UNIVERSITY SYSTEM OF GEORGIA

Cybersecurity

# 2024 Report

# Table of Contents

# Introduction

## 2024 - A year in transition.

USG Cybersecurity has undergone considerable change in the past year. Nevertheless, our approach to digital risk continues to be undergirded by five core pillars: governance, management, people, process and technology.

In this, my first annual report to the USG community and the people of Georgia, we seek to highlight the incredible efforts underway to safeguard information entrusted to us and improve our resilience to cyber threats.

Cyber-risk continues to evolve and safeguards are continuously adjusted to accommodate the ever changing landscape. USG Cybersecurity added third-party risk management capabilities and a Virtual ISO program in the service portfolio, equipping our institutions with additional resources to identify and reduce digital risk.

Although change is essential, our focus remains toward a cohesive approach for cybersecurity risk across USG.

Looking ahead, USG Cybersecurity will continue its mission to be an affordable and efficient partner enabling unmatched opportunites for teaching, leadership and service.

Dr. W. Todd Watson, CISSP
Associate Vice Chancellor,
Systemwide Chief Information Security Officer
University System of Georgia

# USG
## By the Numbers

**364,525**

Student enrollment

**100,000**

Employees and contractors

**26**

Number of USG institutions

**$10B**

Annual Budget

**$22B+**

Economic Imact

**210+**

Total Cybersecurity Staff

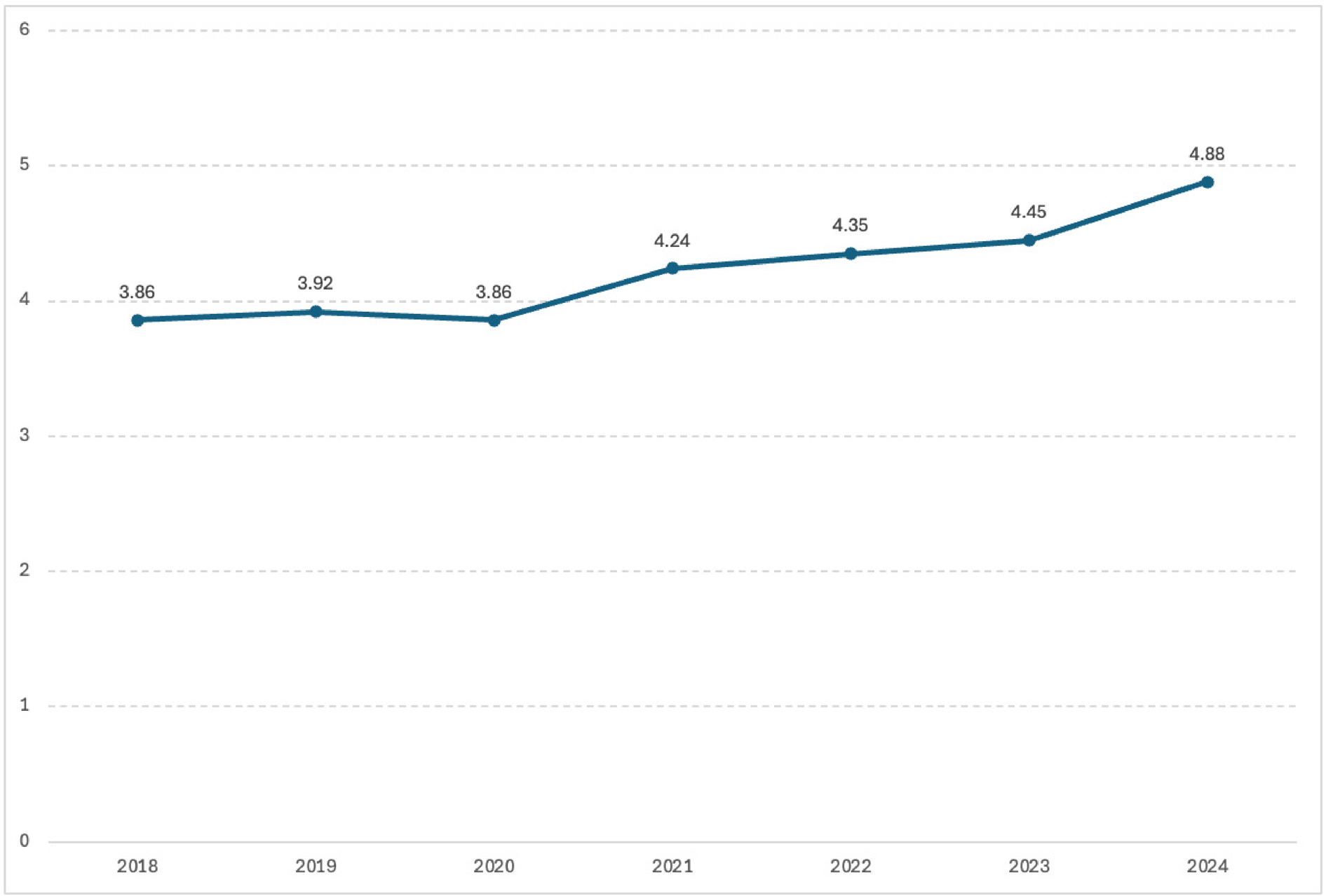
# An Evolving Threat Landscape

Based on USG data and research results from our partners, the cyber threat landscape continues to evolve. Notable changes include the following observations.

- Additional investments in offensive cybersecurity activities by the CCP have resulted in **more than a 100% increase** in cyber activity originating from China.
- Voice phishing, "Vishing," activities have **increased more than 400%** since the beginning of 2024.
- Significantly fewer threat detections in 2024 involved **malicious software**.
- Threat actors are becoming more efficient. The average time from network infiltration to lateral movement has been **reduced to about 48 minutes**, down from about 72 minutes.
- Evidence suggests **AI is being leveraged** by adversaries to shorten the path, and therefore the time, between access and exploitation.
