AuditCon

by ACUA

Louisville Kentucky | September 14-18, 2025

ACUA

CYBERSECURITY AUDITS TRENDS FOR HIGHER EDUCATION INSTITUTIONS

September 16, 2025

INTRODUCTION

P. Dimitris Bantileskas, CPA/CFF/CITP, CVA, CFE, ISACA Cybersecurity Audit Certificate

Partner at Nawrocki Smith's Forensic Accounting & Internal Audit Group. Dimitris provides leadership and support in directing financial, operational, and cybersecurity audits to determine the adequacy of internal control systems and the degree of compliance with these controls. He is also charged with conducting special investigations as requested, and making recommendations for improved controls, operating procedures, and systems designs.

TODAY'S DISCUSSION POINTS

Cybersecurity Vulnerability Trends in Higher Education

Risk Management Strategies

Scenario Based Exercises

CYBERSECURITY VULNERABILITY TRENDS IN HIGHER EDUCATION

CYBERSECURITY CHALLENGES

ESCALATION OF RANSOMWARE ATTACKS

- Ransomware attacks have surged, with 66% of higher education institutions reporting incidents in 2024, a slight decrease from 79% in 2023.
- The average ransom payment reached $5.85 million in 2024, with institutions often paying more than the initial demand.
- Only 2% of institutions that paid ransoms recovered all their data. Ransom payments are unreliable for data restoration.

Resources:

31 Must-Know Education Cybersecurity Statistics - October 3, 2024: https://www.varonis.com/blog/education-cybersecurity-statistics

The State of Higher Education Cybersecurity: Top Insights and Trends – August 18, 2025: https://www.bitlyft.com/resources/the-state-of-higher-education-cybersecurity-insights-trends

The State of University Cybersecurity: 3 Major Problems in 2025 – July 7, 2025: https://www.upguard.com/blog/top-cybersecurity-problems-for-universities-colleges

CYBERSECURITY CHALLENGES (cont'd)

BUDGET CONSTRAINTS AND RESOURCE LIMITATIONS

- Many institutions face budgetary constraints that limit their ability to invest in comprehensive cybersecurity measures.
- A lack of dedicated cybersecurity personnel can hinder the development and implementation of effective security strategies.

COMPLIANCE AND REGULATORY CHALLENGES

- Institutions must navigate a complex array of regulations, including FERPA, GLBA, HIPAA, and CMMC, to ensure data privacy and security.
- Meeting compliance requirements necessitates regular audits and updates to security protocols, which can strain limited resources.

DECENTRALIZED IT INFRASTRUCTURES

RISK

- Many departments manage their own IT assets, leading to inconsistent policies and controls.
- A broad network of devices expands the potential entry points for attackers.

AUDIT APPROACH

- Review IT governance structure, roles, and policies.
- Interview central and departmental IT staff.
- Test for duplicative or conflicting security settings.

LEGACY SYSTEMS

RISK

Outdated OS, applications, and unsupported hardware increase attack surface.

AUDIT APPROACH

- Conduct sample testing of patch management logs.
- Review asset inventory for unsupported systems.
- Validate controls over software updates and end-of-life systems.

WEAK ACCESS MANAGEMENT

RISK

Overprovisioned or inactive accounts, poor password practices, and a lack of MFA.

AUDIT APPROACH

- Extract and analyze user access logs.
- Review onboarding/offboarding processes.
- Test compliance with password policy and MFA implementation.

INSUFFICIENT NETWORK SEGMENTATION

RISK

Flat networks allow lateral movement if one device is compromised.

AUDIT APPROACH

- Review network architecture diagrams.
- Perform vulnerability scans or simulate lateral access.
- Assess firewall and VLAN configurations.

INADEQUATE DATA CLASSIFICATION AND PROTECTION

RISK

Sensitive data (student PII, research, health info) not adequately protected.

AUDIT APPROACH

- Test data loss prevention (DLP) controls.
- Evaluate encryption practices.
- Review data classification policy and application.

