CU policy PRO Newsletter

February 2015

Dear CU PolicyPro Clients,

In the NCUA's Supervisory Priority List for 2015 (15-CU-01), Cybersecurity was listed as the first topic. The letter to federally insured credit unions goes on to indicate that cybersecurity assessments conducted in 2014 found that many credit unions are not taking basic cybersecurity actions. Efforts by the NCUA will be redoubled in 2015 to ensure that the credit union system is prepared for a range of cybersecurity threats.

In order to make sure your credit union is prepared for the cybersecurity scrutiny in your upcoming exam, we encourage credit unions to review CU PolicyPro policies in the 4000 series related to "Security." Policy 4120 specifically addresses most of the proactive measures to protect both credit union and member data that the NCUA will be looking for, including:

- Encrypting sensitive data;
- Developing a comprehensive information security policy;
- Performing due diligence over third parties that handle credit union data;
- Monitoring cybersecurity risk exposure;
- Monitoring transactions; and
- Testing security measures.

During their 2015 examinations, the NCUA will also be evaluating credit unions' capacity to recover and resume operations if a security breach does occur. Guidelines for the requirements of a credit union's incident response program in Appendix B to NCUA Rules Part 748 can be found in Model Policy 4125, Incident Response.

In this edition:

- Monthly OPS Notes Release: 2015 – Cybersecurity
- Content FAQs
- Technical FAQ
- Content Updates Reminder
- Questions?

Monthly OPS Notes Release: 2015 – Cybersecurity

With the NCUA focus on cybersecurity, it's important that credit unions review their existing policies and procedures to make sure they are prepared for a potential security breach.

In 2014, the Federal Financial Institutions Examinations Council (FFIEC) piloted a cybersecurity examination work program at over 500 community financial institutions to evaluate their preparedness to mitigate cyber risks. The FFIEC published their general observations from the Cybersecurity Assessment and provided suggested questions for CEOs and boards of directors to consider, based on topic, when assessing their own financial institutions cybersecurity preparedness.

Connection Types

- What types of connections does my financial institution have (virtual private networks, wireless networks, etc.)?
- How are we managing these connections in light of the rapidly evolving threat and vulnerability landscape?
- Do we need all of our connections? Would reducing the types and frequency of connections improve our risk management?
- How do we evaluate evolving cyber threats and vulnerabilities in our risk assessment process for the technologies we use and the products and services we offer?
- How do our connections, products and services offered, and technologies used collectively affect our financial institution's overall inherent cybersecurity risk?

Risk Management and Oversight

- What is the process for ensuring ongoing and routine discussions by the board and senior management about cyber threats and vulnerabilities to our financial institutions?
- How is accountability determined for managing cyber risks across our financial institution? Does this include management's accountability for business decisions that may introduce new cyber risks?
- What is the process for ensuring ongoing employee awareness and effective response to cyber risks?

Threat Intelligence and Collaboration

- What is the process to gather and analyze threat and vulnerability information from multiple sources?
- How do we leverage this information to improve risk management practices?
- What reports are provided to our board on cyber events and trends?
- Who is accountable for maintaining relationships with law enforcement?

Cybersecurity Controls

- What is the process for determining and implementing preventative, detective, and corrective controls on our financial institution's network?
- Does the process call for a review and update of controls when our financial institution changes its IT environment?
- What is our financial institution's process for classifying data and determining appropriate controls based on risk?
- What is our process for ensuring that risks identified through our detective controls are remediated?

External Dependency Management

- How is our financial institution connecting to third parties and ensuring they are managing their cybersecurity controls?
- What are our third parties' responsibilities during a cyber attack? How are these outlined in incident response plans?

Cyber Incident Management and Resilience

- In the event of a cyber attack, how will our financial institution respond internally and with customers, third parties, regulators, and law enforcement?
- How are cyber incident scenarios incorporated in our financial institution's business continuity and disaster recovery plans? Have these plans been tested?

How prepared is your credit union? Unfortunately, it's not just the policy components that mitigate cyber risks. Credit unions should also be evaluating existing systems, procedures, and training programs they have in place to address cybersecurity vulnerabilities.

Credit unions can also visit the NCUA's webpage specifically devoted to Cybersecurity Resources.

This edition of OPS NOTES was prepared by the Michigan Credit Union League.

Content FAQs

Question. One of the components of a Response Program in Appendix B of the NCUA rules indicates notifying the appropriate NCUA Regional Director, and for state-charted credit unions its applicable state authority, as soon as possible when the credit union becomes aware of an incident involving unauthorized access to our use of sensitive member information. What type of unauthorized access would warrant NCUA notification, say for example if a teller inadvertently places the receipt in the wrong tube at a drive through?

Answer. In a NCUA Legal Opinion Letter dated April 17, 2006, the NCUA indicates that "when an incident occurs, the first step is to assess the risk and scope and the likelihood of harm to the member whose information is affected." The NCUA goes on to further clarify where "an incident, even involving sensitive member information, involves little or no likelihood of harm to the member, a credit union not notify the NCUA." Therefore, the credit union should be conducting a risk assessment for every unauthorized access to member information and documenting their decision whether to notify their regulator.

Question. Our credit union wants to prepare for the heightened focus on cybersecurity, what should we do first?

Answer. Credit unions are encouraged to utilize the AIRES IT Questionnaires to review the adequacy of their current security programs. When reviewing the questionnaires, which are in excel format, be sure to "enable editing" and hover over the red triangles in the corner of the cell to obtain more detailed information on the requirements outlined. This review will assist the credit union in determining any potential weakness. Additionally, the credit union is encouraged to maintain these AIRES Questionnaires because examiners utilize these same questionnaires in their examination.

Technical FAQ

Question: How do I add spacing in a numbered list?

Answer: The model policies are double spaced to make reading the policies a bit easier. However, by default, the CU PolicyPro system will single space each item in a numbered list.

The following steps are the best practice method for creating double spaced lines in a numbered list. It is recommended to take care of spacing last, after all content is in the numbered list, with each item in the correct position and correctly formatted.

1. Place your cursor at the end of the first item that is single spaced.

2. Hold the SHIFT key as you press ENTER (SHIFT+ENTER). This will drop the cursor down one line without creating a new item in the numbered list, effectively creating a double space.

3. Use the space bar to add a “space” in the newly created line break. Some printers will not recognize the SHIFT+ENTER code and will remove the double spacing during printing. The “space” character acts as a place holder, making the spacing appear as expected.

Click here for a printed guide on best practices for working with numbered lists.

If you have additional questions, please contact the CU PolicyPro Support Team at policysupport@cusolutionsgroup.com.

Content Updates Reminder

This is a reminder that a large update was made to the model policy content in December. The updated included **forty two policy updates**. For more information on which policies were updated, the next steps for your credit union and training materials on how to incorporate the updates into your Working Manual, please visit the CU PolicyPro Support Site.

Another update is scheduled for March, so it is important to make the updates from December as soon as possible so you don’t fall behind!

If you have any questions, please contact the CU PolicyPro support team at policysupport@cusolutionsgroup.com.

Questions?

If you have any questions regarding the CU PolicyPro content, or questions on how to use the system, please contact policysupport@cusolutionsgroup.com.

If this information was forwarded to you, and you'd like to be on the distribution list to receive information and updates related to CU PolicyPro, contact policysupport@cusolutionsgroup.com.

Thanks and have a great week!