HealthCare
Kentucky Regional Extension Center

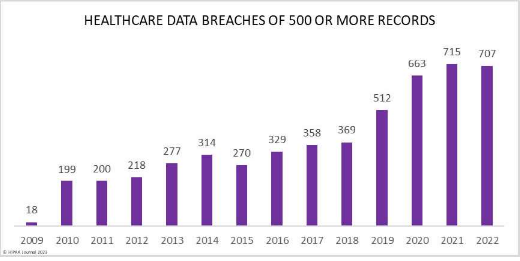
Security Incident Response & Reporting: Creating a Plan

Presented by:
Amy Daley, CHPS, Kentucky REC
Ryan Lewis, Region 4 Cybersecurity Advisor, CISA

Disclaimer

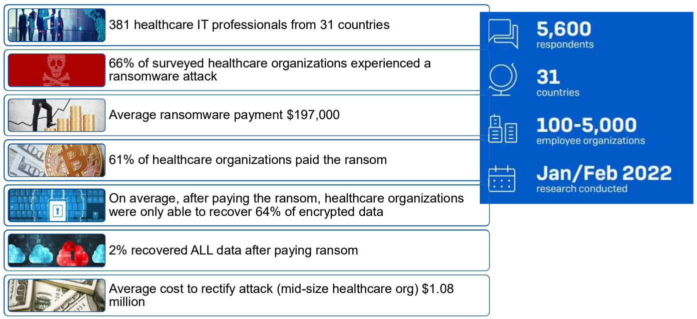
The information contained in this presentation is for general information purposes only. The information is provided by UK HealthCare's Kentucky Regional Extension Center and while we endeavor to keep the information up to date and correct, we make no representations or warranties of any kind, expressed or implied, about the completeness, accuracy, reliability, suitability or availability with respect to content.

History of Healthcare Data Breaches



HIPAA Journal/HHS.gov

2022 State of Ransomware Report - Sophos



- 381 healthcare IT professionals from 31 countries
- 66% of surveyed healthcare organizations experienced a ransomware attack
- Average ransomware payment $197,000
- 61% of healthcare organizations paid the ransom
- On average, after paying the ransom, healthcare organizations were only able to recover 64% of encrypted data
- 2% recovered ALL data after paying ransom
- Average cost to rectify attack (mid-size healthcare org) $1.08 million

5,600
respondents

31
countries

100-5,000
employee organizations

Jan/Feb 2022
research conducted

HIPAA Security Safeguard Standards

ADMINISTRATIVE	ADMINISTRATIVE	PHYSICAL	TECHNICAL
• **Security Management Process (R)** • Risk Analysis (R) • Risk Management (R) • Sanction Policy (R) • Information System Activity Review (R) • **Assigned Security Responsibility**(R) • **Workforce Security (R)** • Authorization and/or Supervision (A) • Workforce Clearance Procedure (A) • Termination Procedures (A) • **Information Access Management** (R) • Isolating Healthcare Clearinghouse Function (R) • Access Authorization (A) • Access Establishment & Modification (A)	• **Security Awareness and Training** (R) • Security Reminders (A) • Protection from Malicious Software(A) • Log-in Monitoring (A) • Password Management (A) • **Security Incident Procedures (R)** • Response and Reporting (R) • **Contingency Plan (R)** • Data Backup Plan (R) • Disaster Recovery Plan (R) • Emergency Mode Operations Plan (R) • Testing and Revision Procedures (A) • Applications and Data Criticality Analysis (A) • **Evaluation (R)** • **Business Associate Contracts and Other Arrangements (R)** • Written Contract or Other Arrangement(R)	• **Facility Access Controls (R)** • Contingency Operations (A) • Facility Security Plan (A) • Access Control and Validation Procedures (A) • Maintenance Records (A) • **Workstation Use (R)** • **Workstation Security (R)** • **Device and Media Controls (R)** • Disposal (R) • Media Re-Use (R) • Accountability (A) • Data Backup and Storage (A)	• **Access Control (R)** • Unique User Identification (R) • Emergency Access Procedure (R) • Automatic Logoff (A) • Encryption and Decryption (A) • **Audit Controls (R)** • **Integrity (R)** • Mechanism to Authenticate ePHI (A) • **Person or Entity Authentication (R)** • **Transmission Security (R)** • Integrity Controls (A) • Encryption (A)

