

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

Are You Protected Against  
Ransomware and Phishing?

HW&Co.<sup>®</sup>

CPAs & Advisors

Presented by:

Mike Shoffner – HW&Co. Chief Compliance and Security Officer

1

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio



HW&Co.<sup>®</sup>

CPAs & Advisors

Mike Shoffner

HW&Co. Chief Compliance and  
Security Officer

2

2



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### CyberSecurity

- ▶ It's all about CONTROL
  - Access to Systems
  - Hardware used with the Systems
  - Movement and storage of all data
- ▶ Monitor Activities
- ▶ Mitigation of Threats
- ▶ Written Information Security Policies

3

3

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### HIPAA Compliance

- ▶ Business Associate Agreements
- ▶ Subcontractor Agreements
- ▶ Make the **all** internal practices, books, and records relating to the Use and Disclosure of PHI received from, or created or received by the company on behalf of the covered entity available for purposes of determining the Covered Entity's compliance with the Privacy Rules.
- ▶ Key Requirements:
  - Use appropriate safeguards to prevent Use or Disclosure of PHI other than as provided by the Privacy Rules / Business Associate Agreements
    - Administrative Safeguards
    - Physical Safeguards
    - Technical Requirements

4

4



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge

Ohio

## HIPAA Compliance Checklist

| GENERAL RULES                                       |               |  |     |
|---|---------------|--|-----|
| Standards   | Sections      | Implementation Specifications (R)= Required, (A)=Addressable   |     |
| General Requirements                                | 164.306(a)    | Ensure the confidentiality, integrity, and availability        | (R) |
|   |               | Protect against any reasonably anticipated threats             | (R) |
|   |               | Protect against any reasonably anticipated uses or disclosures | (R) |
|   |               | Ensure compliance  | (R) |
| Flexibility of Approach                             | 164.306(b)    | Reasonably and appropriately implement the standards           | (R) |
| Standards   | 164.306(c)    | Decide which security measures to use                          | (R) |
| Implementation Specifications                       | 164.306(d)    |  |     |
| Maintenance   | 164.306(e)    |  |     |
| ADMINISTRATIVE SAFEGUARDS                           |               |  |     |
| Standards   | Sections      | Implementation Specifications (R)= Required, (A)=Addressable   |     |
| Security Management Process                         | 164.308(a)(1) | Risk Analysis  | (R) |
|   |               | Risk Management  | (R) |
|   |               | Sanction Policy  | (R) |
| Assigned Security Responsibility                    | 164.308(a)(2) | Information System Activity Review                             | (R) |
| Workforce Security                                  | 164.308(a)(3) | Authorization and/or Supervision                               | (A) |
|   |               | Workforce Clearance Procedure                                  | (A) |
|   |               | Termination Procedures   | (A) |
| Information Access Management                       | 164.308(a)(4) | Isolating Health Care Clearinghouse Functions                  | (R) |
|   |               | Access Authorization   | (A) |
| Security Awareness and Training                     | 164.308(a)(5) | Access Establishment and Modification                          | (A) |
|   |               | Security Reminders   | (A) |
|   |               | Protection from Malicious Software                             | (A) |
|   |               | Log-in Monitoring  | (A) |
|   |               | Password Management  | (A) |
| Security Incident Procedures                        | 164.308(a)(6) | Response and Reporting   | (R) |
|   |               | Data Backup Plan   | (R) |
| Contingency Plan                                    | 164.308(a)(7) | Disaster Recovery Plan   | (R) |
|   |               | Emergency Mode Operation Plan                                  | (R) |
|   |               | Testing and Revision Procedures                                | (A) |
|   |               | Applications and Data Criticality Analysis                     | (A) |
| Evaluation  | 164.308(a)(8) |  |     |
| Business Associate Contracts and Other Arrangements | 164.308(b)(1) | Written Contract or Other Arrangement                          | (R) |

5

5

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge

Ohio

## HIPAA Compliance Checklist

| PHYSICAL SAFEGUARDS             |               |   |     |
|---------------------------------|---------------|---|-----|
| Standards                       | Sections      | Implementation Specifications (R)= Required, (A)=Addressable      |     |
| Facility Access Controls        | 164.310(a)(1) | Contingency Operations  | (A) |
|                                 |               | Facility Security Plan  | (A) |
|                                 |               | Access Control and Validation Procedures                          | (A) |
|                                 |               | Maintenance Records   | (A) |
| Workstation Use                 | 164.310(b)    |   |     |
| Workstation Security            | 164.310(c)    |   |     |
| Device and Media Controls       | 164.310(d)(1) | Disposal  | (R) |
|                                 |               | Media Re-use  | (R) |
|                                 |               | Accountability  | (A) |
|                                 |               | Data Backup and Storage   | (A) |
| TECHNICAL SAFEGUARDS            |               |   |     |
| Standards                       | Sections      | Implementation Specifications (R)= Required, (A)=Addressable      |     |
| Access Control                  | 164.312(a)(1) | Unique User Identification  | (R) |
|                                 |               | Emergency Access Procedure  | (R) |
|                                 |               | Automatic Logoff  | (A) |
|                                 |               | Encryption and Decryption   | (A) |
| Audit Controls                  | 164.312(b)    |   |     |
| Integrity                       | 164.312(c)(1) | Mechanism to Authenticate Electronic Protected Health Information | (A) |
| Person or Entity Authentication | 164.312(d)    |   |     |
| Transmission Security           | 164.312(e)(1) | Integrity Controls  | (A) |
|                                 |               | Encryption  | (A) |

6

6



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge

Ohio

## HIPAA Compliance Checklist

| ORGANIZATIONAL REQUIREMENTS                            |               |  |     |
|--|---------------|--|-----|
| Standards  | Sections      | Implementation Specifications (R)= Required, (A)=Addressable |     |
| Business associate contracts or other arrangements     | 164.314(a)(1) | Business Associate Contracts                                 | (R) |
|  |               | Other Arrangements   | (R) |
| Requirements for Group Health Plans                    | 164.314(b)(1) | Implementation Specifications                                | (R) |
| POLICIES AND PROCEDURES AND DOCUMENTATION REQUIREMENTS |               |  |     |
| Standards  | Sections      | Implementation Specifications (R)= Required, (A)=Addressable |     |
| Policies and Procedures                                | 164.316(a)    |  |     |
|  |               | Time Limit   | (R) |
|  |               | Availability   | (R) |
|  |               | Updates  | (R) |
| Documentation  | 164.316(b)(1) |  |     |

7

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge

Ohio

## HIPAA “Protected” Items

“Individually Identifiable Health Information” means any of the following:

1. Name
2. Address (all geographic subdivisions smaller than state, including street address, city county, and zip code)
3. All elements (except years) of dates related to an individual (including birthdate, admission date, discharge date, date of death, and exact age if over 89)
4. Telephone numbers or Fax number
5. Email address
6. Social Security Number
7. Medical record number or Health plan beneficiary number
8. Account number
9. Certificate or license number
10. Any vehicle or other device serial number
11. Web URL or Internet Protocol (IP) Address
12. Finger or voice print
13. Photographic image - Photographic images are not limited to images of the face.
14. Any other characteristic that could uniquely identify the individual

8



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge

Ohio

## HIPAA Policies

1. The size, complexity and capabilities of the **Company**.

2. The **Company's** technical infrastructure, hardware and software security capabilities.

3. Cost of implementing security controls.

4. Probability and criticality of risks to E-PHI/ePHI.

Relevant Security Policies and Procedures include:

• BYOD Device Policy

• Contingency Policy

• Data Protection Suite Policy

• Hardcopy Policy

• Hardware Policy

• Information Authentication Policy

• Information Destruction Policy

• Infrastructure Policy

• Malware Protection Suite Policy

• Mobile Device Policy

• Network Backup Policy

• Physical Access Controls Policy

• Physical Security Policy

• Portable Storage Device Policy

• Risk Analysis and Management Policy

• Sanctions Policy

• Secure Portal Policy

• Secure Transmission Policy

• Security Incidents Policy

• Security Officer Job Description Policy

• Separation Policy

• Software Policy

• Systems Security and Usage Policy

• Visitor Policy

9

9

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge

Ohio

## Written Information Security Policies

► Ohio Safe Harbor

▪ The entity’s cybersecurity measures must also “reasonably conform” to one of the industry-recognized frameworks listed in R.C. 1354.03. These frameworks include the National Institute of Standards and Technology’s (NIST) Cybersecurity Framework, the Security Rule of the Health Insurance Portability and Accountability Act (HIPAA) (45 CFR § 164.302, et seq.) for healthcare-industry businesses regulated by HIPAA, and the Safeguards Rule of the Gramm-Leach-Bliley Act (16 CFR § 314.1, et seq.) for certain financial institutions. R.C. 1354.03.

▪ Creates affirmative defense to tort causes of action brought under Ohio law stemming from breaches of personal information.

10

10

Leading Age Momentum 2022

5



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

## Written Information Security Policies

- ▶ H.R. 7898 was signed into law on January 5, 2021. Amending the Health Information Technology for Economic and Clinical Health Act creating a “HIPAA safe harbor.”
- ▶ The “HIPAA safe harbor” requires that, when calculating fines, evaluating audits or reviewing proposed mitigation steps, the Department of Health & Human Services (HHS) must consider whether the covered entity or business associate adequately demonstrated that it had in place “recognized security practices” for at least 12 months prior that would:
  - Mitigate HIPAA fines
  - Result in the early, favorable termination of a HIPAA audit
  - Mitigate the remedies in a HIPAA resolution agreement with HHS
- ▶ Under the law, the term “recognized security practices” means “the standards, guidelines, best practices, methodologies, procedures, and processes developed under...the NIST Act, the approaches promulgated under...the Cybersecurity Act of 2015, and other programs and processes that address cybersecurity and that are developed, recognized, or promulgated through regulations under other statutory authorities.”

11

11

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

## Risk Assessment

**Risk Severity Matrix**

|                   |   |                    |          |          |          |          |
|-------------------|---|--------------------|----------|----------|----------|----------|
| <b>Likelihood</b> |   |                    |          |          |          |          |
| Almost Certain    | 5 | Moderate           | High     | Extreme  | Extreme  | Extreme  |
| Likely            | 4 | Moderate           | Moderate | High     | Extreme  | Extreme  |
| Possible          | 3 | Low                | Moderate | Moderate | High     | Extreme  |
| Unlikely          | 2 | Low                | Low      | Moderate | High     | High     |
| Rare              | 1 | Low                | Low      | Low      | Moderate | Moderate |
|                   |   | 1                  | 2        | 3        | 4        | 5        |
|                   |   | Insignificant      | Minor    | Moderate | Major    | Critical |
|                   |   | <b>Consequence</b> |          |          |          |          |

12

12



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge

Ohio

Risk Assessment

What is the Security Risk Assessment Tool (SRA Tool)?

The Office of the National Coordinator for Health Information Technology (ONC), in collaboration with the HHS Office for Civil Rights (OCR), developed a downloadable Security Risk Assessment (SRA) Tool to help guide you through the process. The tool is designed to help healthcare providers conduct a security risk assessment as required by the HIPAA Security Rule and the Centers for Medicare and Medicaid Service (CMS) Electronic Health Record (EHR) Incentive Program. The target audience of this tool is medium and small providers; thus, use of this tool may not be appropriate for larger organizations.

13

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge

Ohio

Risk Assessment

SRA Tool for Windows

The SRA Tool is a desktop application that walks users through the security risk assessment process using a simple, wizard-based approach. Users are guided through multiple-choice questions, threat and vulnerability assessments, and asset and vendor management. References and additional guidance are given along the way. Reports are available to save and print after the assessment is completed.

This application can be installed on computers running 64-bit versions of Microsoft Windows 7/8/10/11. All information entered into the tool is stored locally on the user's computer. HHS does not collect, view, store, or transmit any information entered into the SRA Tool.

Download Version 3.3 of the SRA Tool for Windows [.msi - 70.3 MB]

14



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

Resources

Cybersecurity Framework Components

Cybersecurity outcomes and informative references  
Enables communication of cyber risk across an organization

CORE

TIERS

PROFILE

CYBERSECURITY  
FRAMEWORK

Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics

Aligns industry standards and best practices to the Framework Core in an implementation scenario  
Supports prioritization and measurement while factoring in business needs

8

15

15

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

Resources

Resources

[www.nist.gov/cyberframework/industry-resources](http://www.nist.gov/cyberframework/industry-resources)

Framework  
New to Framework  
Perspectives  
Success Stories  
Online Learning  
Evolution  
Frequently Asked Questions  
Events and Presentations  
Related Efforts (Roadmap)  
Informative References  
Resources  
Newsroom

Framework Resources

RECOVER

IDENTIFY

PROTECT

DETECT

RESPOND

FRAMEWORK

General Resources sorted by User Group:

- Critical Infrastructure
- Small and Medium Business
- International
- Federal
- State Local Tribal Territorial Governments
- Academia
- Assessments & Auditing
- General

Over 150 Unique Resources for Your Understanding and Use!

35

16

16

Leading Age Momentum 2022

8



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

Resources

Core

A Catalog of Cybersecurity Outcomes

|   | Function |   |
|---|----------|---|
| What processes and assets need protection?        | Identify | • Understandable by everyone                  |
| What safeguards are available?                    | Protect  | • Applies to any type of risk management      |
| What techniques can identify incidents?           | Detect   | • Defines the entire breadth of cybersecurity |
| What techniques can contain impacts of incidents? | Respond  | • Spans both prevention and reaction          |
| What techniques can restore capabilities?         | Recover  |   |

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

Crosswalks for Compliance

| Function  | Category | Subcategory  | 800-53 Sub Cat | NIST SP 800-53 Rev 4    | 800-1 | HIPAA Security Rule 45 C.F.R. §§   |
|---|----------|--|----------------|-------------------------|-------|--|
| Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. |          | ID.AM-1: Physical devices and systems within the organization are inventoried  | ID.AM-1        | CM-8, PM-5              | CM-8  | 164.308(a)(1)(ii)(A), 164.310(a)(2)(ii), 164.310(d)  |
|   |          | ID.AM-2: Software platforms and applications within the organization are inventoried   | ID.AM-2        | CM-8, PM-5              | CM-8  | 164.308(a)(1)(ii)(A), 164.308(a)(7)(ii)(E)   |
|   |          | ID.AM-3: Organizational communication and data flows are mapped  | ID.AM-3        | AC-4, CA-3, CA-9, PL-8  | AC-4  | 164.308(a)(1)(ii)(A), 164.308(a)(8), 164.310(d)  |
|   |          | ID.AM-4: External information systems are catalogued   | ID.AM-4        | AC-20, SA-9             | AC-20 | 164.308(a)(4)(ii)(A), 164.308(b), 164.314(a)(1), 164.314(a)(2)(i)(B), 164.314(a)(2)(ii), 164.316(b)(2) |
|   |          | ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value | ID.AM-5        | CP-2, RA-2, SA-14, SC-6 | CP-2  | 164.308(a)(7)(ii)(E)   |
|   |          | ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established   | ID.AM-6        | CP-2, PS-7, PM-11       | CP-2  | 164.308(a)(2), 164.308(a)(3), 164.308(a)(4), 164.308(b)(1), 164.314                                    |