- **Almost 70%** of breaches across all business segments involved a human element.
- More than 30% of breaches resulted in **some form of extortion**, such as ransomware.
- Nearly 30% of information system breaches are the result of **some type of Error**.
- The median time for users to fall for phishing **email is less than 60 seconds** of delivery.
- Exploitation of software vulnerabilities has **risen by nearly 200%** since 2023.
- **Compromised credentials and phishing** were the primary initiators for over 30% of breaches.
- 98% of organizations worldwide that use AI are **exposing confidential information** unwittingly.

# An Evolving Threat Landscape

## Global average cost of a data breach, millions USD




Sources: IBM, Verizon

## Prevention continues to be the most cost-effective cybersecurity strategy.

The cost to mitigate data breaches continues to rise. A combination of increased sophistication in conjunction with rising resource costs continue to push overall prices upward.  Recent studies suggest that organizations investing in proactive cybersecurity efforts, along with incident response teams and regularly tested cybersecurity plans saved, on average, over $2.5 million in costs per security breach.

# Five Pillars of USG Cybersecurity

**Governance**

An effective culture of governance requires we ensure our purposes remain consistent, the culture remains open and collegial, we remain accountable to the process and structure of governance and each organization ensures compliance with our frameworks.

**Management**

Effective cybersecurity management must uphold key principles of confidentiality, integrity and availability of information resources. In addition, nonrepudiation, authentication, risk, vulnerability, asset, identity, monitoring, and incident management are necessary attributes for establishing confidence in our work.

**People**

People are our most precious resources. While mission success remains our goal, we acknowledge that achieving our objectives rely upon ensuring our people are supported, respected, provided opportunities for personal and professional growth, rewarded for their contributions, and encouraged to participate as key contributors of our program.

**Processes**

USG Cybersecurity promulgates consistent processes to drive efficiency, repeatability, and continuous improvement. Processes are undergirded by documentation and periodic reviews to ensure continuity.