Incident Response & Reporting

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

CYBER THREAT OVERVIEW: UK HEALTH

CISA CYBER SERVICES

Ryan Lewis
Cybersecurity Advisor, Region 4, Kentucky
Cybersecurity Advisor Program
Cybersecurity and Infrastructure Security Agency (CISA)

CISA Mission and Vision

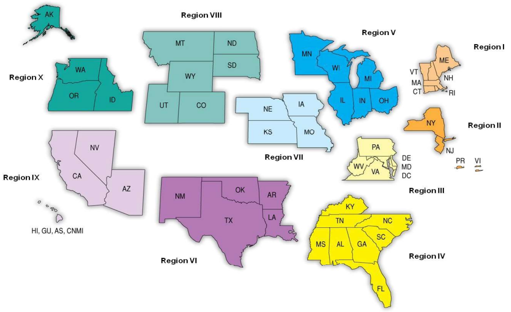
MISSION:

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

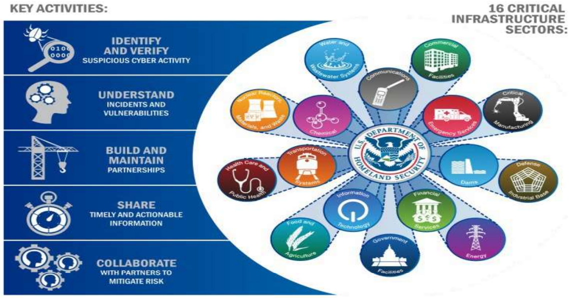
VISION:

Secure and resilient infrastructure for the American people.

Regionally Deployed Personnel



Serving Critical Infrastructure



KEY ACTIVITIES:

IDENTIFY AND VERIFY SUSPICIOUS CYBER ACTIVITY

UNDERSTAND INCIDENTS AND VULNERABILITIES

BUILD AND MAINTAIN PARTNERSHIPS

SHARE TIMELY AND ACTIONABLE INFORMATION

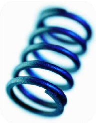
COLLABORATE WITH PARTNERS TO MITIGATE RISK

16 CRITICAL INFRASTRUCTURE SECTORS:

Resiliency Defined

"… the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…"

- Presidential Policy Directive 21
February 12, 2013



Protect (Security)	Sustain (Continuity)
Perform (Capability)	Repeat (Maturity)

Operational Resilience in Practice

Operational resilience emerges from what we do, such as:

- Identifying and mitigating risks,
- Planning for and managing vulnerabilities and incidents,
- Performing service-continuity processes and planning,
- Managing IT operations,
- Managing, training, & deploying people,
- Protecting and securing important assets, and
- Working with external partners.

Cyber Threats of Today

Business Email Compromise

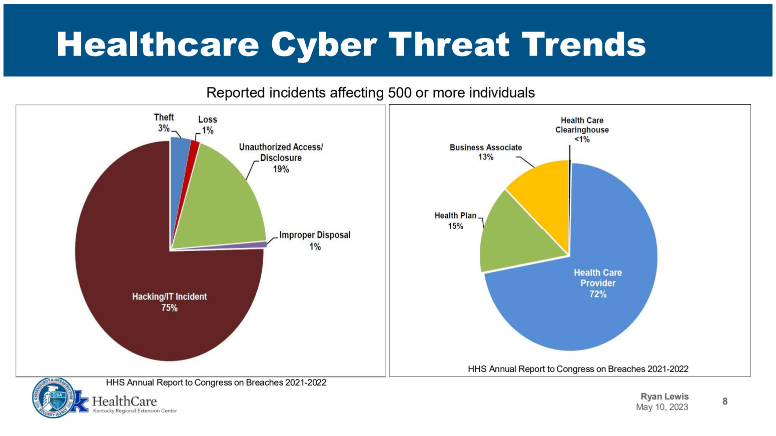
- 2 Billion in U.S. Loss FY-22
- Credential Stealing
- Phishing/ PopUps/ Poison Domains/ Onsite Exchange Vulnerabilities
- Steals Data
- Finance Diversions
- SupplyChain/External Dependencies Exploitation