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### Crosswalks for Compliance

| Function  | Category   | Subcategory | CIS | CIS - 1 | CIS - 2 | CIS - 3 | CIS - 4 | CIS - 5 | CIS - 6 | CIS - 7 | CIS - 8 | HW&Co. Policy - 1                            | HW&Co. Policy - 2                            | HW&Co. Policy - 3                 | HW&Co. Policy - 4                 | HW&Co. Policy - 5               |
|---|--|-------------|-----|---------|---------|---------|---------|---------|---------|---------|---------|--|--|-----------------------------------|-----------------------------------|---------------------------------|
| Asset Management (ID-AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. | ID-AM-1: Physical devices and systems within the organization are inventoried  | CSC 1       | 1   |         |         |         |         |         |         |         |         | Risk Analysis and Management Policy          | Physical Access Controls Policy              | Mobile Device Policy              | SYSTEMS Security and Usage Policy | Malware Protection Suite Policy |
|   | ID-AM-2: Software platforms and applications within the organization are inventoried   | CSC 2       | 2   |         |         |         |         |         |         |         |         | Risk Analysis and Management Policy          | Security Incidents Policy                    | SYSTEMS Security and Usage Policy | Contingency Policy                | Network Backup Policy           |
|   | ID-AM-3: Organizational communication and data flows are mapped  | CSC 12      | 12  |         |         |         |         |         |         |         |         | Risk Analysis and Management Policy          | Security Sanctions Policy                    | Mobile Device Policy              | SYSTEMS Security and Usage Policy | Separation Policy               |
|   | ID-AM-4: External information systems are catalogued   | CSC 12      | 12  |         |         |         |         |         |         |         |         | HIPAA Privacy and Security Compliance Policy |  |                                   |                                   |                                 |
|   | ID-AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value | CSC 13, 14  | 13  | 14      |         |         |         |         |         |         |         | SYSTEMS Security and Usage Policy            | Security Incidents Policy                    | Contingency Policy                | Network Backup Policy             |                                 |
|   | ID-AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established   | CSC 17, 19  | 17  | 19      |         |         |         |         |         |         |         | Security Officer Job Description             | HIPAA Privacy and Security Compliance Policy | SYSTEMS Security and Usage Policy | Credentials Policy                | Physical Access Control Policy  |

NIST has over 109 sub-categories

19

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### Security Policies - BYOD

Device Management

▶ Control Access to Information

▶ Enforce Policies

- “Allowed” Applications
- Encryption

▶ Allow Security

- Password Requirements
- Lock Screen/Time Out

▶ Remote Wipe of Information

▶ Sandbox for Corporate Data

Tablet PC

IPAD

smart phone

iPhone 4/4s/5

Notebook

computer

WIFI

20

20

Leading Age Momentum 2022

10



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### Mobile Device Issues: Studies Show

- ▶ Users are more susceptible to social attacks they receive on mobile devices. This is the case for email-based spear phishing, spoofing attacks that attempt to mimic legitimate webpages, as well as attacks via social media.
- ▶ Mobile software also enhances the ease of action - accept, reply, send, like, and such - which makes it easier for users to respond to a request.
- ▶ They make it easier for users to make snap decisions.
- ▶ Users often interact with their mobile devices while walking, talking, driving, and doing all manner of other activities that interfere with their ability to pay careful attention to incoming information.

21

21

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### Easy Preventions

- ▶ 2nd Factor is the easiest/best protection against a hacker gaining access by either guessing credentials or tricking a user into giving them up
- ▶ Something you know + something you have
- ▶ A dedicated APP is better than a text message



22

22



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### Work Area Suggestions

- ▶ Be sure your work space is kept organized and ‘generic’
- ▶ Ensure proper destruction of material, not just the trash
- ▶ Don’t leave printers or faxes un-attended with printouts
- ▶ Ensure file cabinets are locked in public areas
- ▶ Don’t just return copiers without sanitizing/wiping/erasing them



23

23


MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### Common Business Problems

- ▶ Ransomware
- ▶ Email Phishing
- ▶ Business Email Compromise
- ▶ Wire Fraud
- ▶ Embezzlement/Insider Threats
- ▶ Stolen Equipment



24

24



**MOMENTUM**  
2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

25

25

**MOMENTUM**  
2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

26

26



**MOMENTUM**

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

## Ransomware-as-a-Service

- ▶ You can now buy a ‘canned’ Ransomware delivery vehicle
  - One time use
  - Rented monthly
  - Percentage of ransom received
  - Available ‘over the web’
- ▶ No longer need to be a super tech programmer to succeed

27

27

**MOMENTUM**

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

## Exploit Time Line – Example 1

- ▶ Microsoft Exchange Server exploit – 2021
- ▶ Jan 5 : First reported
- ▶ Jan 6 – Feb 2 : Continued reports of exploitation
- ▶ Mar 2 : Microsoft releases patches
- ▶ Ongoing : Ransomware Groups engage in mass exploitation of exploit

28

28



**MOMENTUM**  
2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge®  
Ohio

## Exploit Time Line – Example 2

- ▶ Log4j Exploit 2021
- ▶ Nov 24 : Vulnerability Reported
- ▶ Dec 9 : Exploits seen “in the wild”
- ▶ Dec 10 : NIST CVE Alert Published
- ▶ Dec 6 – 16 : Updates released
- ▶ Dec – Ongoing : Attackers scan for vulnerable systems

29

29

**MOMENTUM**  
2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge®  
Ohio

## National Cyber Awareness System

- ▶ Cybersecurity and Infrastructure Security Agency
- ▶ Publishes information in conjunction with DHS, FBI & Secret Service
- ▶ Usually contains reference material as well as detailed steps to detect, defend and mitigate

30

30





MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### Sample CISA Email/Alert



DEFEND TODAY, SECURE TOMORROW

You are subscribed to National Cyber Awareness System Current Activity for Cybersecurity and Infrastructure Security Agency. This information has recently been updated, and is now available.

[CISA Issues Emergency Directive and Alert on Microsoft Exchange Vulnerabilities](#)

03/03/2021 03:14 PM EST

Original release date: March 3, 2021

CISA has issued Emergency Directive (ED) 21-02 and Alert AA21-062A addressing critical vulnerabilities in Microsoft Exchange products. Successful exploitation of these vulnerabilities allows an attacker to access on-premises Exchange servers, enabling them to gain persistent system access and control of an enterprise network.

