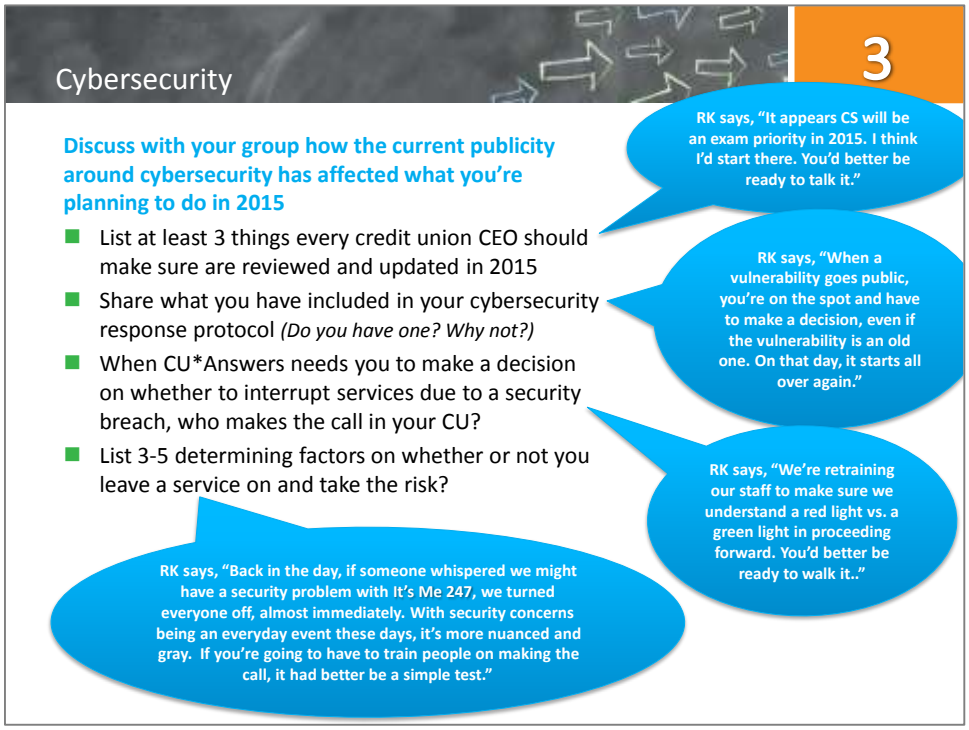
CU*ANSWERS

Notes from the 2014 CEO Roundtable

At the Frederik Meijer Gardens, November 5, 2014

Compiled From Notes Taken By the "Table Scribes"
Revised November 14, 2014

Topic 3: Cybersecurity



Participants

Grp	Scribe	CEO Participants	Grp	Scribe	CEO Participants
1	Barb Cooper	Philip Heinlen, Northwest Consumers FCU Sheila Schinke, Prospera CU Donna Bullard, Clarkston Brandon Bob McDonald, CU*South	7	Julie Gessner	Barb Mills, Calcite Chuck Papenfus, Inland Valley Scott Pauly, Awakon Kim Burdo, Service 1 Val Mindak, Park City
2	Starla Honea	Martin Carter, Parkside CU John Rupert, Muskegon Co-op Vickie Schmitzer, Frankenmuth CU	8	LizWinninger	Scott Harriman – Cumberland County FCU Jeff Jorgensen – Sioux Empire FCU Rudy Callen – KALSEE CU Greg Smith – CU*NorthWest Mike Williams – Colorado CU
3	Janelle Krupa	Andy Fogle, Des Moines Police Officers Jim Miles, MidUSA CU Donald Mills, Alpena Alcona Area CU Jordan Modell, Internet Archive CU	9	Laura Zazakis	Susan Fisher, Tongass FCU William Burke, Day Air CU Janet Borer, Members 1st Comm CU Scott McFarland, Honor CU Linda Bodie, Element FCU
4	Pete Meyers	Chris Butler, Community CU Walter Swanson, Superior Choice CU Jason Matley, Washtenaw FCU Kim Kniola, First Trust Kevin Ralofsky, CitizensFirst	10	Vic Pantea	Tracy Miller, Kellogg Comm FCU Terri Maloney, Catholic United CU Dennis Degenhardt, Glacier Hills CU Christy Leslie, Bridge CU

Grp	Scribe	CEO Participants
5	Annalyn Hawkes	Corinne Coyle, Advantage CU Mark Richter, First United CU Steve Janssen, Brewery CU Cathy Ellis, Meijer CU Scott Collins, Xtend
6	Karen Sorensen	Eric Jones, Kansas City CU Ernie Jackson, CommStar CU Dean Wilson, FOCUS CU David Wright, Services Center FCU Jennifer Oliver, South Bay

Grp	Scribe	CEO Participants
11	Pete Winninger	Chris Ison, Tahquamenon Area CU Barbara Bean, Cal Poly FCU Steve Kelly, Metrum Community CU Barbara Mathey, IBEW / United Workers FCU Janelle Franke, River Valley CU Sara Redeker, Tri Cities CU

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.