Ransomware

- 34 Million in Loss FY-22
- 700K per Victim
- Lockbit, Royal, AvosLocker, Conti, Darkside, Maui
- Russian and North Korea State Actors
- Steals and Encrypts Data
- Double Extortion
- Destructive Malware Trends- Russia
  - Hermeticwiper and Wispergate

Common Defensive Measures

- Multifactor Authentication (MFA)
- Backups- Off Network
- Vulnerability Management – Patching
- Configuration Management - RDP, SMB, etc

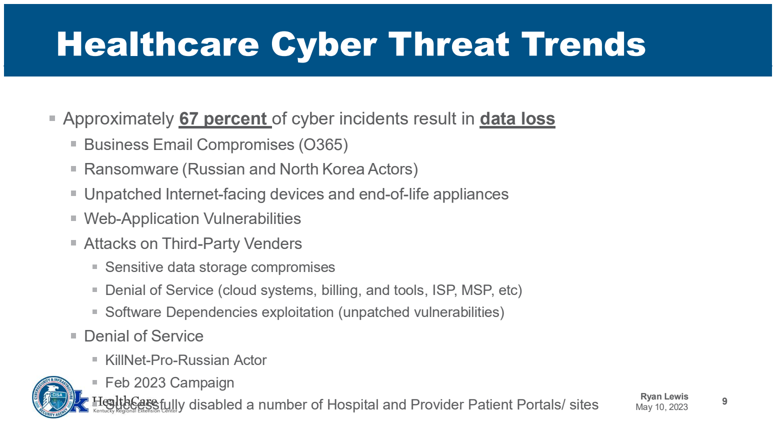


Healthcare Cyber Threat Trends

Reported incidents affecting 500 or more individuals

HHS Annual Report to Congress on Breaches 2021-2022

HHS Annual Report to Congress on Breaches 2021-2022



Healthcare Cyber Threat Trends

- Approximately **67 percent** of cyber incidents result in **data loss**
  - Business Email Compromises (O365)
  - Ransomware (Russian and North Korea Actors)
  - Unpatched Internet-facing devices and end-of-life appliances
  - Web-Application Vulnerabilities
  - Attacks on Third-Party Venders
    - Sensitive data storage compromises
    - Denial of Service (cloud systems, billing, and tools, ISP, MSP, etc)
    - Software Dependencies exploitation (unpatched vulnerabilities)
  - Denial of Service
    - KillNet-Pro-Russian Actor
    - Feb 2023 Campaign
    - Successfully disabled a number of Hospital and Provider Patient Portals/ sites

Any Good News?

CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

CISA CYBERSECURITY SERVICES

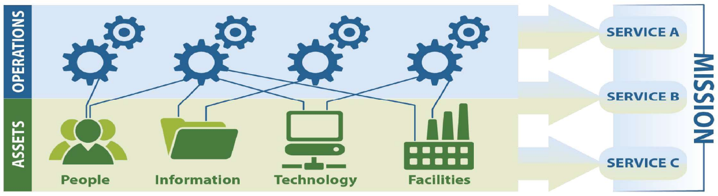
Protected Critical Infrastructure Information Program

Protected Critical Infrastructure Information (PCII) Program Guards Your Information

- Sensitive critical infrastructure information voluntarily given to CISA is protected by law from
  - Public release under Freedom of Information Act requests,
  - Public release under State, local, tribal, or territorial disclosure laws,
  - Use in civil litigation and
  - Use in regulatory purposes.