ENDPOINT SECURITY GAPS

RISK

Bring Your Own Devices (BYOD) often lack consistent security controls.

AUDIT APPROACH

- Verify endpoint protection (AV/EDR) deployment logs.
- Review BYOD policy enforcement.
- Sample test devices for compliance.

INCONSISTENT INCIDENT RESPONSE PREPAREDNESS

RISK

Lack of structured, tested plans for cyber incidents.

AUDIT APPROACH

- Review incident response (IR) plan and tabletop test results.
- Interview stakeholders on past IR events.
- Assess notification and escalation protocols.

PHISHING AND SOCIAL ENGINEERING EXPOSURE

RISK

Users remain highly vulnerable to deceptive emails.

Phishing remains a prevalent method for attackers to gain unauthorized access, with 100% of surveyed institutions experiencing at least one phishing attack in the past year.

AUDIT APPROACH

- Request phishing test results and awareness training logs.
- Examine email filtering controls.
- Test sample users' awareness via survey or interview.

RISK MANAGEMENT STRATEGIES

RANSOMWARE RISK MANAGEMENT

Key Area	Audit Objectives	Audit Procedures	Audit Recommendations	Rationale
Backup & Recovery	Ensure regular, tested, and secure backups exist.	• Review backup policies, logs, and test schedules. • Verify use of offline/offsite or immutable backups. • Confirm backup encryption and access controls.	Enforce use of encrypted, immutable, and offsite backups; conduct semi-annual restoration testing.	Ensures data recoverability and limits impact of ransomware.
Endpoint Protection	Verify controls to detect and block ransomware.	• Test deployment of antivirus/EDR solutions. • Confirm auto-update settings and threat response capabilities. • Review EDR alert logs.	Deploy advanced EDR solutions institution-wide; centrally manage and monitor endpoint security.	Improves detection and containment of ransomware infections.
Email Filtering & Phishing Defense	Evaluate protections against phishing-based delivery.	• Review email gateway settings (e.g., SPF, DKIM, DMARC). • Examine phishing simulation and awareness training results.	Ensure that email gateway configurations include enforced and properly aligned SPF, DKIM, and DMARC policies to authenticate senders and reduce spoofed emails. Implement routine phishing simulation campaigns and track user response metrics over time.	Validates the authenticity of incoming emails and reduce spoofing attempts
Incident Response Planning	Assess preparedness for ransomware events.	• Review ransomware-specific playbooks. • Examine logs from tabletop exercises or live drills. • Confirm documented escalation and communication protocols.	Develop and test a ransomware-specific incident response playbook with clearly defined roles.	Enhances preparedness and response coordination during an event.

CLOUD SECURITY RISK MANAGEMENT

Key Area	Audit Objectives	Audit Procedures	Audit Recommendations	Rationale
Data Classification & Encryption	Ensure sensitive data is protected in transit and at rest.	• Review encryption settings in cloud platforms (e.g., S3, Azure Blob). • Verify classification of cloud-stored data. • Test configurations for compliance.	Implement automated classification tools or enforce manual tagging to categorize data by sensitivity (e.g., PII, FERPA, HIPAA, financial).	Inadequate classification leads to inconsistent application of security protocols, leaving sensitive data vulnerable to exposure or improper management.
Access Controls	Confirm strong access controls in cloud environments.	• Review IAM policies and logs (least privilege, MFA, role-based access). • Verify logging of admin actions. • Sample-test user access levels.	Enforce MFA for all cloud access; apply least privilege access and conduct periodic access reviews.	Reduces risk of unauthorized access and privilege escalation.
Configuration Management	Detect misconfigurations or open access.	• Assess cloud security posture via tools (e.g., AWS Config, Azure Security Center). • Test for public access to storage buckets. • Review change management logs.	Implement automated tools (e.g., CSPM) to detect misconfigurations; enforce security baselines.	Minimizes misconfiguration risks in SaaS, IaaS, and PaaS platforms.
Logging & Monitoring	Ensure continuous visibility into cloud activity.	• Confirm centralized logging (e.g., CloudTrail, Azure Monitor). • Verify alerting for anomalous behavior. • Examine retention policies for audit logs.	Enable and retain detailed audit logs for cloud environments; integrate with SIEM tools.	Ensures visibility and forensics capability for cloud incidents.