**Technology**

Highly-specialized technology is employed to ensure our teams can achieve their mission goals with a minimum of visibility gaps, sacrifices to performance, while also maintaining safety and security. Technology is reviewed periodically and updated to more cost-effective solutions.

# Tools & Service Catalog

A range of specialized tools and services equip USG organizations to protect information and technical resources.

## *POLICIES, STANDARDS & GUIDELINES*

Protecting USG information and IT resources is a shared responsibiity across all units. Guided by regulatory, compliance and operational requirements, USG Cybersecurity leads changes to policies, standards and guidelines through a collaborative governance process.

## *CONSULTING SERVICES*

Consulting services are available to all USG organizations to understand and assess risk, ensure appropriate technologies are employed for identifiying, protecting and mitigating cyber-threats, and assisting with compliance requirements.

### Virtual Information Security Officer Program (VISO)

The VISO program was developed to ensure USG organizations are equipped with adequate assistance for maintaining and maturing their cyber program. VISOs provide continuity during cyber employee transitions, expert reviews of progam elements, consultative engagements, and tabletop exercises to ensure readiness.

## TRAINING & AWARENESS

Mandatory and customized cybersecurity training includes skill builders, workshops, and opportunities to raise awareness. Tools, communities of practice and role-based training complement the training and awareness program

### Mandatory Cybersecurity Training

Mandatory cybersecurity awareness training for USG employees and contractors is conducted semi-annually in accordance with USG standards to ensure faculty and staff are apprised of current an ongoing threats.

### *Customized Training*

Cybersecurity periodically provides training for specific and emerging technologies, such as artificial intelligence, ransomware, data protection, and privacy rules. In addition, training to cybersecurity professionals pertaining to product and tools they use improves efficiencies and effectiveness.

### *Cybersecurity Program Review*

Organizations participate in a bi-annual mandatory cybersecurity program review to assess the key performance indicators of each cybersecurity program.

### *Phishing Simulations*

USG leverages leading phishing simulation tools to continually identify and address social engineering vulnerabilities. Our tools measure propensity for phishing based on behavioral analysis, enabling our organizations to identify training opportunities for improving our resilence to social engineering attacks.

### *CISO/CIO Workshops*

USG hosts a bi-annual workshop for Information Security Officers and Chief Information Officers. These 2-day sessions are an opportunity for information sharing, collaboration, skills development, and open discussion on new and emerging topics relevant to the technology and cyber leadership.

## *RISK ASSESSMENTS*

Cybersecurity Risk Assessments identify risk and compliance issues to manage address risk proactively.

### *Supplier Risk*

Supplier risk has emerged as a significant factor for all organizations entrusting information to third parties. USG is identifying and closing supplier risk gaps.

## *THREAT MANAGEMENT*

Proactive identification and mitigation of vulnerabilities is a significant saving to taxpayers. Resolving system weaknesses before a compromise reduces the likelihood or consequences resulting from cybersecuriy incidents.

### *Vulnerability Management*

In 2024, USG initiated a systemwide vulnerability management program. This program identifies ongoing an emerging vulnerabilities, such as patching cadence or outdated systems. Vulnerabilities are reported centrally to the Enterprise Security Operations Center for mitigation and assurance efforts.

### *Penetration Testing*

Cybersecurity facilitates numerous penetration tests annually that analyze pre-scoped targets using the tools tactics and procedures adversaries are known to leverage. Issues that are identified are remediated and retested to ensure information resources are adequately hardened against cyber-threat actors.

### *Hardware Assessments*

The Internet-of-Things (IoT) holds great promise for conveniently managing special-purpose products. However, significant enterprise risks result from installing poorly designed or manufactured products on the network. Cybersecurity performs technical analysis of IoT products from a risk view to identify risk, ensure resilience, and maintainability.