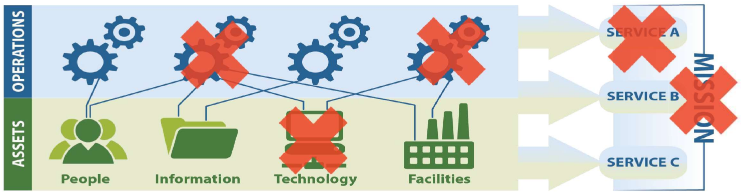
Critical Service Focus

Organizations use **assets (people, information, technology, and facilities)** to provide operational **services** and accomplish **missions.**



Critical Service Focus

- Disruption of business processes can lead to **mission failure**.



Cybersecurity Resources and Assessments

Regional Resources:

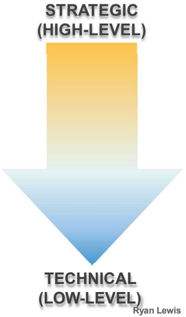
- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Cyber Infrastructure Survey (CIS)
- Cyber Incident Management Review (IMR)
- Cybersecurity Performance Goals (CPG)
- Ransomware Readiness Assessment (RRA)
- Workshops

National Resources:

- Cyber Tabletop Exercises (CTTX)
- Vulnerability Scanning Service (CyHy)

Tools:

- Known Exploited Vulnerabilities (KEV)
- Cyber Security Evaluation Tool (CSET)
- Decider (MITRE ATT&CK)
- Untitled Goose (Azure)



CISA.GOV

Criticality of Periodic Assessments

- Periodic assessments are essential for resilience
- Can't protect if you don't know what needs protection
- Can't fix what needs fixing if you don't know what's wrong

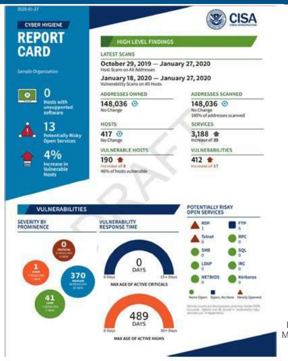
Cyber Hygiene Report Card

High Level Findings

- Latest Scans
- Addresses Owned
- Addresses Scanned
- Hosts
- Services
- Vulnerable Hosts
- Vulnerabilities

Vulnerabilities

- Severity by Prominence
- Vulnerability Response Time
- Potentially Risky Open Services



2020-01-27

CYBER HYGIENE
REPORT CARD

Sample Organization

0 Hosts with unsupported software

13 Potentially Risky Open Services

4% Increase in Vulnerable Hosts

CISA

HIGH LEVEL FINDINGS

LATEST SCANS

October 29, 2019 — January 27, 2020
Host Scans on All Addresses

January 18, 2020 — January 27, 2020
Vulnerability Scans on All Hosts

ADDRESSES OWNED
148,036
No Change

ADDRESSES SCANNED
148,036
No Change
100% of addresses scanned

HOSTS
417
No Change

SERVICES
3,188
Increase of 39

VULNERABLE HOSTS
190
Increase of 8
46% of hosts vulnerable

VULNERABILITIES
412
Increase of 17

VULNERABILITIES

SEVERITY BY PROMINENCE

0 CRITICAL

1 HIGH

370 MEDIUM

41 LOW

VULNERABILITY RESPONSE TIME

0 DAYS
0 Days 15+ Days
MAX AGE OF ACTIVE CRITICALS

489 DAYS
0 Days 30+ Days
MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP 1	FTP 6
Telnet 6	RPC 0
SMB 0	SQL 0
LDAP 0	IRC 0
NETBIOS 0	Kerberos 0

