

# 2021 THIRD-PARTY RISK PULSE: CREDIT UNIONS & VENDOR ECOSYSTEMS

*Challenges, Pain Points & Lessons  
Learned from U.S. Credit Unions'  
Cyber Risk Landscape*



BLACK KITE

# TABLE OF CONTENTS

- 3 Introduction & Key Findings
- 4 Security Issue Analysis: Credit Unions
- 7 Financial Risk for Credit Unions
- 8 Security Issue Analysis: Third-Party Vendors
- 10 Financial Risk from Third-Party Vendors
- 11 Recap & Recommendations



# KEY FINDINGS

Estimated financial losses due to third-party cyber attacks could exceed \$1 million per event

86% of credit unions and 76% of vendors that service credit unions have breached employee credentials available on the Dark Web

66% of credit unions and 88% of vendors have not deployed the necessary configurations (such as DMARC record) to prevent email spoofing attacks

More than 70% of credit unions have at least one website with a login form that does not restrict excessive authentication attempts by deploying bot detection

## CREDIT UNION SIZES

*According to assets under management*

SMALL: < \$2B

MEDIUM: \$2B - \$9B

LARGE: > \$9B

# INTRODUCTION

Today, more than 5,200 credit unions with 122 million members operate in the United States alone<sup>[1]</sup>. Housing some of the largest databases of sensitive information, financial services are a prime target for opportunistic cybercriminals. Surfacing global regulations are now risk-driven, and are increasing the importance of accurate and continuous cyber risk monitoring.

This year, the National Credit Union Administration (NCUA) introduced the InTREx-CU examination solution to better evaluate credit unions' critical security controls. InTREx helps examiners and credit unions identify and remediate potential high-risk areas by identifying critical information security program deficiencies<sup>[2]</sup>

InTREx brings NCUA's IT and cybersecurity examination procedures in line with those used by the Federal Deposit Insurance Corporation (FDIC), the Federal Reserve System, and some state financial regulators to ensure consistent approaches apply to community financial institutions.

As part of the InTREx examination, participants will have to say whether they have assessed their cybersecurity risk and preparedness in the last 12 months. That means the bar for proper cybersecurity compliance is about to reach new heights. All credit unions will have to take a closer look at their cybersecurity posture and the available tools they have to detect, prevent, and correct risks and threats facing their organizations.

Black Kite analyzed 250 credit unions identified by the NCUA and 150 associated vendors<sup>[3]</sup> in terms of their cybersecurity posture and risk. Black Kite researchers examined these credit unions and their respective vendors to identify the most common security issues, as well as the estimated financial risk in the case of a cyber breach.

Deciphering what the latest cyber intelligence means and how to act on it adds to the list of unique challenges facing security professionals at credit unions that already includes:

- **Limited Resources**

Because credit unions are small-profit entities, the budgets allocated to operating expenses are limited. However, the likelihood of incurring a cyber breach is almost identical to high-profit enterprises. Therefore, credit unions that lack maturity in their security posture face higher consequences.

- **Increasing Regulations and Exposure**

Depending on the number of assets under management, regulatory principles and guidance (NCUA, CFPB, etc.) drive policies and procedures for credit unions, as well as increasing regulatory burdens and costs.

