IT Examination Hot Topics – Cybersecurity

March 18, 2020

WIPFLi CPAs and Consultants

1

Contact Information

Jim Rumph
Senior Manager
Wipfli LLP
404.420.5639
jim.rumph@wipfli.com

Joel Lego
Manager
Wipfli LLP
815.265.6950
jlego@wipfli.com

WIPFLi CPAs and Consultants

 2

2

3

FFIEC's Cybersecurity Assessment Tool

- A look back
  - Based on other frameworks
  - Regulators expect a robust risk management process for cybersecurity
  - Not mandatory, but baseline reflects "minimum expectations required"

WIPFLI
CPAs and Consultants

© Wipfli LLP 4

4

FFIEC's Cybersecurity Assessment Tool

- Where are we now?
  - Establish desired maturity levels
  - Be consistent
  - Be able to explain your rationale
  - Need someone to review it
  - Ensure sufficient Board reporting

WIPFLi CPAs and Consultants

 5

5

FFIEC's Cybersecurity Assessment Tool

- A look forward
  - Focus is on baseline; however, more will be expected
  - Expect updates
  - Consider NIST Cybersecurity Framework

WIPFLi CPAs and Consultants

 6

6

FDIC/OCC Joint Statement on Cybersecurity

- Issued in January
  - Response and Resilience Capabilities
  - Authentication
  - System Configuration
  - Employee Training
  - Monitoring
  - Data Protection

WIPFLi CPAs and Consultants

 7

7

Security Awareness Training

- Need for a comprehensive Security Awareness Training Program
- For who?
  - Board
  - Employees
  - Customers

WIPFLi CPAs and Consultants

 8

8

Security Awareness Training

- Board-Level Training
  - Real-world scenarios
  - Incident response
  - Monitoring
  - Results
  - Not too technical
  - More than once a year

WIPFLi CPAs and Consultants

 9

9

Security Awareness Training

- Employee Training
  - Not just phishing
  - More than once a year
  - Frequent/shorter communications
    - Emails
    - Short videos
  - Communications should be bi-directional

WIPFLi CPAs and Consultants

 10

10

Security Awareness Training

- Customer Training
  - Focus on high-risk customers
  - Customers' controls are typically weaker
  - Opportunity to engage your customers

WIPFLi CPAs and Consultants

 11

11

Information Security Officer Role

- Smaller FIs continue to struggle with independence
- Trends
  - Outsourcing
  - Committee approach
  - Creativity with compensating controls

WIPFLi CPAs and Consultants

 12

12

Vendor Management

- Ensure we review all vendors
- Focus on higher-risk vendors
- Always consider what a vendor does for you

WIPFLi CPAs and Consultants

 13

13

Vendor Management

- BCP and cyber resilience
- Trend toward reviewing vendor's subservice organization

WIPFLi CPAs and Consultants

 14

14

Office 365 Security

- Ensure MFA is turned on for EVERYONE!
- Review access levels within Azure
- Restrict Mobile Device Access
  - Consider Mobile Device Management solutions
- Ensure sufficient alerting is in place
- Check your Microsoft Secure Score

WIPFLi CPAs and Consultants

 15

15

Email Security

- Use MFA!
- Block attachment file types that are not needed
- Use spam filtering
- Implement deep inspection of attachments and links
- Provide a secure method to transfer files
- Consider SSL/TLS decryption

WIPFLi CPAs and Consultants

 16

16

Ransomware Update

- We're seeing more specific targeting
- Criminal organizations are threatening to release data if you don't pay
  - Data exfiltration controls
- Ensure backups are adequate

WIPFLI CPAs and Consultants

 17

17

New Password Expectations

- Regulatory agencies are beginning to expect stronger passwords
  - 12-15 character minimums
  - 8 character passwords can now be cracked in less than 2.5 hours*
  - Passphrase is preferred rather than a password
  - Expiration expectations

WIPFLI CPAs and Consultants

 18

18

New Password Expectations

- Password Vaults
  - So many passwords!
  - Many password vaults support enterprise environments
  - There are open-source (free) alternatives
  - To access your vault, use strong passwords and/or MFA
  - Easier on the user, but potentially still harmful

WIPFLi CPAs and Consultants

 19

19

New Password Expectations

- Single Sign-On and Multi-Factor Authentication
  - Pass-through vs. vault
  - Better to supplement with multi-factor authentication
  - MFA for initial login
    - Becoming more affordable
    - Hard and soft token, text and email codes, fingerprint pattern
    - Possible HR policy issues with soft token

WIPFLi CPAs and Consultants

 20

20

Software End of Support/End of Life

- Microsoft
  - Windows 7 and 2008 Server support ended January 14, 2020
  - End of free security updates and support
  - Options for these operating systems
    - Paid support – Extended Security Update (ESU)
    - Additional support for upgrade commitments
  - Make sure your ATMs are upgraded!

