



Cyber Security & Internal Audit

Craig Sanders, Partner
Financial Services Consulting





To Regulatory Concerns for 2018

- **Cyber Security**
- **BSA**
- **Lending Compliance**



Cyber Security & IA

- **Cybersecurity**
- **Social Media - Impact**
- **Internal Audit**



Cybersecurity Threat Update

Let's take a quick look back...

According to the Verizon 2017 Data Breach Investigation Report, in 2016 Financial Services was 3rd highest in reported incidents of all industry categories, and #1 in confirmed data loss.

That status hasn't changed much.....

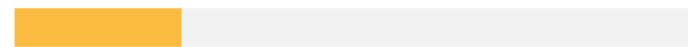


Cybersecurity Threat Update



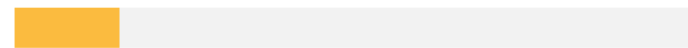
Who are the victims?

24%



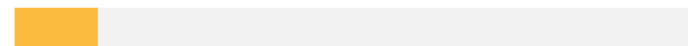
of breaches affected financial organizations.

15%



of breaches involved healthcare organizations.

12%



Public sector entities were the third most prevalent breach victim at 12%.

15%



Retail and Accommodation combined to account for 15% of breaches.



Verizon Data Breach Investigations Report

In 2016...

- **1,368 security incidents**
- **795 confirmed breaches**
- **48% of incidents resulted in a breach**
- **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 (15+% increase)



The Big Picture

According to the Verizon 2018 Data Breach Investigation Report, in 2017 Financial Services was ranked 4th in reported incidents among all industry categories...

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



2017 Financial Sector Breaches

-Number of breaches has grown from and average of 40 per entity in 2012 to 125 in 2017



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).