● None Open ■ Open, No New ▲ Newly Opened

DRAFT

Information Sharing Opportunities

- **Sector Coordinating Councils:**
  - **Sector Coordinating Councils** (SCCs) are self-organized and self-governed councils that enable critical infrastructure owners and operators, their trade associations, and other industry representatives to interact on a wide range of sector-specific strategies, policies, and activities.
  - The SCCs coordinate and collaborate with sector-specific agencies (SSAs) and related Government Coordinating Councils (GCCs) to address the entire range of critical infrastructure security and resilience policies and efforts for that sector.
- **ISACs and ISAOs:**
  - **Information Sharing and Analysis Centers** (ISACs) or **Organizations** (ISAOs) are communities of interest sharing cybersecurity risk, threat information, and incident management to members. For more information on ISACs, visit www.nationalisacs.org. For more on ISAOs visit www.isao.org/about.

AUTO-ISAC
Automotive Information Sharing and Analysis Center
MS-ISAC
Multi-State Information Sharing & Analysis Center
Elections Infrastructure ISAC
ONG-ISAC
National Defense ISAC
WATER ISAC
SPACE ISAC
DNG-ISAC

Incident Reporting

Why report cyber incidents?

- For situational awareness
- For decision making
- Requesting response assistance

When to report a cyber incident?

If there is a suspected or confirmed cyber attack or incident that:

- Affects core or critical business functions;
- Results in the loss of data, system confidentiality, integrity, and/ or availability; or control of systems;
- Indicates malicious software is present on critical systems

Who to report cyber incidents to?

- Leadership, public affairs, legal and other internal stakeholders
- Relevant vendors
- Law enforcement and other government agencies
- Cyber insurance providers
- Appropriate 3rd party incident response teams

Asset Response:

CISA Watch provides real-time threat analysis and incident reporting capabilities
24x7 contact 1-888-282-0870 or
CISAservicedesk@cisa.dhs.gov

US-CERT: us-cert.cisa.gov/report;
24x7 Ops cte: 1-888-282-0870

https://www.cisa.gov/ and click on REPORT A CYBER ISSUE

Federal Bureau of Investigation
1-855-292-7896 or
cywatch@ic.fbi.gov

FBI/ Internet Crime Complaint Center (IC3): www.ic3.gov

Think about it

How would law enforcement coordinate with you as an affected organization, in the wake of cyber attacks?

What do you want to know in the first 30 minutes of a disruptive cyber attack?

What are you willing to share within the first 30 minutes of a disruptive cyber attack?

Who is allowed to share it?

What steps are you going to take in the next 30 days to improve cyber security in your operations?

Resources: CISA.GOV

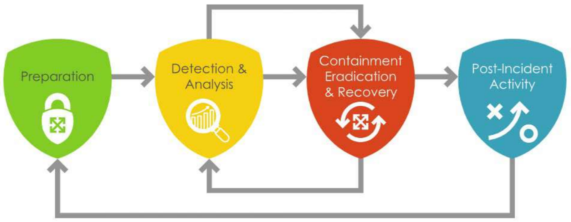
Contact Information

Ryan Lewis
Region 4 Cybersecurity Advisor – Kentucky
Ryan.Lewis@cisa.dhs.gov
(202) 975-9453 (Cell)

Colin Glover
Region 4Cybersecurity State Coordinator - Kentucky
Colin.glover@cisa.dhs.gov
(202) 380-5741 (Cell)

Sean McCloskey, CISSP
Region 4 Cybersecurity Advisor - North Carolina, South Carolina
Sean.McCloskey@hq.dhs.gov
(202) 578-8853 (Cell)

