Credit Union Cyber Crisis: Gaining Awareness and Combatting Cyber Threats Without Breaking the Bank
Introduction

The 6,331 credit unions in the United States face a unique challenge when it comes to cybersecurity. With more locations than commercial banks and nearly $1.2 trillion in assets, there is ample opportunity for cybercrime activity. However, those credit unions and small banks must address the variety of cyber issues with less staff and less resources than their larger counterparts.

In addition, the more than 100 million credit union members often expect a similar always-on environment offered by the big banks -- despite the fact those commercial banks have the capital on hand to invest at a record pace in this technology:

- 24-hour deposit
- Mobile banking
- Mobile deposit
- Other convenience services

Top this off with the sensitive nature of the information involved as well as the large amount of outsourcing and trust placed in third parties, and it is easy to see why credit unions are often viewed as soft targets when it comes to both traditional cyber threats and threats from the Dark Web.

In fact, in looking at Dark Web threat data from a one-month snapshot, SurfWatch Labs has observed:

- Over a hundred new or repeat credit union targets across a wide variety of cyber and business exploits
- Over 10,000 stolen credit union payment card numbers gained via a variety of mechanisms including point-of-sale systems and ATM card readers
- Myriad of hacked corporate and personal accounts for sale
- Dozens of software exploits for sale relevant to online banking, web server technologies, mobile technologies, and other tools used by credit unions
- Thousand of customer identities and credit info for sale to support criminal activity such as identity fraud

Keeping up with the ever-changing cyber threats can be both costly and resource intensive. That poses an important question: how can an organization move towards better cybersecurity in a more practical, cost-effective manner?

This paper explores how credit unions can leverage cyber risk intelligence to improve their cybersecurity practice and reduce the level of effort.
A Quick Look at Credit Union Cybercrime

According to a recent NCUA letter to credit unions (15-CU-01):

“Credit unions, like all financial institutions, remain vulnerable to internal and external cybersecurity threats. Last year’s interagency cybersecurity assessment conducted through the Federal Financial Institutions Examination Council (FFIEC) found that many credit unions and banks are not taking basic cybersecurity actions.”

In 2015 the NCUA plans to redouble its efforts to ensure credit union systems are prepared for a wide range of cybersecurity threats.

Data and analysis from SurfWatch Labs backs up the FFIEC assessment, with new credit union-related information being traded on the Dark Web every day.

<table>
<thead>
<tr>
<th>Industry Targets</th>
<th>Actors</th>
<th>Targets</th>
<th>Effects</th>
<th>Practices</th>
</tr>
</thead>
<tbody>
<tr>
<td>Visa Inc.</td>
<td>AlphaBay Market</td>
<td>payment card data</td>
<td>leaked names, leaked expiration dates, leaked mailing addresses</td>
<td>payment card data trade</td>
</tr>
<tr>
<td>Cyprus Federal Credit Union</td>
<td>AccessGranted</td>
<td>蔌</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visa Inc.</td>
<td>BroomBroomVends</td>
<td>payment card data</td>
<td>leaked mailing addresses, leaked payment card numbers, leaked card verification values (CVV)</td>
<td>payment card data trade</td>
</tr>
<tr>
<td>Allegacy Federal Credit Union</td>
<td>AlphaBay Market</td>
<td>蔌</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visa Inc.</td>
<td>BroomBroomVends</td>
<td>payment card data</td>
<td>leaked payment card numbers, leaked names, leaked expiration dates, leaked card verification values (CVV)</td>
<td>payment card data trade</td>
</tr>
<tr>
<td>Washington State Employees Credit Union</td>
<td>AlphaBay Market</td>
<td>payment card data</td>
<td>leaked names, leaked card verification values (CVV)</td>
<td>payment card data trade</td>
</tr>
<tr>
<td>Visa Inc.</td>
<td>BroomBroomVends</td>
<td>蔌</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pennsylvania State Employees Credit Union (PSECU)</td>
<td>AlphaBay Market</td>
<td>payment card data</td>
<td>leaked expiration dates, leaked card verification values (CVV)</td>
<td>payment card data trade</td>
</tr>
<tr>
<td>Visa Inc.</td>
<td>BroomBroomVends</td>
<td>蔌</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visa Inc.</td>
<td>BroomBroomVends</td>
<td>payment card data</td>
<td>leaked names, leaked payment card numbers, leaked mailing addresses</td>
<td>payment card data trade</td>
</tr>
<tr>
<td>Michigan Schools and Government Credit Union</td>
<td>AlphaBay Market</td>
<td>payment card data</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Visa Inc.</td>
<td>BroomBroomVends</td>
<td>蔌</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CAMPUS USA Credit Union</td>
<td>AlphaBay Market</td>
<td>payment card data</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

SurfWatch Labs scours the Dark Web daily for stolen payment cards, customer information, business and personal accounts, vulnerabilities for sale, and other sensitive and valuable information.
A variety of cybercrime actors openly sell stolen payment card information on the Dark Web. Many sites even offer discounts, refunds, and additional customer service like traditional e-commerce stores.