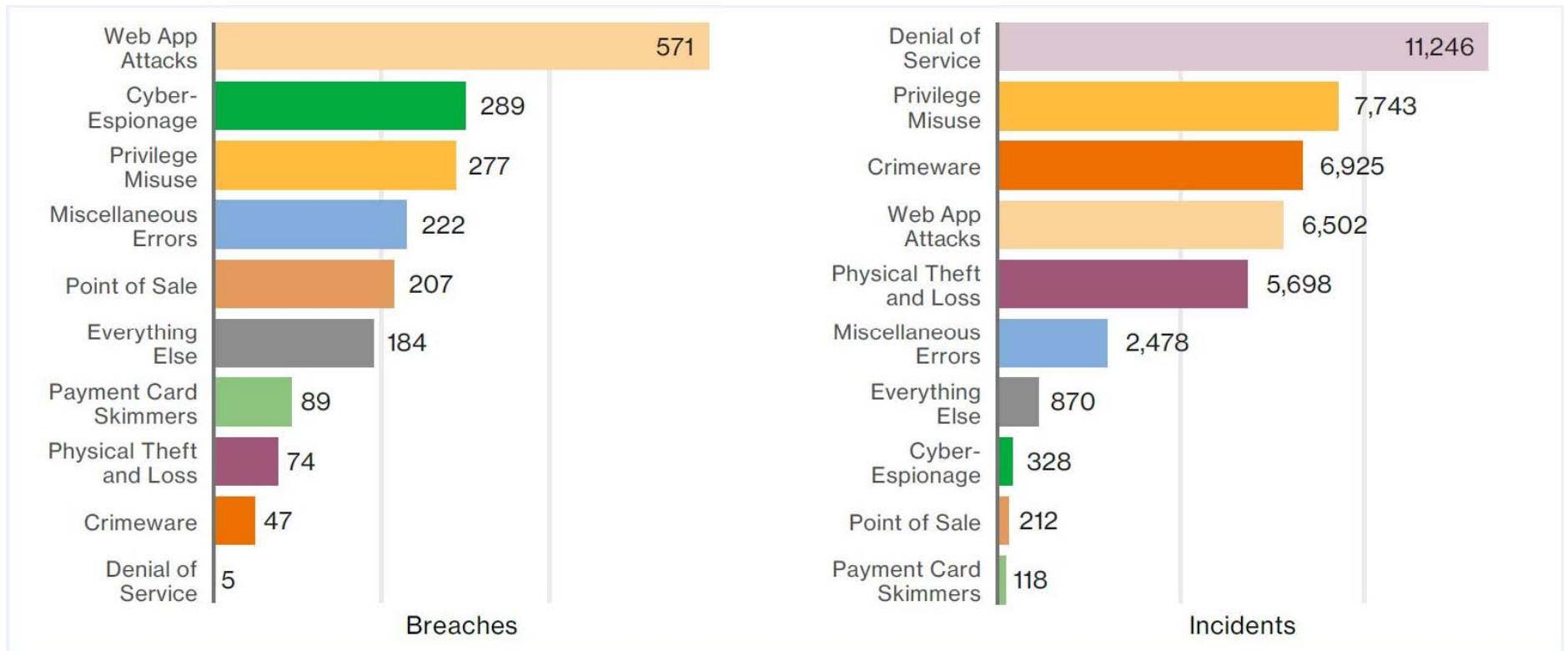


Regulatory Movement

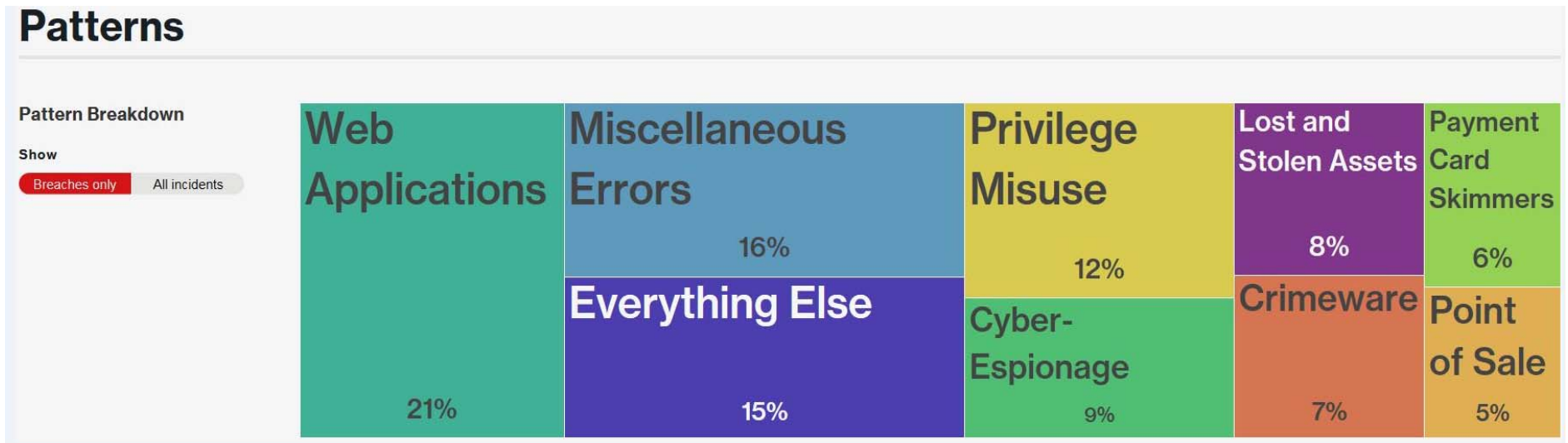
-Cyber Security Programs

- CAT Tool (recommended vs. required)
- SEC announces Cyber change (Feb 2018)
- Colorado Cyber change for CU's (May 2018)
- Increase the Maturity Level
 - Real-time vs. On Demand Systems
 - Increased Involvement (Executive Management)

By the numbers



By the numbers





By the numbers




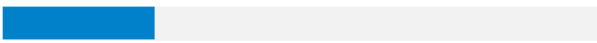


By the numbers

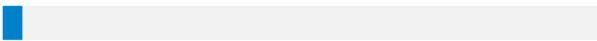


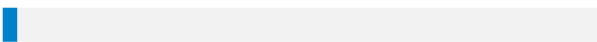
Who's behind the breaches?


75% 
perpetrated by outsiders.

25% 
involved internal actors.

18% 
conducted by state-affiliated actors.

3% 
featured multiple parties.

2% 
involved partners.


