Cybersecurity for Home Care and Hospice Providers

Virtual Forum

April 2, 2025

HCP | NYS Home Care Providers FOUNDATION

Research & Educational Resources for Home and Community-Based Care

EDUCATION & RESEARCH, INC
HCA
E&R
501(c)(3)

Hospice & Palliative Care Association of New York State

Representing Home and Community-based Care

- New York State Association of Health Care Providers (HCP)
- Home Care Association of New York State (HCANYS)
- Hospice & Palliative Care Association of New York State (HPCANYS)

Housekeeping

For today's program, you have the option for dial in or computer audio. Please note that computer audio can be impacted by your internet connection.

Please feel free to ask questions during today's presentation using the chat box. Note that direct messages cannot be retained after the close of the webinar. Remember that we do have an open discussion period near the end of the Forum.

We ask that you **keep your microphone muted** for the duration of the program. Repeatedly interrupting the program with unmuted conversations may lead to us removing you from the webinar and we would hate for you to miss this important and timely update.

Slides and a recording of the program will be emailed to all registrants. These materials will also be publicly available on each association's website.

Grant Disclaimer and Acknowledgments

- This project was supported by the Department of Health and Human Services' Administration for Strategic Preparedness and Response under award number 1U3REP240780-01. Its content is solely the responsibility of the authors and does not necessarily represent the official views of the Department of Health and Human Services' Administration for Strategic Preparedness and Response.

- This Emergency Preparedness Forum was made possible by a grant from the NYC Department of Health and Mental Hygiene (DOHMH) Office of Emergency Preparedness and Response (OEPR).

- Special thanks to Fidelle Munroe, Senior Program Manager, LTC, Bureau of Healthcare and Community Readiness, Office of Emergency Preparedness and Response, NYC Department of Health and Mental Hygiene for her support of the associations' emergency preparedness work.

Emergency Management Forum for NYC Home Care and Hospice Providers

AGENDA

- Welcome and Introductions
- Cybersecurity Expert Panel Presentation
- Panel Question & Answer
- Association Emergency Management Updates
- Open Discussion

Introductions

- Eva Cohen, Director of Regulatory and Community Affairs, HPCANYS
- Al Cardillo, President and CEO, HCANYS
- Rebecca Gray, Executive Vice President for Clinical and Program Affairs, HCANYS
- Fidelle Munroe, Senior Program Manager for Long Term Care (LTC) in the New York City Department of Health and Mental Hygiene (NYC DOHMH) in the Office of Emergency Preparedness and Response (OEPR), in the Bureau of Health Care and Community Readiness (BHCR)
- Carole Deyoe, RPh, Director of Regulatory and Special Programs, HCP

Expert Panel

- **Dennis O'Connell**

Director of Security Solutions at Custom Computer Specialists

- **Justin Bain**

CISSP, HCISPP, VP Information Security Officer VNS Health

- **Crystal Wilson**

CISA Cyber State Coordinator Region 2

Dennis Ast, OneGroup

Dennis Ast has over 30 years of experience in the insurance and risk management industry, and has been a Senior Account Executive with OneGroup since 2017. Dennis looks for opportunities to help his clients reduce their overall cost of risk by developing a deep understanding of their business and risk management needs. He has become an expert resource for cyber insurance, among other topics, for both his colleagues and clients.

Dennis graduated from the State University College at Buffalo with a Bachelor of Science in Mathematics and earned his Master’s Degree from Boston University in Insurance Management. Dennis completed Chubb and Carnegie Mellon University’s Heinz College of Information Systems and Public Policy’s Cyber COPE Insurance Certification SM for his CCIC designation.

Cybersecurity for Home Care and Hospice Providers

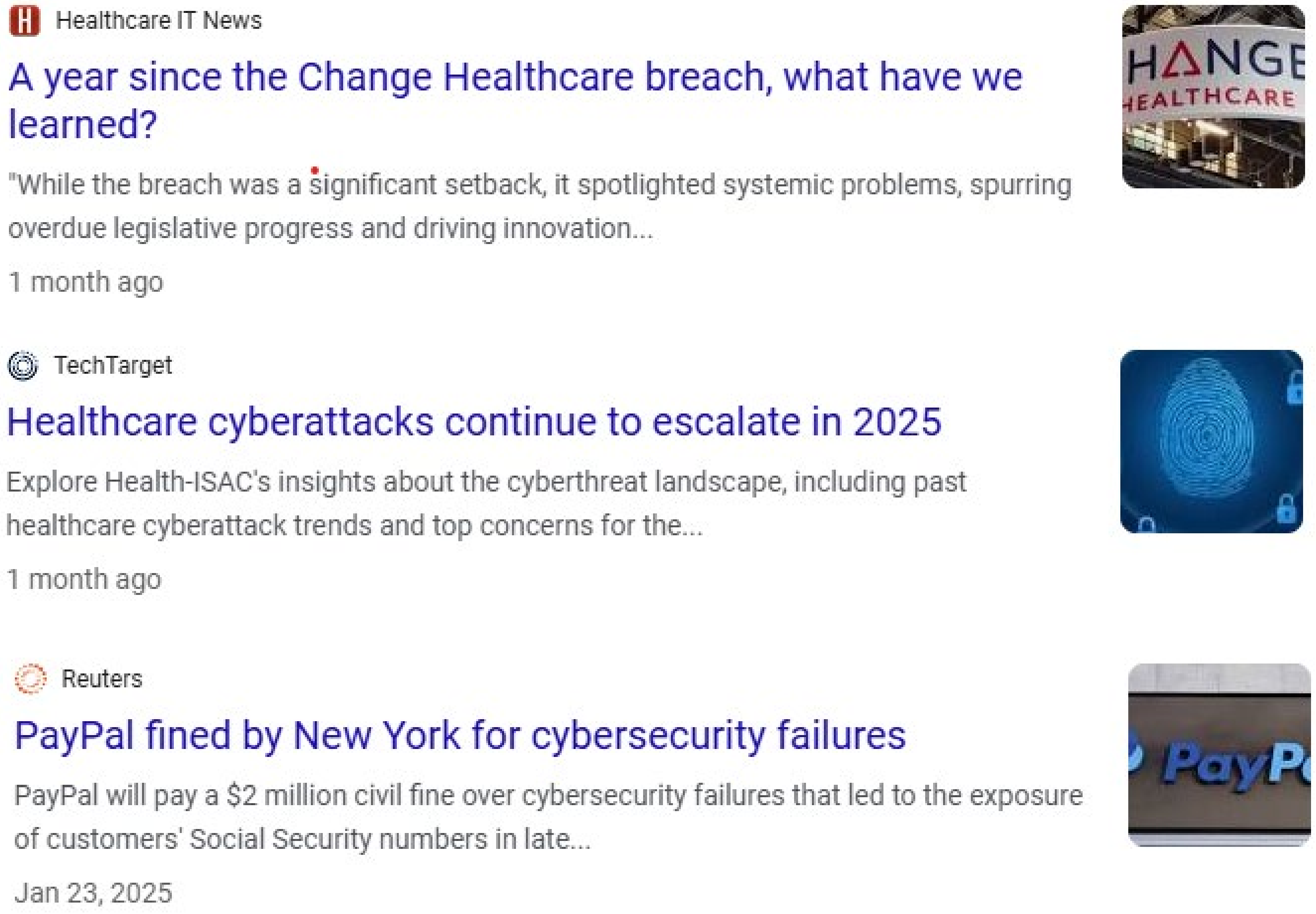
PRESENTED BY

DENNIS AST, CPCU, CCIC

ONEGROUP®

A World of Risk Management and Insurance Expertise

In the News:



Healthcare IT News

A year since the Change Healthcare breach, what have we learned?

