



19 MAY 2016

# MANAGING CYBER RISK: THE HUMAN ELEMENTS OF CYBERSECURITY



CHRIS FURLOW  
PRESIDENT  
RIDGE GLOBAL  
[cfurlow@ridgeglobal.com](mailto:cfurlow@ridgeglobal.com)  
[www.ridgeglobal.com](http://www.ridgeglobal.com)



World Council  
of Credit Unions



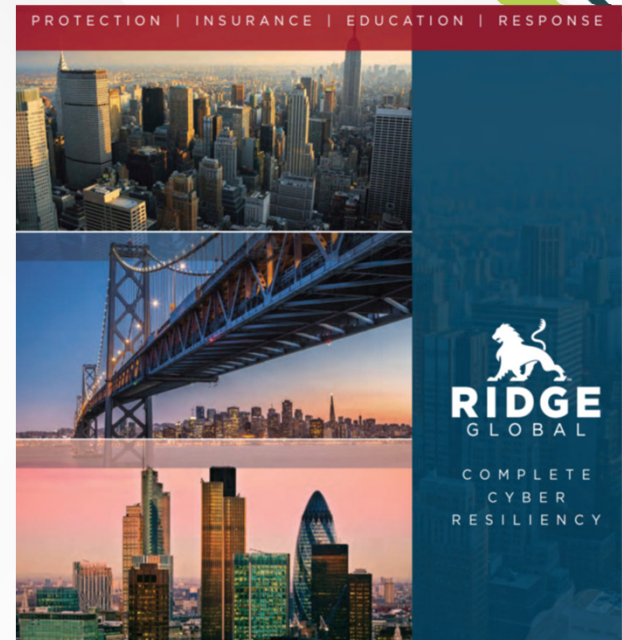
*Irish League*  
of Credit Unions



## ABOUT RIDGE GLOBAL

Ridge Global is the risk management advisory firm led by Gov. Tom Ridge, the first US Secretary of Homeland Security. Ridge Global works with companies and their executives around the world to reduce enterprise cyber risk and to build more resilient enterprises.

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

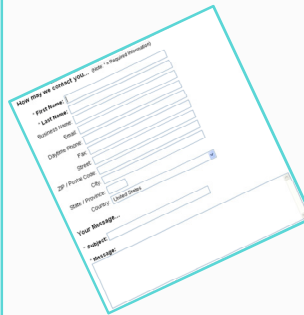


## KEY CONCEPTS

- ☐ Recognize the importance of human factors in cyber security
- ☐ Control what you can control to reduce risk
- ☐ Focus on People & Processes as well as Technology
- ☐ Training and education are critical to a cyber resilient culture
- ☐ Cybersecurity is a Team Sport--Don't forget your members



# CHALLENGE FOR CUSTOMER / MEMBER-ORIENTED ORGANIZATIONS



As technology makes the lives of your members more **more convenient**, it also has the potential to make them **more vulnerable**.





## OF, FOR, AND BY THE PEOPLE

**Technology is developed by people**  
**Technology is made for people**  
**Technology is administered by people**

**That means there will be RISK,  
but it can be reduced.**





## SOCIAL ENGINEERING: “DIGITAL DECEPTION”



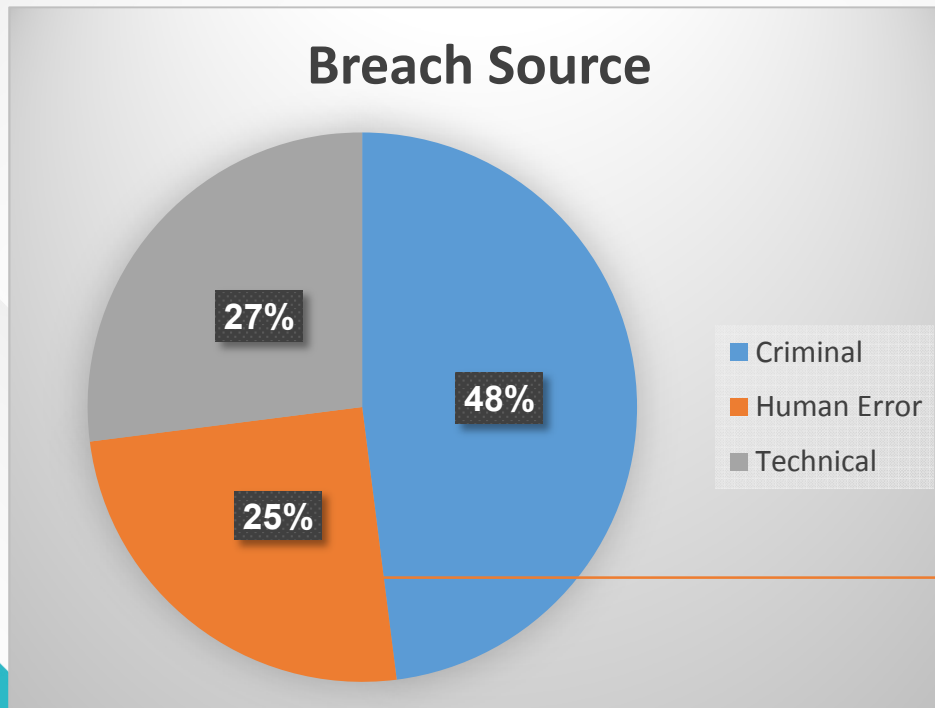
Prevalent technique of criminal organizations