# Tools and Services Catalog

## *THREAT DETECTION & IDENTIFICATION*

Threat detection and identification comprises the combination of cybersecurity staff, technologies, and processes for identifying potential cyber threats, achieving network and endpoint visibility, and categorizing existential threats. USG Cybersecurity is amidst a multi-year plan to converge on common toolsets, enabling a consistent view of  security stance systemwide, which is essential for informing readiness, allocating budget efficiently, and measuring risk reduction while consistently identifying adversaries, malware, and system compromises for rapid, uniform responses.

### DDoS Protection

USG PeachNet® provides all customers with protection from distributed denial of services attacks, enabling availability of information services to students, employees and constituents.

### Attack Surface Management

ASM services continuously monitor, identify, and manage the cybersecurity vulnerabilities and potential attack vectors in the cloud and on-premise infrastruc-tures from the attackers' point of view.

### Digital Threat Monitoring

Threat monitoring detects malicious targeting and potential attacks with visibility into the open, deep, and dark web. Threat monitoring helps to identify threats early, disrupt sophisticated attack campaigns, and detect breaches or volumetric data leaks.

### Leaked Credentials

Millions of user credentials are acquired, aggregated and sold on the dark web daily. If a compromised credential of a USG organization is identified, Cybersecurity notifies the organization to determine if the password was reused and assist the affected individual reset their password.

### *Suspicious Domain Alerts*

Cybersecurity monitors for suspicious domains and webservices, such as fake domains or websites that presume to be sanctioned by a USG organization.  When a potentially malicious domain or website is found, the domain or site is investigated and potentially taken down to protect students, employees and constiutents from counterfeit services.

### *Network Detection and Response*

Each organization is monitored by network detection and response technology to identify emerging and existential threats. A systemwide level of visibilty helps to correlate attack levied against multiple sites simultaneously for a coordinated defensive strategy.

### *Endpoint Management and Protection*

USG has a requirement that all state-owned user devices be centrally managed. In addition each device is protected by advanced antivirus and anti-malware software to limit the potential of damage from malicious software.

### *Security Operation Center*

USG operates one of the largest by volume higher education-focused Security Operations Centers in the world. Several billion events are detected daily. Analysts leverage detection technologies, AI machine learning, and real-time intelligence to identify and mitigate cyber-risks to USG organizations.

## *INCIDENT RESPONSE COORDINATION*

Incident response coordination services provide an organized and systematic approach to a cybersecurity incident or breach and communicate information about the situation.

### *Incident Response Coordination and Communication*

During a cyber incident, a System-level coordination and communication process is initiated to ensure that all stakeholders are informed as details emerge. Internal experts in incident response, legal, privacy, compliance, and communications are rallied. If required, statutory communications is performed. If external resources for mitigation are required, Cybersecurity works with the USG organization to make the determination.

### *Information Awareness Sharing*

If indicated, Cybersecurity will share information pertinent to other USG organizations for awareness and visibiity. As details emerge, tools, tactics and procedures used by an adversary are shared within the community to ensure a coordinated response for protecting USG information.

## *THREAT INTELLIGENCE SHARING*

Partnering with a range of local, state, and federal organizations as well as strategic partners, Cybersecurity produces and shares threat intelligence products. Information sources include published cyber threats, cybercrime, trends from global partners, vulnerability analyses, dark web monitoring, regional or local threats, and related intelligence sources.

# Standards and Strategies

USG technology standards are promulgated through a transparent governance process and ultimately published in the USG's Information Technology Handbook. The Handbook is updated periodically to address new compliance and audit requirements, technology advancments, and operational needs.

## Section 3.6 - Managed File Transfer Services

For organizations operating managed file transfer services (MFTs), this new standard formalizes the expectations for managing the service responsibly, to include access rights, storage and encryption requirements, and data retention limitations within MFTs.

## Section 3.7 - Automation Management

As computational efficiency increases, the ability to automate repetitive tasks has become within reach of most organizations. Nevertheless, to ensure we remain grounded in our fundamental principles for managing risk, consistent practices are essential.

This new section addresses intelligent automation (IA), robotic processing automation (RPA) and artificial intelligence (AI) systems by ensuring appropriate business and implementation requirements are contemplated, activities are logged apropriately, risks are assessed and managed, and business continuity considerations are part of an implementation.

## AI Companion Guide

Cybersecurity believes implementing AI to automate business processes and unlock additional insights within data is emerging as a new inflection point of technological advancement. This noted, USG will adopt an informed approach to the use of AI to ensure we protect people, their information, and enable ethical application of the technology. The Companion Guide defines USG's overarching philosophy for advancing AI in innovative ways to be more efficient while also remaining true to our core principles.

# Cohesion and Collaboration: Virtual Information Security Officers

USG Board Policy directs all organization heads to follow an approach promulgated by the System CISO for identifying, managing and reducing cyber risk. One specific requirement is appointing a trained and qualified leader of the cybersecurity program.

As a practical matter, hiring and retaining qualified cybersecurity professionals and ensuring compliance with both USG and institution requirements has been a challenge for some units. In addition, the ability to effectively execute cyber leadership while simultaneously delivering on priorities and projects is difficult, particularly for smaller institutions.

## The VISO Program

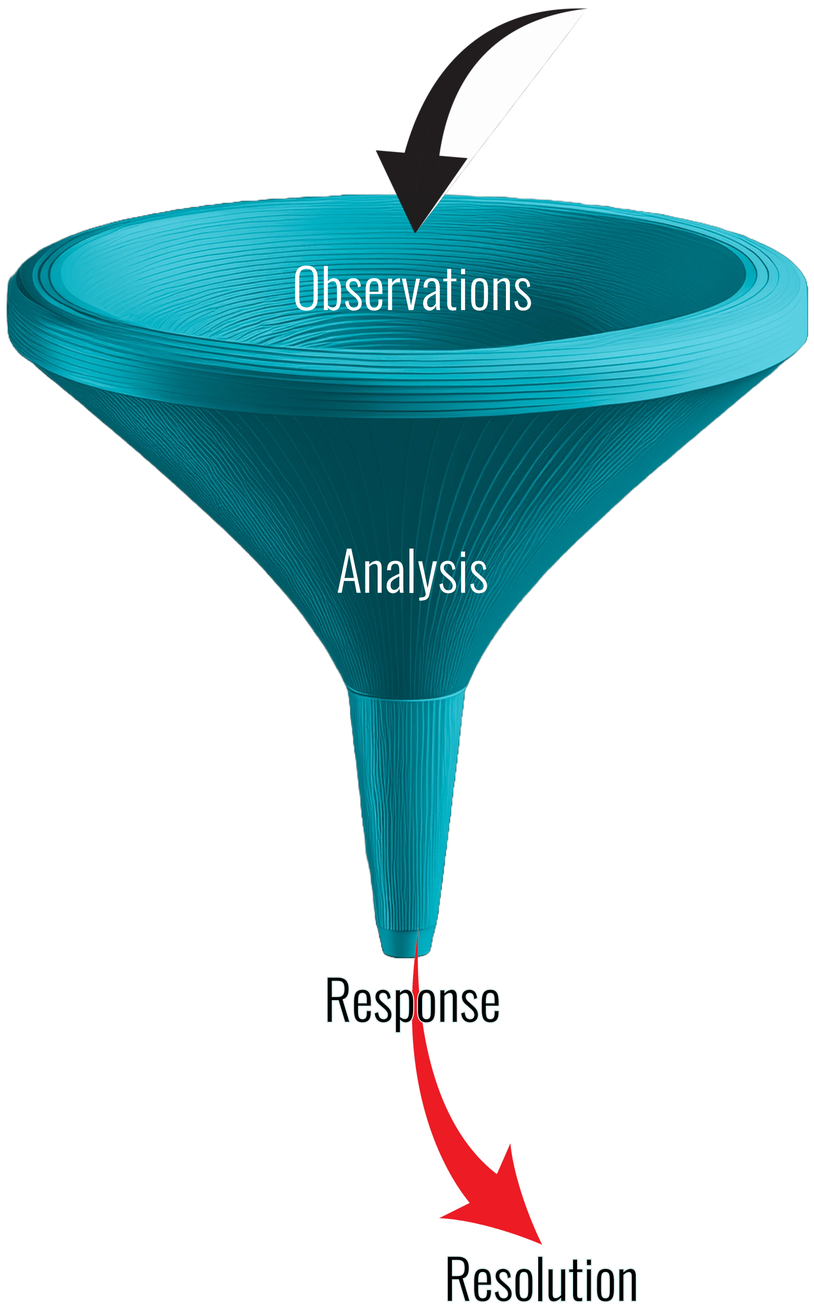
Collaboration between the USG CIO and CISO enabled the creation of the Virtual Information Security Officer (VISO) program in 2024.