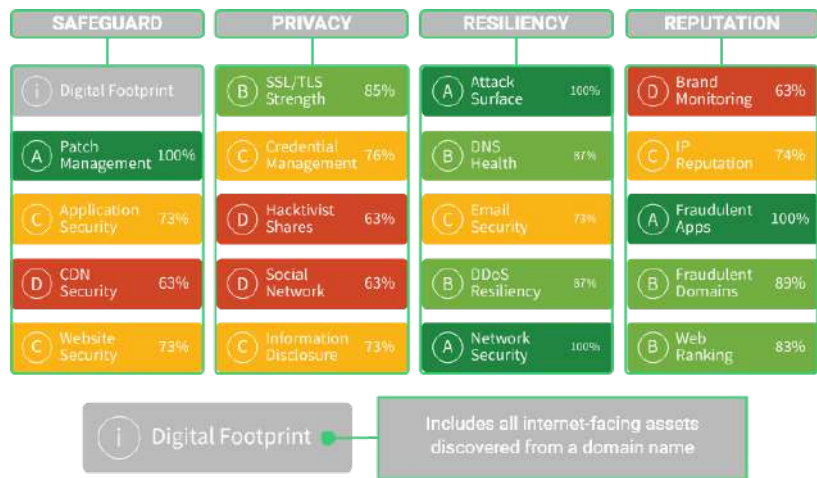
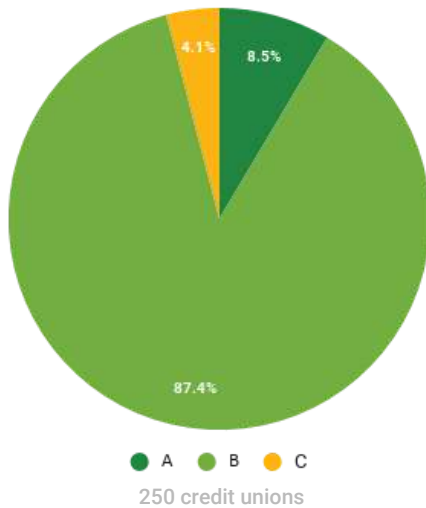
- **High Liability**

Adherence to regulatory requirements and industry best practices becomes more demanding every year. The more assets a credit union acquires, the more complex the annual audit of risk, controls, and response becomes.

# SECURITY ISSUE ANALYSIS: CREDIT UNIONS

Black Kite researchers leveraged the company’s cyber rating platform and open-source intelligence tools that hackers use to provide visibility into the cyber posture of credit unions. Black Kite yields the largest digital footprint with unique controls to eliminate false positives and provide relevant data. Simplified letter grades are assigned to allow risk professionals to clearly understand security issues and make better risk-based business decisions.

Credit Union Grade Distribution



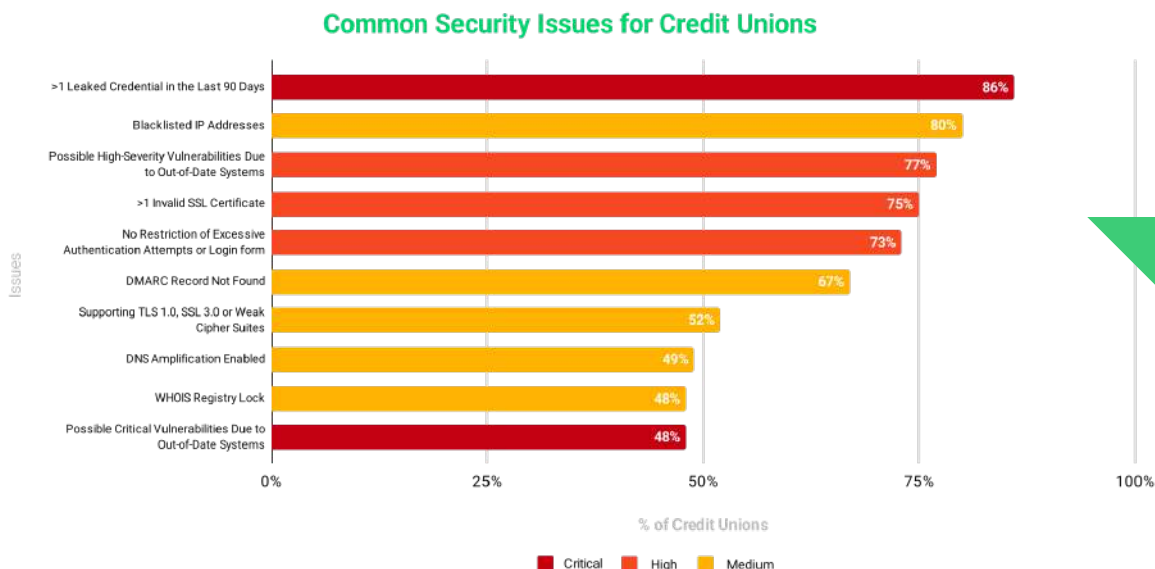
The Black Kite technical rating provides easy-to-understand letter grades and defensible data details behind 20 risk categories.