"While the breach was a significant setback, it spotlighted systemic problems, spurring overdue legislative progress and driving innovation...

1 month ago

TechTarget

Healthcare cyberattacks continue to escalate in 2025

Explore Health-ISAC's insights about the cyberthreat landscape, including past healthcare cyberattack trends and top concerns for the...

1 month ago

Reuters

PayPal fined by New York for cybersecurity failures

PayPal will pay a $2 million civil fine over cybersecurity failures that led to the exposure of customers' Social Security numbers in late...

Jan 23, 2025

CHANGE HEALTHCARE
Part of Optum

CDK Global

CROWDSTRIKE

Quick Facts

- Business email compromise is now the top method of cyberattack, according to a survey from cybersecurity firm Arctic Wolf.
- Roughly one-third of all breaches involved Ransomware or some other Extortion technique. (Verizon Data Breach Report 2024)
- Per the 2024 DBIR for Healthcare Threat Actors 70% Internal and 30% External ((Verizon Data Breach Report 2024)
- On average, it takes a business 277 days to identify and contain a breach. Under 200 days average cost was $3.93m compared to over 200 days average of $4.95m (IBM Cost of Data Breach Report 2023)
- The human element continues to drive breaches. This year, 68% of breaches involved the human element (Verizon Data Breach Report 2024)

Healthcare Trends

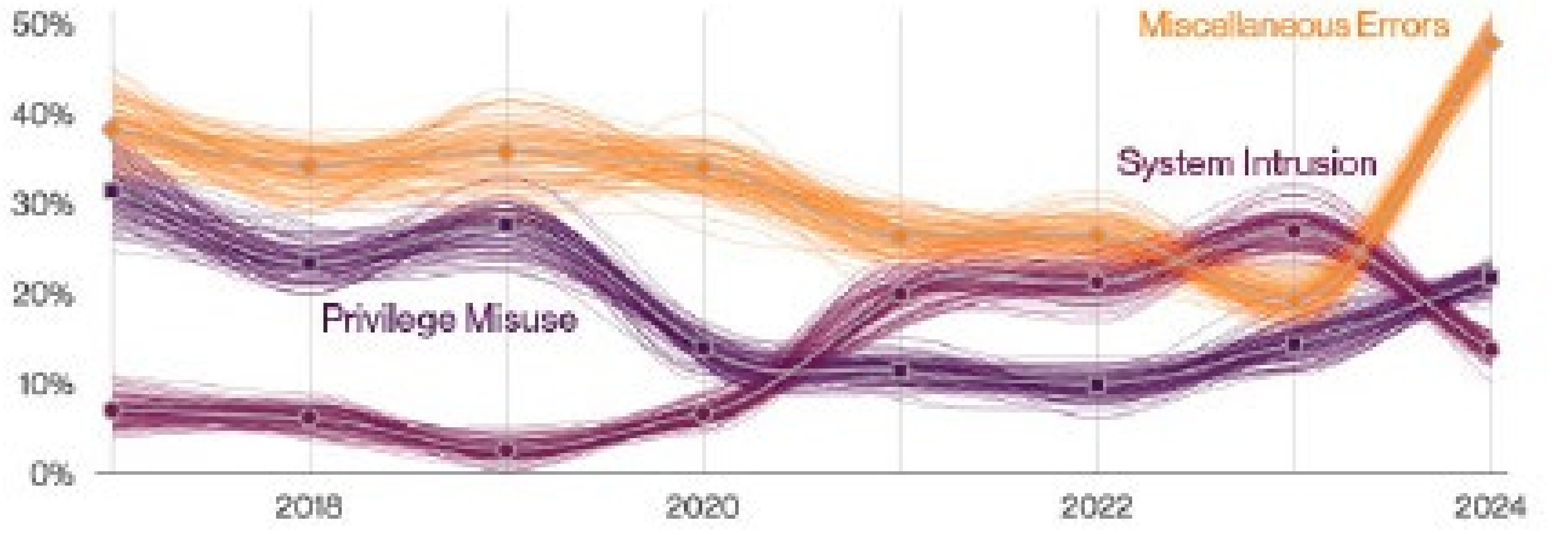


Figure 62. Top patterns in Healthcare industry breaches

https://www.verizon.com/business/resources/T346/reports/2024-dbir-data-breach-investigations-report.pdf