The technology consumers demand from credit unions also requires complex connectivity, which creates additional areas for vulnerabilities as well as additional access points that cybercriminal actors can exploit. This is particularly true when features and applications are rushed through the development cycle in order to keep up with market demand.

In addition to a variety of threats from both external and internal actors, poor security at outside organizations can lead to significant financial costs for a credit unions such as when they have to re-issue payment cards following point-of-sale breaches in the retail sector. Data loss can also lead to other issues such as potential litigation.

Despite all the challenges facing small banks and credit unions, it is important to take a step back and note that the FFIEC found “basic cybersecurity actions” to be lacking in many instances. Increased technology investment and convenience applications may lead to new attack vectors, but tried-and-true cybersecurity practices, if done properly, can go a long way towards mitigating that increased cyber risk.

This includes focusing on a few key areas:

- **Data** - Information should to be classified by its level of risk with higher-risk data having increased protections such as encryption to help limit risk exposure
- **Supply Chain** - Third parties that handle credit union data as well as any others in the organization’s supply chain are often exploited; therefore, it is important to monitor those risk areas for potential threats
• **Fraudulent Activity** - Many point-of-sale breaches are first discovered when fraudsters begin using stolen payment cards or when information goes up for sale on the Dark Web; quick action can shorten the “lifespan” of this stolen data and help limit financial losses

• **Technology Infrastructure** - It is crucial to have a method in place to monitor, test and update the applications and security measures used by an organization

A large part of each of those four areas is having the proper awareness of the associated cyber risk so that the limited time, money, and resources can be pointed in the proper direction.

That often starts at the top of an organization – with the board of directors.

### Using Cyber Risk Intelligence to Ensure Situational Awareness of the Relevant Threat Landscape

A FFIEC study released in November 2014 outlined threat intelligence as one of the key observations needing attention in order to mitigate today’s cyber risks.

Clearly, those in the C-suite and on the board need more information in order to close the “cyber gap” that has existed between them and the information security department. However, that reporting, whether it addresses internal security compliance or external threats or situational risk awareness, can be resource-intensive and lead to precious time being taken away from an already resource-strapped team.

Automated cyber risk reporting can keep the board informed while simultaneously saving the time, money and effort of manually creating spreadsheets, charts and other presentation materials.

Cyber risk intelligence overlays and aligns the data of an organization’s make-up on top of cyber threat data and is used to focus on making decisions and taking the right action.

---

**Cyber Risk Intelligence from the Top of the Organization Down**

“*The board or appropriate committee must oversee the development, implementation, and maintenance of the credit union’s information security program.*”

- NCUA Part 748, Appendix A

Duties include “assigning specific responsibility for implementing the program and reviewing reports prepared by management.”

While board members need not be experts, they should have high-level situational awareness of their organization’s cyber risk in order to answer a few “burning” questions:

- What threats are active and how might they impact our business unit goals?
- What is the likelihood of occurrence of those threats?
- What business process could be affected if an event occurs?
- What are the threat’s consequences?
- Have peers/competitors been impacted and if so how?
- Can we reduce the likelihood or consequence of a threat?
- Does the threat impact revenue, customer or product activities?
- How can the threat impact our regulatory posture?

It is crucial that staff play an important part by organizing relevant information to help inform the board, address threats, and provide feedback on the program so it can be continually improved.
Cyber risk intelligence should be used to help a credit union solve three key questions:

1. **How well is your company currently positioned?**

2. **How do you compare to others in your industry?**

3. **What people, process and technology is needed in order to reduce your risk exposure throughout all levels of the organization?**

Cyber risk intelligence allows an organization to address cybersecurity issues in the same way it uses other business intelligence metrics to make informed business decisions. It also helps to provide a common risk language so that the team can make better, more cost-effective decisions that address the most important threats and create long-lasting value.

Debunking the Threat Intelligence Myth: Is More Data Better?