The average credit union security score consistently reflects a “B”, or “Good”, rating. Statistics show financial institutions are more diligent about their security posture due to frequent compulsory audits. Financial institutions also have more digital assets, which incur a higher number of vulnerabilities that need to be continuously monitored. With a relatively smaller digital footprint than most financial institutions and additional due diligence, credit unions typically reflect higher cyber rating scores.

- A Grade A**  
It would take world-class, state sponsored hackers to exploit.
- B Grade B**  
Skills of persistent, highly experienced hackers are required.
- C Grade C**  
Average to professional hackers are capable of exploiting.

- D Grade D**  
Beginner hacker practicing their skills.
- F Grade F**  
Script kiddies can hack (i.e. 6th Graders).

Although credit unions' cyber hygiene is in relatively good standing, the industry still faces **critical and highly severe issues** that could lead to significant cyber and financial risk.



**FINDING SEVERITY SCALE**

**CRITICAL: 9 - 10**  
**HIGH: 7 - 8.9**  
**MEDIUM: 4 - 6.9**

## 1. Patch Management

Due to out-of-date systems, **77% of credit unions have possible high-severity vulnerabilities while 44% have possible critical vulnerabilities.**

Out-of-date systems accessible by the internet may have vulnerabilities that are either related to the application servers or the application framework. They can be design flaws or implementation bugs that enable attackers to compromise the system itself or associated applications.

## 2. SSL/TLS Strength

SSL protocol ensures user information travels safely through the internet in a secure manner. For **75% of credit unions, at least one SSL certificate is invalid, incorrect, expired, or self-signed.**

Black Kite verifies both certificate-related issues (i.e, it is valid, present in the browser trust chains) and the configuration of cipher-suites. Credit union websites allow member logins and digital banking. Lacking SSL controls puts the credit union and members' credentials, financial information, and other sensitive data at risk.


## 3. Application Security

**72% of credit unions have at least one website with a login form that has no restriction of excessive authentication attempts, which can allow a human or an automated process, such as a bot, to infiltrate systems.**



