

Michigan Credit Union League & Affiliates

Annual Convention and Exposition

Helping Credit Unions Serve, Grow and Remain Strong

#mculace

Data Breaches and Cyber Liability

June 5, 2014 | 1:30 – 3:00 pm

Ken Otsuka

Sponsored by



www.mcul.org

CUP-9053301.1-0414-0516 ©CUNA Mutual Group, 2014 All Rights Reserved



www.uniteforgood.org

Common Purpose. Uncommon Commitment.

Data Breaches and Cyber Liability

Presented by: Ken Otsuka

Credit Union Protection Risk Management

CUNA Mutual Group



CUP-9053301.1-0414-0516 ©CUNA Mutual Group, 2014 All Rights Reserved

Common Purpose. Uncommon Commitment.

Data Breaches – How do they Happen?

- Network hackers
- Employee negligence / theft
- Lost / stolen laptops, backup tapes / disks and other data-bearing mobile devices
- Vendor leaks
- Electronic or non-electronic data



Data Breaches

- Financial risk
- Compliance / Legal risk
- Reputation risk



A data breach can result in more than lost data. It can damage the credit union's reputation, shake member trust, and cost tens of thousands to repair.

Agenda

- Fraud and data breach studies
- Data breach insurance claims study – NetDiligence
- Overview of NCUA Rules and Regulations Part 748
- Best practices for securing members' confidential data
- Employee mistakes
- Distributed denial of service (DDoS) attacks
- Training

2012/2013 Kroll Annual Global Fraud Report

Data theft is a leading form of fraud

Chart 1. Percentage of companies affected by the following frauds

	2012	2011
Theft of physical assets	24%	25%
Information theft	21%	23%
Management conflict of interest	14%	21%
Vendor, supplier or procurement fraud	12%	20%
Internal financial fraud	12%	19%
Corruption and bribery	11%	19%
Regulatory or compliance breach	11%	11%
IP theft	8%	10%
Market collusion	3%	9%
Money laundering	1%	4%

Source: Kroll's 2012/2013 Global Fraud Report

2012/2013 Kroll Annual Global Fraud Report

Complacency could be the biggest threat

Chart 2. Proportion of all companies describing themselves as highly or moderately vulnerable to the following frauds, this year and last year

	2012	2011
Information theft	30%	50%
Regulatory or compliance breach	28%	41%
Theft of physical assets	26%	46%
Internal financial fraud	26%	38%
Vendor, supplier or procurement fraud	24%	42%
Corruption and bribery	24%	47%
Management conflict of interest	23%	44%
IP theft	21%	40%
Market collusion	15%	31%
Money laundering	13%	25%

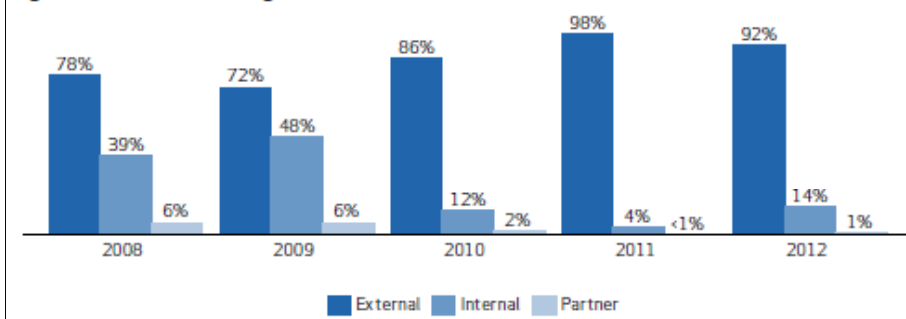
Source: Kroll's 2012/2013 Global Fraud Report

2013 Verizon Data Breach Investigations Report

Threat Agents

- **External threats** – originate from outside of the organization (hackers, organized crime, etc.)
- **Internal threats** – includes employees and independent contractors
- **Partner threats** – third party vendors used by the organization

