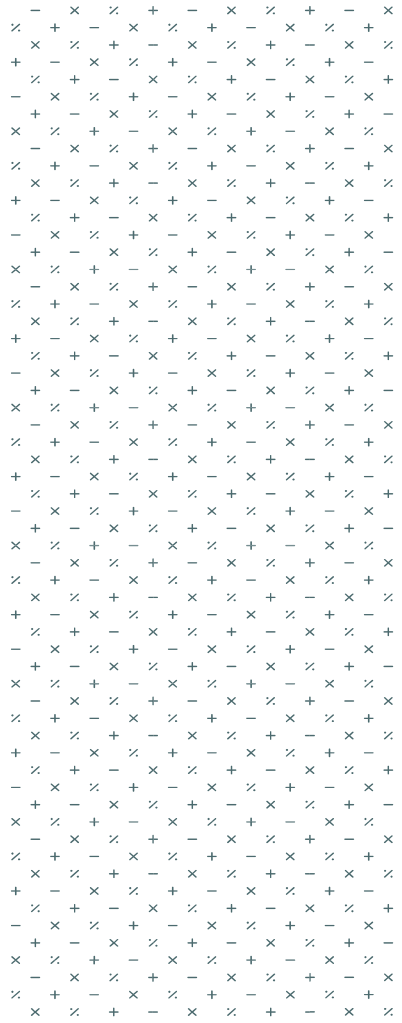
MOSSADAMS

Information Technology Trends

Chris Wetzel, Senior Manager
Financial Services Consulting



IT Trends in 2017

- Cybersecurity
- Social Media
- Digital Currency
- IT Control Challenges

Cybersecurity Threat Update

Let's take a quick look back...

According to the Verizon 2016 Data Breach Investigation Report, in 2015 Financial Services was 3rd highest in reported incidents of all industry categories, and #1 in confirmed data loss.

Verizon Data Breach Investigations Report

In 2016...

- 1,368 security incidents reported within Financial Services industry in 2015
- 795 confirmed breaches resulted in data loss (58%)
- 48% were a result of Web Application Attacks
- Motive: Financial Gain – Over 80%

Verizon Data Breach Investigations Report

In 2017...

- 998 security incidents reported within Financial Services industry in 2016 (27% decrease)
- 471 confirmed breaches resulted in data disclosure/loss (47% success rate)
- Top 3 Patterns: Denial of Service, Web App Attacks, and Payment Card Skimming (ATMs, gas pumps, POS terminals)
- Threat Actors: 94% External
- Motives: 96% Financial Gain (18+% increase)

The Big Picture

According to the Verizon 2017 Data Breach Investigation Report, in 2016 Financial Services was ranked 4th in reported incidents among all industry categories...

...and (still) ranked 1st in confirmed data disclosure/loss.

2016 Financial Sector Breaches

Company or Agency	State	# of Records Exposed
Southern Michigan Bank & Trust	MI	38,601
M Holdings Securities	OR	19,012
Primary Residential Mortgage	UT	2,889
Freddie Mac	VA	2,361
Credit Union of the Berkshires	MA	2,200
Rockland Trust	MA	2,182
QR Lending	FL	1,487
First Home Mortgage Corp.	MD	1,300
One Nevada Credit Union	NV	1,000
Nationwide Retirement Solutions	OH	457
Ash Brokerage Firm	IN	423
Ameriprise	MN	350

Source: Data Breach Reports: 2016 End of Year Report, Identity Theft Resource Center

Social Media

Which of the following sites does your financial institution actively use as a corporate social media platform?

a. Facebook

b. LinkedIn

c. Twitter

d. Instagram

e. YouTube

f. Other not listed

Social Media

- 2.3 billion social media users worldwide[1]
- Avg. time on social media daily = 118 minutes[1]
- 69% of U.S. adults use some type of social media[2]
- 160,000+ Facebook accounts compromised daily[3]

[1] Statista, 2016
[2] Pew Research Center, 2016
[3] NY Post, 2015

Security Threats

Social Engineering

- One of the greatest weapons of a hacker or fraudster is information
- Social media culture has led to lack of filtering information
- More data = More customized

Security Threats

Site Compromise

- Modify content
- Insert malicious code, spyware, etc., into advertisements
- Information leaks

Security Threats

Internal Threats

- Employees click on links or messages sent through social media sites
  - “Who Viewed Your Facebook Profile?” Or LinkedIn, etc.
  - “Shark Attacks Teen in California” Shocking Video
- Employees use personal social media account to distribute work-related information
- Disgruntled employees who have access to the company social media sites