51% 
involved organized criminal groups.





By the numbers




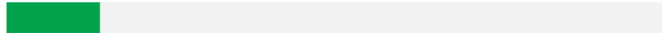
What tactics do they use?

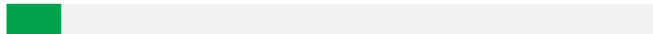
62% 
of breaches featured hacking.

51% 
over half of breaches included malware.

81% 
of hacking-related breaches leveraged either stolen and/or weak passwords.

43% 
were social attacks.

14% 
Errors were causal events in 14% of breaches. The same proportion involved privilege misuse.

8% 
Physical actions were present in 8% of breaches.



By the numbers



What else is common?



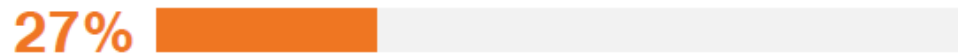
of malware was installed via malicious email attachments.



of breaches were financially motivated.



of breaches were related to espionage.



of breaches were discovered by third parties.



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

- **2.4 billion social media users worldwide¹ (Up 1.0b from 2016)**
- **71% of internet users are on social media**
- **600,000+ Facebook accounts compromised daily²**
- **Facebook users spend 700 Billion minutes per month on the site.²**

¹ CNN.com

² NY Daily News



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

Internal Threats (**81% +**)

- 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



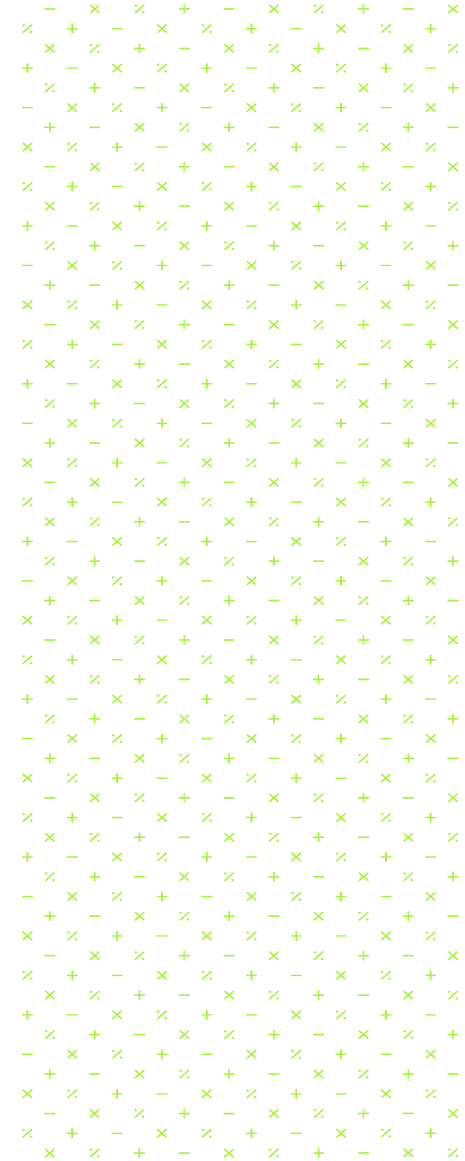
Regulatory Concerns

- Approval of a Cyber Program
- Skilled / Knowledgeable Team
- Advancing the Maturity Level



