alloya
Corporate Federal Credit Union

Identify & Mitigate | Protecting Your Credit Union from Cyber Threats

Dean Choudhri, CISSP, CISM, CRISC
Vice President, Cybersecurity and Information Assurance,
Alloya Corporate FCU

1

Agenda

- Cybersecurity Goal and Strategy
- Cyber Landscape
  - Ransomware
  - Business Email Compromise
- PART: Best practices that your credit union needs to follow to avoid becoming a victim.
- Reporting

2

Cybersecurity Goals

- What is/are the goals of your cybersecurity program?
  - To reduce vulnerabilities?
  - Reduce tools?
  - Increase protection capabilities?
  - Be an industry leader or a follower?

3

Cybersecurity Strategy

- Needs to be tied to the business strategy
  - Senior management sponsorship is critical
  - Tell the organization ALL of what you're doing (it's more than patching)
- Limit your attack surface
  - Harden your systems
  - Patch regularly
  - Restrict and limit access
- Monitor
  - Visibility and monitoring
  - Threat intelligence
    - What's going on? What impacts the U.S.?

4

Cybersecurity Strategy

- Visibility and Monitoring
  - Ensure visibility into all assets
  - Allocate appropriate time for monitoring
    - Helps you learn what's normal
  - Threat intelligence
- Culture of Security
  - Continuous training
  - Support from all business units
- Incident Response Plan
  - Prepare to recover
  - Test your plan via tabletop exercises

5

Cybersecurity Strategy

- Accept that some attacks may defeat your defenses, and plan on this basis. Use layered controls.
- Be prepared (incident response) for a successful cyber attack.
- Ensure your CU has the skills and resources to quickly identify and isolate problems, determine the level of investigation and response required, and maintain business as usual.
- Importantly, security measures should make organizations more resilient, and not restrict core business.

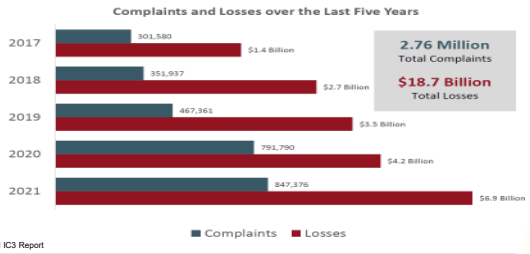
6

Cybersecurity Landscape
Covid, War, Geopolitics…

www.alloyacorp.org

7

U.S. *Reported* Cybercrime

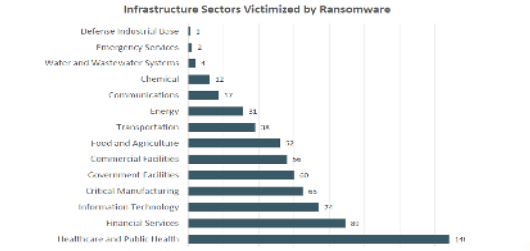


Source: 2021 FBI IC3 Report

www.alloyacorp.org

8

Business: Who Are the Victims

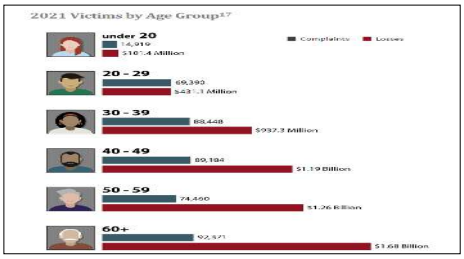


Source: 2021 FBI IC3 Report

www.alloyacorp.org

9

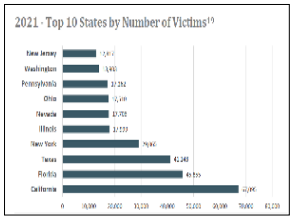
Consumers: Who Are the Victims?

