OFFICE OF HOMELAND SECURITY
MISSISSIPPI
VIGILANCE AND PREPAREDNESS
DEPARTMENT OF PUBLIC SAFETY

DEPARTMENT OF PUBLIC SAFETY

MISSISSIPPI

OFFICE OF HOMELAND SECURITY

MOHS Mission

The Mississippi Office of Homeland Security (MOHS) ensures the safety and security of our state’s citizens through effective planning, coordination, and collaboration with federal, state, tribal, and local partners. Our goal is to prevent, protect from, and respond to threats and acts of terrorism and violence, while maintaining the civil liberties and privacy of our citizens. We are committed to promoting a culture of preparedness, resilience, and readiness, and to providing timely and accurate information to our stakeholders and the public.

MOHS Divisions:

- Operations
- Mississippi Analysis and Information Center (MSAIC)
- Mississippi Cyber Unit (MCU)
- Digital Forensics
- Grants

Mississippi Cyber Unit Mission

To protect and safeguard Mississippi, its resources, and its citizens from cyber threats by providing a center for cybersecurity preparedness and response. The Mississippi Cyber Unit (MCU) is achieving this through intelligence sharing, active monitoring, and effective defense.

Monitoring and Intelligence – Cyber Threat Protection Program (CTPP)

- Focuses on hardening and improving the security of current infrastructure
- Conducting risk and threat assessments
- Developing and maintaining sensors and honeypots across participating networks
- Performing real time threat sharing and gather intelligence on emerging cyber threats

Training and Response – Cyber Incident Response Team (CIRT)

- Statewide incident response team
- Working dynamically to detect and prevent cyber-attacks, respond to ongoing attacks
- Working to provide outreach services and in person training when not engaged in incident response

About us…

Bobby Freeman, Director MCU

- 25+ years of IT, security, and leadership experience
- Branch Chief for Defensive Cyber Operations Element with MS Army National Guard
- 2 mobilizations with Task Force Echo supporting US Cyber Command
- 1 mobilization overseas as Base Defense Signal Officer and Electronic Warfare Officer

Richard Stewart, Cybersecurity Team Lead

- 25+ years of IT, intel, security, and leadership experience
- USAF Retired – Cybersecurity, Adversarial Threat & Emerging Technologies
- Former Joint Cyber Analysis Course Instructor: Digital Forensics & Malware Analysis

John Dees, Cybersecurity Specialist

- 25+ years of IT, security, and training experience
- Former IT certification trainer in the private sector

Grace Mims, Cyber Threat Intel Analyst

- 2023 Graduate of the University of Mississippi – Bachelor's in Criminal Justice
- Intel Analyst Internship with MSAIC

Chris Bragg, Cyber Incident Response Specialist/K9 Handler

- 10+ years in IT, 5+ years in cybersecurity, working in the private sector
- Association of Information Technology Professionals Jackson, MS – Board Member

Ashlyn Phillips, Cyber Incident Response Specialist

- 2025 Graduate of Mississippi State University – Master's in Computer Science
- Cyber Intel Analyst Internship with MCU

Electronic Storage Detection K9

Name: Chip
Breed: Labrador Retriever
DOB: October 9, 2022
Handler: Chris Bragg
Specialized Training: Expert in Electronic Storage Detection (ESD)
Locates Hidden Evidence: Skilled at finding:

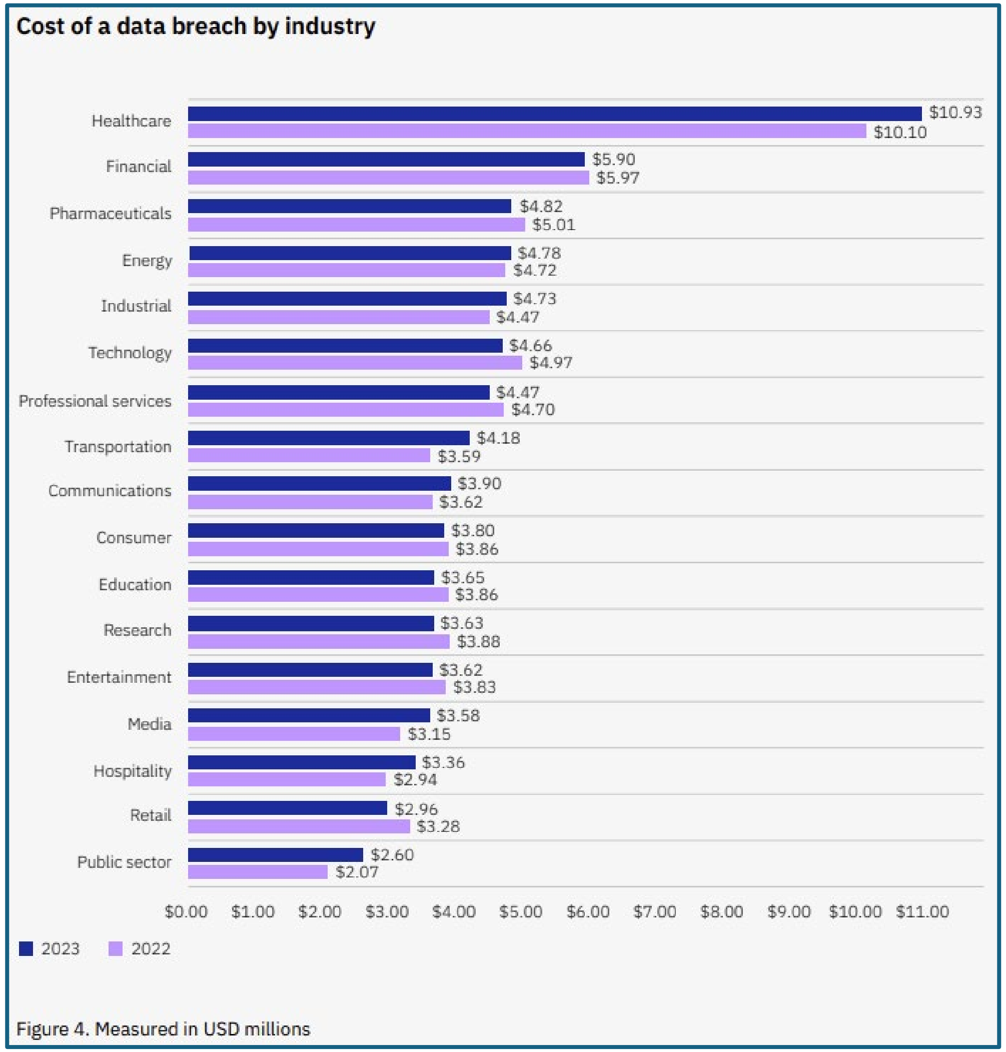
- Computers
- Micro-SD cards
- Other electronic storage devices

Enhances Investigations: A critical asset for the MCU in digital evidence recovery

Our ESD K9, Chip, received his specialized training from Jordan Detection K9 in Indianapolis, IN. His deployment with the MCU was facilitated by the National Computer Forensics Institute (NCFI). As a cutting-edge training facility run by the U.S. Secret Service, the NCFI is instrumental in empowering state and local entities to effectively investigate and prosecute cybercrimes, thereby bolstering our collective cybersecurity.

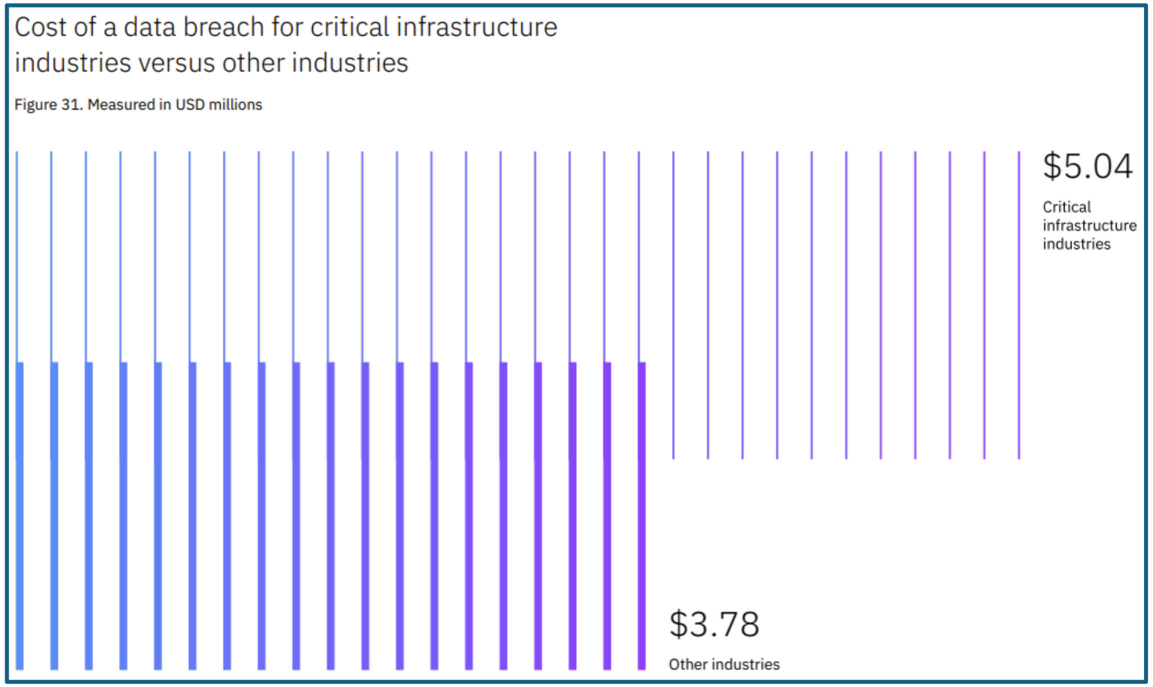
MISSISSIPPI CYBER UNIT

Cyber Threat Landscape



Cost of a data breach by industry

Figure 4. Measured in USD millions



Cost of a data breach for critical infrastructure industries versus other industries

Figure 31. Measured in USD millions

Security, IBM Corporation. (2023, March). Cost of a Data Breach Report. Retrieved from IBM Security: https://www.ibm.com/downloads/cas/E3G5JMBP

Cyber Incidents

What to do When You Have a Cyber Incident…

General Cyber Incident Response Steps:

- **Identify and Contain the Threat**
  - *Isolate the Threat:* Isolate the affected device (computer, server, network) from the rest of your network to prevent the spread of malware or data breaches.
    Do not turn affected devices off.
  - *Assess the Damage:* Determine the extent of the breach. What systems or data have been compromised?
- Notify Relevant Parties
- Gather Information
- Notify Data Breach Victims
- Recover and Restore Systems
- Learn and Improve

What to do When You Have a Cyber Incident…

General Cyber Incident Response Steps:

- Identify and Contain the Threat
- **Notify Relevant Parties**
    - *Law Enforcement*: Report the incident to law enforcement, especially if you suspect criminal activity (i.e., ransomware, suspicious network activity, etc.).
        - Local Law Enforcement
        - MS Cyber Unit (MOHS)
        - Cyber Crime Division (MS AG Office)
        - Federal (FBI, CISA, USSS)
    - *Insurance Company:* Contact your insurance provider to understand your coverage and file a claim if applicable.
- Gather Information
- Notify Data Breach Victims
- Recover and Restore Systems
- Learn and Improve

What to do When You Have a Cyber Incident…

General Cyber Incident Response Steps:

- Identify and Contain the Threat
- Notify Relevant Parties
- **Gather Information**
  - *Document Everything:* Record all actions taken, observations made, and any evidence collected. This documentation will be crucial for investigation and recovery.
  - *Identify the Source:* If possible, determine the source of the attack (e.g., phishing email, infected website, malicious software).
- Notify Data Breach Victims
- Recover and Restore Systems
- Learn and Improve

What to do When You Have a Cyber Incident…

General Cyber Incident Response Steps:

- Identify and Contain the Threat
- Notify Relevant Parties
- Gather Information
- **Notify Data Breach Victims**
  - *Customers:* If customer data has been compromised, notify them immediately in accordance with relevant data privacy laws (like GDPR or CCPA).
- Recover and Restore Systems
- Learn and Improve

What to do When You Have a Cyber Incident…

General Cyber Incident Response Steps:

- Identify and Contain the Threat
- Notify Relevant Parties
- Gather Information
- Notify Data Breach Victims
- **Recover and Restore Systems**
    - *Restore from Backups:* Use backups to restore affected systems and data to their pre-incident state.
    - *Implement Security Measures:* Strengthen your cybersecurity measures to prevent future attacks. This may include installing security patches, updating software, implementing multi-factor authentication, and conducting employee security training.
- Learn and Improve

What to do When You Have a Cyber Incident…

General Cyber Incident Response Steps:

- Identify and Contain the Threat
- Notify Relevant Parties
- Gather Information
- Notify Data Breach Victims
- Recover and Restore Systems
- **Learn and Improve**

  - *Conduct a Post-Incident Review:* Analyze the incident to understand what went wrong and how to prevent similar attacks in the future.

  - *Update Your Incident Response Plan:* Revise your incident response plan based on the lessons learned from the incident.

Important Considerations:

- **Speed is Crucial:** The faster you respond to a cyber incident, the less damage it will likely cause.

- **Have a Plan in Place:** A well-defined incident response plan will help you react quickly and effectively when a cyber incident occurs.

- **Seek Professional Help:** A cyber incident is a traumatic event, seek professional assistance from law enforcement, cybersecurity experts, or IT consultants. You do not have to go through it alone.

Cyber Services

Attack Surface Management Platform

Imagine having an invisible security guard constantly checking your public-facing assets, looking for weaknesses and potential threats. That’s what an Attack Surface Management Platform (ASM) does for your organization!

Increase your protection from cyberattacks with peace of mind:

- **Find hidden vulnerabilities**: ASM scans all your external connections, even those you might have forgotten, uncovering unpatched and internet-facing operating systems, open ports, and database weaknesses before attackers can exploit them.
- **Reduce the risk of breaches**: By continuously monitoring your external network, ASM helps you avoid potential threats, so you can address them before they can cause damage.
- **Simplify security management**: Gives you a clear picture of your overall external security posture and provides actionable recommendations for improvement.

We provide the ASM platform - We assist with monitoring - We work as your partner

State and Local Cybersecurity Grant Program

In 2022, the Department of Homeland Security announced a first-of-its-kind cybersecurity grant program specifically for state, local, and territorial governments across the country.

3-Phase Implementation:

- **Phase 1** – Cyber Readiness Assessments *(On-going/Batch 2)*
- **Phase 2** – Review assessments and address identified vulnerabilities and gaps
- **Phase 3** – Resources for maintenance, education, and training

FY22 and FY23 SLCGP Grants have been notified of award *(Batch 1)*

- Awarded over 50 sub-grants with a total of $3.8 million in funds

Accepting Batch 3 participation forms thru 31 October 2025.

- Information Session 14 October 2025

Visit *https://www.homelandsecurity.ms.gov* for more information
or email *mohsgrants@dps.ms.gov.*

Questions

Mississippi Cyber Unit

Mississippi Office of Homeland Security | 601-933-7200

MS-Cyber@dps.ms.gov | www.homelandsecurity.ms.gov