NIST Incident Handling Process

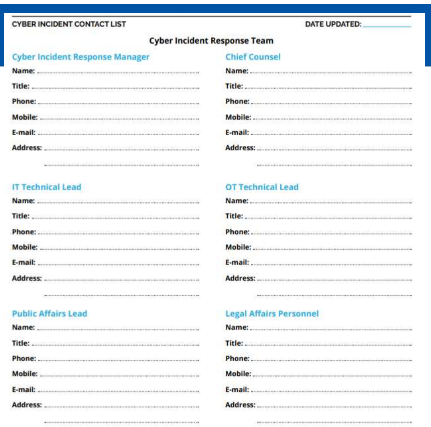


NIST Incident Handling Process

Preparation

- Documenting and understanding policies and procedures for incident response
- Instrumenting the environment to detect suspicious and malicious activity
- Establishing staffing plans and CIRT (Cyber Incident Response Team)
- Educating users on cyber threats and notification procedures (Training & Awareness)
- Leveraging cyber threat intelligence (CTI) to proactively identify potential malicious activity
- Having infrastructure in place to handle complex incidents
- Developing and testing courses of action (COAs) for containment and eradication
- Establishing means for collecting digital forensics and other data or evidence
- Develop and maintain an accurate picture of infrastructure (systems, networks, cloud platforms, and contractor-hosted networks)
- Risk Assessments
- Third party services (Review Service Level Agreements)
- Reporting Incidents

CIRT Contacts



CYBER INCIDENT CONTACT LIST DATE UPDATED: ____________

Cyber Incident Response Team

Cyber Incident Response Manager

Name: ....
Title: ....
Phone: ....
Mobile: ....
E-mail: ....
Address: ....
....

IT Technical Lead

Name: ....
Title: ....
Phone: ....
Mobile: ....
E-mail: ....
Address: ....
....

Public Affairs Lead

Name: ....
Title: ....
Phone: ....
Mobile: ....
E-mail: ....
Address: ....
....

Chief Counsel

Name: ....
Title: ....
Phone: ....
Mobile: ....
E-mail: ....
Address: ....
....

OT Technical Lead

Name: ....
Title: ....
Phone: ....
Mobile: ....
E-mail: ....
Address: ....
....

Legal Affairs Personnel

Name: ....
Title: ....
Phone: ....
Mobile: ....
E-mail: ....
Address: ....
....

Detection & Analysis

Identification of Incident Begins

- Email or phone notification from an intrusion detection tool.
- Suspicious entries in system or network accounting, or logs.
- Discrepancies between logs.
- Repetitive unsuccessful logon attempts within a short time interval.
- Unexplained new user accounts.
- Unexplained new files or unfamiliar file names.
- Unexplained modifications to file lengths and/or dates, especially in system files.
- Unexplained attempts to write to system files or changes in system files.
- Unexplained modification or deletion of data.
- Denial/disruption of service or inability of one or more users to login to an account.
- System crashes.
- Poor system performance of dedicated servers.
- Operation of a program or sniffer device used to capture network traffic.
- Unusual time of usage (e.g., users login during unusual times)
- Unusual system resource consumption. (High CPU usage)
- Last logon (or usage) for a user account does not correspond to the actual last time the user used the account.
- Unusual usage patterns (e.g., a user account associated with a user in Finance is being used to login to an HR database).
- Unauthorized changes to user permission or access.

Detection & Analysis

- **Incident Categorization** – Type of incident (Phishing, Ransomware, Other)
- **Incident Scope**
  - How many systems are affected by this incident?
  - Is Confidential or Protected information involved?
  - What is/was the entry point for the incident (e.g., Internet, network, physical)?
  - What is the potential damage caused by the incident?
  - What is the estimated time to recover from the incident?
  - What resources are required to manage the situation?
  - How could the assessment be performed most effectively?
- **Incident Impact** – Low, Medium, High
- **Documentation**

Containment, Eradication & Recovery

- **Containment**:

  Prevent further damage and reduce the immediate impact of the incident by removing the adversary’s access.

- **Eradication & Recovery**:

  Allow the return of normal operations by eliminating artifacts of the incident (e.g., remove malicious code, re-image infected systems) and mitigating the vulnerabilities or other conditions that were exploited.