Cyber Insurance as a Resource

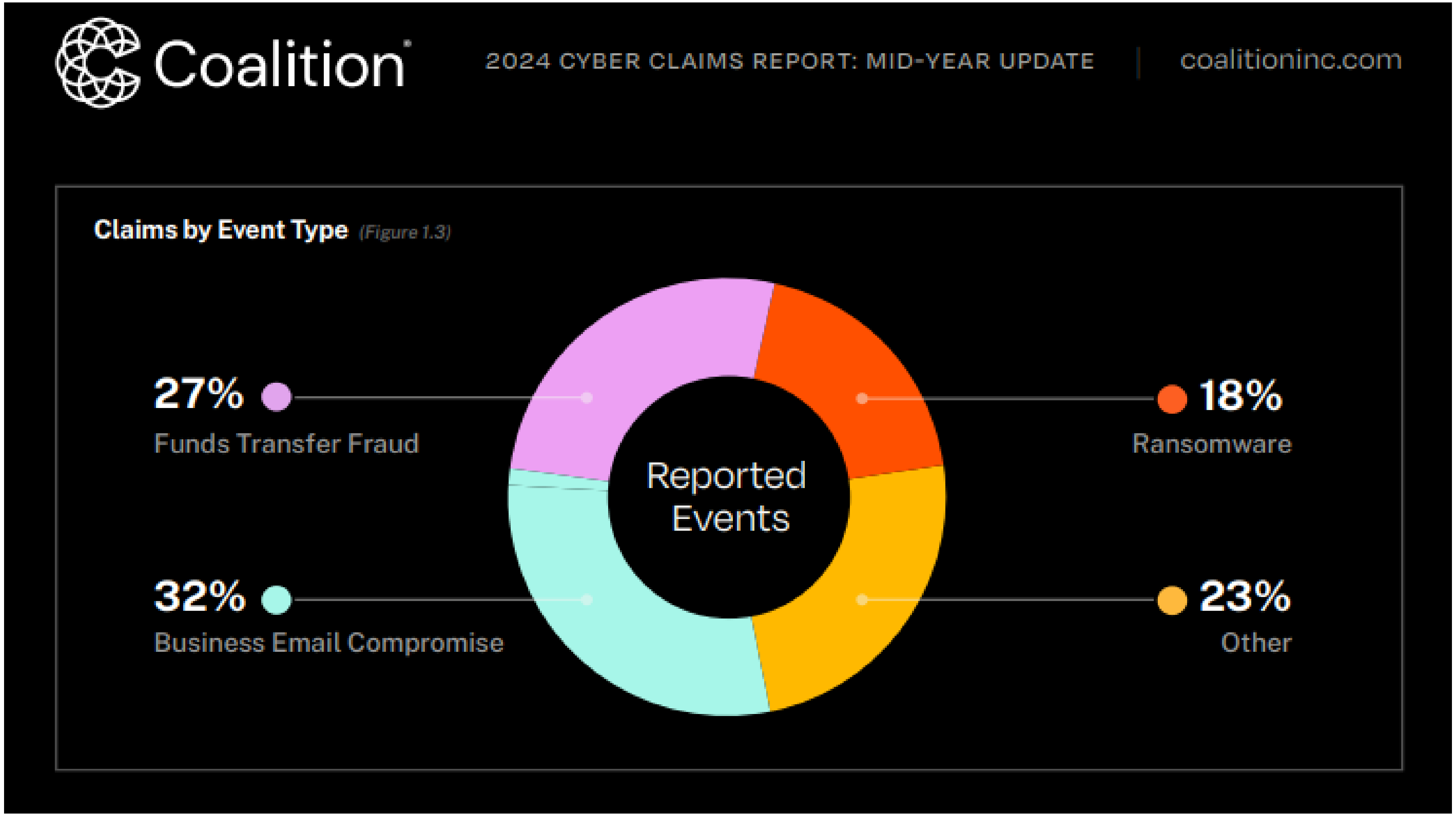
- Access to Expertise and Resources
  - Vulnerability Assessments
  - Training
  - Incident Response Templates
  - Cybersecurity Experts
  - Active Monitoring

- Financial Protection
  - Risk Transfer

How Does It Apply to Cyber Insurance

- Cyber Market hardened; premiums increased but moderating
- More in-depth underwriting – Full applications, supplementals, scans, pen tests
- Security requirements – MFA, EDR, back-ups, training
- Lower coverages limits – be aware of sub-limits
- Increased subjectivities and contingencies – you may not have the coverage you think
- Increased retentions and co-insurance clauses – how do they apply
- New Endorsements – there are many limiting endorsement: widespread events, patching cadence, war exclusion, named vulnerability, lack of MFA reduction
- More declinations – industry, controls, prior losses

Types of Claims



Coalition

2024 CYBER CLAIMS REPORT: MID-YEAR UPDATE | coalitioninc.com

Claims by Event Type *(Figure 1.3)*

How to Position Yourself Best for Cyber Insurance

- Start the Renewal Process 4-6 months prior to renewal
- Ask your Broker for a Cyber Assessment – What vulnerabilities do you have? Resolve them prior to doing applications.
- Implement Multi-Factor Authentication Email, Remote and Privileged Access
- Implement EDR – Endpoint Detection and Response
- Increase Email Security and Phishing Training
- Have a regular patching cadence
- Encrypt all sensitive data
- Create a Cyber Security Awareness Training Program as well as a Cyber Incident Response Program
- Have Back-ups – Regular, encrypted, air-gaped & tested

Cyber Insurance Is Different

- Stand alone Cyber Policy vs a Cyber Endorsement
- Cyber Policies are not created equally
- Admitted vs Non-Admitted
- Claim Reporting
- Claims Handling – Breach Coach
- Pre Loss Services

Cyber Insurance Coverages You Should Have

3rd Party Liability:

- Network Security & Privacy Liability
- Regulatory Defense and Penalties
- Media Liability
- PCI Fines and Assessments
- Bodily Injury and Property Damage

1st Party Coverages:

- Breach Responses
- Crisis Management and Public Relations
- Cyber Extortion including ransomware payment
- Business Interruption and Extra Expense
- Dependent Business Interruption and Extra Expense
- Digital Asset Restoration
- Computer Hardware Replacement (Bricking)
- Cyber Crime & Social Engineering (Fund Transfer Fraud)

Cybersecurity Best Practices

- Increase Email Security & Phishing Training
- Implement Multi-factor Authentication (MFA)
- Maintain Full Data Backups (Encrypt, Air gap & Test)
- Secure all Remote Access
- Update/Patch Your Software Regularly
- Use a Password Manager
- Scan for Malicious Software (EDR Tools)
- Encrypt All Your Data (Phone, Tablets, etc.)
- Utilize Favorable 3rd Party and Vendor Contracts
- Setup a Security Awareness Training Program
- Create and Practice a Cyber Incident Response Program
- Develop practices to minimize Fund Transfer Fraud

Dennis O'Connell, Custom Computer Specialists

Dennis O’Connell serves as the Director of Security Solutions at Custom Computer Specialists. He has over 30 years of extensive experience in technology, specializing in the development of data security solutions. He is dedicated to designing and creating tailored security solutions specifically for health care facilities across the United States.

A recognized authority in his field, Dennis is a frequent guest speaker and panelist at regional conferences, seminars, and webinars. He shares his expertise on topics ranging from cyber security to disaster recovery and cloud migration. Additionally, Mr. O’Connell has authored numerous articles, providing insights into cyber security best practices.