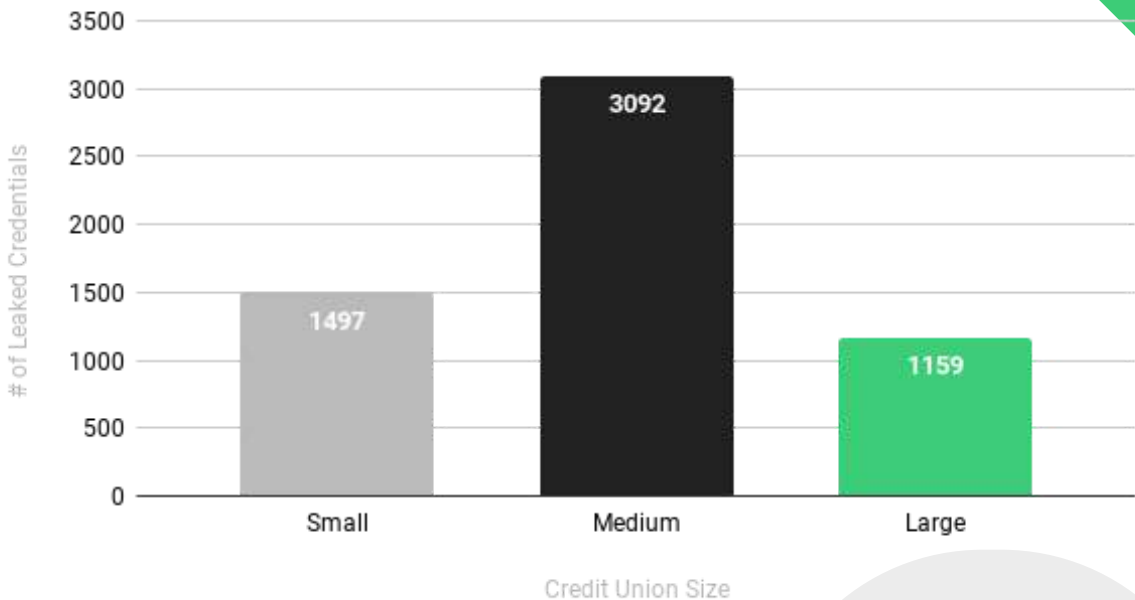
## 4. Credential Management

**86% of credit unions have had at least one leaked credential in the last 90 days.** Combined, **more than 5700 credentials were leaked** amongst the 250 credit unions examined. Leaked credentials are often a result of employees using their corporate email addresses to sign into external platforms. If the external platforms suffer a breach, the credentials become available through that platform as well—causing a ripple effect.