Figure 9: Threat actor categories over time



Source: 2013 Verizon Data Breach Investigations Report

NetDiligence: Cyber Liability & Data Breach Insurance Claims

2013 NetDiligence® Cyber Liability & Data Breach Claims Study

- Per breach costs
 - Average payout: \$954,253
 - Claim range
 - Typical claim
 - Per record costs
 - Average cost per record: \$6,790
 - Average records lost: 2.3 million
 - Crisis service costs
 - Average cost of crisis services: \$737,473
 - Crisis services include the cost of forensics, legal counsel, notification and credit monitoring
 - Legal costs
 - Average cost of legal defense: \$574,984
 - Average cost of settlement: \$258,099
- | |
|---|
| Median payout: \$242,500 |
| \$2,500 to \$20 million |
| \$25,000 to \$400,000 |
| Median cost per record: \$107.14 |
| Median records lost: 1,000 |
| Median cost of crisis services: \$209,625 |
| Median cost of legal defense: \$7,500 |
| Median cost of settlement: \$22,500 |

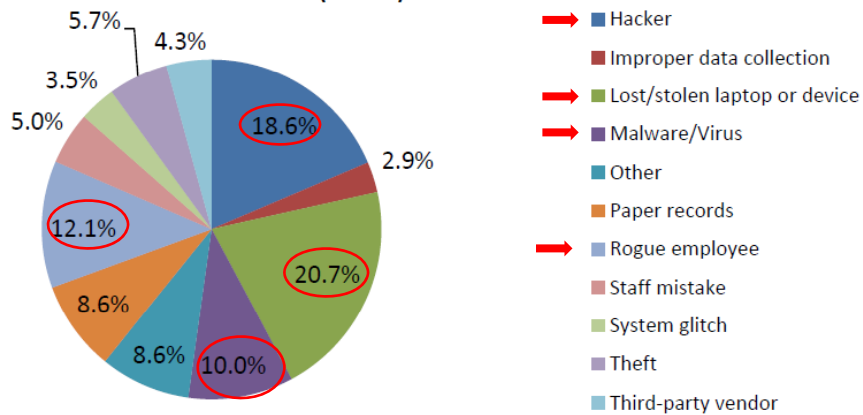
Source: NetDiligence 2013 Cyber Liability & Data Breach Claims Study



Common Purpose. Uncommon Commitment. 9

NetDiligence Cyber Liability & Data Breach Insurance Claims

Percentage of Claims by Cause of Loss
(N=140)



Source: NetDiligence 2013 Cyber Liability & Data Breach Claims Study



Common Purpose. Uncommon Commitment. 10

Why the Problem?

The Internet is an open network

- Credit unions collect, store and share a vast amount of member confidential data
- Websites are porous and need constant care
 - Hardening and patching
- Intrusion detection is weak
- Cyber thieves take advantage of human error
 - Unchanged default settings
 - Failing to install patches
 - Failing to protect laptops
 - Improper disposal of paper records
 - Weak passwords

Rank	Password
1	123456
2	12345
3	123456789
4	Password
5	iloveyou
6	princess
7	rockyou
8	1234567
9	12345678
10	abc123

Source: Imperva - Consumer Password Worst Practices

Common Weak Spots



IDS or 'Intrusion Detection Software' (bad guy alert system)

- > Studies show 70% of actual breach events are NOT detected by the victim-company, but by 3rd parties (many more go undetected)
- > Federal Trade Commission and plaintiff lawyers often cite 'failure to detect'



Patch Management challenges

- > All systems need constant care (patching) to keep bad guys out
- > Many organizations don't have staff to stay on top of this
- > Lack of time: Gartner Group estimates that "IT Managers spend an average of 2 hours per day managing patches."



Encryption of private data

- > Problem spans all sizes & sectors
- > ITRC (Identity Theft Resource Center): only 2.4% of all breaches had 'encryption'
- > Issues include budgets, complexities and partner systems
- > Key soft spots: data 'at rest' for database & laptops (lesser extent)
- > Benefits: safe harbor (usually)

Source: CyberRisk Hub, NetDiligence®

Information Security Program

- Access controls to computer systems containing member information
 - Limit access to authorized employees only
 - User IDs and passwords
 - Authentication methods
 - Data loss prevention tools
- Physical access restrictions to computer systems
- Encryption of member information in electronic format
 - In-transit
 - Stored on the network or systems
 - Stored on external media
- Internal controls
 - Dual controls, segregation of duties and employee background checks
- Network/systems protection
 - Firewall
 - Antivirus software
 - Intrusion detection
 - Vulnerability assessments
- Third-party reviews of network security
- Response programs
- Proper disposal of records containing member information
- Employee training
- Third party service providers
 - Due diligence is critical

Source: NCUA Letter No. 06-CU-07 – IT Security Compliance Guide for Credit Unions

Best Practices

Protect data wherever it is located

- ✓ At rest
- ✓ In motion
- ✓ In use

- Operating system patches
- Encryption
 - Data residing on the network and workstation hard drives
 - Data residing on mobile devices
 - Laptops
 - External storage media
 - Smartphones and tablets
 - Data transmitted over the Internet and in emails
- Intrusion detection system
- Endpoint security
 - Protects the access points to credit union networks
 - Includes typical protections such as a firewall, antivirus software, anti-spam controls, website content filtering, etc.