Cyber Observations from 2024 – Offensive

- CCS supports several hundred organizations in the Mid-Atlantic, Ohio Valley, and Northeast
- We assisted in the remediation and forensics investigation of 19 major attacks impacting nearly 20,000 computers
- Organizations are constantly under attack
  - Phishing
  - Old systems
  - Misconfigurations/Patching
  - Remote Desktop Services
- Threat Actors were in the network for months setting up the attack
- Most victims of major attacks had no Cyber/Disaster recovery plan in place and tested

Cyber Observations from 2024 – Defensive

- Access Devices (Computers, Laptops, Tablets, and Phones)
  - Encryption
  - Multifactor for Remote Access
  - Multifactor for Network Access

- Servers, Backup, and Network
  - Encryption
  - Multifactor
  - Privilege Access Management
  - Disaster Recovery vs. Backup

- Cloud
  - Multifactor
  - Privilege Access Management
  - Backup

Typical Attack

- Prior to Attack (3-6 months)
  - The network is compromised, and the threat actor gains knowledge about victim to prepare for the attack

- The Attack (Day One)
  - Systems are compromised
  - Usually on a Friday or when key people are unavailable
  - Ransom demand is received

- The Response (Days 1-3)
  - Containment
  - Assess the damage and determine if systems can be restored and do the backups work
  - Notify Cyber Insurance Company
  - Engage external organizations to help (Forensics and Remediation)

Remediation (Week 1-2)

- Creation of server images for forensic examination
- Installation of Next Gen Antivirus (EDR/MDR)
- Creation of Clean Network
  - Compromised Network is Isolated and New Network to host clean systems
  - Identification of clean systems and movement to clean network if possible
- Application/System Assessment
  - Identify and rank the most critical systems for restoration
- Procurement
  - New servers and workstations are ordered for critical systems
  - Equipment is staged and applications are installed

Remediation (Month 2-6)

- Secondary Systems are Identified and Prioritized
- Plan is developed to bring these systems back online
- Computers are reimaged or replaced
- New Security Tools are put in place to try to prevent future attacks

Review of Attack (6 Months +)

- Review of Systems, Tools, People and Processes leading up to attack
- Review of Incident Response and Remediation
- Identification of Security Gaps
- Review of Disaster Recovery Tolerance
- Development of plans for Post Incident

How Prepared are You for an Attack?

Maturity Level 1

- I have a plan in my head
- My data is backed up, but restoration is not tested
- I don't know how long it will take to get my business up and running

Maturity Level 2

- I have done a Risk Assessment
- My data is backed up and tested
- I have an idea of how long it will take to restore business operations

Maturity Level 3

- We have done a Risk Assessment
- We have developed a plan, it is documented, and it is tested periodically
- Backup/Disaster Recovery systems are in place and tested periodically
- We know how long it will take to restore critical business functions

Justin Bain
VNS Health

Justin leads the Information Security team at VNS Health (formerly known as the Visiting Nurse Service of New York). In their 130+ year history, VNS Health has been at the cutting edge of home and community-based healthcare and technology in and around New York City. With 25 years of experience in post-acute healthcare and supporting technology, Justin leads the efforts to protect information system and ensure compliance with industry regulations.

VNS Health

HIPAA Security Rule NPRM 12/27/2024

From Office of Civil Rights (OCR) fact sheet.

- **HIPAA Security Rule** has been virtually unchanged since 2004.
- Notice of Proposed Rulemaking (NPRM) to Strengthen Cybersecurity
  - issued in December 2024
  - published in January 2025
  - 60-day comment period ended March 7
- New rules are intended to strengthen requirements for cybersecurity
- Clarifications on terms and mandates reflect current enforcement
- More documentation, more planning, new audits, and some stronger technical controls.
- Many comments emphasized the burdensome impact on the industry.

Analysis by Justin Bain, VNS Health.

VNS Health

HIPAA Security Rule NPRM 12/27/2024

From Office of Civil Rights (OCR) fact sheet.

Administrative Changes

- No distinction between “Required v. Addressable” – all Required
- Increased mandatory written documentation of P&Ps, plans, and analyses
- Updated definitions and specifications for clarity
- Specific compliance time periods for existing requirements
- Technology Asset Inventory and Network Map
- Risk Analysis must include Inventory, Map, Threats, Vulnerabilities, and Risk-level
- Notification to certain regulated entities within 24hrs when a workforce member’s access is terminated
- Contingency Planning and Incident Response Planning: 72hr restoration, criticality analysis, and testing the plans
- Compliance Audits every 12 months
- Notification of contingency plan activation to group health plans within 24hrs

Analysis by Justin Bain, VNS Health

VNS Health

HIPAA Security Rule NPRM 12/27/2024

From Office of Civil Rights (OCR) fact sheet.

Technical Changes

- Encryption required at rest and in transit with limited exceptions
- Expanded “identity” to include technology assets as well as humans
- Consistent configuration of systems, workstations included
- Anti-malware protection
- Removal of Extraneous Software
- Disabling Network Ports
- Multi-factor Authentication
- Vulnerability Scanning and Penetration Testing
- Network Segmentation
- Backup and Recovery Controls

Analysis by Justin Bain, VNS Health

Crystal Wilson, CISA

Crystal J. Wilson is a Cyber State Coordinator (CSC) for Albany in Region 2 within the Cybersecurity and Infrastructure Security Agency (CISA). Region 2 covers New York, New Jersey, Puerto Rico, and the U.S. Virgin Islands.

Crystal has over 16 years of experience in the intelligence and cybersecurity fields and over 20 years of service in the New York Army National Guard where she is a Warrant Officer in the Cyber Corps and Veteran of Operation Iraqi Freedom. Crystal also spent two years as a targeting analyst in Afghanistan working with Special Operations.

She holds a BS in Digital Forensics from the University at Albany and is currently studying for her credentials as a Certified Information Systems Security Professional (CISSP).

Cybersecurity and Infrastructure Security Agency (CISA)

As America’s Cyber Defense Agency and the National Coordinator for critical infrastructure resiliency and security, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