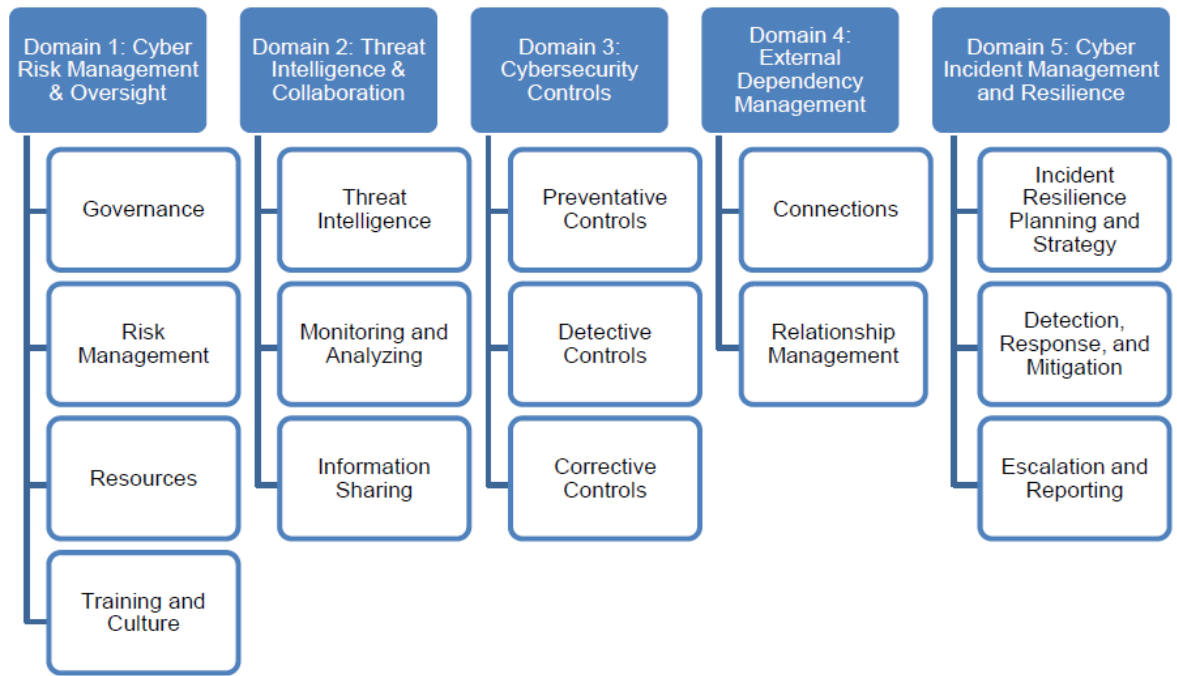
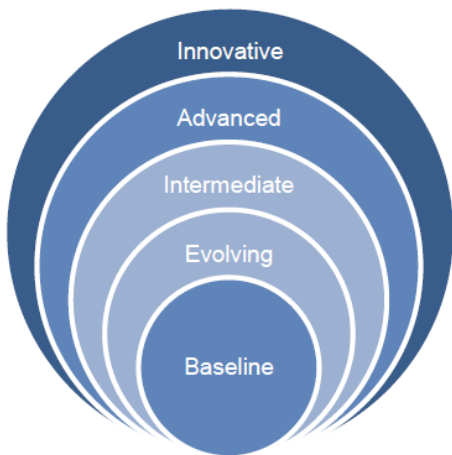
Internal Audit

Supervisory Committee Workshop





Cyber Maturity



All declarative statements in each maturity level, and previous levels, must be attained and sustained to achieve that domain's maturity level.



Domain 1 – Nine Element Areas One Hundred Twenty-Nine tests



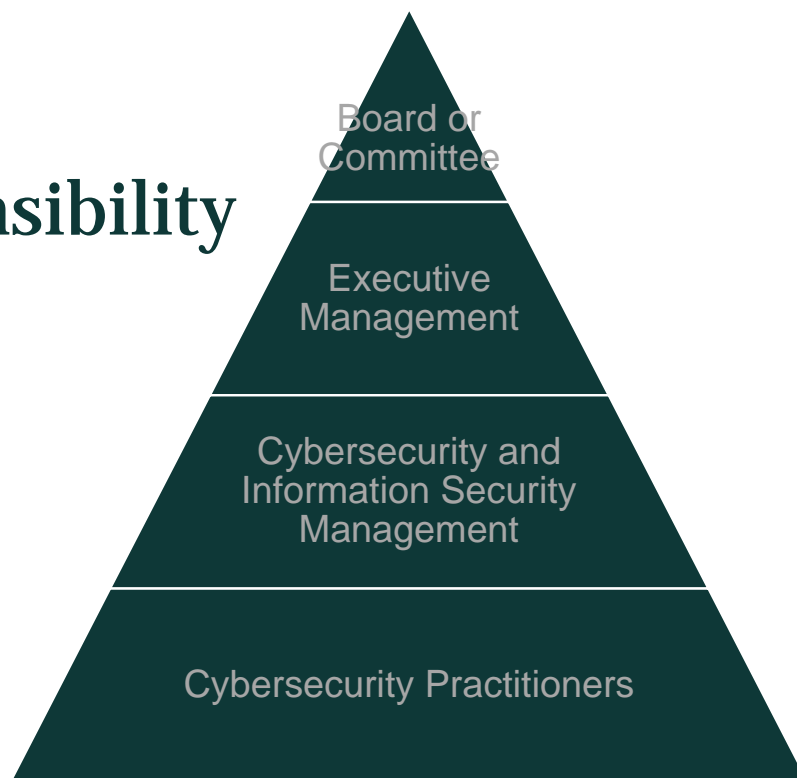
- **Baseline**
 - Thirty tests
- **Evolving**
 - Thirty-four tests
- **Intermediate**
 - Thirty-three tests
- **Advance**
 - Twenty-seven tests
- **Innovative**
 - Fifteen tests