Posing as or leveraging a trusted organization in order to trick individuals into surrendering passwords, sensitive data, financial or personally identifiable information.

Examples: Phishing, Spearphishing (targeted phishing), “Watering holes”

# THE HUMAN FACTOR

Ponemon/IBM 2016 Cost of Data Breach Report:



**“NEGLIGENT EMPLOYEES  
OR CONTRACTORS”**



# THE HUMAN CONDITION

In addition to fighting the technological weapons of the nefarious actor of which we are familiar (the embedded malicious code, the virus, etc.), we are just as challenged by those traits we find embedded in the Human Condition:

**Nescience**

**Curious**

**Apathy**

**Hubris**



# CYBERSECURITY AND RESILIENCE: DEFENSE-IN-DEPTH

Defense-In-Depth originally a military strategy to “buy time” when impossible to prevent attack by a potentially overwhelming adversary

NSA applied to digital domain:

- ☐ Establish layers of defense
- ☐ Allow time to identify intruders and mitigate
- ☐ Build redundancies and **resilience**



# THE NIST FRAMEWORK

## NIST

[www.nist.gov/cyberframework](http://www.nist.gov/cyberframework)

### Framework Core Functions

Identify

Protect

Detect

Respond

Recover

- Public-Private Collaboration led through the Commerce Department's National Institute of Standards and Technology (NIST).
- Result of E.O. 13636 signed by President Obama in 2013.
- After a year of public-private sector engagement, the Framework was released in Feb. 2014

*"Organizations can use the framework to **determine their current level of cybersecurity**, **set goals** for cybersecurity that are in sync with their business environment, and **establish a plan** for improving or maintaining their cybersecurity. It also offers a methodology to **protect privacy and civil liberties** to help organizations incorporate those protections into a comprehensive cybersecurity program."*

Source: <http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm>



# PPT: BUILDING BLOCKS FOR A CYBER SECURE & RESILIENT ORGANIZATION

**People**

**Processes**

**Technology**



# Technology

Do you utilize firewalls as well as anti-virus and anti-malware software?

Are these technologies kept up to date?

What monitoring capabilities do you employ?

Do you encrypt data?

## Processes

Do you have enterprise cybersecurity policies in place?

Do your onboarding/off-boarding/termination procedures include cyber elements?

Do you have established procedures for allowing access to your networks and infrastructure?

Do you have plans and procedures for emergency response?



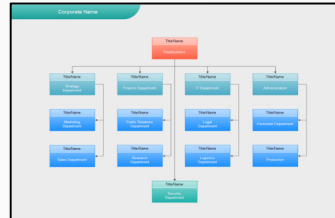
# People

Do you have a culture for cybersecurity?

Are roles and responsibilities and their priorities defined?

Does your org chart reflect the importance of cybersecurity to your organization?

# LEVERAGE THE ORG CHART



Do you have a CIO/CISO?

Do you have someone designated?

Is it a full-time position?

Where is your IT security leadership on the org chart?

Are they lost in middle management?

How often do senior leaders engage them?

# MISSING LINK: CYBER EDUCATION



## C-Suite & Board

C-Suite & Board members understand critical concepts for leading a culture of resiliency backed by prioritized resources



## Managers (Business Units, Facilities)

Mid-level Managers  
Both technical and business unit managers are trained in leading cyber resilience within their areas of responsibility



## All Enterprise Users

All end-users are trained regularly on cyber policy and risk-avoidance

**A Culture of Cybersecurity & Resilience Across the Enterprise**





# EDUCATION & TRAINING QUESTIONS

## C-Suite & Board

Do C-Suite and Board Members lead the culture by example?

Do they receive basic cyber training and adhere to cyber policies like other employees?