CISA strongly recommends organizations examine their systems to detect any malicious activity detailed in Alert AA21-062A. Review the following resources for more information:

- [CISA Emergency Directive 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities](#)
- [AA21-062A: Mitigate Microsoft Exchange Server Vulnerabilities](#)
- [Microsoft Security Blog Post: Multiple Security Updates Released for Exchange Server](#)

31

31

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### Ransomware “Gangs”

- ▶ 15 or so Active Groups
  - Conti – 15.5%
  - Revil/Sodinokibi – 7.1%
  - Remainder 4.8% or less

**Most use multi-extortion tactics to try and boost their ‘payments’**

32

32



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

Conti Group

▶ Avg ransomware demand 2021 - \$1.78 million

▶ Over 600 companies affected during 2020-2022

▶ “Ruthless” in their approach

- No observance of any “code of honor” that is used by some other groups
  - Targets hospitals
  - Emergency services
  - Law enforcement

▶ Uses double extortion to ‘shame’ companies into paying

33

33

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

Demands vs Payments

▶ 2020 : Demand - \$906,000

▶ 2020 : Payment - \$303,000

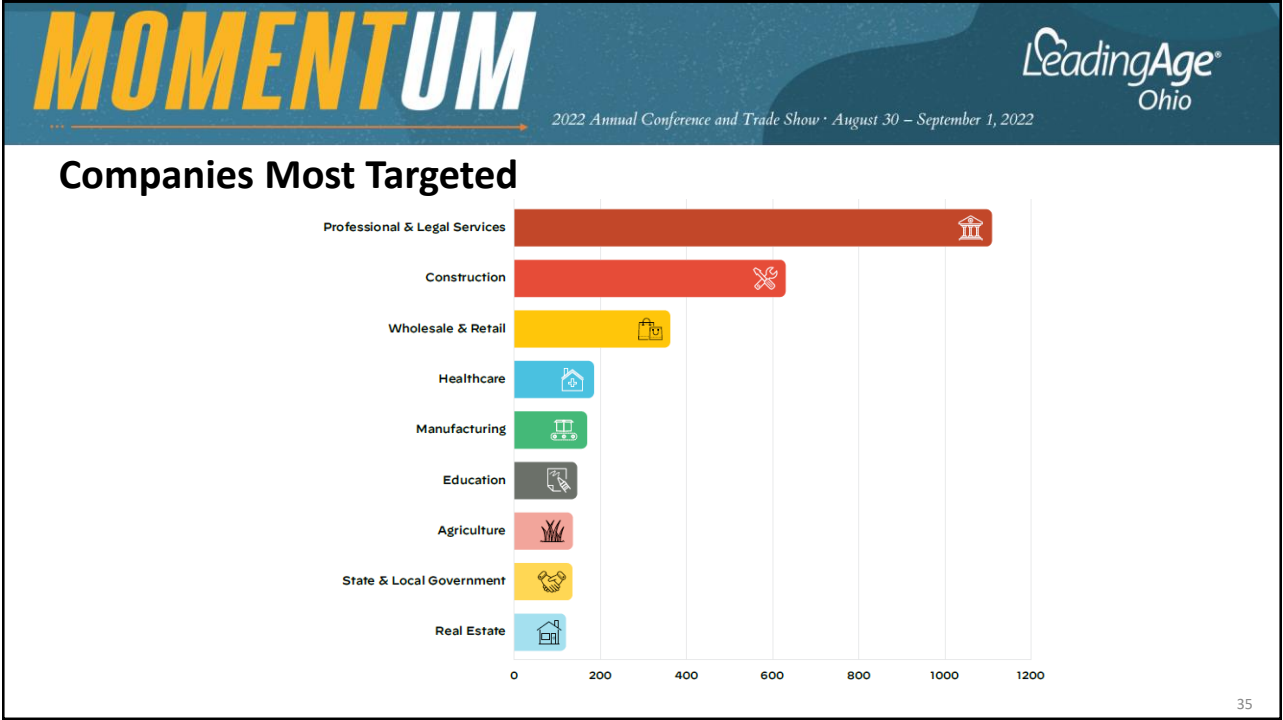
▶ 2021 : Demand - \$2,200,000

▶ 2021 : Payment - \$540,000

34

34





35



36



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### Recovery Times

- ▶ 41% recovered within 1 Month
- ▶ 58% recovered in 2 to > 6 Months
- ▶ 58% paid the ransom
- ▶ 14% paid more than once

37

37

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### Payments and Data Recovery

- ▶ 99% got some encrypted data back after paying
- ▶ After paying : Only got 61% of data back
- ▶ Only 4% got all their data back

38

38



**MOMENTUM**  
... —————→ 2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge®  
Ohio

39

39

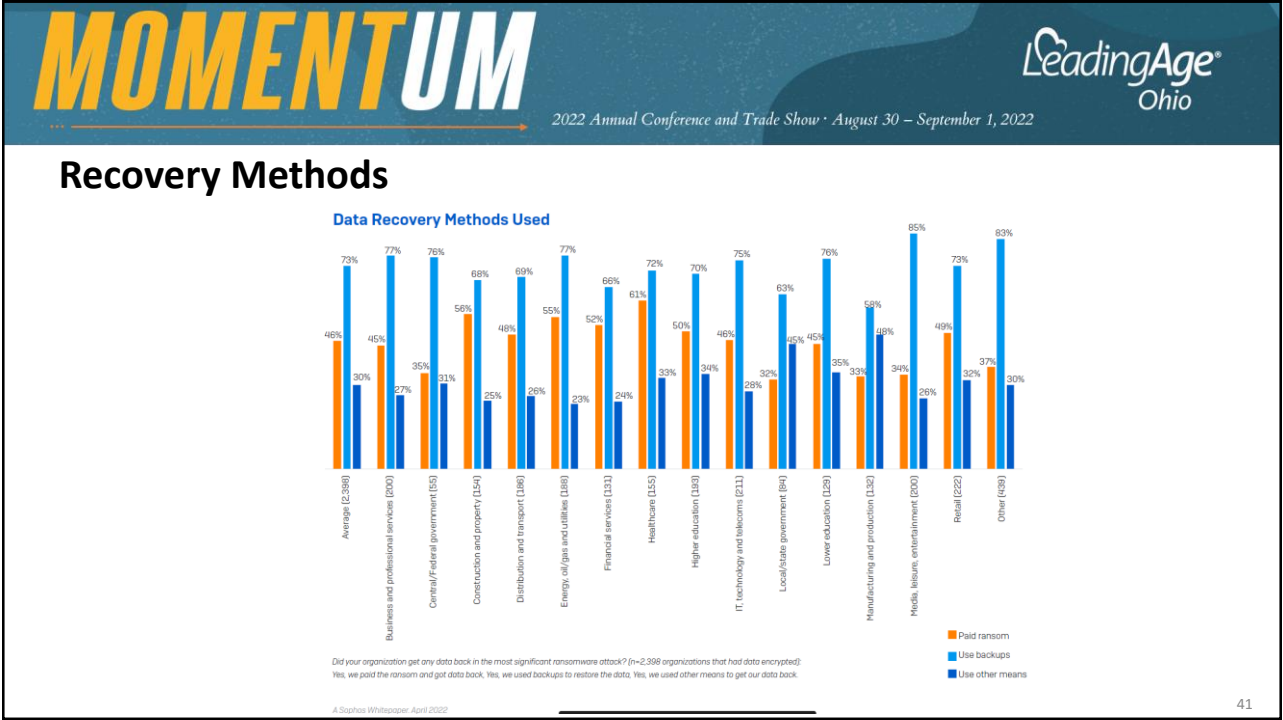
**MOMENTUM**  
... —————→ 2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge®  
Ohio