Assessment – All Domains
Five Domains
Nine Element Areas
Five Hundred Tests



Cyber Responsibility



BOARD OR COMMITTEE

Oversee identification of key assets, and verify protection levels and priorities are appropriate

EXECUTIVE MANAGEMENT

Set the tone for cybersecurity management; provide necessary functions, resources and infrastructure, and oversee the effectiveness

CYBERSECURITY AND INFORMATION SECURITY MANAGEMENT

Develop security and risk mitigation strategies; implement policies and programs; manage incidents and remediation efforts

CYBERSECURITY PRACTITIONERS

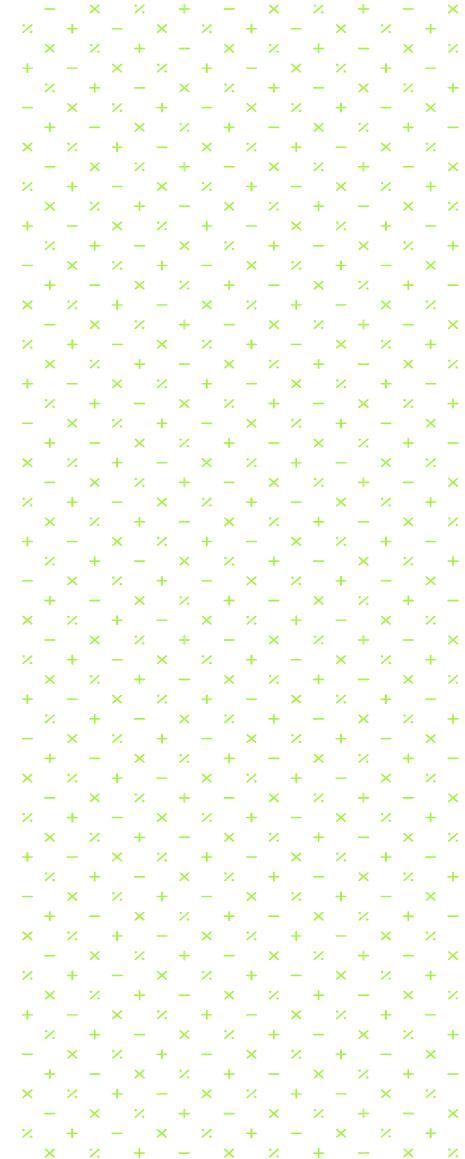
Design, implement and administer technical controls and processes; respond to incidents



Questions?

Supervisory Committee Workshop

Craig Sanders, Partner
Financial Services Consulting
Craig.sanders@mossadams.com





The material appearing in this presentation is for informational purposes only and should not be construed as advice of any kind, including, without limitation, legal, accounting, or investment advice. This information is not intended to create, and receipt does not constitute, a legal relationship, including, but not limited to, an accountant-client relationship. Although this information may have been prepared by professionals, it should not be used as a substitute for professional services. If legal, accounting, investment, or other professional advice is required, the services of a professional should be sought.

Assurance, tax, and consulting offered through Moss Adams LLP. Wealth management offered through Moss Adams Wealth Advisors LLC. Investment banking offered through Moss Adams Capital LLC.

THANK YOU