WIPFLi CPAs and Consultants

 21

21

Software End of Support/End of Life

- Other Microsoft software and third-party software
  - MS Office client 2010, SharePoint Server 2010, Project Server 2010, Windows Embedded Standard 7 – 10/13/2020
  - See Microsoft and Adobe sites for additional information. Adobe Flash Player will be discontinued December 31, 2020
    - Ask any vendors using the product about migration plans
    - Most popular browsers are working toward or already blocking flash (though it can be turned back on if needed)

WIPFLi CPAs and Consultants

 22

22

Pandemic Plans

- Updates for Pandemic
  - COVID-19 should have prompted review and plans to test your Pandemic policy and procedures
  - FFIEC released an updated statement 3/6/20 on Pandemic Plans at
    - https://www.ffiec.gov/press/pr030620.htm
  - FFIEC fully updated guidance:
    - https://www.ffiec.gov/press/PDF/FFIEC%20Statement%20on%20Pandemic%20Planning.pdf

WIPFLi CPAs and Consultants

 23

23

Pandemic Plans

- Not many differences from before, mostly some updated language
- Guidance provides very good information and additional resources to help update your plans as needed

"…the institution's business continuity plan(s) (BCP) should address pandemics and provide for a preventive program, a documented strategy scaled to the stages of a pandemic outbreak, a comprehensive framework to ensure the continuance of critical operations, a testing program, and an oversight program to ensure that the plan is reviewed and updated. The pandemic segment of the BCP must be sufficiently flexible to address a wide range of possible effects that could result from a pandemic, and also be reflective of the institution's size, complexity, and business activities."

TEST YOUR PLAN!!!

WIPFLi CPAs and Consultants

 24

24

FFIEC Guidance on Disaster Recovery

- Updated guidance now titled “Business Continuity Management (BCM) Information Technology Handbook” released November 2019
  - Press release - https://www.ffiec.gov/press/pr111419.htm
  - Placing more emphasis on enterprise-wide approaches that address technology, business operations, testing and updating, and communication strategies than before.
  - Expect more focus on updating, testing, and defining social media guidelines
  - Incident response now directly in the BCM guideline – training, testing, communication, forensics

WIPFLI CPAs and Consultants

 25

25

Social Engineering

- Pretext Calling
  - Most institutions are doing well with testing phishing. Keep it going!
  - There appears to be an uptick in recommending testing in some regions.
  - There are merits to third-party testing.
  - Ensure the procedures are effective through testing, adjust as necessary. Then train, train, train, and test, test, test!

WIPFLI CPAs and Consultants

 26

26

Social Engineering

- Physical Pen Testing
  - Financial institutions should test employees' ability to follow procedures for vendors and visitors.
  - It's ok to say "no" or "please come back after making an appointment," etc.
  - Stress that testing is a way to educate, not humiliate.

WIPFLi CPAs and Consultants

 27

27

Quick Hits

- Mobile Device Security
- Incident Response Testing
- Monitoring
- Firewall Review
- Access Reviews
- Patch Management
- PVA vs. Pen Test

WIPFLi CPAs and Consultants

 28

28

29

FBI Internet Crime Report – 2019

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,776,549,688	Employment	$42,618,705
Confidence Fraud/Romance	$475,014,032	Civil Matter	$20,242,867
Spoofing	$300,478,433	Harassment/Threats of Violence	$19,866,654
Investment	$222,186,195	Misrepresentation	$12,371,573
Real Estate/Rental	$221,365,911	IPR/Copyright and Counterfeit	$10,293,307
Non-Payment/Non-Delivery	$196,563,497	Ransomware	**$8,965,847
Identity Theft	$160,305,789	Denial of Service/TDoS	$7,598,198
Government Impersonation	$124,292,606	Charity	$2,214,383
Personal Data Breach	$120,102,501	Malware/Scareware/ Virus	$2,009,119
Credit Card Fraud	$111,491,163	Re-shipping	$1,772,692
Extortion	$107,498,956	Gambling	$1,458,118
Advanced Fee	$100,602,297	Health Care Related	$1,128,838
Other	$66,223,160	Crimes Against Children	$975,311
Phishing/Vishing/Smishing/Pharming	$57,836,379	Hacktivist	$129,000
Overpayment	$55,820,212	Terrorism	$49,589
Tech Support	$54,041,053		
Corporate Data Breach	$53,398,278		
Lottery/Sweepstakes/Inheritance	$48,642,332		

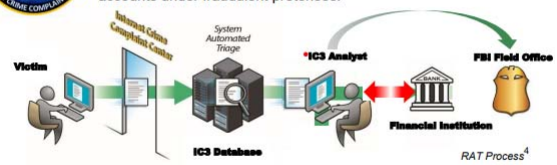
WIPFLi CPAs and Consultants

30

FBI Internet Crime Report – 2019

- Recovery Asset Team
  - Establish relationships with law enforcement

The Recovery Asset Team (RAT) was established in February 2018 to streamline communication with financial institutions and assist FBI field offices with the recovery of funds for victims who made transfers to domestic accounts under fraudulent pretenses.