THIRD-PARTY RISK MANAGEMENT

Key Area	Audit Objectives	Audit Procedures	Audit Recommendations	Rationale
Due Diligence & Onboarding	Verify that vendors undergo risk screening.	• Review vendor onboarding policies and checklists. • Request SOC 2/ISO 27001 reports or risk assessments. • Examine data security clauses in contracts.	Require all third parties handling sensitive data to provide SOC 2 Type II or equivalent security attestations.	Establishes minimum baseline for vendor security posture.
Data Handling & Compliance	Ensure data sharing complies with FERPA, HIPAA, GLBA.	• Validate vendor access logs and DLP controls. • Review data sharing agreements and compliance attestations.	Standardize data protection language in contracts, including breach notification timelines and audit rights.	Protects institutional data and supports legal compliance (FERPA, HIPAA, GLBA).
Ongoing Monitoring	Assess mechanisms to track vendor performance and risk.	• Review periodic vendor evaluations and audit rights clauses. • Examine breach notification procedures and response timelines.	Maintain a centralized vendor inventory; conduct annual risk reviews of high-impact vendors.	Enables continuous oversight and reassessment of evolving risks.
Offboarding & Contract Termination	Confirm secure data return or destruction post-engagement.	• Review contract exit clauses. • Verify vendor offboarding logs and certifications of data deletion.	Ensure all contracts include specific exit clauses requiring secure data disposal, return, or transfer in accordance with data classification and regulatory requirements.	Exit clauses in contracts protect the institution by ensuring clear expectations for secure data disposition.

Source: 2021 Nationwide Cybersecurity Review Summary Report

SCENARIO BASED EXERCISES

RANSOMWARE ATTACK ON STUDENT RECORDS SYSTEM

Objective

Test incident response coordination and data recovery readiness.

Scenario

At 7:00 AM, the university's registrar office reports that access to the student information system is denied. IT staff identify a ransomware note demanding $250,000 in cryptocurrency. The attackers claim to have exfiltrated student PII and academic records.

Who leads the incident response?

Chief Information Security Officer (CISO) or IT Director

0%

Executive Leadership

0%

External Incident Response Vendor / MSSP

0%

Not clearly defined in our current plan

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Who is notified first?

