SUCCESS STORY

CASE WESTERN RESERVE UNIVERSITY

CHALLENGES

A private, R1 research institution, Case Western Reserve University prioritizes the protection of data confidentiality and integrity. For a campus dedicated to quality & integrity, effectively addressing cybersecurity incidents is an essential element of its commitment to excellence.

In the past, the CWRU Cybersecurity team used a combination of Google Sheets and Adobe Connect for cyber incident tracking and management. Google Sheets provided a place to store incident data like ID, type, and dates. Adobe Connect provided a chat room for team journaling of incident response (IR) activities and storing files.

Although this approach accomplished the task, over time it became apparent the Google-Adobe approach had key limitations:

- Lack of a single, compliant, and secure repository for sensitive data with risk of possible disclosure
- Inability to search across incidents
- Slow, error-prone collection of data
- Time-consuming manual creation of incident reporting
- High training burden and slow on-boarding of new users

SOLUTION

In searching for a better way, Case Western considered a number of solutions. Many were too time-consuming to manage and did not offer the high level of security required to protect sensitive incident information. They also lacked turnkey, purpose-built capabilities tailored for cyber security incident management. Yakabod was the best option.

Built on NIST standards and supporting GLBA and CMMC compliance, Yakabod Cyber Incident Manager provides efficient software-based processes for managing cyber security incidents and IR along with comprehensive protections for sensitive data documentation, and communication.

"Deployment and integration were really smooth... Yakabod has made my life a lot easier"

Ruth Cannon
Lead Information Assurance Analyst

YAKABOD
340 East Patrick Street
Frederick, Maryland 21701
yakabod.com

AT A GLANCE

Challenges

- Lack of security
- Lack of standardized data collection and reporting insights
- Cumbersome & manual IR processes
- Lack of department continuity and incident response maturity

Outcomes

- Secure & compliant to NIST, GLBA & CMMC
- Reduced time to resolution
- Automated report generation
- Scalable and efficient IR
- Improved insights into IR
- Improved maturity of incident response

"Our previous method of managing incidents was a big time drain."

Ruth Cannon
Lead Information Assurance Analyst

OUTCOMES

1. A single, centralized repository to securely store and manage incidents

Case Western now has a system of record for the secure storage of incident data such as evidence and artifacts, and records of Incident Response communication. All incident data is now documented, indexed and searchable. They can manage the entire incident lifecycle in a single, secure and centralized location.

2. Standardized data collection and robust reporting

Case Western eliminated inconsistent, manual data collection with Yakabod's NIST 800-61r2-based incident forms. They can now easily collect, retrieve, and report on historical data and incident handling, giving the department increased visibility into its incident landscape and trends to help improve its strategic posture.

3. Historical Repository for Training, On-boarding

By leveraging a standardized, centralized repository of past incidents, Case Western saved time onboarding personnel, reduced the burden on management, and decreased time for new IR personnel to contribute to their team.

YAKABOD

"Yakabod provides the security that's needed and is built specifically for cyber incidents. There's really nothing else like it."

CWRU CISO