Best Practices

Protect data wherever it is located

- ✓ At rest
- ✓ In motion
- ✓ In use

- Data loss prevention (DLP) solutions
 - Identifies, monitors, and protects data at rest, in motion, and in use
 - DLP tools allow credit unions to see which databases, file servers, desktops and laptops hold sensitive data
 - Identifies when someone is transmitting data via email or downloading to external storage devices
- Disable / lockdown workstation USB ports and CD Rom drives
 - Helps prevent insider theft of confidential member data
- Secure paper records

Best Practices

Protect data wherever it is located

- ✓ At rest
- ✓ In motion
- ✓ In use

- Accessing network/systems remotely
 - Telecommuters working from home/third-party vendors

Remote Access Best Practices

- Prohibit remote employees from using home computers to access network
 - Unless virtual desktop is used
 - Alternative is to issue remote employees laptops protected with security software
- Establish a virtual private network (VPN)
 - A VPN is a network that uses the Internet to provide remote employees with secure access to the credit union's network
- Prohibit employees from using unsecure wireless networks (public Wi-Fi)
- Require multifactor authentication – not just usernames and passwords
 - One-time-password tokens
 - Plug-in tokens

Planning and Responding

Incident Response Plan

- Written incident response plan to address incidents of unauthorized access to member information
- Required by NCUA
(Rules and Regulations Part 748, Appendix B)
- Minimum requirements include:
 - Assess nature and scope of incident
 - Identify what member information systems and the member information breached
 - Take appropriate action to contain and control the incident to prevent further unauthorized access to or use of member information
 - Notify NCUA Regional Director or appropriate state supervisory authority
 - File Suspicious Activity Report
 - Notify appropriate law enforcement agency
 - Notify impacted members

Suggested Practices

- Contain the breach
- Activate incident response team
- Analyze the breach
 - Record all information relevant to breach
 - Who, what, when and how
 - Forensics
- Contact breach coach / legal counsel specializing in privacy issues
**Can be done immediately after discovery*
- Notify CUNA Mutual Group of potential loss
- Notify regulator
- File Suspicious Activity Report
- Analyze legal implications
 - Identify federal, state and local laws / regulations impacted
 - State data breach notification and timing requirements

Mobile Devices: Laptops / Tablets / Smartphones

- Credit union issued versus employee use of personal devices
 - Both should be secured
- If personal mobile devices are used for business purposes secure the business side of the device (sandboxing)
 - Good Technology
 - MaaS360

Common BYOD comment:
"We don't want to inconvenience management by requiring mobile device security."

Mobile Devices Used for Business Purposes

- Antivirus software
- Password protect the device/time-out feature to lock the device
- Remote wipe capability
- Prohibit employees from storing confidential member data to the device
 - ✓ If it is necessary to store such data on the device, the data should be encrypted
- Encrypt confidential member data transmitted in emails
- Prohibit employees from downloading app's – should be done by IT department
- Prohibit employees from downloading software without IT department's approval

Employee Mistakes

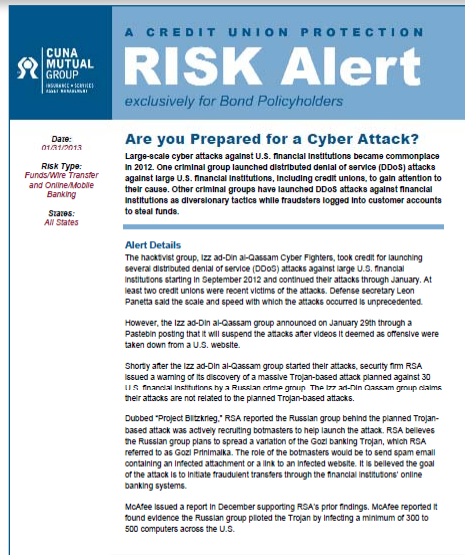
- Credit union employee accidentally published a file on the credit union's public-facing website
 - File contained member names, addresses, Social Security numbers, account numbers and account passwords
- Credit union employee accidently emailed a spreadsheet to a member
 - Spreadsheet contained member names and account numbers

This is for educational purposes only.