**MORE THAN 5,700 CREDIT UNION EMPLOYEE CREDENTIALS WERE LEAKED ON THE DARK WEB BETWEEN JANUARY - MARCH 2021**

### Leaked Credentials on the Dark Web

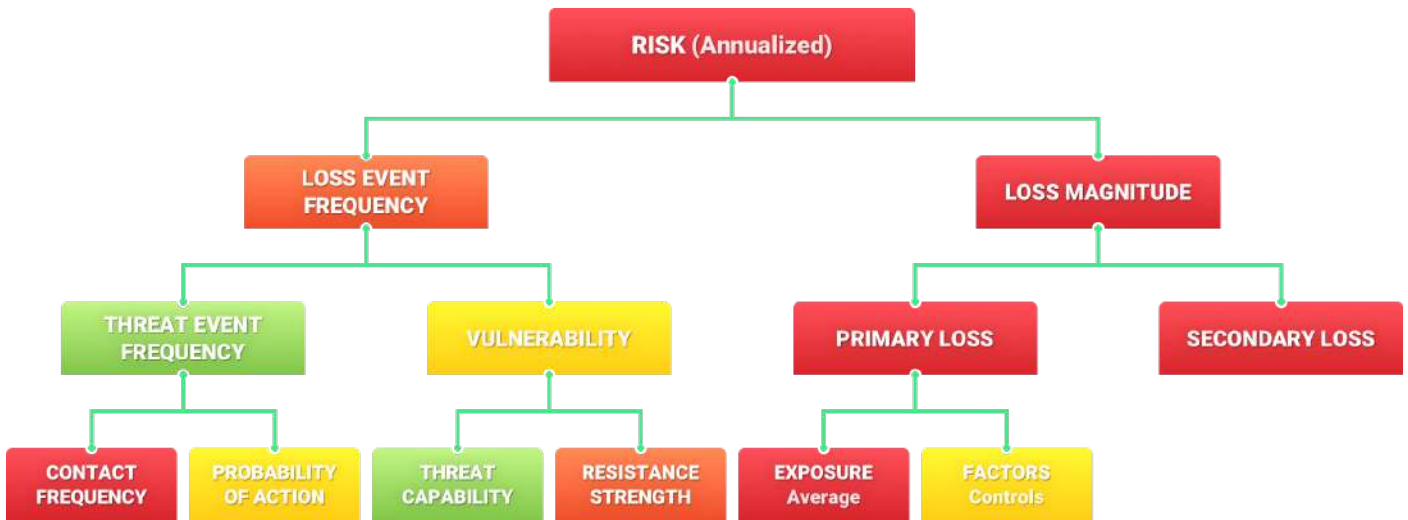


## 5. Email Security

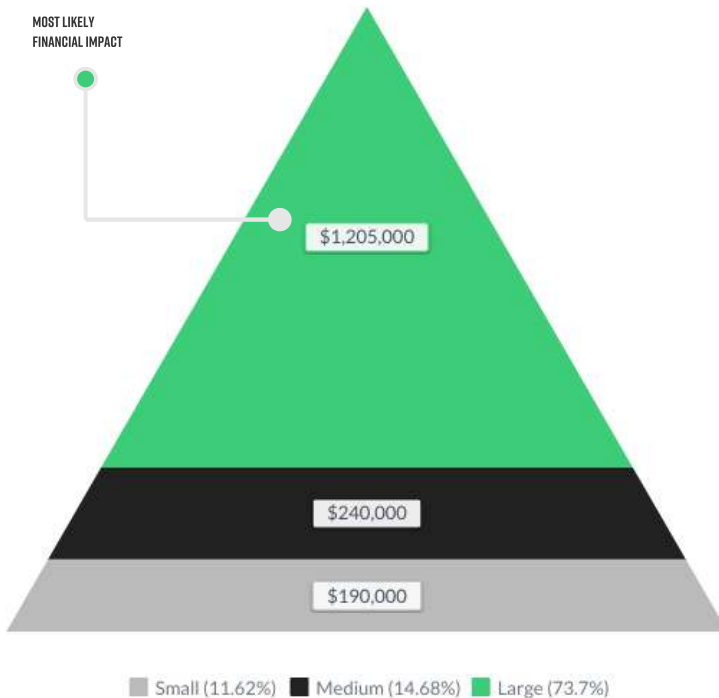
A DMARC policy is intended to combat certain techniques often used in phishing and email spam, such as emails with forged sender addresses that appear to originate from legitimate organizations. **66% of credit unions lack DMARC policy records**, leaving the door open for spam and phishing campaigns.

# FINANCIAL RISK FOR CREDIT UNIONS

Black Kite leverages the OpenFAIR™ methodology to transform cyber risk into financial terms. The FAIR calculation is an annual risk quantification that allows a company to estimate the cost of a cyber breach to the organization itself, or caused by a third party.



## Financial Risk for Credit Unions



### BLACK KITE'S TAKE

As expected, larger credit unions have a higher financial risk due to the increased assets under management. Credit Unions are member-owned financial cooperatives, therefore the risk to the organization is shared among its members. Large credit unions can tolerate a higher risk appetite, however a cyber breach could be devastating to members of smaller credit unions.

\*\*\* In the case a credit union experiences a cyberattack through a security loophole at the organization itself, the sensitive information of its members is exposed. Therefore, member sizes of each credit union are used as input parameters for each FAIR calculation.

# SECURITY ISSUE ANALYSIS: THIRD-PARTY VENDORS

One of the most common data breach amplifiers is third-party involvement, which **increased the total cost of a breach by over \$200,000<sup>[4]</sup>** in 2020.

Cybercriminals know that third parties often have access to, share, and/or maintain data critical to everyday operations. Third parties are considered “weaker links”, and are often leveraged as a means to infiltrate major organizations.

A total of **150 vendors<sup>[3]</sup>** from nine categories were examined:

## Credit Union Vendors Grade Distribution

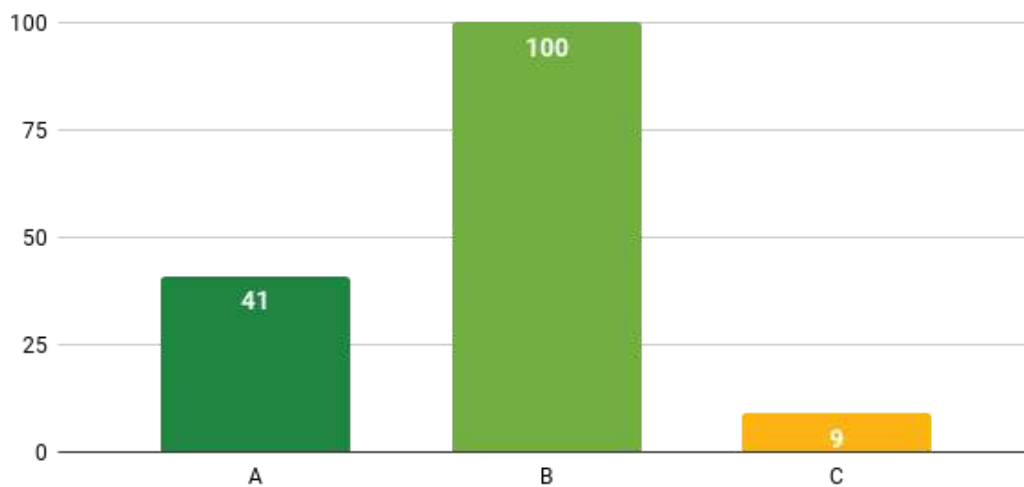


Fig 9. Vendor Grade Distribution

Vendor Function	Avg. Cyber Score
MARKETING	88.59
HR TRAINING	87.17
PROFESSIONAL SERVICES & CONSULTING	86.47
LENDING	86.33
OPERATIONS & TECHNOLOGY	86.28
DELIVERY CHANNELS	86.06
MEMBER SERVICES	84.83
CREDIT, DEBIT & CHECKING	84.07
MOBILE ONLINE SERVICES	84.00

Although the average cyber rating score is a “B”, or considered “Good”, several problematic vulnerabilities exist, including:

- Credential Management
- Patch Management
- SSL/ TLS Strength



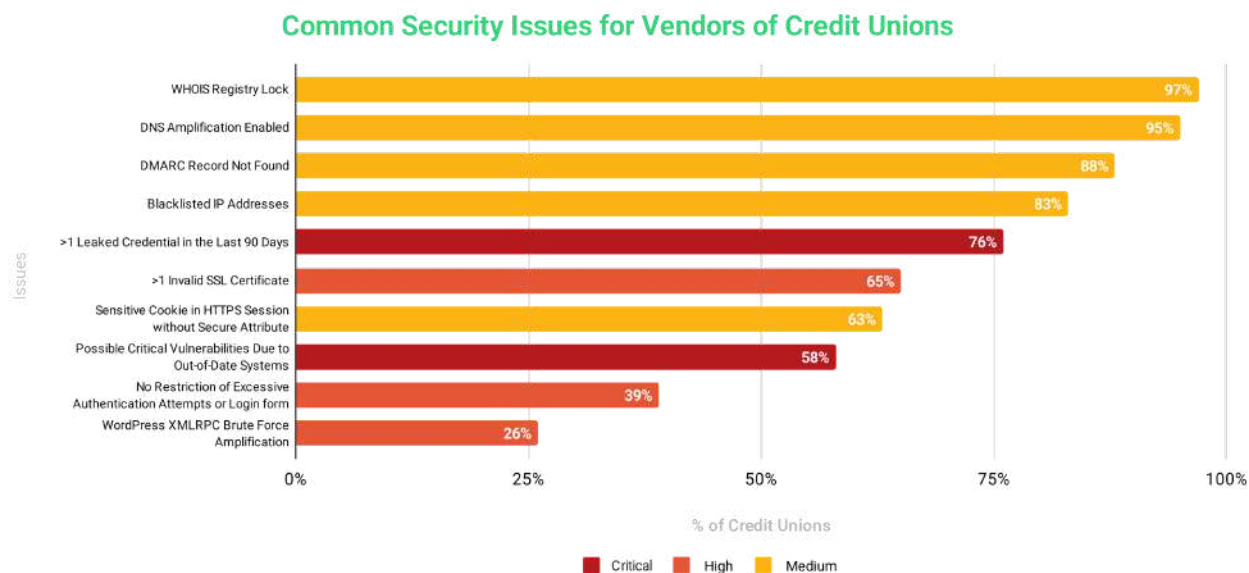


Fig 10. Common Security Issues among Vendors

## 1. DDoS Resiliency

DNS amplification allows threat actors to orchestrate amplified DDoS (Distributed Denial-of-Service) attacks where the attacker instructs bots or a botnet to send signals such as DNS queries with a forged source address to a legitimate server. This means a vendor's server does not have the proper controls against being used in an amplified DDoS attack. **95% of credit union vendors enable DNS amplification that might lead to amplified DDoS attacks.**

## 2. Email Security

**88% of credit unions vendors lack a DMARC policy record**, leaving the door open for spam and phishing campaigns through email spoofing.