Internal IT/Cybersecurity Team 0%

Legal Counsel 0%

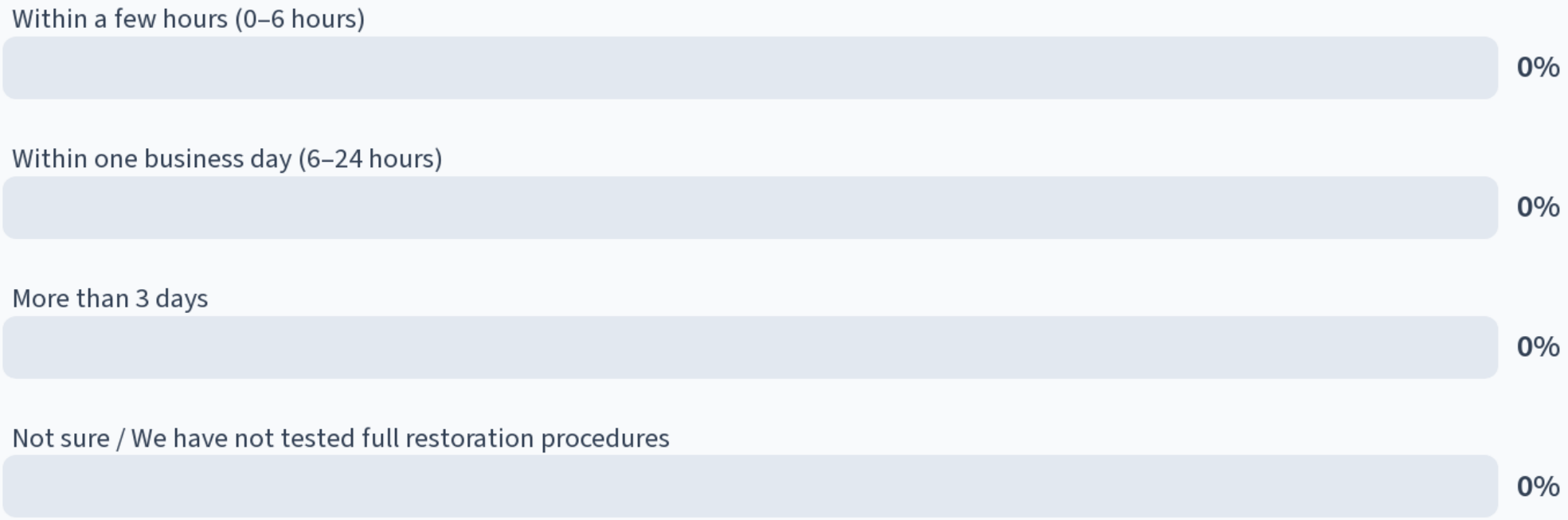
Law Enforcement (e.g., FBI, local police) 0%

Cyber Insurance Provider 0%

We do not have a defined notification sequence 0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

How long would it take your organization to fully restore operations from backup?



Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

What's the process for engaging cyber insurance?

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

LESSONS LEARNED

Preparedness Requires Practice

- Institutions must maintain tested and isolated backups. Simulations should confirm that data can be restored without paying a ransom.

Incident Response Matters

- Incident response roles must be pre-assigned and trained (e.g., IT, legal, executive, comms). FERPA implications, mandatory breach notifications, and pre-vetted communication templates must be part of the playbook.

Internal Audit Value

- Auditors help ensure disaster recovery plans are actionable, not just documented.