months | years | decades

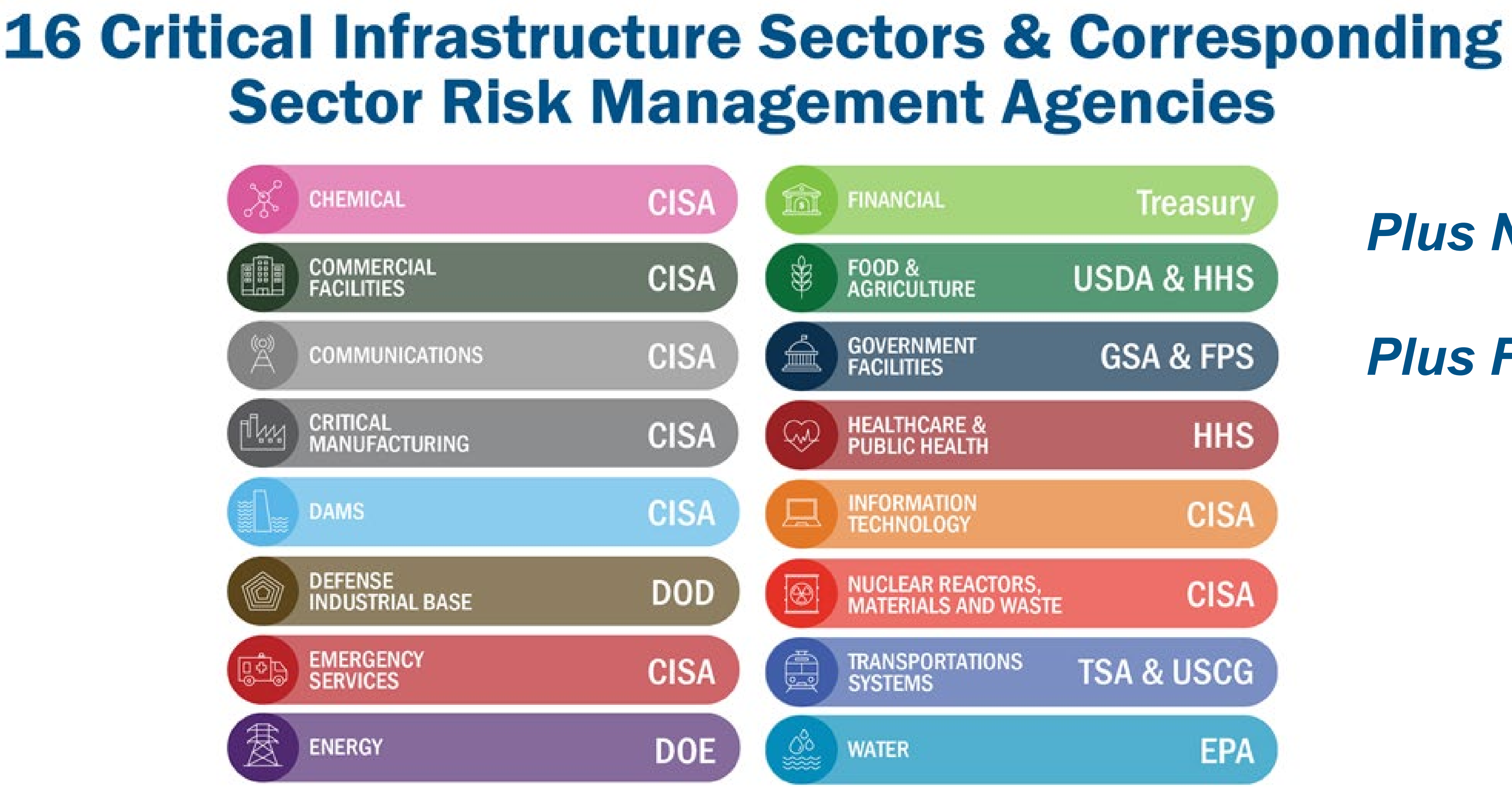
CISA Central

CISA Central is CISA’s hub for staying on top of threats and emerging risks to our nation’s critical infrastructure, whether they’re of cyber, communications or physical origin**:**

Services offered by CISA:

- Vulnerability Scanning
- Phishing Campaign Assessment
- Web Application Scanning

Who Does CISA Work With?



16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

Sector	Agency
CHEMICAL	CISA
COMMERCIAL FACILITIES	CISA
COMMUNICATIONS	CISA
CRITICAL MANUFACTURING	CISA
DAMS	CISA
DEFENSE INDUSTRIAL BASE	DOD
EMERGENCY SERVICES	CISA
ENERGY	DOE
FINANCIAL	Treasury
FOOD & AGRICULTURE	USDA & HHS
GOVERNMENT FACILITIES	GSA & FPS
HEALTHCARE & PUBLIC HEALTH	HHS
INFORMATION TECHNOLOGY	CISA
NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
TRANSPORTATIONS SYSTEMS	TSA & USCG
WATER	EPA

Plus Non-Profits

Plus Faith-Based

CISA Offers No-Cost Cybersecurity Services

- **Preparedness Activities**
  - Cybersecurity Assessments
  - Cybersecurity Training and Awareness
  - Cyber Exercises and “Playbooks”
  - Information / Threat Indicator Sharing
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices

- **Response Assistance**
  - Remote / On-Site Response and Assistance
  - Incident Coordination
  - Threat intelligence and information sharing
  - Malware Analysis

- **Cybersecurity Advisors**
  - Incident response coordination
  - Cyber assessments
  - Working group collaboration
  - Advisory assistance
  - Public Private Partnership Development

Contact CISA to report a cyber incident

Call 1-888-282-0870 | email CISAservicedesk@cisa.dhs.gov | visit https://www.cisa.gov

Cybersecurity Advisor Program

CISA mission: Lead the collaborative national effort to strengthen the security and resilience of America’s critical infrastructure

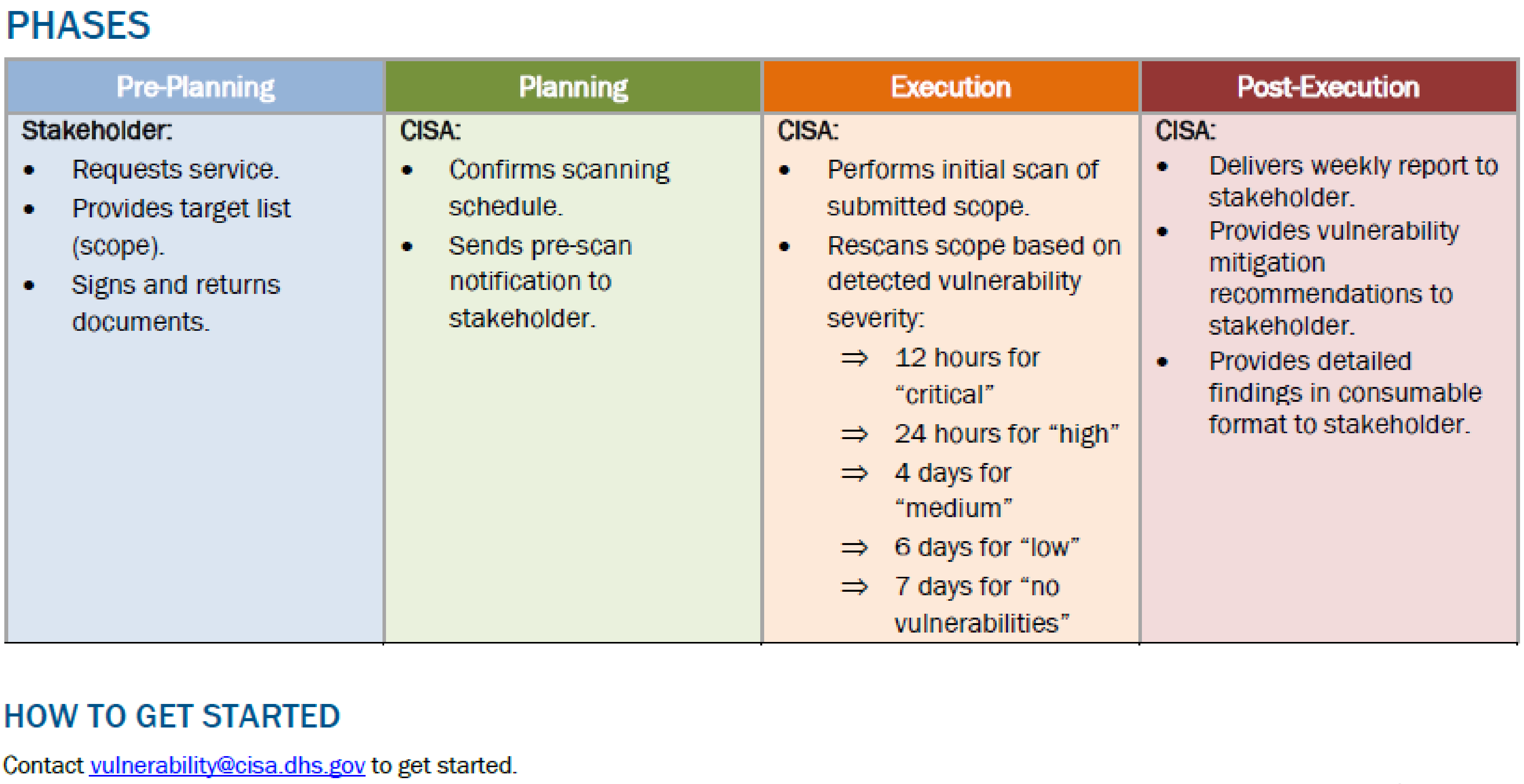
In support of that mission: Cybersecurity Advisors (CSAs):