## 4. IP Reputation

**83% of credit union vendors have at least one blacklisted IP address.** The most common abuse category among these lists is spam, however, there are also blacklists that focus on malware propagation, botnets, or even Tor exit nodes.

## 5. Credential Management

Breached credentials are a common denominator in the majority of sophisticated attacks. **76% of credit union vendors have at least one leaked credential in the last 90 days.**

## 6. SSL/TLS Strength

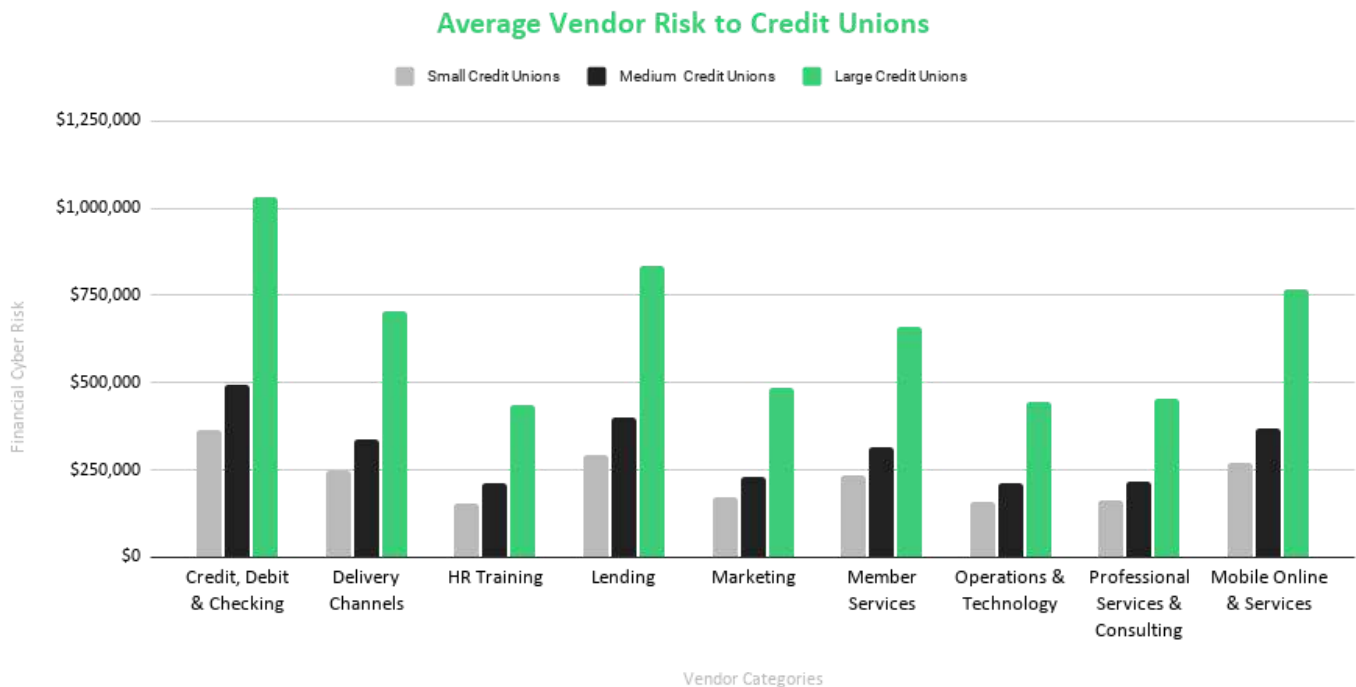
SSL protocol makes sure user information travels safely through the internet in a secure manner if the certificate is trusted. **At least one SSL certificate is invalid, incorrect, expired, or self-signed for 65% of credit union vendors.**

# FINANCIAL RISK FROM THIRD-PARTY VENDORS

## WHAT'S THE RISK?

When it comes to vendors or third parties, business executives care about more than the cyber posture of their vendors. Instead, they want to know whether there could be an intolerable cost if they engage in business with any given organization. With **an average breach costing organizations a total of \$3.86 million**, it's clear as to why that's the case.<sup>[4]</sup>

Black Kite researchers conducted a "Financial Impact Rating" to derive the estimated financial risk of a third party breach to credit unions today.