Security Disclosure Risk

- Online banking login security challenge questions could be found on Facebook
- A fraudster could gather information about your employees from LinkedIn to perform a targeted social engineering attack on your organization
- Reminder: Include social media risks and controls in your GLBA Information Security program

Tips to Avoid Social Media Security Risks

- Create a Social Media Policy – get input from various business units which would be impacted
- Ensure your security awareness and training programs includes social media (for employees and customers)
  - Use non-Facebook passwords and challenge question answers
  - Do not disclose work related information
  - Educate users on the common attacks that utilize information gathered from social media (real life example are more effective than generalities)
  - Ensure employees understand the mobile technology in use

Tips to Avoid Social Media Security Risks

- Ensure the person(s) responsible for managing social media sites is properly trained
- Limit access to social media sites
- Actively monitor social media venues for information leakage
- Ensure the GLBA Information Security program includes social media technologies
- Keep security technology current – antivirus/antimalware, firewall, content filtering, IPS/IDS, browser version

MOSSADAMS

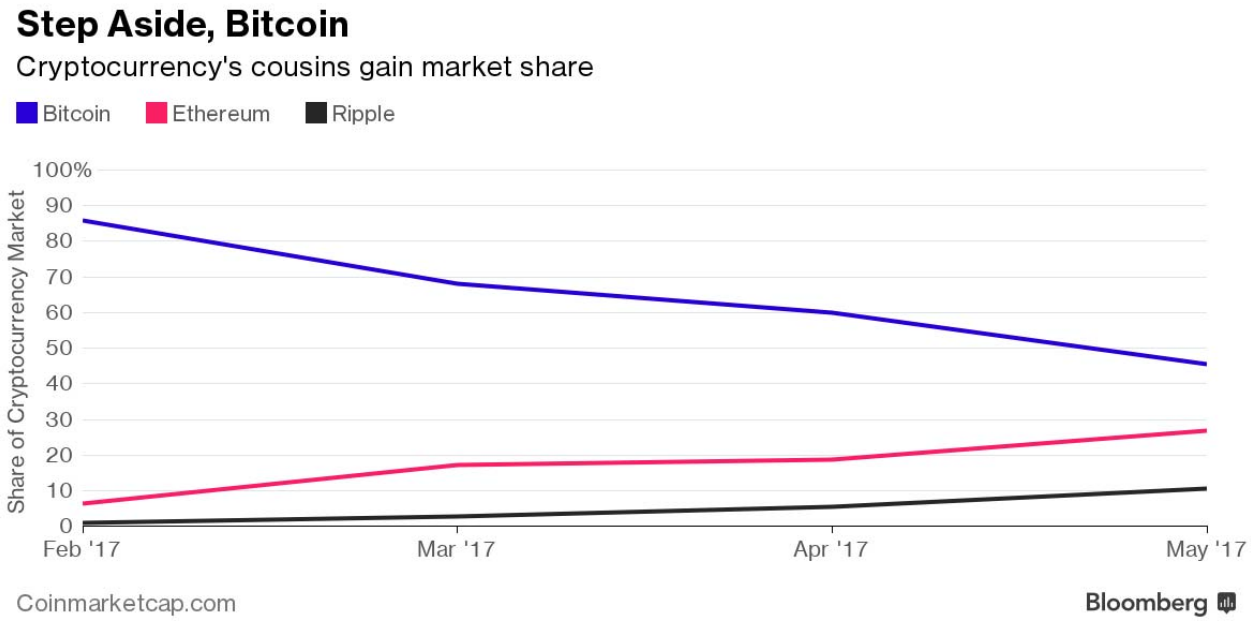
Digital Currency

Bitcoin and Blockchain, and Cryptocurrency, oh my!

Digital Currency 101

- Blockchain: a digital ledger in which transactions made in bitcoin, or another cryptocurrency, are recorded chronologically and publicly
  - All transactions are time-stamped
  - All information exists as a shared database, broken up into thousands of “blocks” and continually reconciled (about every 10 minutes)
  - Each user/owner maintains a public key, which acts as an address on the blockchain, and a private key, which gives access to the owner’s digital assets

Cryptocurrencies



As of May 2017, there are 881 different cryptocurrencies, with a total market capitalization of nearly $107B.