CLOUD MISCONFIGURATION EXPOSES RESEARCH DATA

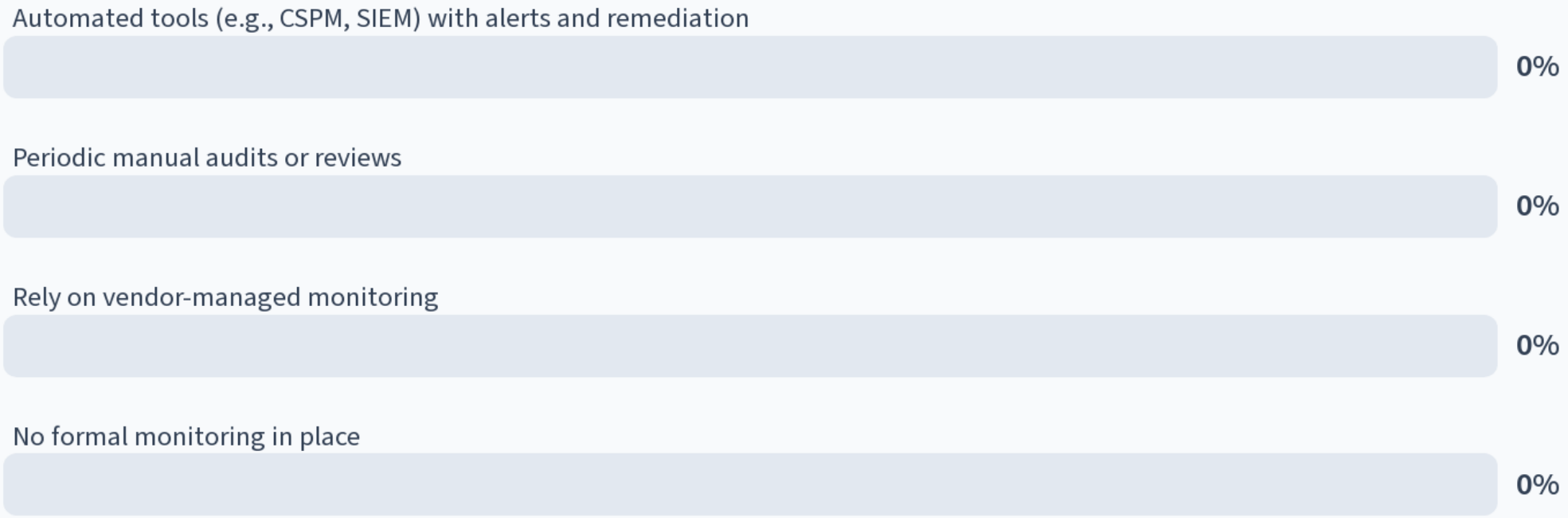
Objective

Evaluate cloud governance and vendor oversight.

Scenario

A faculty member discovered an online folder that contained protected research data but was accessible to the public. The misconfiguration resulted from a third-party cloud migration vendor.

How does your organization monitor cloud environments for misconfigurations?



Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Does your organization require a Data Protection Agreement (DPA) with third-party cloud vendors?

Yes – DPAs are mandatory and reviewed regularly

0%

Sometimes – Depends on the type of data or vendor

0%

No – Not currently a standard practice

0%

Unsure / Not involved in contract negotiations

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

What is your organization's first step when a cloud misconfiguration is discovered?

Disable public access and isolate the affected resource

0%

Notify cloud security and IT teams to assess the exposure

0%

Alert legal/compliance units to begin documentation and response

0%

Unsure / No formal containment procedures exist

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

LESSONS LEARNED

Cloud Misconfigurations Are Preventable

- Institutions need continuous cloud posture management (CSPM) tools and policies that detect misconfigured storage and access controls.

Vendors Extend Your Risk Surface

- Even when using third-party infrastructure, the university retains accountability for protecting research subjects and data. Third-party vendors must be bound by Data Protection Agreements (DPAs) that outline security expectations, breach response obligations, and audit rights.

Internal Audit Value

- Auditors can identify gaps in third-party risk management.

COMPROMISED USER ACCOUNT USED FOR INTERNAL PHISHING

Objective

Test detection and response to insider-origin threats.

Scenario

A user’s credentials are compromised through a phishing campaign. The attacker uses the account to send malicious links to 500+ staff and students using the university’s mail system.

How quickly is the compromise detected?

Within minutes (via automated alerting)

0%

Within a few hours (via user reports or review)