Do C-Suite and Board executives clearly understand enterprise roles and responsibilities—particularly in regard to managing key relationships and decision-making in crisis?

Do they participate in exercises?



# EDUCATION & TRAINING QUESTIONS

**Managers  
(Business Units,  
Facilities)**

Do managers understand organizational cyber policies?

Do they know how to enforce them in a positive manner?

Do they know how to look for insider threats?

Do they understand the importance of monitoring third-part access  
To your networks (vendors, partners, consultants, etc.)

Do they understand the important links between physical and  
cybersecurity?



# EDUCATION & TRAINING QUESTIONS

All Enterprise Users

Do employees understand their responsibilities when operating on your systems?

Are policies in place to outline appropriate cyber hygiene, behavior and, in the case of a breach, expectations?

In the age of mobile devices and telework, are there policies for working from personal and connecting while on travel?

Do employees know how to recognize online threats and how to report them?

## CYBER EDUCATION: AVOID “DEATH BY POWERPOINT”



Should not be “check the box”

Focus on retention of key information important to your institution

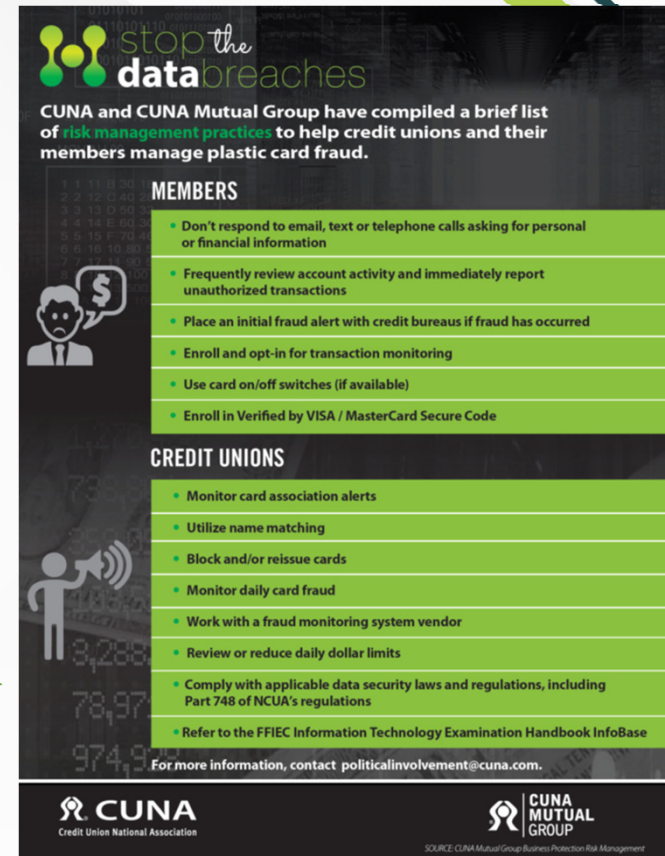
# CYBERSECURITY IS A TEAM SPORT



In addition to your employees and partners, consider member education programs.

CUNA Stop the Data Breaches Toolkit

<http://www.stopthedatabreaches.com>



**stop the data breaches**

CUNA and CUNA Mutual Group have compiled a brief list of **risk management practices** to help credit unions and their members manage plastic card fraud.

**MEMBERS**

- Don't respond to email, text or telephone calls asking for personal or financial information
- Frequently review account activity and immediately report unauthorized transactions
- Place an initial fraud alert with credit bureaus if fraud has occurred
- Enroll and opt-in for transaction monitoring
- Use card on/off switches (if available)
- Enroll in Verified by VISA / MasterCard Secure Code

**CREDIT UNIONS**

- Monitor card association alerts
- Utilize name matching
- Block and/or reissue cards
- Monitor daily card fraud
- Work with a fraud monitoring system vendor
- Review or reduce daily dollar limits
- Comply with applicable data security laws and regulations, including Part 748 of NCUA's regulations
- Refer to the FFIEC Information Technology Examination Handbook InfoBase

For more information, contact [politicalinvolvement@cuna.com](mailto:politicalinvolvement@cuna.com).

**CUNA**  
Credit Union National Association

**CUNA MUTUAL GROUP**  
SOURCE: CUNA Mutual Group Business Protection Risk Management



# THANK YOU

For more information about Ridge Global Cybersecurity Advisory Services for C-Suite leaders, board members, and senior executives, contact Chris Furlow at +1.202.833.2008 or by email at [cfurlow@ridgeglobal.com](mailto:cfurlow@ridgeglobal.com)

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