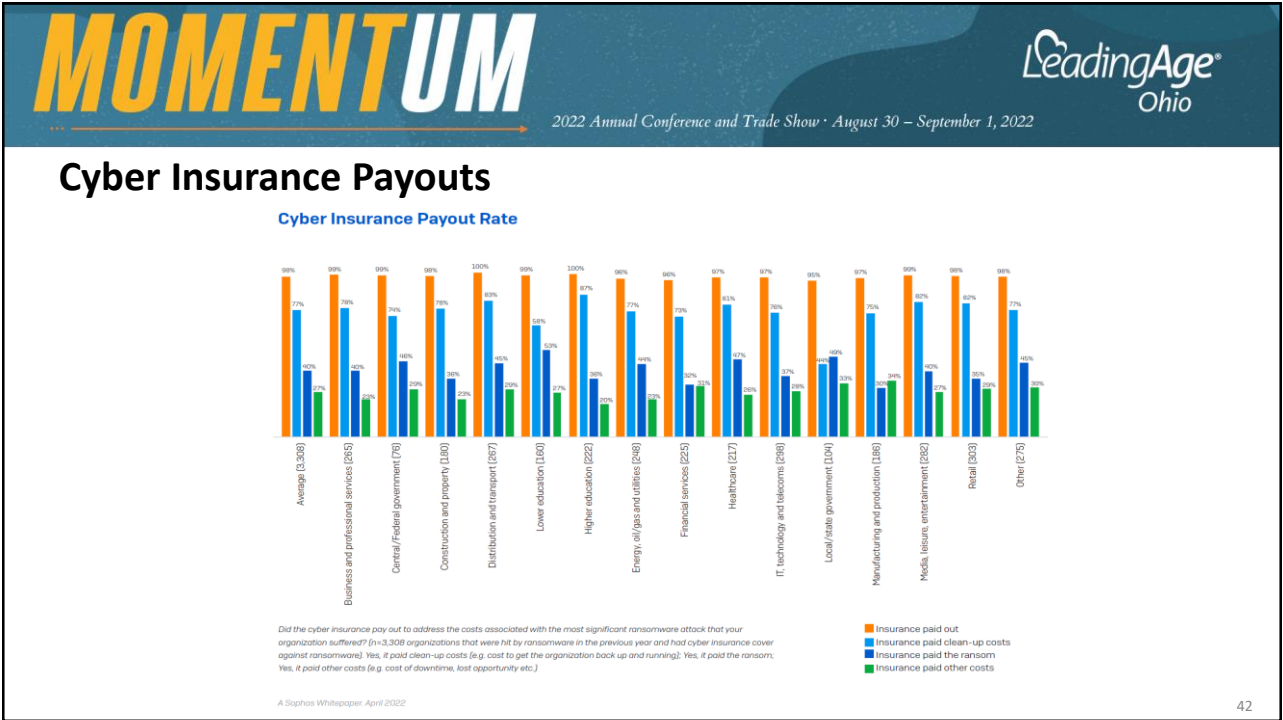
40

40





41



42



**MOMENTUM**  
... → 2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge®  
Ohio

## Ransomware Protections

1. Email education
2. Software/Equipment patching
3. 2<sup>nd</sup> factor authentication
4. GEO restrictions on logins
5. Limit concurrent logins
6. Network permissions segregation

43

43

**MOMENTUM**  
... → 2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge®  
Ohio

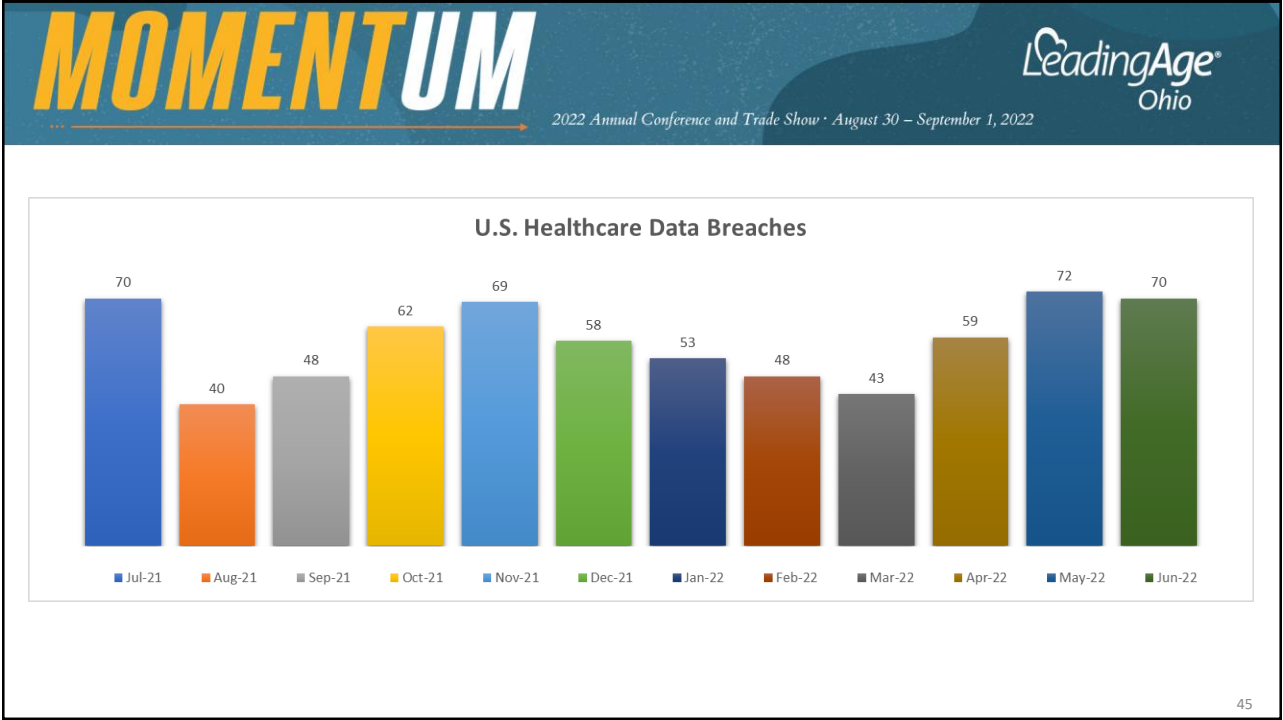
## Ransomware Mitigations

1. Complete backups – offline
2. Disaster Plan / Incident Plan
3. Data loss prevention protocols
4. Written Information Security Policies
5. Cyber Insurance