0%

More than 24 hours

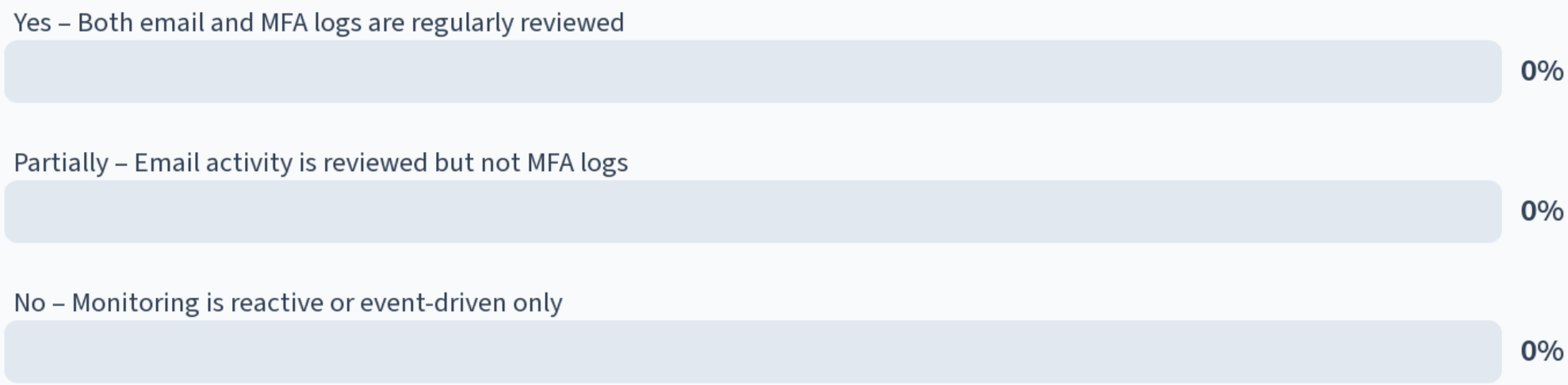
0%

Unknown / Not monitored

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Does your organization actively monitor email activity logs and multi-factor authentication (MFA) usage for anomalies?



Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Who is primarily responsible for internal notification and response communication when an account is compromised?

IT or Information Security Team

0%

Communications/Public Affairs with IT input

0%

Departmental or Academic Leadership

0%

No defined communications protocol exists

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

How does your organization measure the effectiveness of phishing awareness training?

Simulated phishing campaigns with tracked click rates

0%

Periodic quizzes or post-training assessments

0%

We do not currently measure training effectiveness

0%

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

LESSONS LEARNED

Detection Speed Directly Impacts Exposure

- Institutions must implement real-time alerting and anomaly detection to reduce response time.

Email Security Must Be Layered

- Advanced filtering and domain spoofing protections are essential for preventing malicious attacks.

Internal Audit Value

- Auditors can help identify root causes in security breaches, such as delayed detection and insufficient defenses.

