CUNA MUTUAL GROUP

It's not IF—It's WHEN
Prepare Your Credit Union for Data Breach Aftermath

With the rise in highly publicized financial data breaches, the first question credit union directors and senior executives should ask themselves may not be how to prevent it from happening to their credit union. Given the most recent cyber-crime statistics (see sidebar), the more appropriate question to ask may be: "What are we going to do *when* it happens to us?" Not *if*, mind you, but *when*.

Beyond lawsuit judgments and defense costs, your credit union may be faced with a variety of other direct and indirect losses a data breach can cause. For example, consider how your credit union would handle these potentially significant expenses:

1. Investigating the data breach's cause and extent

You may need to hire a forensic auditor, network security specialist, or other professionals to determine which databases and files have been compromised, which members may be affected, the types of member data breached, how hackers gained access to the data, etc.

2. Extortion threats

Imagine your CEO gets a call from a hacker who can confirm the acquisition of confidential member information. The hacker demands $1 million not to release the information to other criminals who will exploit the information.

3. Public relations to counter reputation damage

Outside public relations professionals may be needed to manage reputation risk if you don't have in-house expertise.

4. Notifying members and protecting their assets

Depending on the size of the breach, the cost in work hours and materials to notify every potentially affected member can be significant. And if your membership crosses state lines, there will be added complexity and expense to your response due to varying state data breach notification laws. Remember that informing members is just a start; you've also got to have the staff or hire a third party to handle the inevitable surge of inquiries from members. In addition, try to estimate these potential expenses for a large-scale breach:

- Credit report monitoring/identity theft restoration services for potentially affected members
- Changing account numbers and following through with members to change their user identification and passwords
- Reissuing checks or share drafts
- Blocking and reissuing plastic cards

Decide how to manage the risk

Unfortunately, the above list of cyber-crime expenses is far from complete. As part of an overall cybersecurity risk management strategy, your credit union needs to determine which insurance coverage (if any) is needed to best protect your credit union from cyber risks.

Be sure you understand whether you have insurance coverage for these risks, and if so, whether is it part of another policy that may not be as comprehensive as a traditional cyber liability insurance policy. Make sure you review the coverage limits to determine if they are sufficient, based on your exposure. Estimating your potential exposure is especially important if your credit union chooses to self-insure against these risks.

Credit union leaders must continue to educate themselves about these threats as criminals adapt and shift tactics.

[SIDEBAR]
2014 DATA BREACH NUMBERS: BE ALARMED (IF THAT'S STILL POSSIBLE)

There have been so many dire data breach reports in recent years that the figures can be mind-numbing. Understandable—especially if your credit union hasn't experienced a direct data breach throughout these months of big headlines. Still, reviewing the annual data breach statistics is eye-opening. They show that the cyber security industry isn't crying "Wolf!" And the problem appears to be getting worse.

Here are some key results from the Identity Theft Resource Center's 2014 data breach report*:

- The 783 data breaches tracked in 2014 establishes a new record.
- The previous record number of breaches had been 662 in 2010. The 2014 total beats that by 18.3%, and beats 2013's total by 27.5%.
- Hacking was the leading cause of 2014 data breaches, at 29% of the total (up from about 26% in 2013), followed for the second year in a row by subcontractor/third-party breaches which were 15.1% of the 2014 total.
- Social security numbers were involved in 41% of all 2014 breaches, which is an improvement over 48% in 2012 and 2013. Exposure of credit/debit card numbers, while significant lower than social security numbers, has been increasing, from 14% in 2012 to 15% in 2013 and 18% in 2014.

Jay Isaacson *is Vice President, Business Protection Product Management, for CUNA Mutual Group. Contact him at 800-356-2644, ext. 6657829, or at* jay.isaacson@cunamutual.com.

* SOURCE: "Identity Theft Resource Center Breach Report Hits Record High in 2014," published on the ITRC website, January 12, 2015.

CUNA MUTUAL GROUP