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.

Cyber Security Evaluation Tool

- **Purpose:** Assesses control system and information technology network security practices against industry standards.
- **Facilitated:** Self-Administered, undertaken independently
- **Benefits:**
  - Immediately available for download upon request
  - Understanding of operational technology and information technology network security practices
  - Ability to drill down on specific areas and issues
  - Helps to integrate cybersecurity into current corporate risk management strategy

Vulnerability Scanning



PHASES

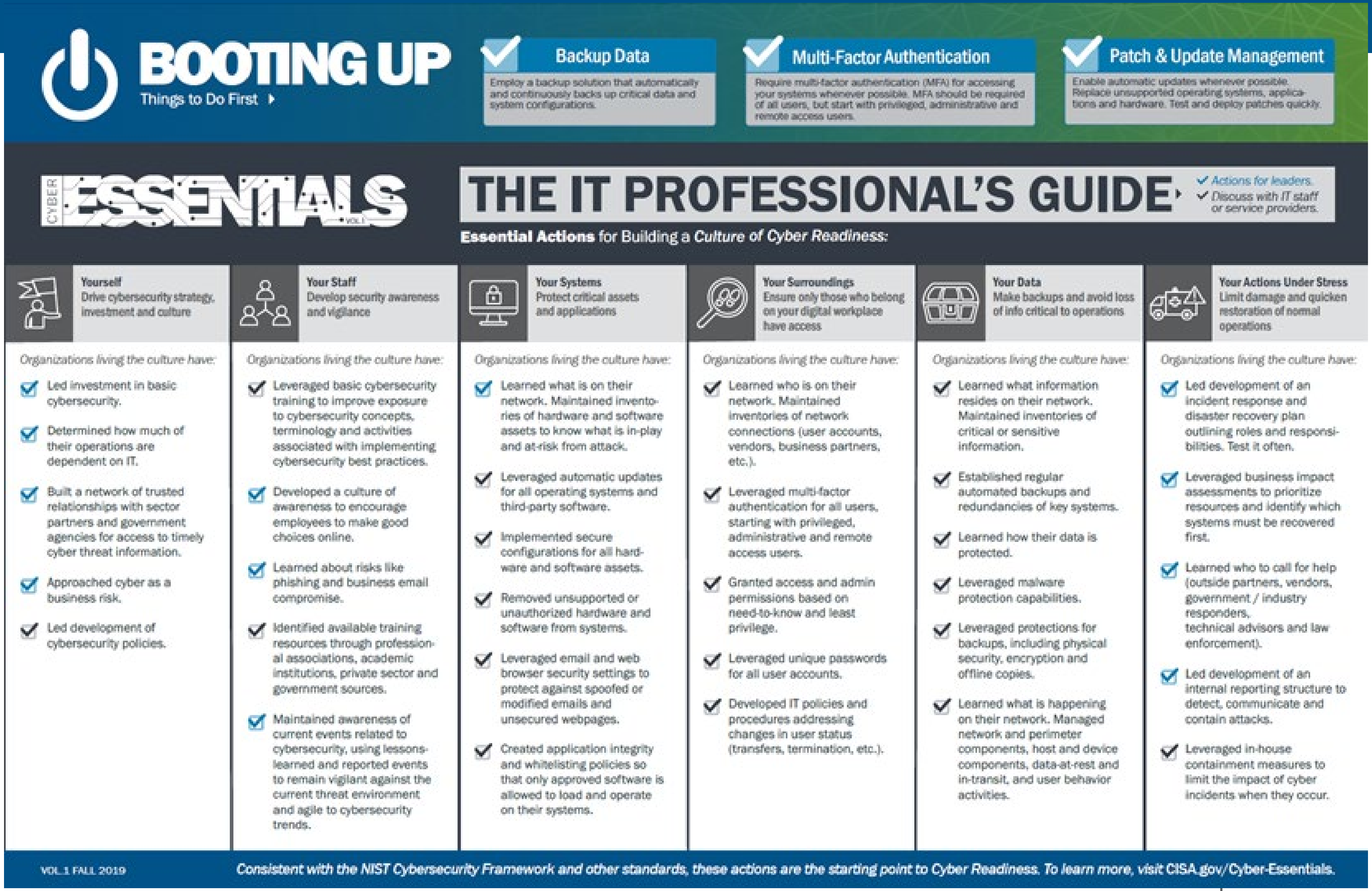
Pre-Planning	Planning	Execution	Post-Execution
Stakeholder: • Requests service. • Provides target list (scope). • Signs and returns documents.	**CISA:** • Confirms scanning schedule. • Sends pre-scan notification to stakeholder.	**CISA:** • Performs initial scan of submitted scope. • Rescans scope based on detected vulnerability severity: ⇒ 12 hours for "critical" ⇒ 24 hours for "high" ⇒ 4 days for "medium" ⇒ 6 days for "low" ⇒ 7 days for "no vulnerabilities"	**CISA:** • Delivers weekly report to stakeholder. • Provides vulnerability mitigation recommendations to stakeholder. • Provides detailed findings in consumable format to stakeholder.

HOW TO GET STARTED

Contact vulnerability@cisa.dhs.gov to get started.

Cyber Essentials

CISA's Cyber Essentials is a guide for leaders of small businesses as well as leaders of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices **to develop a culture of awareness.**



BOOTING UP
Things to Do First ▸

Backup Data
Employ a backup solution that automatically and continuously backs up critical data and system configurations.