Distributed Denial of Service (DDoS) Attacks

In the news...

- An Islamic group, Izz ad-Din al-Qassam, started its DDoS attacks against some of the nation's largest banks in September 2012
 - At least 2 credit unions were attacked
 - Disrupted the institutions' online banking service preventing customers from logging into their account



CUNA MUTUAL GROUP
A CREDIT UNION PROTECTION
RISK Alert
exclusively for Bond Policyholders

Date:
01/23/2013

Risk Type:
Funds/Wire Transfer
and Online/Mobile
Banking

States:
All States

Are you Prepared for a Cyber Attack?

Large-scale cyber attacks against U.S. financial institutions became commonplace in 2012. One criminal group launched distributed denial of service (DDoS) attacks against large U.S. financial institutions, including credit unions, to gain attention to their cause. Other criminal groups have launched DDoS attacks against financial institutions as diversionary tactics while fraudsters logged into customer accounts to steal funds.

Alert Details

The hacktivist group, Izz ad-Din al-Qassam Cyber Fighters, took credit for launching several distributed denial of service (DDoS) attacks against large U.S. financial institutions starting in September 2012 and continued their attacks through January. At least two credit unions were recent victims of the attacks. Defense secretary Leon Panetta said the scale and speed with which the attacks occurred is unprecedented.

However, the Izz ad-Din al-Qassam group announced on January 29th through a PasteBin posting that it will suspend the attacks after videos it deemed as offensive were taken down from a U.S. website.

Shortly after the Izz ad-Din al-Qassam group started their attacks, security firm RSA issued a warning of its discovery of a massive Trojan-based attack planned against 30 U.S. financial institutions by a Russian crime group. The Izz ad-Din al-Qassam group claims their attacks are not related to the planned Trojan-based attacks.

Dubbed "Project Blitzkrieg," RSA reported the Russian group behind the planned Trojan-based attack was actively recruiting botmasters to help launch the attack. RSA believes the Russian group plans to spread a variation of the Zeus banking Trojan, which RSA referred to as Goot Priminka. The role of the botmasters would be to send spam email containing an infected attachment or a link to an infected website. It is believed the goal of the attack is to initiate fraudulent transfers through the financial institutions' online banking systems.

McAfee issued a report in December supporting RSA's prior findings. McAfee reported it found evidence the Russian group piloted the Trojan by infecting a minimum of 300 to 500 computers across the U.S.

DDoS Attacks – Diversionary Tactics

- Cyber crime groups may launch a DDoS attack as a diversionary tactic for concurrent fraudulent activities
 - Theft of member data
 - Theft of member funds via online banking
 - Referred to as account takeovers
- Employees are distracted by the DDoS attacks
 - Fail to notice unauthorized transfers initiated by the thieves and / or unauthorized access to network / systems



A CREDIT UNION PROTECTION

RISK Alert

exclusively for Bond Policyholders

Online Banking Risks and Controls
[Download the white paper](#)
(Protection Resource Center Access Required)

RSA Warns of Massive Attacks on 30 U.S. Banks
 Security firm, RSA, recently posted a blog that details its discovery of a planned cyber attack to be launched against 30 U.S. banks. RSA reported the attack is planned for this fall and will involve distributing a banking Trojan, dubbed "Gozi Prinimalka," through approximately 100 botmasters.



A CREDIT UNION PROTECTION

RISK Alert

exclusively for Bond Policyholders

Massive Cyberheist Planned against U.S. Financial Institutions
 RSA, a security firm, issued a warning in October of a planned attack on 30 U.S. financial institutions. McAfee recently issued a report supporting RSA's prior findings. The attack, which is planned for this spring, has been coined Project Blitzkrieg. The objective is to steal money from accounts at the financial institutions by compromising online banking login credentials.