Discuss with your group how the current publicity around cybersecurity has affected what you're planning to do in 2015

List at least 3 things every credit union CEO should make sure are reviewed and updated in 2015

Table 1

Phil – 1. Online banking, Facebook (Social Media), firewall performance (both directions)
Sheila – 2. Staff education as well
Donna – 3. Penetration testing

Table 2

Make sure board has some idea of IT security. Don't just have policies, show how they are being executed.
Certifications and services: Cyber security insuance , vendor management school cuna

Table 3

1. Anti-Virus Software
2. Penetration test
3. A point person, and chain of command

Member who was a teacher had an internet relationship from someone in Iraq and had never met, started sending him money, gave him her It's me 24 information. He was a front for a cybersecurity outfit in Iraq. They immediately shut it down. Real member who fell in love with someone that was a fraud. Educate members of what cyber security involves so examples like this don't happen. How do you notify members?

Make sure board is being updated and trained on issue.

Table 4

Have a plan in place - it's all about communication

Do you have specific canned messages for issues?
- identify who will respond
- determine roles & have alternates in place — know who will pull the trigger

Look at policies & procedures
- review from the outside

Table 6

1. Use Network Services IST risk audit service for improving Cybersecurity
2. Include CU*Answers testing in board minutes (disaster recovery, high availability rollover)
3. Staff training about IT risks-
1. Make sure you are not running XP on any computers
2. Protect the WiFi used by credit union employees
3. Maintain a diagram of how the system is put together

Note: Commstar CU recently revamped entire network of PCs at the credit union, laptops that go out of the office must be encrypted.

Table 7

1. Security Protocol
2. Incident Response
3. Business Continuity
4. Web Site Policy - how often is it checked-Who Checks, who has authority to change - Scheduled testing and roll out of these changesTemplates may be available from the state.
5. Internet Policy
6. Define each of your audits and test them.
7. Internal cyber security committee to create an understanding of these issues within the 4 walls of the credit union.
8. Learning how to handle the information we need to provide to examiner when we do not have an internal team of our own. (Folks who use CUA Network Services)
9. Read the policies and templates and make sure that you can do what you have wrote.

Table 8

- The consensus at the table was each credit union brings in a person who will pretend to be an employee, se
- Social engineering annually, pin test 4 times
- The first time it happens several of the senior management team failed.
- A full blown risk assessment is costly and time consuming. DMZ's and IBM testing.

Table 9

1. Make sure and update with the Leadership team what (internal team members to make decision) puts your CU at risk. Protocol if it happens.
2. Business Continuity / Cyber Security – business Swat Team. Need Vendor list and how are they connected with CU*A
3. Knowledge of what you IT department has done. What is Cyber protocol now?
4. Mobile devices to be included.
5. Investigate bond insurance and document decision.

Honor - Evaluated bond insurance but found you would pay for insurance and never get a paid out on a cyber-breach. Should revisit yearly

Table 10

- Look for help. Identify a third party for help with vulnerability testing and support for policies and procedures. Expanding into other areas of risk, special media, etc.
- Manage Firewall reports. Increase communications and education with CU*A concerning the process. Audit-link
- Review Training cycle to account for turnover.

Table 11

1. Chris Ison is updating cyber security policy in 2015
2. Document annual staff training and social engineering (quarterly for Mathey)
3. Budget and plan for data breeches

Sara – independent audit found things Network Services isn't doing for firewall and is not responding to fast enough and wants out of contract

Share what you have included in your cybersecurity response protocol *(Do you have one? Why not?)*

Table 1

Currently, Donna as CEO, VP as 2nd in line in her policy
Phil – has no cybersecurity policy or plan. However in practice, CEO would be first, then 2nd in command
Sheila – They have a policy, but is unfamiliar. Her IT staff monitors.

Table 2

What is cyber security anyway? Just a new fancy name
Cyber insurance through Allied.

Table 4

Have a plan, have a team, have roles and responsibilities
have external sources and legal team verify

Table 5

- Most in the group do not have a documented cybersecurity response protocol established at this time.
    - We did not have one until something happened which required us to figure out our response to the threat.
    - There are so many different potential threats that could be guarded against that it is difficult to prepare for them all. It also may even be true that we are more vulnerable to internal threats/fraud, than anything online from the outside.

Table 6

- South Bay does have a policy which includes filling out a form. The others do not have a policy.
- Hooking up phones to desktop at work, how safe it that?
- Focus plans to activate requiring usernames in It's Me 247. Also, they are forcing everyone to e-statements otherwise pay a $3 charge per month.

Table 7

- Create internal organizational chart on who to call
- Understanding the differences between IT Exam and Cyber Security
- Train employees on what to say should they receive a phone call
- CPD Training modules thru CUNA as a required class
- Use awareness weeks as a catalyst to train staff
- Employees sign a cyber-security policy including that they have received training retained in the employee file
- Hire a third party to try to perform a vulnerability assessment
- Understand when to shut off employee access to certain network protocols -if not doing this then have a way to verify what employees are doing and accessing while away

Table 8

- No one has a cyber-security response policy, with the exception of CU*Northwest. As a CEO, if you are not in the office, how are decisions made when you are not there? Are the same people who

- Xtend needs to call out the purpose of the contact sheet document, at that point the credit union could use that document to place in their Cyber-Security plan. The table each spoke to how their teams handle issues as they are out of the office.
- The table called it data security, not cyber security, they will use this as an action item when they go back to their credit unions to update their documents.