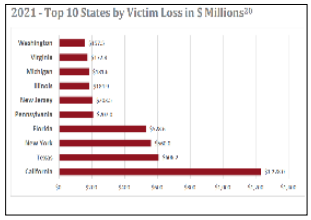


Source: 2021 FBI IC3 Report

10

Where Are the Victims





Source: 2021 FBI IC3 Report

11

Reported Crime Types

The stuff we must look out for all the time. **PLUS, these two.**

Source: 2021 FBI IC3 Report

12

Largest Dollars Lost

BEC: Not in top five of reported crimes, but 1st in dollars lost.

By Victim Loss

Crime Type	Loss	Crime Type	Loss
BEC/EAC	$2,395,953,296	Lottery/Sweepstakes/Inheritance	$71,289,089
Investment	$1,455,943,193	Extortion	$60,577,741
Confidence Fraud/Romance	$956,039,740	Ransomware	*$49,207,908
Personal Data Breach	$517,021,289	Employment	$47,231,023
Real Estate/Rental	$350,328,166	Phishing/Vishing/Smishing/Pharming	$43,218,707
Tech Support	$347,657,432	Overpayment	$33,407,671
Non-Payment/Non-Delivery	$265,011,249	Computer Intrusion	$19,603,037
Identity Theft	$278,267,918	IPR/Copyright/Counterfeit	$16,365,011
Credit Card Fraud	$172,998,385	Health Care Related	$7,042,942
Corporate Data Breach	$151,568,225	Malware/Scareware/Virus	$5,596,889
Government Impersonation	$142,643,253	Terrorism/Threats of Violence	$4,390,720
Advanced Fee	$98,694,137	Gambling	$1,940,237
Civil Matter	$85,049,939	Re-shipping	$931,486
Spoofing	$82,169,806	Denial of Service/TDos	$217,981
Other	$75,837,524	Crimes Against Children	$198,950
Threats of Violence**			
Social Media	$235,279,057	Virtual Currency	$1,602,647,341

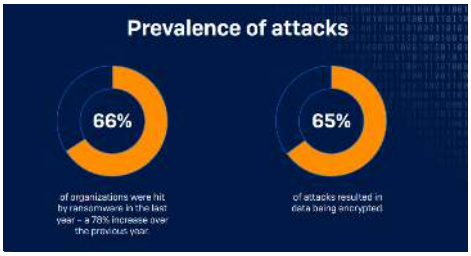
Source: 2021 FBI IC3 Report

13

Ransomware

14

It's Still A Thing

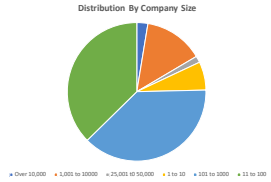


Source: Coveware Q4 2021

15

Who Are the Targets

75% are against businesses with between 11 to 1000 employees.



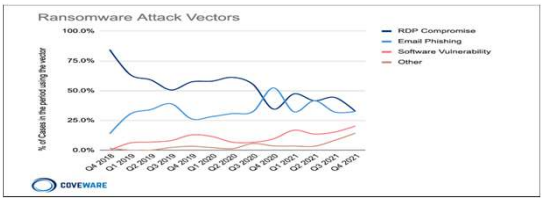
Source: Coveware Q4 2021

www.alloyxcorp.org

16

How Does It Happen?

- Remote Desktop (RDP from the internet) and Email Phishing are primary vectors
- Exploiting software vulnerabilities is rising



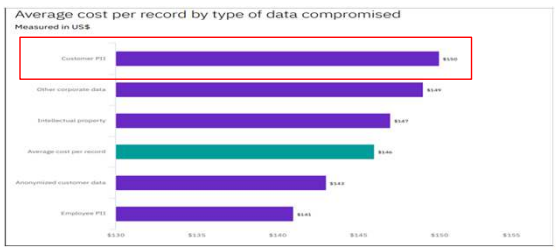
Source: Coveware Q4 2021

www.alloyxcorp.org

17

Impact = High

84% of Ransomware attacks included data exfiltration.