*If criteria is met, transaction details are forwarded to the identified point of contact at the recipient bank to notify of fraudulent activity and request freezing of the account. Once response is received from the recipient bank, RAT contacts the appropriate FBI field office(s).

WIPFLi CPAs and Consultants

 31

31

Verizon Data Breach Report – 2019

- Attack patterns continue to show email as a primary threat vector

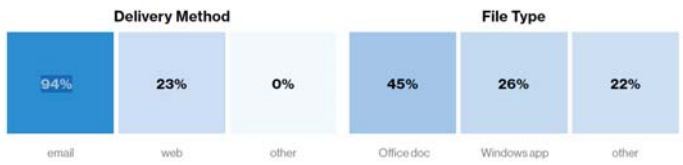


Figure 19. Malware types and delivery methods

WIPFLi CPAs and Consultants

Source: Verizon's Data Breach Investigations Report

 32

32

Verizon Data Breach Report – 2019

- Financial Services Breach Statistics

Action	Asset	Count
Hacking - Use of stolen creds	Server - Mail	43
Social - Phishing	Server - Mail	41
Hacking - Use of backdoor or C2	User Dev - Desktop	17
Malware - C2	User Dev - Desktop	16
Physical - Skimmer	Kiosk/Term - ATM	16
Misuse - Privilege abuse	Server - Database	14
Hacking - Use of stolen creds	Server - Web application	10
Social - Phishing	User Dev - Desktop	10
Error - Misdelivery	User Dev - Desktop	9
Malware - Backdoor	User Dev - Desktop	9

WIPFLi CPAs and Consultants

Source: Verizon's Data Breach Investigations Report

 33

33

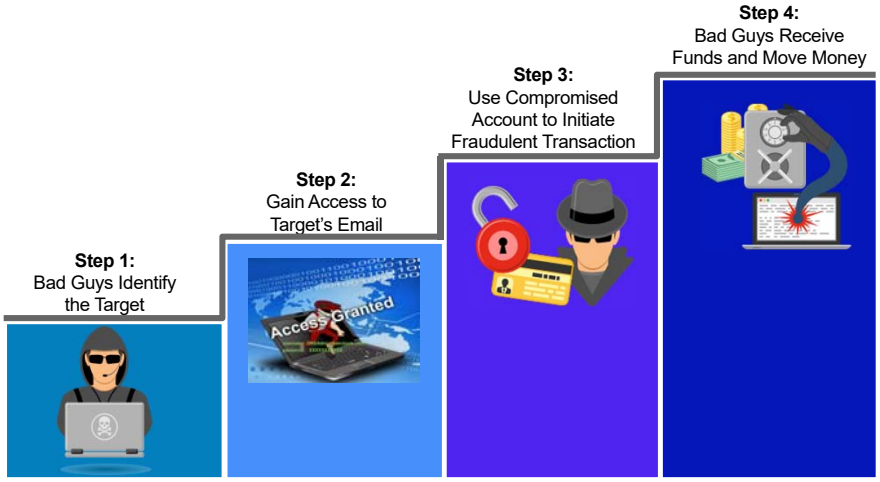
Case Study – Business Email Compromise

WIPFLi CPAs and Consultants

 34

34

Business Email Compromise Timeline



WIPFLI CPAs and Consultants

 35

35

Case Study – Business Email Compromise

- How to Prevent
  - Educate your commercial customers
  - Treat email as a critical asset
  - Be on alert for warning signs
  - Ensure your callback/verification procedures are effective
    - Recording callbacks
    - Verification can't be bypassed

WIPFLI CPAs and Consultants

 36

36

How Can We Help?

- IT Examinations
- External Testing
  - Perimeter vulnerability assessments
  - External penetration test
- Internal Testing
  - Internal vulnerability scan
  - Internal penetration test

WIPFLI CPAs and Consultants

 37

37

How Can We Help?

- Social Engineering
  - Email spoofing/phishing tests
  - Pretext calling
  - Physical penetration testing
- Assessments
  - Cybersecurity Assessment Tool
  - GLBA Information Security Risk Assessments
  - IT Audit Risk Assessments

WIPFLI CPAs and Consultants

 38

38

How Can We Help?

- Firewall/Router Configuration Review
- Disaster Recovery and Incident Response
  - Policy development
  - Facilitated tabletop testing
- Forensics Readiness Assessment

WIPFLi CPAs and Consultants

 39

39

Questions

WIPFLi CPAs and Consultants

 40

40

Closing

WIPFLi CPAs and Consultants

 41

41

WIPFLi LLP
CPAs and Consultants

www.wipfli.com/fi

42

42