Multi-Factor Authentication
Require multi-factor authentication (MFA) for accessing your systems whenever possible. MFA should be required of all users, but start with privileged, administrative and remote access users.

Patch & Update Management
Enable automatic updates whenever possible. Replace unsupported operating systems, applications and hardware. Test and deploy patches quickly.

CYBER ESSENTIALS VOL.1

THE IT PROFESSIONAL'S GUIDE ▸
✓ Actions for leaders.
✓ Discuss with IT staff or service providers.

Essential Actions for Building a *Culture of Cyber Readiness:*

Yourself
Drive cybersecurity strategy, investment and culture

Organizations living the culture have:

- ✓ Led investment in basic cybersecurity.
- ✓ Determined how much of their operations are dependent on IT.
- ✓ Built a network of trusted relationships with sector partners and government agencies for access to timely cyber threat information.
- ✓ Approached cyber as a business risk.
- ✓ Led development of cybersecurity policies.

Your Staff
Develop security awareness and vigilance

Organizations living the culture have:

- ✓ Leveraged basic cybersecurity training to improve exposure to cybersecurity concepts, terminology and activities associated with implementing cybersecurity best practices.
- ✓ Developed a culture of awareness to encourage employees to make good choices online.
- ✓ Learned about risks like phishing and business email compromise.
- ✓ Identified available training resources through professional associations, academic institutions, private sector and government sources.
- ✓ Maintained awareness of current events related to cybersecurity, using lessons-learned and reported events to remain vigilant against the current threat environment and agile to cybersecurity trends.

Your Systems
Protect critical assets and applications

Organizations living the culture have:

- ✓ Learned what is on their network. Maintained inventories of hardware and software assets to know what is in-play and at-risk from attack.
- ✓ Leveraged automatic updates for all operating systems and third-party software.
- ✓ Implemented secure configurations for all hardware and software assets.
- ✓ Removed unsupported or unauthorized hardware and software from systems.
- ✓ Leveraged email and web browser security settings to protect against spoofed or modified emails and unsecured webpages.
- ✓ Created application integrity and whitelisting policies so that only approved software is allowed to load and operate on their systems.

Your Surroundings
Ensure only those who belong on your digital workplace have access

Organizations living the culture have:

- ✓ Learned who is on their network. Maintained inventories of network connections (user accounts, vendors, business partners, etc.).
- ✓ Leveraged multi-factor authentication for all users, starting with privileged, administrative and remote access users.
- ✓ Granted access and admin permissions based on need-to-know and least privilege.
- ✓ Leveraged unique passwords for all user accounts.
- ✓ Developed IT policies and procedures addressing changes in user status (transfers, termination, etc.).

Your Data
Make backups and avoid loss of info critical to operations

Organizations living the culture have:

- ✓ Learned what information resides on their network. Maintained inventories of critical or sensitive information.
- ✓ Established regular automated backups and redundancies of key systems.
- ✓ Learned how their data is protected.
- ✓ Leveraged malware protection capabilities.
- ✓ Leveraged protections for backups, including physical security, encryption and offline copies.
- ✓ Learned what is happening on their network. Managed network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities.

Your Actions Under Stress
Limit damage and quicken restoration of normal operations

Organizations living the culture have:

- ✓ Led development of an incident response and disaster recovery plan outlining roles and responsibilities. Test it often.
- ✓ Leveraged business impact assessments to prioritize resources and identify which systems must be recovered first.
- ✓ Learned who to call for help (outside partners, vendors, government / industry responders, technical advisors and law enforcement).
- ✓ Led development of an internal reporting structure to detect, communicate and contain attacks.
- ✓ Leveraged in-house containment measures to limit the impact of cyber incidents when they occur.

VOL.1 FALL 2019

Consistent with the NIST Cybersecurity Framework and other standards, these actions are the starting point to Cyber Readiness. To learn more, visit CISA.gov/Cyber-Essentials.

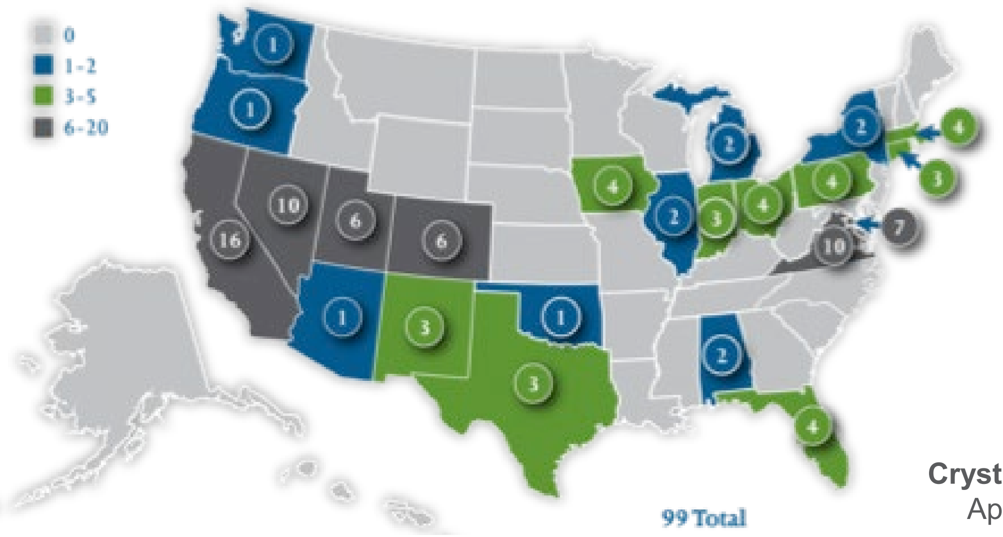
https://www.cisa.gov/resources-tools/resources/cyber-essentials

Cyber Exercises and Planning

CISA’s National Cyber Exercise and Planning Program develops, conducts, and evaluates cyber exercises and planning activities for state, local, tribal and territorial governments and public and private sector critical infrastructure organizations.

- Cyber Storm Exercise – DHS’s flagship national-level biennial exercise
- Exercise Planning and Conduct
- Cyber Exercise Consulting and Subject Expertise Support
- Cyber Planning Support
- Off-the-Shelf Resources

https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages



StopRansomware.gov

https://www.cisa.gov/stopransomware

- Mitigations
- Best Practices
- Ransomware Alerts

Provides essential knowledge to prepare you and your organization to prevent, mitigate, and respond to the ever-growing threat of ransomware attacks.

Questions?