Source: Varonis

www.alloyxcorp.org

18

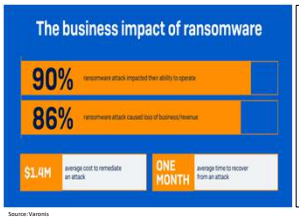
Ransomware Recovery

- Backups are key to Ransomware recovery
- Allocate time to validate backups and test restoration

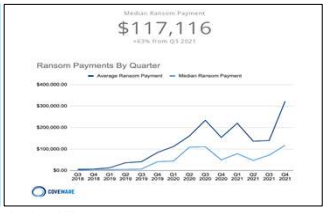
Source: Coveware Q4 2021

19

Impact and Cost



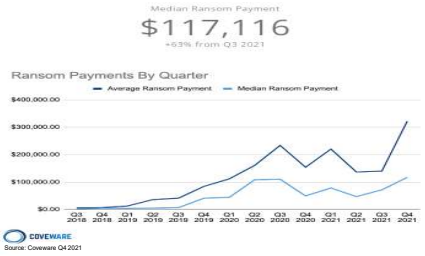
Source: Varonis



Source: Coveware Q4 2021

20

Ransomware



Source: Coveware Q4 2021

21

Insurance Can Play A Role

- If you can get, it still plays a role
- Members and regulators expect it

Source: Veronis

22

Ransomware Protection

- Backup your data / have a resilient backup strategy
- Patch (more on this later)
- Business interruption is the most significant cost (figuring out what happened, who to tell, how to recover, etc.)
- Average impact is 20 days

23

Phishing/Business Email Compromise

- Phishing
  - Emails that appear to be from legitimate institutions
    - NACHA, Amazon, FedEx, Microsoft, LinkedIn, Facebook, etc.
  - Entice you to click on link or attachment
  - 4% of users will always click!
- Business Email Compromise (BEC)
  - Spoof company email accounts and impersonate executives
  - Use hacked email accounts of your vendors to send invoices to AP department

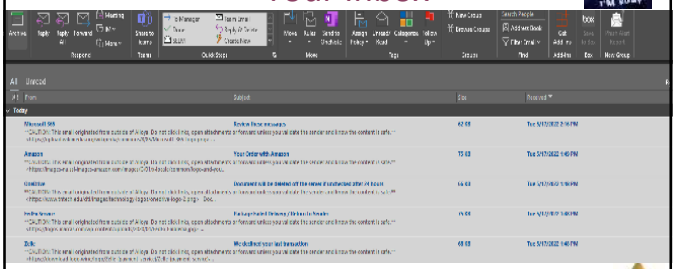
24

Spotting a Phish

- One thing all phishing messages have in common is they will include a link, attachment or picture for you to click on.
- Clicking on this item will:
  - Direct you to a website that appears to be legitimate and ask for some type of account information or username and password.
  - Or install malicious software *(malware)* on your computer which will steal your information or credentials without your knowledge.