A cybersecurity program should be based around one simple premise: understanding what cyber risks are facing an organization and then taking action to address high-risk risk areas in the best, most efficient way possible. In that sense, threat intelligence is not always about more data, but about better data.

In fact, many security teams report that they are overwhelmed with all the data at their fingertips, but what good is “intelligence” if it is not being utilized to better protect the organization, its customers and partners? It is like having an army full of soldiers but no generals surveying the landscape and providing the necessary direction and tactical guidance in order to succeed. This can lead to misplaced investments, slower reaction time, and increased cyber risk for an organization – credit unions can ill afford to fall into this trap.

Cyber risk intelligence can provide the necessary guidance so that smarter and more effective decisions can be made in a timely manner. This requires surveying the overall landscape as well as the organization’s corporate operations, customers, suppliers, brand reputation, and financials in order to identify the likelihood of a negative cyber event occurring and the potential consequences of that event.
Traditional Cybersecurity vs. Analytics-Driven Cyber Risk Intelligence

In the past, many cyber risks were viewed as a problem to be delegated to the IT department. However, as more services have come online and the cybercriminal world has developed its business model, those cyber risks have increased to the point where many organizations are finding this “risk gap” no longer acceptable. This shift in culture requires a different approach to cybersecurity and, ultimately, an organization’s risk.

<table>
<thead>
<tr>
<th>Traditional Cybersecurity</th>
<th>Analytics-Driven Cyber Risk Intelligence</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Technology issues are an “IT problem” and the board and IT rarely interact</td>
<td>• Focuses on business impact by connecting the server room to the board room</td>
</tr>
<tr>
<td>• Attempts to create a wall between any malicious actors and the organization’s data and network in order to protect everything equally</td>
<td>• Evaluates cyber risk areas and their impact in order to protect what’s most valuable and provide increased risk mitigation at a lower cost</td>
</tr>
<tr>
<td>• Detection-based focus – identifying and responding to threats after they happen</td>
<td>• Prevention-based focus – provides awareness so that risks can be addressed from the outset</td>
</tr>
<tr>
<td>• Has a security culture that is focused on compliance</td>
<td>• Security culture starts at the board and runs throughout the entire organization</td>
</tr>
<tr>
<td>• Often lacks high-level situational awareness around cyber risks</td>
<td>• Automated risk reporting monitors the threat landscape and provides awareness</td>
</tr>
<tr>
<td>• Security is often viewed as a wasted resource and does not connect to other business metrics</td>
<td>• Uses a business language to show how ongoing operational costs and investments support business activities</td>
</tr>
</tbody>
</table>

In short, an analytics-driven cyber risk intelligence approach takes a wide-angle view of relevant cyber event data in order to help piece together all the pieces of the puzzle and to provide the proper context. This approach is mindful that regulators, insurers and risk committees expect due diligence and due care in mitigating threats, but the approach goes beyond the typical “checkbox compliance” mentality and creates a level of cyber risk awareness and understanding that permeates throughout the entire organization, starting at the top.

Conclusion

When it comes to cybersecurity, credit unions and other small banks face a difficult situation. Despite having fewer resources, their customers expect a similar level of convenient, technology-driven services as the large commercial banks. This attempt to keep pace can lead to increased cyber risk exposure and a variety of potential negative effects including data breaches, service downtime, and brand damage.

However, not all cyber risks are created equal. Cyber risk intelligence can help organizations to understand those threats, prioritize their limited security resources so they address the right problem at the right time, and demonstrate the due diligence that investors, regulators and risk committees require. This can help to build a cybersecurity program that improves security without increasing labor and costs.
About SurfWatch Labs

SurfWatch Labs delivers powerful cyber risk intelligence analytics and applications through a business intelligence approach that helps organizations improve their long-term cyber resilience.

Created in 2013 by former US Government intelligence analysts, SurfWatch Labs solutions go beyond the low-level threat data and security tactics that organizations can drown in, by providing insights into cyber risks and their impact on key business operations. SurfWatch empowers customers to:

- Easily visualize and comprehend how cybercrime affects all aspects of the business
- Continuously monitor personalized cyber risk Key Performance Indicators (KPI's)
- Include cybersecurity as a strategic, foundational component of the business operation

SurfWatch Labs: Cyber In Sight. For more information, visit [www.surfwatchlabs.com](http://www.surfwatchlabs.com).

Contact us at:

info@surfwatchlabs.com

(866) 855-5444

Follow us at: