SPOTLIGHT

Sponsored by: Proofpoint

Protecting sensitive and confidential data in higher education requires balancing security and collaboration. Focusing on the outside attacks that target users, as well as on user activity, provides valuable context to achieve this balance.

Reducing Data Loss and Insider Risks in Higher Education

May 2024

Written by: Jennifer Glenn, Research Director, Security and Trust

Introduction

Data is one of the most valuable assets in higher education. It provides the foundation for education but also comprises confidential research, personal details of students and staff, and financial information for students, alumni, and the athletic department. Often, the ability to easily access information in a university setting is vital to the free flow of ideas.

The amount of valuable information in higher education makes these institutions prime targets for data compromise and theft. Ransomware, phishing, and other attacks continue to hit organizations at a high rate and often result in data exfiltration. IDC's December 2023 *Future Enterprise Resiliency and Spending Survey, Wave 11,* revealed that almost a quarter (22%) of government/education respondents indicated that sensitive, confidential, or secret data had been exfiltrated (see Figure 1).

AT A GLANCE

WHAT'S IMPORTANT

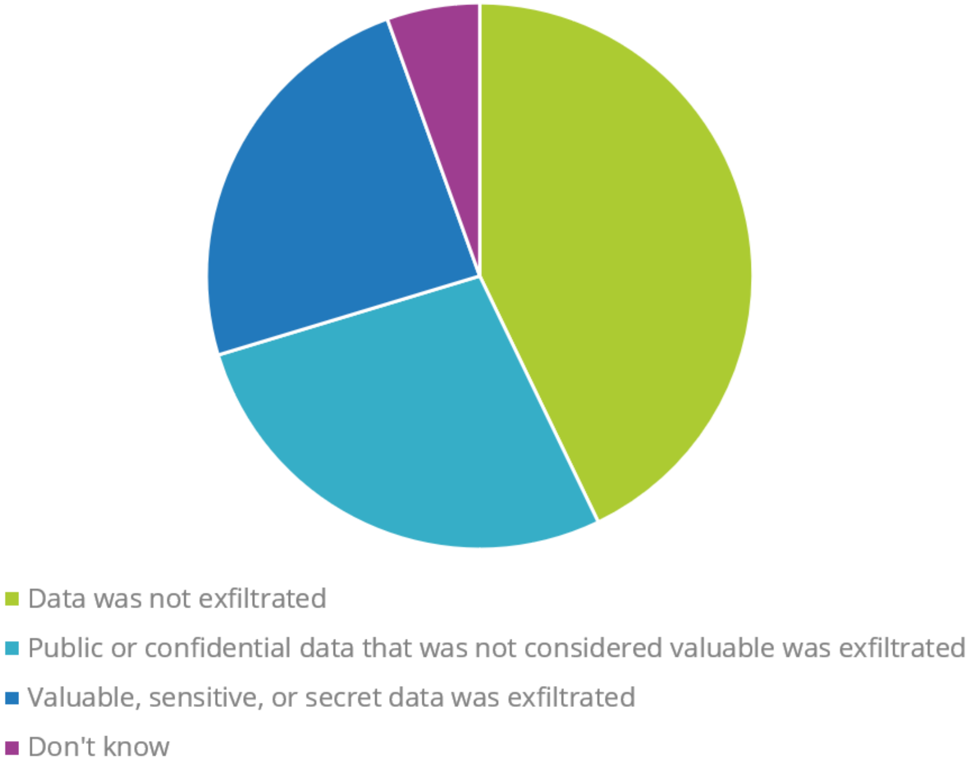
» Higher ed institutions are home to a significant amount of confidential and sensitive data, including research findings and financial information.

» Limited resources and the need to remain open and collaborative make it difficult to effectively secure data.

» Analyzing the users or departments that attackers are targeting helps to pinpoint where security efforts should be prioritized.

FIGURE 1: ***Government/Education Organizations Reporting Ransomware with Exfiltration***

Q ***For your most recent ransomware incident that blocked access to systems or data, which of the following occurred?***



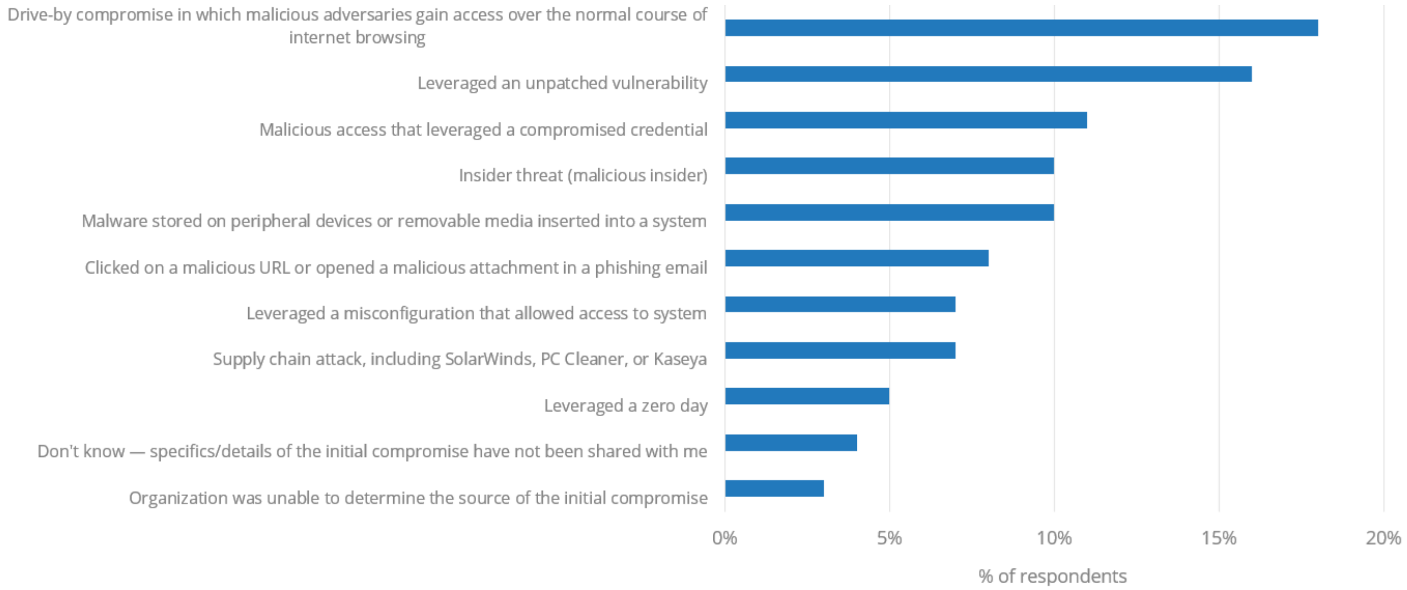
n = 550 (finance = 67, government/education = 58, health/life = 53, manufacturing = 67, retail = 58, utilities = 56, other = 191)