25

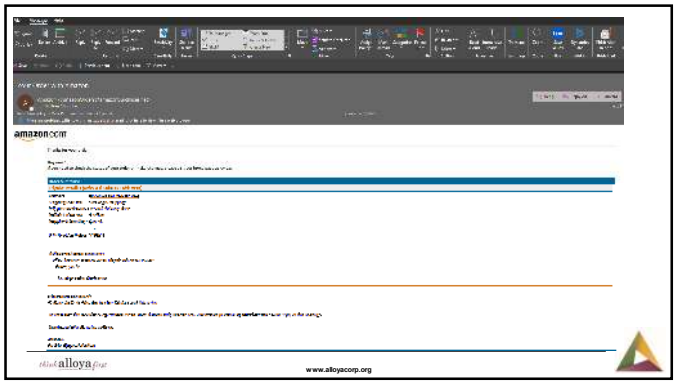
Your Inbox



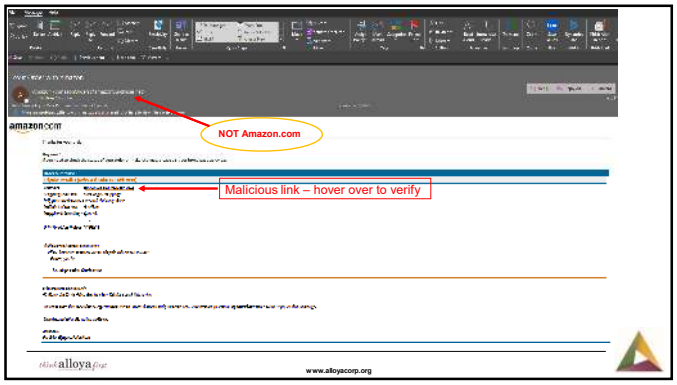
26

Business Email Compromise (BEC)

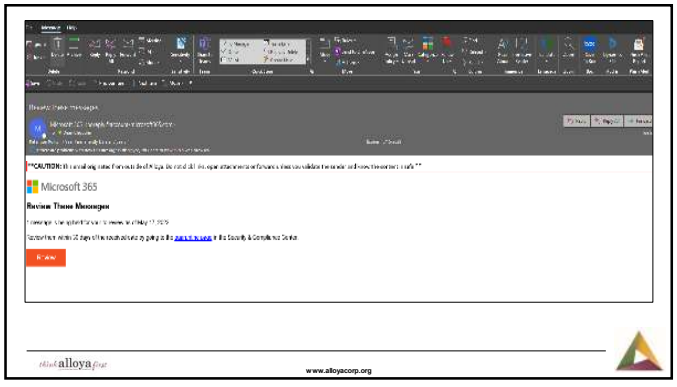
27


amazon.com
www.alloyacorp.org

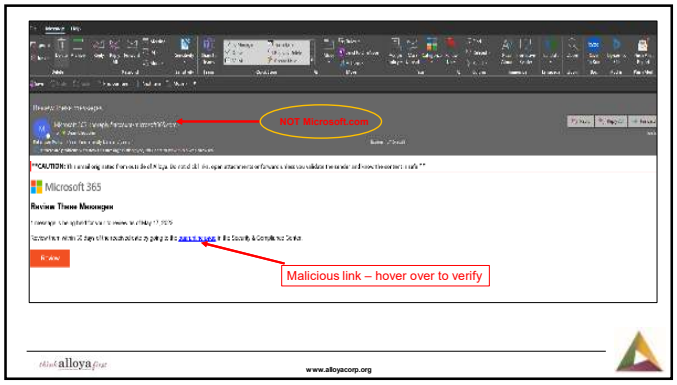
28


NOT Amazon.com
Malicious link – hover over to verify
www.alloyacorp.org

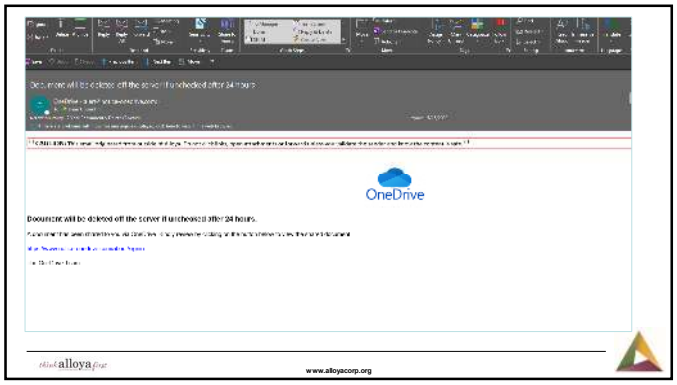
29


Microsoft 365
Review These Messages
www.alloyacorp.org

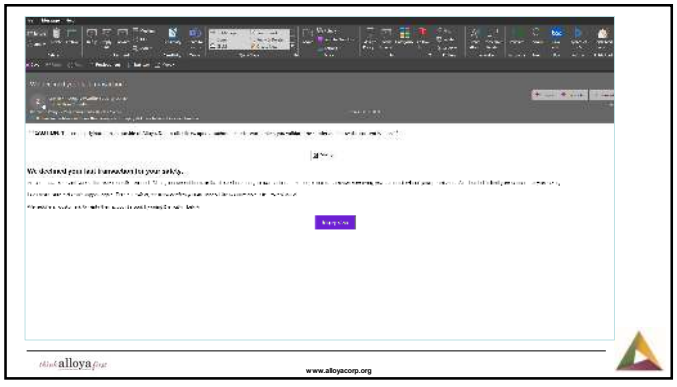
30


NOT Microsoft.com
Microsoft 365
Review These Messages
Malicious link – hover over to verify
www.alloyacorp.org