Containment Strategies

- Isolating impacted systems and network segments from each other and/or from non-impacted systems and networks. If this is needed, consider the mission or business needs and how to provide services so missions can continue during this phase to the extent possible.
- Capturing forensic images to preserve evidence for legal use (if applicable) and further investigation of the incident.
- Updating firewall filtering.
- Blocking (and logging) of unauthorized accesses; blocking malware sources.
- Closing specific ports and mail servers or other relevant servers and services.
- Changing system admin passwords, rotating private keys, and service/application account secrets where compromise is suspected and revocation of privileged access.
- Directing the adversary to a sandbox (a form of containment) to monitor the actor’s activity, gather additional evidence, and identify attack vectors. Note: this containment activity is limited to advanced SOCs with mature capabilities.

Containment, Eradication & Recovery

Containment:

- Stolen credentials – disable account credentials, reset all active connections, review user activity, reverse changes, increase alerting, harden from future attacks.
- Ransomware – isolate the impacted system, validate the ransomware claim, contact insurance carrier, identify whether additional systems have been impacted and isolate as needed.
- If DOS/DDOS - control WAN/ISP.
- Virus outbreak – contain LAN/system.
- Data loss – review user activity, implement data breach response procedures.
- Website defacement – repair site, harden from future attacks.
- Compromised API – review changes made, repair API, harden from future attacks.

Containment, Eradication & Recovery

Eradication:

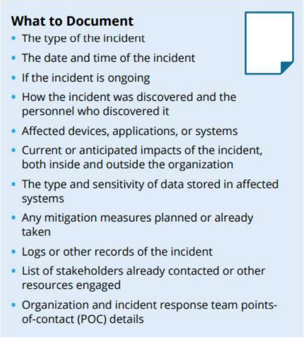
- Remediating all infected IT environments (e.g., cloud, OT, hybrid, host, and network systems).
- Reimaging affected systems (often from ‘gold’ sources), rebuilding systems from scratch.
- Rebuilding hardware (required when the incident involves rootkits).
- Replacing compromised files with clean versions.
- Installing patches.
- Resetting passwords on compromised accounts.
- Monitoring for any signs of adversary response to containment activities.
- Incident Categorization
- Incident Scope
- Incident Impact
- Documentation

Containment, Eradication & Recovery

Recovery:

- Reconnecting rebuilt/new systems to networks.
- Tightening perimeter security (e.g., firewall rulesets, boundary router access control lists) and zero trust access rules.
- Testing systems thoroughly, including security controls.
- Monitoring operations for abnormal behaviors.
- Documentation

Documentation



What to Document

- The type of the incident
- The date and time of the incident
- If the incident is ongoing
- How the incident was discovered and the personnel who discovered it
- Affected devices, applications, or systems
- Current or anticipated impacts of the incident, both inside and outside the organization
- The type and sensitivity of data stored in affected systems
- Any mitigation measures planned or already taken
- Logs or other records of the incident
- List of stakeholders already contacted or other resources engaged
- Organization and incident response team points-of-contact (POC) details

Advanced security controls include the following:

- Anti-theft devices
- Business continuity and disaster recovery plan
- Digital forensics
- Multi-factor authentication
- Network segmentation
- Penetration testing
- Threat intelligence sharing (also called information sharing)
- Vulnerability scans

Source - https://www.himss.org/resources/cybersecurity-healthcare#Part3

Subscription Services

CISA Alerts
https://public.govdelivery.com/accounts/USDHSCISA/subscriber/new?qsp=CODE_RED

OCR Privacy & Security Listserv
https://www.hhs.gov/guidance/document/sign-ocr-privacy-security-listserv

Connect with Kentucky REC!

Like us on Facebook:
facebook.com/KentuckyREC

Follow us on Twitter: @KentuckyREC

Follow us on LinkedIn:
linkedin.com/company/kentucky-rec

Check out our Website: www.kentuckyrec.com

- Call us: 859-323-3090
- Email us: kyrec@uky.edu