**Credit, debit and checking, lending, and mobile online service vendors pose the highest risk among the nine categories of vendors.**

## BLACK KITE'S TAKE

It's critical to be just as diligent with third parties as you are with protecting your own organization from cyber threats. A company's cyber posture is only as strong as its weakest link.

# RECAP & RECOMMENDATIONS

## Beware of Attack Vectors

As discussed earlier in this report, credit unions experience commonalities when it comes to security issues. Breached credentials and misconfigurations in email security leave room for certain attack vectors (i.e phishing and spamming). A phishing attack on an employee serves as an insertion point to many other sophisticated attacks, such as APT or ransomware. At the end of the day, thousands of members' sensitive information can be at risk due to a simple vulnerability.

## Continuous Oversight on Vendor Ecosystems

The term "continuous oversight" has been overused in third party risk monitoring contexts, convoluting its real meaning. Point-in-time assessments, such as penetration tests and questionnaires, are lengthy and time-consuming and do not display the vendor's security performance trends or signals that a breach is likely. Continuous monitoring is only possible with security automation, which allows you to be alerted to any emerging vulnerability to the credit union or associated vendor.

## GLOSSARY

**Credit Union:** Member-owned financial cooperative, controlled by its members and operated on a not-for profit basis.

**OpenFAIR™:** Factor Analysis of Information Risk (FAIR) calculates the estimated financial impact in the case of a cyber breach.

**Risk:** Probable frequency and probable magnitude of future financial loss.

## Adopt a Risk-Aware Approach for Vendor Ecosystems

Financial services face regulatory requirements demanding detailed enterprise risk assessment processes. However, the third-party assessment process is designed to assess security through questionnaires or surveys, regardless of the vendor's industry, and/or criticality. This report clearly demonstrates certain vendor categories pose various levels of risk to credit unions. Regardless of which tools or framework a credit union leverages, industry best practices come in handy to calculate accurate risk figures in vendor risk assessments, including:

- Classify vendors according to their industry or the services they provide
- Keep track of sensitive data shared with each vendor
- Include the number of sensitive records shared with the vendors as parameters to the risk management methodology

## REFERENCES

- [1] CUNA. *Credit Union Snapshot*. Retrieved March 2021 from <https://www.cuna.org/Research-And-Strategy/Credit-Union-Data-And-Statistics/>
- [2] Tandem. *ACET vs. InTReX-CU: Expected Changes in the NCUA Examination Process*. Retrieved March 2021 from <https://tandem.app/blog/acet-vs-intrex-cu>.
- [3] CreditUnions.com. Retrieved March 2021 from <https://www.creditunions.com>
- [4] IBM. *Cost of a Data Breach Report (2020)*. <https://www.ibm.com/security/digital-assets/cost-data-breach-report/#/>.

LOOKING FOR A LITTLE SOMETHING EXTRA?

REQUEST A DEMO



Black Kite, Inc. is led by a team of innovative thinkers and cybersecurity experts. Our goal is to provide you with the most accurate and comprehensive cyber rating results, with the fewest false positives. Our people and platform do the work for you, highlighting risk areas that require attention and automating feedback on how to address them. We're committed to serving our customers — and we're proud of our five-star customer service rating.

## CONTACT

120 St. James Ave  
Boston, MA 02116  
+1 (571) 335-0222  
info@blackkitech.com

[www.blackkitech.com](http://www.blackkitech.com)