Contact:

Crystal Wilson
Cyber State Coordinator, Region 2
Cybersecurity & Infrastructure Security Agency
Email: crystal.wilson@cisa.dhs.gov
Phone: 202-445-4290

Cybersecurity Expert Panel

Q and A

©2025

HCP | NYS Home Care Providers FOUNDATION
Research & Educational Resources for Home and Community-Based Care

EDUCATION & RESEARCH, INC
HCA E&R
501(c)(3)

Hospice & Palliative Care Association of New York State

Updates On Current Emergency-related Issues

Health Commerce System

Comprehensive Emergency Management Program (CEMP)

Multi-Factor Authentication (MFA)

Sign up for Communications List

Health Topics

Measles Outbreak

H5N1 and Influenza

Proposed Federal Rule

- Cybersecurity
- HIPAA

Open Discussion

Evaluation

Your feedback drives our programming!

EVALUATION LINK:

https://www.surveymonkey.com/r/EP040225

HCP NYS Home Care Providers FOUNDATION
Research & Educational Resources for Home and Community-Based Care

EDUCATION & HCA E&R 501(c)(3) RESEARCH, INC

Hospice & Palliative Care Association of New York State

Contact Information

HCP

Deyoe@nyshcp.org

HCA

acardillo@hcanys.org

HPCANYS

ecohen@hpcanys.org

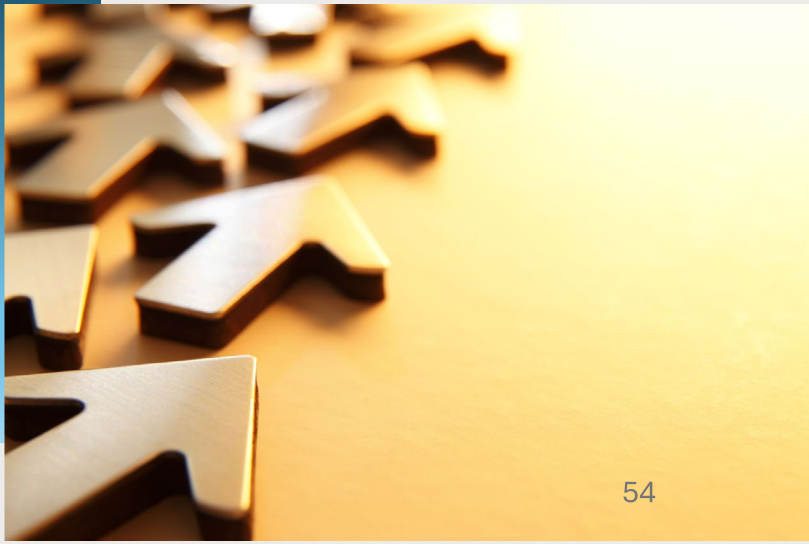
HCP NYS Home Care Providers FOUNDATION

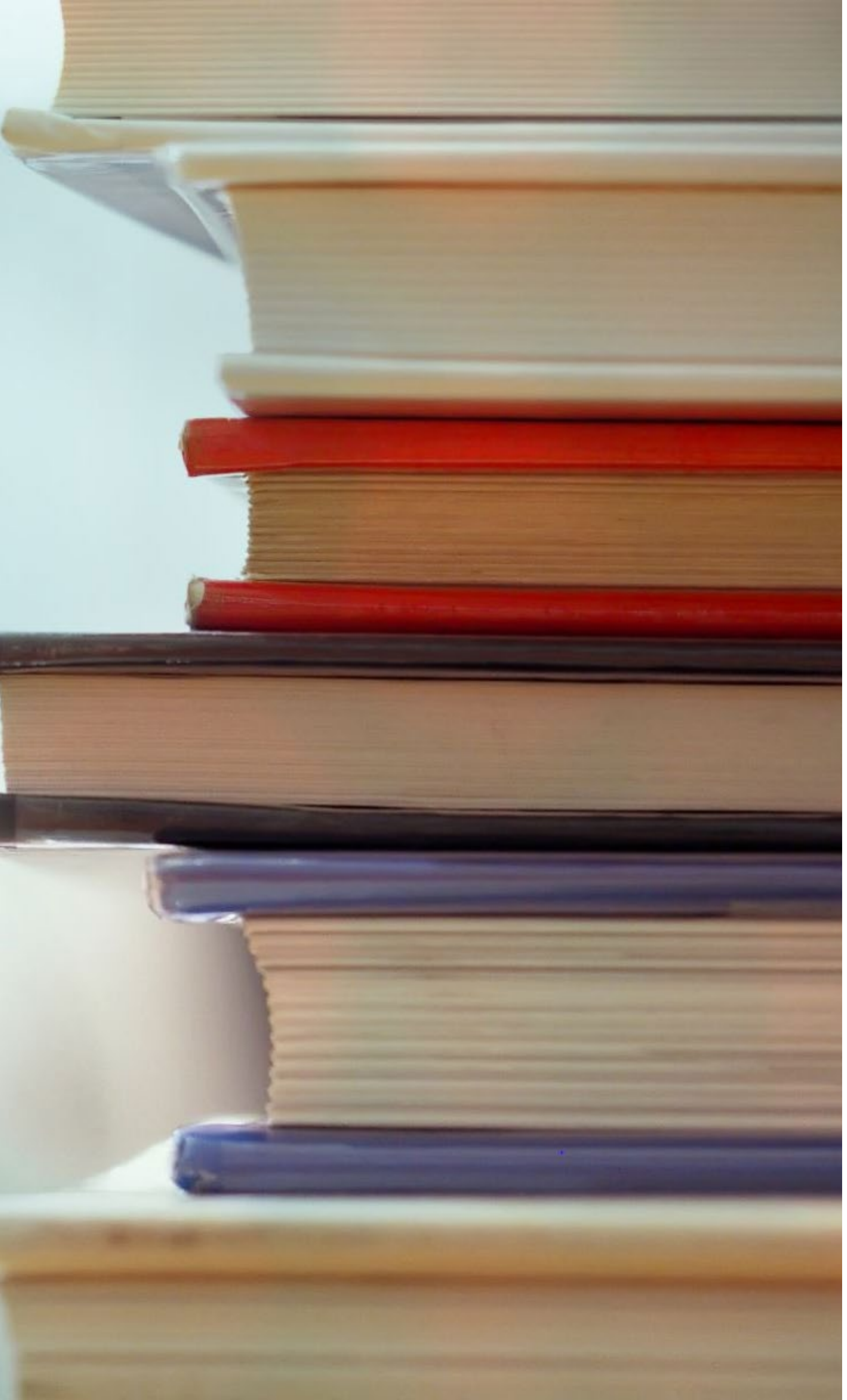
Research & Educational Resources for Home and Community-Based Care

EDUCATION & HCA E&R 501(c)(3) RESEARCH, INC

Hospice & Palliative Care Association of New York State

THANK YOU!!!





Useful Links

- NYS Influenza Surveillance
- Find a Vaccine NYC
- NYC Health Care Coalition
- Advance Warning System – NYC
- NY Alert
- NYS Measles Information
- CDC H5 Bird Flu
- HCS CEMP Training
- NYC Emergency Management Program Recordings