DDOS ATTACK DURING ONLINE FINAL EXAMS

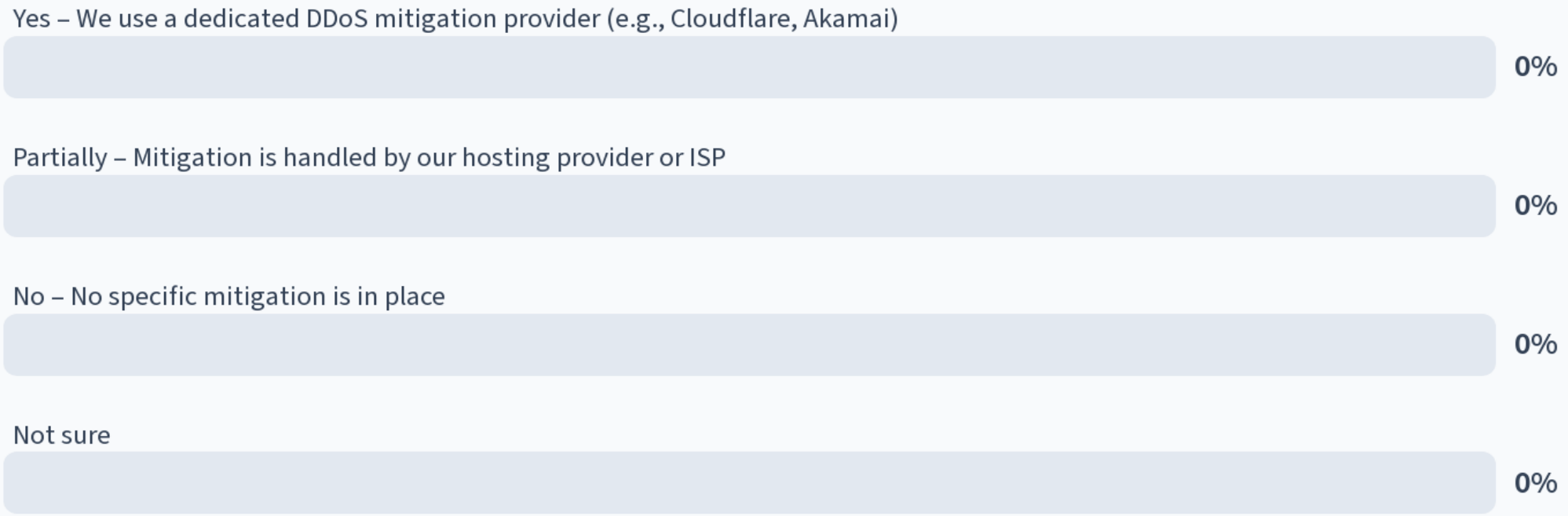
Objective

Assess continuity planning and external coordination.

Scenario

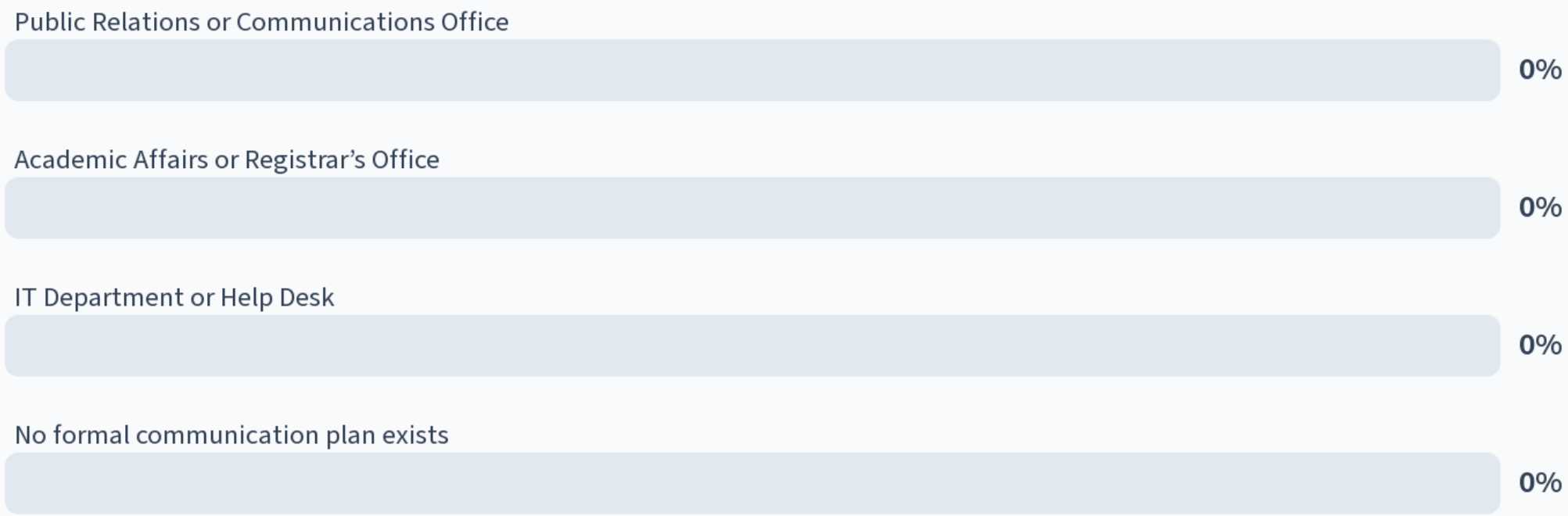
The university’s learning management system (LMS) goes offline due to a distributed denial-of-service (DDoS) attack. The outage lasts 3 hours.

Is there a DDoS mitigation service in place to protect online academic platforms?