Institutions can book engagements with the VISO team to address challenges for achieving policy and standards compliance, risk assessments, developing or improving security plans, tabletop exercises, and other strategic and tactical needs.

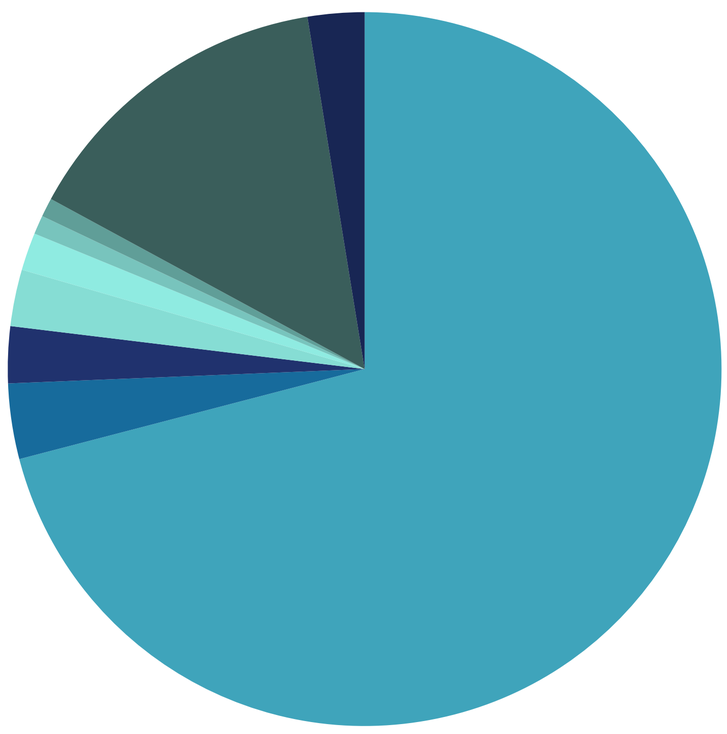
This program offers trained and qualified staff to supply capacity while also creating community connections.

# Cybersecurity Observations

Using a combination of manual and automated tools, Cybersecurity receives and analyzes more than 4 billion observations every day. Tools leveraging AI and tuned algorithms assist our analysts so they focus energies on correlated and identified risks.




## Incidents by Type




**4B**

Number of daily observations analyzed

**4,000 +**

Number of supplier risk assessments performed

**6,000 +**

Incidents investigated and resolved

**7,000**

Number of manually investigated incidents

**93.9%**

Average completion rate for mandatory cybersecurirty awareness training

**10.5%**

Average clickrate during phish tests

# University Spotlight


(L to R) Rus Parham, GRC Manager, Amanda Flippen, GRC Analyst, Jeremy Willoughby, GRC Analyst

## Augusta University GRC Team

Augusta University's (AU) Cyber Defense Governance, Risk and Compliance (GRC) Team manages a cutting-edge program focused on producing highly skilled cybersecurity professionals while also serving as a vital component to the success of the AU cyber defense strategy for a hybrid entity of academics and healthcare. The team consists of three full-time employees.  A small team, but with a big punch!