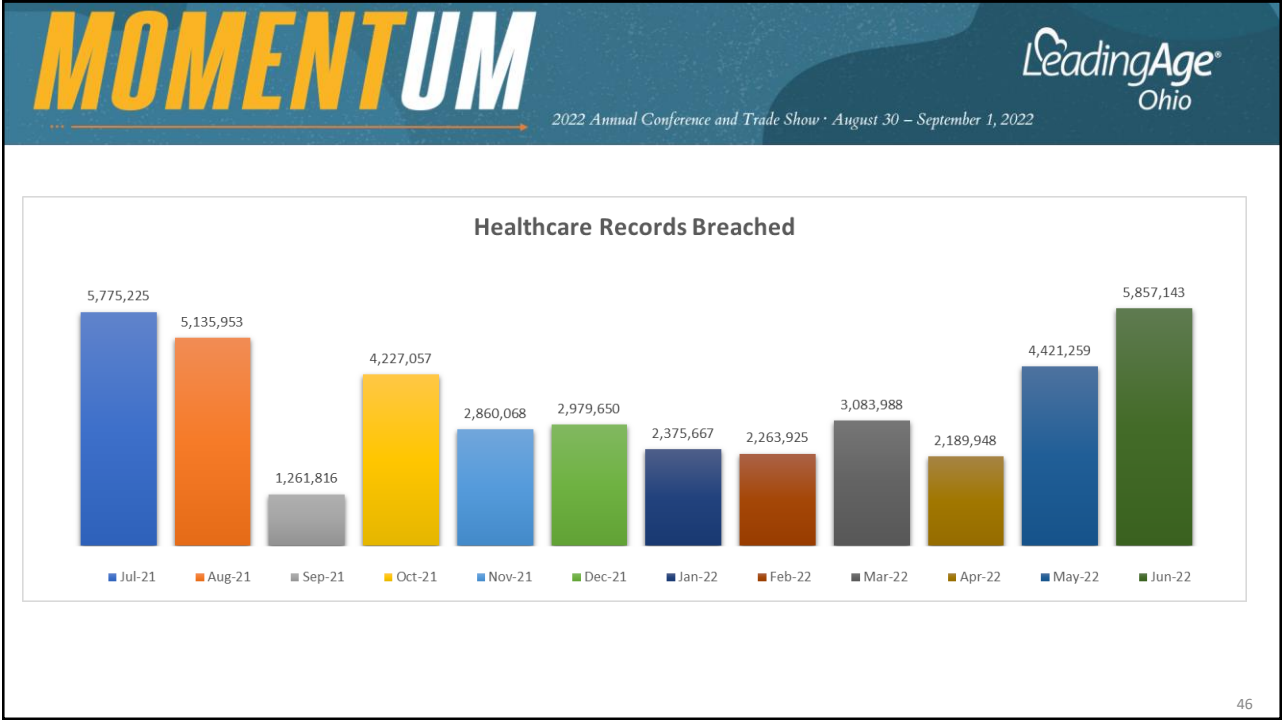
44

44



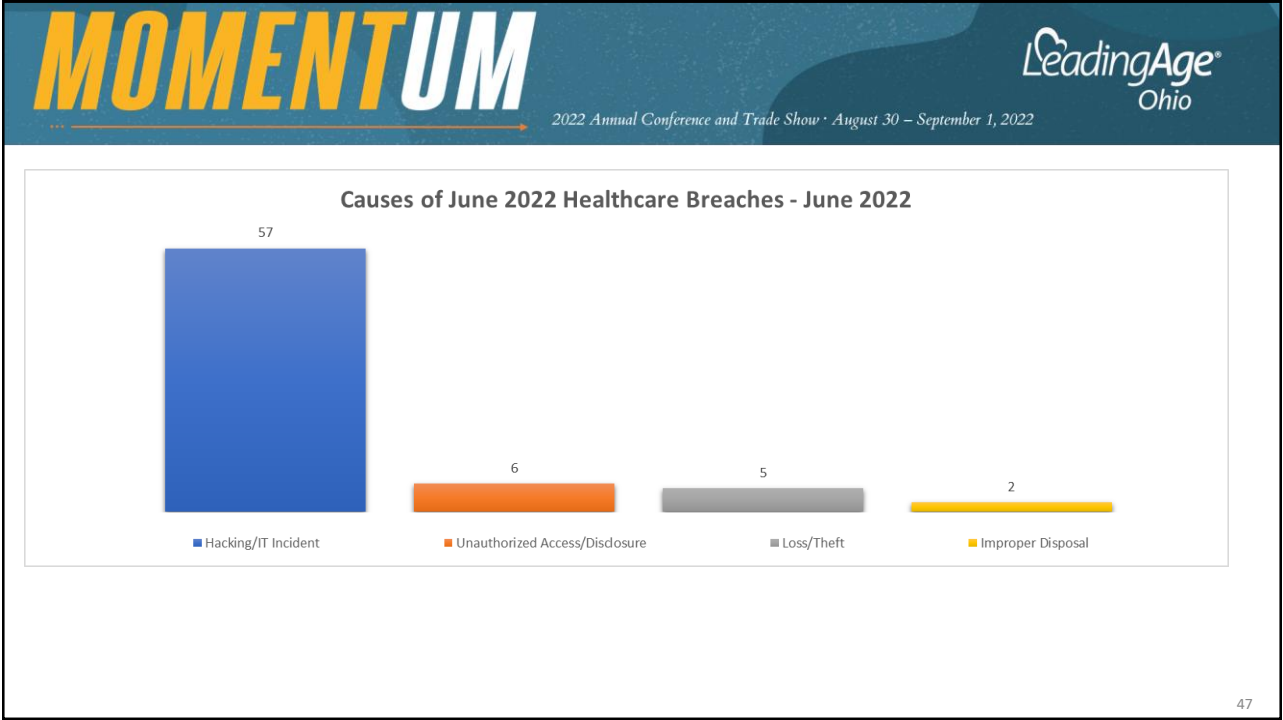


45

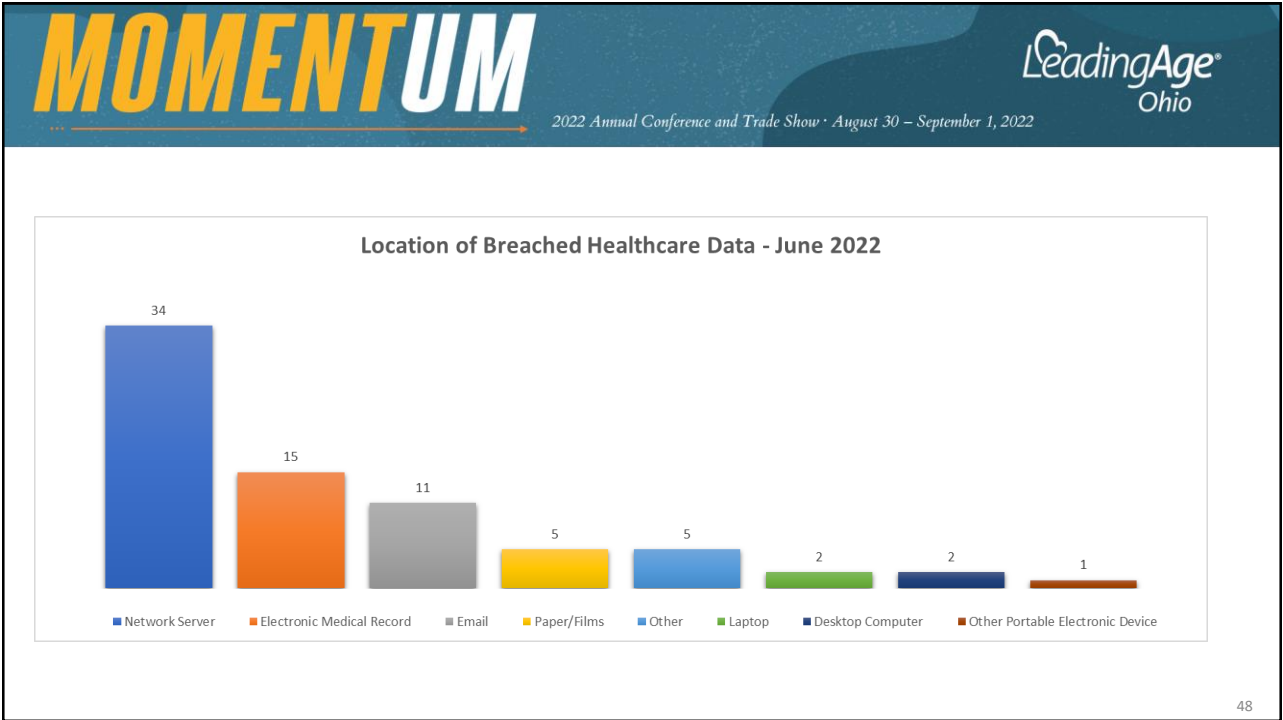


46



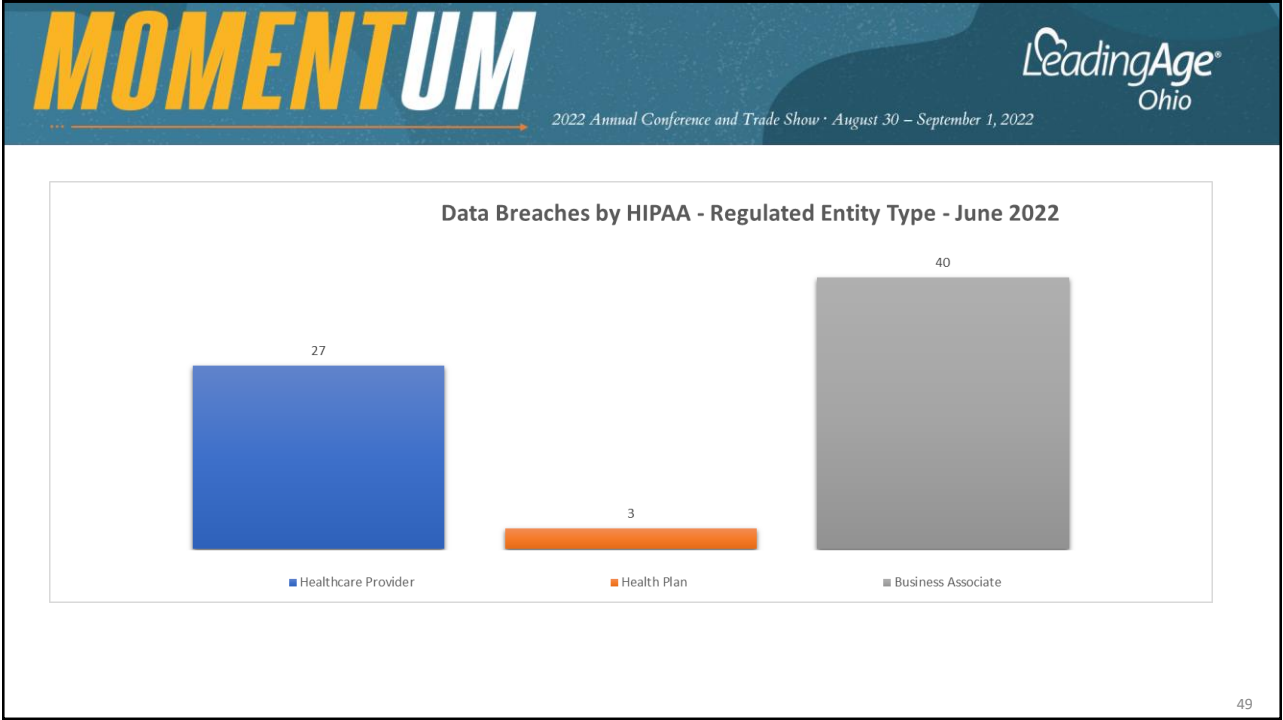


47

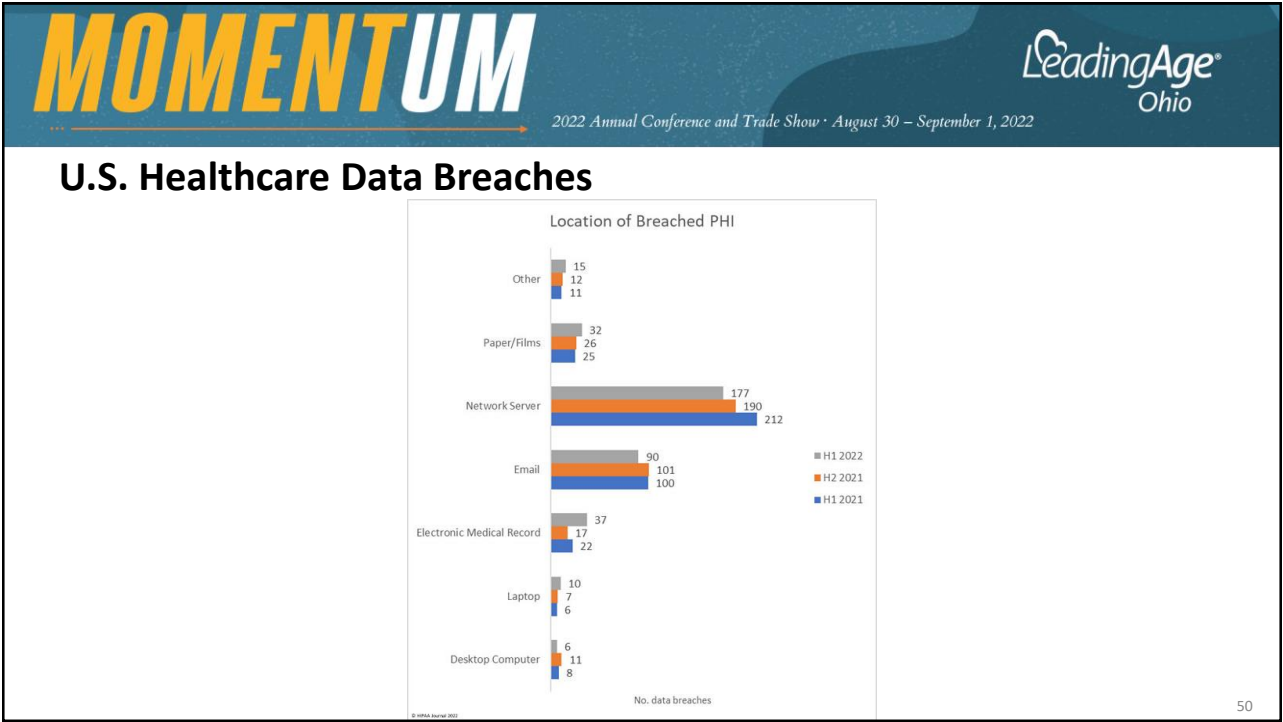


48





49



50



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### U.S. Healthcare Data Breaches – May

| State   | Number of Data Breaches |
|---|-------------------------|
| New York  | 7                       |
| Ohio  | 6                       |
| California  | 4                       |
| Arizona, Georgia, Kansas, Michigan, Tennessee, & Virginia   | 3                       |
| Florida, Maryland, North Carolina & New Hampshire   | 2                       |
| Alabama, Arkansas, Colorado, Connecticut, Illinois, Nebraska, North Dakota, Pennsylvania, South Carolina, Utah, Vermont, Washington & West Virginia | 1                       |