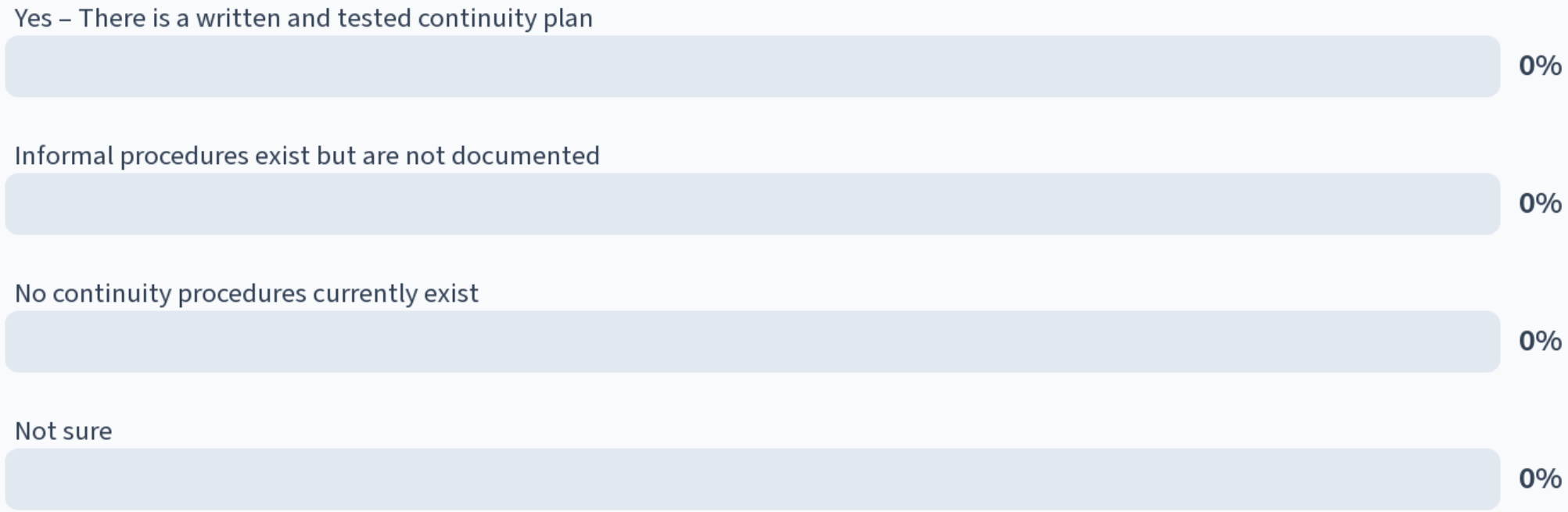
Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Who is responsible for communicating with students and faculty during a DDoS-related service outage?



Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Does your institution have documented academic continuity procedures for final exams disrupted by a cyberattack?



Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

Is there a documented protocol for escalating service outages to your ISP or cloud hosting provider during a DDoS attack?

Start the presentation to see live content. For screen share software, share the entire screen. Get help at **pollev.com/app**

LESSONS LEARNED

Continuity Planning Is Essential

- Universities must have redundant delivery methods and service-level objectives documented and tested.

DDoS Mitigation Must Be Proactive

- ISP-level filtering and rapid escalation paths with providers are essential to reduce downtime.

Internal Audit Value

- Auditors can help assess continuity planning and external coordination.

THANK YOU

P. Dimitris Bantileskas, CPA/CFF/CITP, CVA, CFE,
ISACA Cybersecurity Audit Certificate
Cybersecurity Audit Partner

Phone
P : 631.756.9500 x 211

Email
dbantileskas@ns.cpa

RESOURCES

- 31 Must-Know Education Cybersecurity Statistics - October 3, 2024: https://www.varonis.com/blog/education-cybersecurity-statistics

- The State of Higher Education Cybersecurity: Top Insights and Trends – August 18, 2025: https://www.bitlyft.com/resources/the-state-of-higher-education-cybersecurity-insights-trends

- The State of University Cybersecurity: 3 Major Problems in 2025 – July 7, 2025: https://www.upguard.com/blog/top-cybersecurity-problems-for-universities-colleges