For GRC provides a real-world environment that incorporates AU student assistants and military Skillbridge personnel to work alongside experienced full-time GRC cyber defense professionals charged with mission to provide proactive cybersecurity solutions such as: risk management, cybersecurity training, auditing response and updates to information security policies. Day-to-day, this might involve using risk assessment tools such as Clearwater IRM Analysis, conducting phishing campaigns or training awareness campaigns, analyzing threat intelligence reports, or collaborating on projects that require them to apply risk management principles. This hands-on experience bridges the gap between theory and practice, preparing students and military partners for the challenges they will face in their cybersecurity professional careers. They gain practical skills in governance frameworks, compliance measures and importantly, risk management, which is crucial in today's landscape.

The GRC team continues to enhance cybersecurity at AU through various initiatives. For example, GRC has enhanced the risk management program through implementation of exceptions to USG policy for multi-factor authentication (MFA) as required by the USG IT Handbook. These exceptions help to monitor compliance and provide transparency on security posturing while enabling research and student experience. Many vendors are still unable to comply with MFA standards, but this effort has enabled AU to use vendors that need a bit more time to meet new industry security standards and USG requirements.

# University Spotlight

## Kennesaw State's Academic Integrity Program

Over the past two years, Kennesaw State University (KSU) has taken big steps to create a more honest and fair learning environment. One of the main goals has been to fight against academic cheating services, also known as contract cheating. These services help students cheat on their course work, but compromises the value of a college degree. These academic cheating services not only impacts KSU, but other universities across the University System of Georgia and world.

KSU Cybersecurity worked closely with different groups on campus and with outside partners to address this issue. By working together, we've added new processes to help detect cheating and act when needed. These efforts help protect the integrity of our academic programs.

To raise awareness, KSU has also given presentations that explain how contract cheating affects students, reputations, and the whole campus communities. By sharing information and teaming up on initiatives, we've become better at recognizing and responding to these challenges.

# University Spotlight

## Fort Valley State University - Training and Awareness

Fort Valley has been intently educating faculty, staff and students in the elements of cyber-risk. They promote the importance of Cybersecurity Awareness training heavily. Based on user feedback, Fort Valley adjusted their awareness training schedule by a month to facilitate on-time completions. The new schedule alleviated a conflict with final examinations and ensured availability of adjunct faculty.

Awareness training was recently added to new hire orientation. The theme is not only training participation but also emphasizing the importance of Cybersecurity awareness by providing examples of real incidents. Fort Valley's Cybersecurity team also speaks to the freshman class every semester to alert new students of historical and emerging risks, with particular attention given to the type of attacks directed at students.

Fort Valley's cybersecurity program recently launched a student-led Cybersecurity Club. The club provides students having similar cybersecurity interests a forum to connect and even compete with their peers. Club members become ambassadors of the cybersecurity program, to help educate their peers in cyber-risk. The club anticipates their second competition beginning in the Spring of 2025. Engaging with professors to speak to classes about cybersecurity also enables students to engage with real professionals and learn more about the profession.

Fort Valley continues to improve network traffic monitoring quality throughout the network, reduce the window for patch management, and shorten the time between incidents and notification. Fort Valley is periodically testing additional cybersecurity tools and finding ongoing opportunities for tabletop exercises to improve visibility and incident response preparedness.

IT and Cybersecurity Teams
Fort Valley State University

For more information, contact:

Dr. W. Todd Watson
Associate Vice Chancellor,
Chief Information Security Officer
University System of Georgia

ciso@usg.edu

UNIVERSITY SYSTEM OF GEORGIA
Cybersecurity