Date:
12/17/2012

Risk Type:
Online/Mobile Banking

States:
All States

FFIEC's Joint Statement on DDoS Attacks

- Maintain an ongoing program to assess information security risks
- Monitor website traffic to detect attacks
- Activate incident response plan if a DDoS attack is suspected
- Ensure sufficient staffing for the duration of the DDoS attack
- Information sharing
- Evaluate any gaps in the response following the attack



A CREDIT UNION PROTECTION

RISK Alert

exclusively for Bond Policyholders

Date:
04/28/2014

Risk Type:
Other

States:
All States

FFIEC's Joint Statement on DDoS Attacks
 The Federal Financial Institutions Examination Council (FFIEC) recently issued a joint statement, Distributed Denial-of-Service (DDoS) Cyber-Attacks, Risk Mitigation, and Additional Resources, warning financial institutions of the risks associated with continued DDoS attacks. The FFIEC expects all financial institutions to address DDoS attacks in their information security and response plans.

Details
 Large-scale DDoS attacks against U.S. financial institutions became commonplace in 2012. One criminal group launched DDoS attacks against several large U.S. financial institutions, including credit unions, to gain attention to their cause. Other criminal groups launched DDoS attacks against financial institutions as diversionary tactics to conceal other concurrent fraudulent activities, such as account takeovers through online banking or a data breach.

DDoS attacks have become more powerful, easily taking down websites due to the growing trend for cyber thieves to use web servers as part of their botnet. In 2012, the hacktivist group, Izz ad-Din al-Qassam Cyber Fighters (Cyber Fighters), deployed web servers in their botnet (referred to as Blood) to launch their attacks. Web servers have significantly more computing and networking capability than a typical home computer making them an ideal choice for the cyber-thief to include in the botnet. This allowed Cyber Fighters to successfully launch DDoS attacks against six financial institutions simultaneously in March 2013. Security experts indicated these attacks used a fraction of the botnet's capabilities.

A "bot" is a computer (or web server) under the control of a cyber-thief. A "botnet" is a network of bots under the control of a cyber-thief.

FFIEC's Joint Statement on DDoS Attacks
 The FFIEC expects all financial institutions to address DDoS readiness as part of ongoing information security and incident response plans. The FFIEC expects all financial institutions to take the following steps:

Security Awareness Training

- Must be addressed in the credit union's information security program
- All employees should receive training on at least an annual basis
- The goal is to change employee behavior to reinforce good data security practices

Session Summary

- Information theft is one of today's most common forms of fraud
- Given the financial, legal, and reputational risks of a data breach -- failing to prepare can be disaster
- Take proactive steps to prevent incidents from occurring in the first place
- Protection Resource Center
@ www.cunamutual.com



Questions & Answers



Ken Otsuka, CPA
Senior Consultant - Risk Management
CUNA Mutual Group
Email: kenneth.otsuka@cunamutual.com



Disclaimer

This presentation was created by the CUNA Mutual Group based on our experience in the credit union and insurance market. It is intended to be used only as a guide, not as legal advice. Any examples provided have been simplified to give you an overview of the importance of selecting appropriate coverage limits, insuring-to-value and implementing loss prevention techniques. No coverage is provided by this publication, nor does it replace any provisions of any insurance policy or bond.

Credit Union Loss Scenarios – Case Studies

The credit union loss scenario claim study examples do not make any representations that coverage does or does not exist for any particular claim or loss, or type of claim or loss, under any policy. Whether or not coverage exists for any particular claim or loss under any policy depends on the facts and circumstances involved in the claim or loss and all applicable policy language.

CUNA Mutual Group is the marketing name for CUNA Mutual Holding Company, a mutual insurance holding company, its subsidiaries and affiliates. Insurance products offered to financial institutions and their affiliates are underwritten by CUMIS Insurance Society, Inc. or CUMIS Specialty Insurance Company, members of the CUNA Mutual Group. Some coverages may not be available in all states. If a coverage is not available from one of our member companies, CUNA Mutual Insurance Agency, Inc., our insurance producer affiliate, may assist us in placing coverage with other insurance carriers in order to serve our customers' needs. For example, the Workers' Compensation Policy is underwritten by non-affiliated admitted carriers. CUMIS Specialty Insurance Company, our excess and surplus lines carrier, underwrites coverages that are not available in the admitted market. Data breach services are offered by Kroll, a member of the Ategrity family of businesses. Cyber liability may be underwritten by Beazley Insurance Group.

This summary is not a contract and no coverage is provided by this publication, nor does it replace any provisions of any insurance policy or bond. Please read the actual policy for specific coverage, terms, conditions, and exclusions.



Common Purpose. Uncommon Commitment.