31

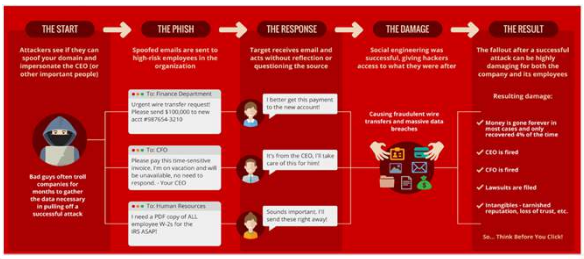

OneDrive
Document will be deleted off the server if unchecked after 24 hours.
www.alloyacorp.org

32


www.alloyacorp.org

33

BEC Attack Progression



Source:

34

Business Email Compromise

- BEC was not even in the top five of reported crimes
- BEC accounted for nearly 35% of the $6.9 billion in reported 2021 losses

IC3 has observed an emergence of newer BEC/EAC schemes that exploit this reliance on virtual meetings to instruct victims to send fraudulent wire transfers. They do so by compromising an employer or financial director's email, such as a CEO or CFO, which would then be used to request employees to participate in virtual meeting platforms. In those meetings, the fraudster would insert a still picture of the CEO with no audio, or a "deep fake" audio through which fraudsters, acting as business executives, would then claim their audio/video was not working properly. The fraudsters would then use the virtual meeting platforms to directly instruct employees to initiate wire transfers or use the executives' compromised email to provide wiring instructions."

35

BEC Protection

1) Protect	2) Authorize	3) Authenticate	4) Simulate
Company Domain • Establish a DMARC record (validates your email servers) **Email accounts** • Enable two-factor authentication and Conditional Access Policy **Awareness** • Attacks occur when execs are out of the office	• Minimize number of people who process/approve wire transfers • Publish a list of authorized folks to all employees	• Require dual approval • Verify new or different payments • Create max dollar amount that can be withdrawn via wire	• Adopt anti-phishing program • Identify real phishing scenarios and incorporate them into your tests

36

BEC Mitigation

- Via Office 365/Exchange Online
  - Use Conditional Access Policies
    - **Only CU managed devices can connect to CU resources**
    - Significantly reduces possibility of exploit
- Require multi-factor authentication

37

Business Email Compromise

- Contact the originating financial institution as soon as fraud is recognized to request a recall or reversal and a Hold Harmless Letter or Letter of Indemnity.
- File a detailed complaint with www.ic3.gov. It is vital the complaint contains all required data in provided fields, including banking information.
- Never make any payment changes without verifying the change with the intended recipient. Verify email addresses are accurate when checking email on a cell phone or other mobile device.

38

PART Principle for Protection

- Patching and Vulnerability Management
- Awareness
- Restrict
- Threat Intel

39

Patching

- Patching and Vulnerability Management
  - Ensure that **all** assets are being scanned regularly (weekly)
- Use asset classification to prioritize patching
  - Create three zones:
    - Zone A: Externally facing servers (web servers, VPN, etc.)
    - Zone B: Internal systems/servers
    - Zone C: Printers/IoT
  - Prioritize patching based on zone and criticality
    - e.g., Critical vulnerability in Zone A is patched *immediately*

40

Awareness

- Provide training to your users regularly (short and frequent).
- Test your users regularly (monthly).
  - Not a game of "gotcha"
  - Tell them you will be doing this-it builds trust
  - Users who fail get more training
  - Users who pass get rewarded
    - Gift card, etc.

