Credit Union Security Survey Results

How Do You Compare with Your Peers?

Survey Details

- Survey: August 2015
- Respondents: 214
- Vertical: Credit Unions
- Titles: CEO, CTO, CIO, CFO, CLO
- Size: $50M to $1B in revenue

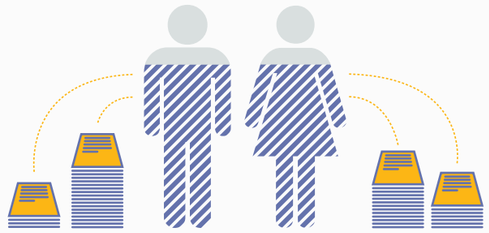
#1. On Security Challenges

#1 security challenge is cyber preparedness.

#2 is meeting regulatory compliance.

#3 is lack of resources, funding and/or talent.

#2. On Data Loss



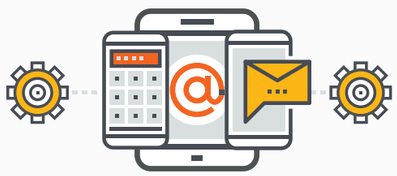
71% said their employees are their biggest area of data loss.

68% conduct employee security awareness training annually (or less than annually).

#3. On Vulnerability Mgmt

50% of all credit unions perform a vulnerability assessment yearly (or longer). Quarterly is recommended.

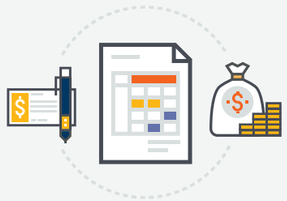
#4. On BYOD



54% don't allow BYOD at all.

Only 4% said they allow employees to BYOD.

#5. On Budgets



In the next 24 months, credits unions plan to invest in:

81% network security.

79% regulatory compliance.

64% email protection.

Not enough is spent on incident response.

#6. On Incident Response

71% said they have an incident response plan in place, but are still refining it.

Only 4 respondents don't have a response plan at all.

BAE SYSTEMS
INSPIRED WORK

Credit Union Security Survey Results

How Do You Compare with Your Peers?

BAE Systems

We help nations, governments and businesses around the world defend themselves against cybercrime, reduce their risk in the connected world, comply with regulation, and transform their operations.

We do this using our unique set of solutions, systems, experience and processes - often collecting and analysing huge volumes of data. These, combined with our Cyber Special forces - some of the most skilled people in the world, enable us to defend against cyber-attacks, fraud and financial crime, enable intelligence-led policing and solve complex data problems.

We currently protect over 1,800 financial institutions, including 400 credit unions.

#1. On Security Challenges

The three elements of comprehensive security and compliance are:

Technology: firewalls, IDPS, VPN remote user access, multi-factor authentication, log mgmt, vulnerability scans, file integrity monitoring, web content filtering

Process: correlate, investigate, alert escalation procedures, communicate, practice and train

People: 24x7 network monitoring by certified security experts; rapid response to security alerts

#2. On Data Loss

Train your employees frequently; annually is not enough.

Testing should always accompany training to enforce the principles.

Mix technology controls with user education.

Email Encryption for sensitive outbound emails.

Email DLP to detect potential data leaks and insider threats.

#3. On Vulnerability Mgmt

A **comprehensive security plan** includes:

- Vulnerability scans
- IT risk assessments
- Penetration testing
- Proper vetting of third-party vendors

These measures will help to meet **compliance** requirements and to know where to invest your **budget.**

#4. On BYOD

Set a corporate BYOD policy that employees must sign.

Create an authorized device list.

Invest in a Mobile Device Management solution to:

- **Encrypt** critical data
- **Set role-based** access policies
- **Wipe** applications/content remotely
- **Protect** CU from potential legal action

#5. On Budgets

It's no longer **if** you will suffer a cyber security breach, it's **when,** so invest in:

Prevention: anti-malware, firewalls, email content filtering, DLP

Detection: log management, 24/7 network monitoring or partner with a MSSP

Response: recruit the team, create a comprehensive incident response plan, practice execution, and continuously refine

#6. On Incident Response

You might not be as secure as you think you are.

Be sure to:

- Measure
- Hack thyself
- Phish your employees
- Break your passwords
- Quantify surprises
- Improve detection

BAE SYSTEMS
INSPIRED WORK