Regulatory Concerns

- Consumer Protection
- Money Laundering
- Tax Compliance
- Privacy and Identity
- Money Transmission Licensing

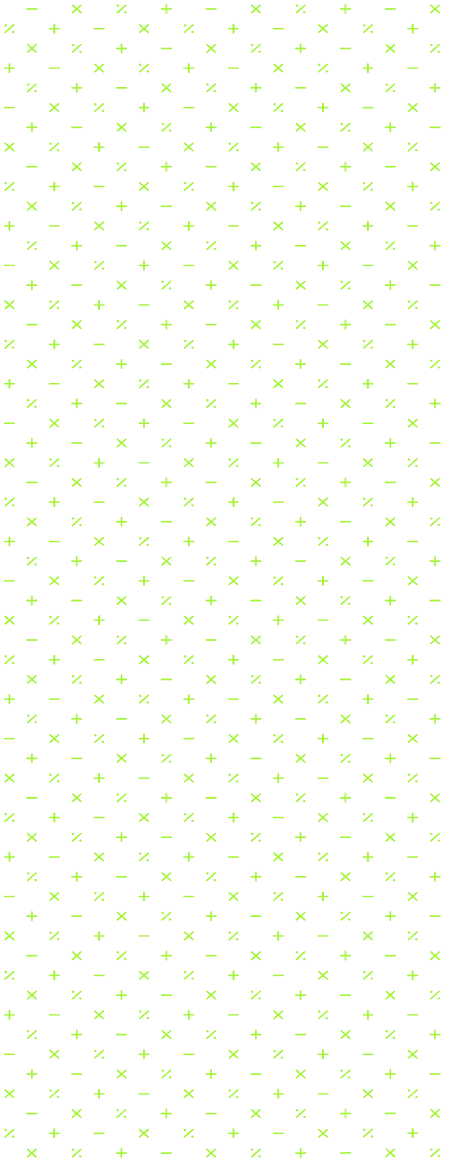
Group Discussion Question

- Identify 2-3 ways digital currency could present challenges or risks to financial institutions.

MOSSADAMS

IT Control Challenges

Supervisory Committee Workshop



Vendor Management of Cloud Providers

- Governance
- Compliance
- Architecture/Software Scalability
- Identity and Access Management
- Data Protection and Security
- Availability
- Incident Response

Patch Management

- Policies and procedures
- Managing the “5%”
- Asset management
- Understand the cost to not patch
- Test for patch management effectiveness
- Document non-deployment decisions

Disaster recovery and business continuity planning

- Business Impact Assessment (BIA)
- Ensure business units can articulate critical processes
- Recovery Time Objective (RTO) and Recovery Point Objective (RPO)
- Test the plan

Cybersecurity Assessment Tool Update

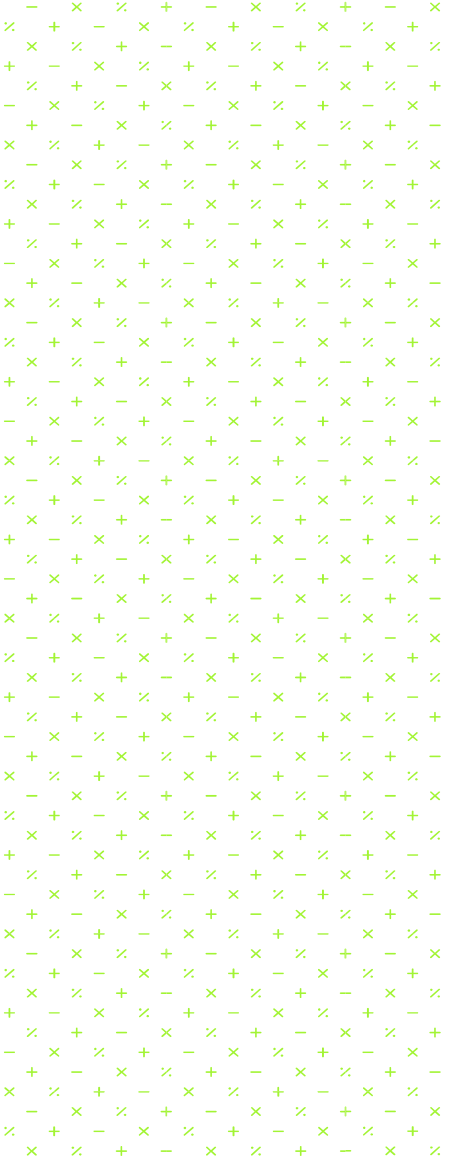
- May 31, 2017 – Press Release: FFIEC Release Update to Cybersecurity Assessment Tool
  - Revised mapping in Appendix A of the FFIEC IT Examination Handbook to the updated Information Security and Management booklets.
  - Additional response option for assessing maturity levels: “Yes with Compensating Controls” (allows management to include supplementary or complementary behaviors, practices and processes that support its cybersecurity activity assessment).

MOSSADAMS

Questions?

Supervisory Committee Workshop

Chris Wetzel, Senior Manager
Financial Services Consulting
chris.wetzel@mossadams.com



THANK YOU