51

51

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### 2021 - 2022 HIPAA Fines/Settlements

|                                 |    |            |           |   |                 |  |
|---------------------------------|----|------------|-----------|---|-----------------|--|
| Memorial Hermann Health System  | TX | Settlement | \$240,000 | 1 | Untimely Access | Records not provided in full for 564 days from the initial request           |
| Lawrence Bell, Jr. D.D.S.       | MD | Settlement | \$5,000   | 1 | Untimely Access | Failure to provide records for more than 3 months                            |
| Danbury Psychiatric Consultants | MA | Settlement | \$3,500   | 1 | Untimely Access | Withheld records for 6 months as the patient had an outstanding medical bill |

| HIPAA Regulated Entity 2021 | Reason   | Individuals Impacted | Amount           |
|-----------------------------|--|----------------------|------------------|
| Misc. 13 Entities           | HIPAA Right of Access failure  | 13                   | \$67,000 average |
| Excellus Health Plan        | Multiple HIPAA Violations: Risk analysis, risk management, information system activity reviews, technical policies | 9,358,891            | \$5,100,000      |

52

52



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### 2020 - 2021 States Fines/Settlements

| Year | State      | Covered Entity   | Amount                         |
|------|------------|--|--------------------------------|
| 2021 | New Jersey | Regional Cancer Care Associates (Regional Cancer Care Associates LLC, RCCA MSO LLC, and RCCA MD LLC) | \$425,000                      |
| 2021 | New Jersey | Command Marketing Innovations, LLC and Strategic Content Imaging LLC                                 | \$130,000 (\$65,000 suspended) |
| 2021 | New Jersey | Diamond Institute for Infertility and Menopause  | \$495,000                      |
| 2021 | Multistate | American Medical Collection Agency   | \$21 million (suspended)       |
| 2020 | Multistate | CHSPSC LLC   | \$5,000,000                    |
| 2020 | Multistate | Anthem Inc.  | \$39.5 million                 |
| 2020 | California | Anthem Inc.  | \$8.7 million                  |

53

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### Effects of Security Lapses

► Reputation Loss


► Litigation

► Fines

► Disruption of Business

► Future Enhanced Audits/Scrutiny

► Financial Losses (external and internal perpetrators)



54



**MOMENTUM**  
... → 2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge®  
Ohio

55

55

**MOMENTUM**  
... → 2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge®  
Ohio

56

56



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### Phishing Email Traits

- ▶ Lots of attachments
- ▶ Sense of urgency
- ▶ Grammatical errors
- ▶ Too good to be true
- ▶ Unusual sender
- ▶ Hyperlinks
- ▶ Generic terms and salutations

57

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### Email Examination

The screenshot shows an email interface with the following details:

- From:** Amazon <management@amazoncanada.ca> on behalf of [redacted] (Annotation: not an Amazon email address (note the missing A in Amazon))
- To:** @shendanc.on.ca
- Cc:**
- Subject:** Suspension

The email body features the Amazon logo and the text "amazon.com". Below this is a red box around "Dear Client," with an annotation: "Generic non-personalized greeting".

The main body text reads: "We have sent you this e-mail, because we have strong reason to belive, your account has been used by someone else. In order to prevent any fraudulent activity from occurring we are required to open an investigation into this matter. We've locked your Amazon account, and you have 36 hours to verify it, or we have the right to terminate it."

Below the text is a red box around the link: "https://www.amazon.com/exec/obidos/sign-in.html". An annotation points to it: "Hovering over the link reveals it points to a non-Amazon site - 'http://redirect.kereskedj.com'".

The email ends with "Sincerely, The Amazon Associates Team" and a small Amazon logo. The footer says "© 1996-2013, Amazon.com, Inc. or its affiliates".

58



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### Sample Phishing Email

From: Internal Revenue Service [irs-service@IRS.GOV]  
To:  
Cc:  
Subject: Official Notification

Sent: Tue 2/3/2009 3:55 PM

After the last annual calculations of your fiscal are eligible to receive a tax refund of \$92.50. Please submit the tax refund request and allow us 3-6 days in order to process it. A refund can be delayed for a variety of reasons. For example submitting invalid records or applying after the deadline.

To access the form for your tax refund, please click here :  
<http://cimaonline.ca/form/Internal/Revenue/Service/index.html>

Regards,  
Internal Revenue Service.

© Copyright 2009, Internal Revenue Service U.S.A.

Phishing emails are often sent from addresses that look official.

Clicking on this link would take you to a fraudulent website with a form to enter your personal information.

Notice that the URL does not direct you to an official IRS website.

59

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### Sample Phishing Email

Re: Office 365 - Update

Office365 - System <gmarsh@noblesys.com>  
To: websupdate@office365.microsoft.com

↩ Reply

↩ Rep

If there are problems with how this message is displayed, click here to view it in a web browser.

Action Items

## Office 365 - Update

Dear user

This message is being sent to you to inform you that your account is to be closed

If you wish to continue using this account please upgrade to our services. Ignoring this message will cause your account to be closed

Update your account

Note: Please take a few moment to update your account now

Thanks

Regards  
Microsoft.com Team

60



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### Common Sense Email Safety

protocol

third-level Domain

second-level domain

top-level domain

directory

file

https://www.exampleurl.com/info/aboutus.html

subdomain name

domain name

page

host name

path

Left to Right, find first “/” after any “//”, stuff right before ‘dot’ something matters most

http://www.email-content.somethingelse.reallylong.chase.com/email.html - probably OK

http://www.chase.really-long.beachwood33k3.com/email.html - probably NOT

61

61

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### Security Incidents Timeline

Compromise, (n=140)

| Time Frame | Percentage |
|------------|------------|
| Seconds    | 0%         |
| Minutes    | ~50%       |
| Hours      | ~20%       |
| Days       | ~15%       |
| Weeks      | ~10%       |
| Months     | ~5%        |
| Years      | ~2%        |

Ransomware has decreased the Discovery and Containment time frames dramatically.

| Time Frame                              | Days |
|---|------|
| Occurrence to Discovery                 | 12   |
| Discovery to Containment                | 0    |
| Time to Complete Forensic Investigation | 36   |
| Discovery to Notification               | 66   |

62

62



63

63

64

64



MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### CyberSecurity Mitigations

1. Use complex Passwords. Use different ones on each site. Consider phrases. Use a password manager.
2. Keep Logins different. Don't use your email address.
3. Don't share Passwords/Logins.
4. Don't trust any email links.
5. Use 2<sup>nd</sup> Factor Authentication on everything.
6. Keep your inbox clean.
7. Logout/Lock your workstation when you leave, don't forget about your phone.
8. Never input your work network credentials on any external site.
9. Encrypt all Flash Drives - Bitlocker
10. Never send confidential info thru regular email, use encryption or a Portal.

65

65

MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio

### Cyber Insurance Check List

- ▶ Breach Response Plan?
- ▶ Insurance Broker/Agent?
  - How to file a claim
  - Contacts at Insurance Company
- ▶ Business Attorney for Cyber?
- ▶ Forensic Company?
- ▶ Secret Service Contact?
- ▶ FBI and Local Law Enforcement?



66

66



67

68



# MOMENTUM

2022 Annual Conference and Trade Show · August 30 – September 1, 2022

LeadingAge  
Ohio



**Mike Shoffner**  
216-378-7284  
Michael.Shoffner@hwco.cpa

HW&Co.  
CPAs & Advisors