41

Restrict

Source: CloudCodes

- Restrict *ANY* device that is not owned and managed by you from connecting to ANY of your resources.
- Restrict (via removal) users from installing software on their machines.
- Restrict web browsing to business related sites. Everyone has a smart phone that can be used for this.
- No personal email (even Gmail) from devices connected to your network.
- Use MFA everywhere and for everyone (especially admins).

42

Threat Intelligence

- Don't be caught by surprise.
- Subscribe to notifications from security vendors.
- CISA is an excellent resource.

43

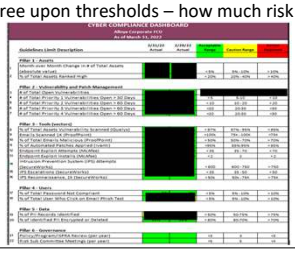
Reporting

- Know your audience and provide regular reports to both BOD and internal committees.
- Board of Directors
  - High level which illustrate CU's current security posture
  - Progress on exam and audit findings
- Internal committees
  - Can be more technical
  - Security posture, plus awareness on other (non-regular) items you worked on

44

Risk Thresholds

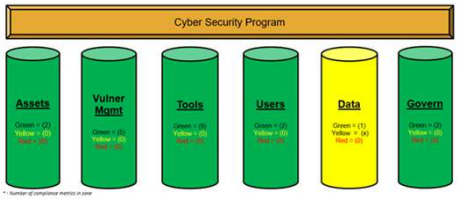
- Cyber risk will always exist
- Establish and agree upon thresholds – how much risk is acceptable?



45

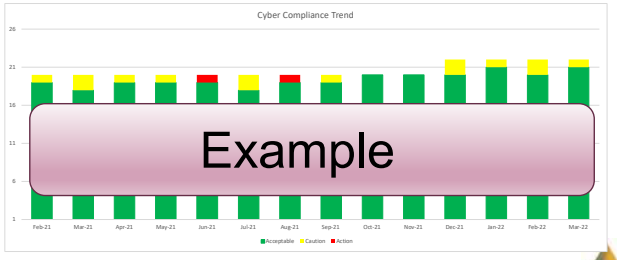
Pillars

Quick snapshot on current cybersecurity risk.



46

Cybersecurity Program Trend



47

Protection/Prevention

- Limit administrator privileges
- Strengthen wireless security (at home and in office)
- Do not allow users to install software
- Email is for work purposes only
- Do not tie your personal business (Amazon, Apple, personal banking) to your work email address
- Patch systems…quickly
- Use and UPDATE your anti-virus software and use anti-malware software. Newer AV uses AI for increased protection.

48

What's Around The Corner?

- Permanent increase in remote workers
- Ransomware will continue to be a growing threat
  - Low cost; hackers make money by asking for money
  - Virtual currency payments
- Social engineering via:
  - Business email compromise
  - Phishing!
  - Phone and text
- Cloud migration increases 3rd party vendor risk
  - Visibility into your vendor's controls

www.alloyacorp.org

49

Free Cybersecurity Resources

- Cybersecurity and Infrastructure Security Agency https://www.cisa.gov/
- FBI Internet Crime Complaint Center https://www.ic3.gov/
- Cyber Assessment Toolkit: https://www.fsscc.org/files/galleries/Copy_of_FSSCC_ACAT_v2.xlsx
- Phishing: http://www.antiphishing.org
- CIS Top 20: https://www.cisecurity.org/controls/cis-controls-list/
- NIST SP 800 Series: https://csrc.nist.gov/publications/sp800
- Premier View! We regularly post alerts regarding the latest security topics. https://premierview.alloyacorp.org

www.alloyacorp.org

50

Thank you!

Dean Choudhri, CISSP, CISM, CRISC
Vice President, Cybersecurity & Information Assurance
(518) 292-3846
Dean.Choudhri@alloyacorp.org

www.alloyacorp.org

51