Table 9
Most have one in process

Card processor has a protocol and would determine when to restrict or shut a card down. Let vendor determine rather than the CU

Day Air has never issued new plastics based on a breach. Do on a case by case basis. Issue notice to members, but let member decide. Don't want them to be without their plastic even for a week.
Take advice of processor.

Table 10
2 yes, 2 no. Looking for model policies
How do we know if someone is probing us?

Table 11
- Group has incident response policy but not cybersecurity policy
- NCUA is urging Barbara Mathey to have independent policy – writing policy now
- Cal Poly has cyber security board but no outside eyes
- Tahquamenon Area CU is reworking old policy
- River Valley CU uses Policy Pro as template for policy
- Michigan CUs required to have IT audit
- Network Services IT review from Matt Sawtell / RedRock / Cindrich & Mahalik
- Group relies heavily on CU*A to make recommendations

When CU*Answers needs you to make a decision on whether to interrupt services due to a security breach, who makes the call in your CU?

Table 1
CEOs, then highest manager on duty or department head of the service in question.

Table 2
CEO
IT manager

Table 3
Should be CU*Answers, if there is a high enough risk, CU*Answers should turn it down.
Reputation rests in the network. Override other concerns of security. If he accepts risk and gets burned, doesn't that look bad on CU*Answers?
Should be minimal risk that you're asking us to interrupt services.

Table 4
have a computer specialist who knows if this is real or not.

Table 5
- Group consensus is that ultimate decision is made by upper-level management staff, with the best scenario including involvement of a team of people with expertise in the departments affected by interrupting the service.

- Ex. If DealerTrack were compromised, the Lending Manager would be an important resource to assess the effect on internal process and potential effects on members if service stays interrupted.
- Anyone with a C at the beginning of their title could make the call

Table 6
The CEO would make the call.
CU*Answers is the one that would flip the switch for larger breaches. Often times it is not the CU that is making the decision to interrupt services.

Table 7
CEO, COO
CEO, CFO
VP IT, CEO
CEO, COO
CEO, COO

Table 8
If one piece needed to be turned off, such as dealer track they would not be effected as much as It'sMe247. The impact is much larger on one than the other.

Table 9
Linda – Leadership/Management Team
Scott – Leadership Team/ Swat Team…..notify CEO immediately.

Table 10
VP IT, exec. Team decision
CU*A should turn off first upon discovery, then ask us if we want turned back on.

Table 11
- CEO or management would make the decision.
- Follow policy…?

List 3-5 determining factors on whether or not you leave a service on and take the risk?

Table 1
1. Balances the cost of assuming the risk, vs loss if income or benefit
2. Reputation Risk
3. Member reaction (high vs. low)

Table 2
Exposure
Cost
Member affect
Discussed compromised cards and policies procedures and how each CU handled it.
The CUs didn't seem very interested in this subject. Not a lot of input.

Table 3
1. How serious the risk is and what we know about it – tell what breach was
2. Insurance to mitigate the breach
3. How many people would be impacted

Table 4
how does it impact business? some of it is gut feel.

FS-izac has a service that will send you alerts regarding attacks/vulnerabilities

Table 5

- What is the impact to members
- Whether the risk involves malware moving in to the system, or data being taken out of the system, or both.
- How long will the security risk last (long-term vs. short-term) and what is the potential reputation risk involved in each type of situation.
- Determining potential costs involved if the service is left on and does become an issue.

Table 6

Am I going to be on the 6:00 news? Is member data at risk?

Table 7

1. What is vulnerable?
2. How will it affect members?
3. How will it affect the organization?
4. Reputation Risk?
5. Am I any less safe now than I was yesterday?
6. Is everyone else doing it?
7. Google the issue- do the research
8. What does Network Services say?
9. The League and other trusted partners

Table 8

1) Level of impact
    - Reputation risk
        - When do we tell them and what do we tell them
        - Where is a marketing opportunity
        - There was good discussion around who does what, particularly with who makes the call and who communicates it, PR/Marketing to members. The idea was proposed to have the list that Xtend is provided annually used by credit unions in their security plan. The information is available in CU*Base, so this would be an easy to access list of employees.
    - How many members are impacted?
2) Time to mitigate
3) Expense

Table 9

1. Potential financial impact
2. Recommendations from core processor and/or vendor. Patrick's dissertation (neutral perspective for how to impact).
3. Potential number of members impacted.
4. Weight of risk / Likelihood of loss. Users going without
5. Reputation risk

William
Leave it on and take the risk. Loss of member data which is probably out there anyway. Transaction data flow versus entire data base comprised determines risk.
Matter of risk management.

Table 10

What data is being breached?
What is extent of economic risk?

What is extent of reputation risk?

Table 11

- How long will service be down
- Chances of actually being hacked – Steve Kelly willing to take the gamble to keep service open