Source: IDC's Future Enterprise Resiliency and Spending Survey, Wave 11, December 2023

While external attacks receive a lot of attention and can create several issues, including exposing sensitive or confidential data to bad actors, they can also result in credential theft, which poses a challenge for insider risk management. According to IDC's December 2023 *Future Enterprise Spending and Resiliency Survey, Wave 11,* insider threats accounted for 10% of the initial compromise, while another 11% of respondents reported that during the initial compromise, attackers leveraged a compromised credential (see Figure 2).

FIGURE 2: *Government/Education Organizations Reporting Initial Compromise During a Ransomware Incident*

Q ***For your most recent ransomware incident that blocked access to systems or data, what was the most significant source of initial compromise?***



n = 550 (finance = 67, government/education = 58, health/life = 53, manufacturing = 67, retail = 58, utilities = 56, other = 191)

Source: IDC's Future Enterprise Resiliency and Spending Survey, Wave 11, December 2023

Insider risk is tremendously difficult to detect and even harder to enforce compliance around because insiders are typically trusted, and data access is conditional (e.g., the user may receive access to a set of data for a limited time or from an institution-managed resource [laptop] only).

There are three types of insider risks that organizations are concerned with:

- **Malicious insiders:** These are employees or contractors (trusted users) who are intentionally accessing data for nefarious purposes. They may be leaving the organization and looking to take corporate data, such as customer lists, with them or may simply have bad intentions.
- **Compromised users:** These are bad actors who have compromised the credentials of trusted users and are using those credentials to access and use data they shouldn't.
- **Negligent users:** These are trusted users with good intentions who make mistakes or bad decisions. For example, an employee may mistakenly send an email containing confidential data to the wrong person. It could also be someone who demonstrates risky behaviors, such as working from a personal laptop, for convenience or to save time.

Security Challenges for Higher Education

Digitized data has facilitated information sharing and project collaboration. However, information security professionals face many challenges in keeping this valuable information secure while promoting a collaborative environment:

- **Increase in volume of data:** With digital information being stored and shared so freely, the volume of data moving into, out of, and throughout the higher education ecosystem is vast and steadily growing. This creates a broader and more complex landscape to protect.
- **Diverse user base:** Higher education organizations are often highly distributed and have a diverse user base, including students, contractors, educators, financial institutions, and researchers. This increases the scope and number of policies created for data security and privacy.
- **Longtime employment and intra-organizational job moves:** Higher education employees may hold many roles. It's also common for them to switch departments or jobs during their employment at the organization. For example, a student may also be an athlete and have accounts in multiple systems. This student may also be employed by the institution through a work-study or research grant. They then may stay on in a staff capacity upon completing their studies. These switches can lead to an individual accruing excess privileges to applications or systems.
- **Limited budget:** Higher education organizations often have budget limitations, particularly for security initiatives. Cost constraints can challenge the implementation of the right policies, technology, and staff to keep valuable data safe.

User-Centric Data Security Balances Protection and Productivity for Higher Education

To effectively control sensitive and confidential data without hindering the flow of information, higher education organizations should rethink their approach to data security implementations. First, they should consider data security as programmatic — that is, a continuous process that requires frequent tuning, measurement, and readjusting to keep pace with the dynamic nature of digital information.

With this in mind, the next step is to focus on where the data is being used (i.e., with the user). Directing attention to users enables security practitioners to identify the information that malicious attackers and motivated insiders are targeting. Are they targeting the athletic department's financial information? Are they targeting interns in the research division, looking for soil sample data? From there, higher education teams can prioritize where to strengthen their data protection.

In addition to this prioritization exercise, there are several steps to reducing data risk in areas that are highly targeted by bad actors, including:

- **Minimizing at-risk data:** The first step is to limit the areas of exposure. Organizations should identify and classify sensitive data to prioritize what is necessary for business processes and applications, adhere to privacy and industry regulations, and then purge any stale, redundant, or irrelevant data.
- **Monitoring user behavior to identify risky activity:** Organizations need to monitor how employees and contractors are accessing and using sensitive data. Defining benign versus risky behavior provides a baseline for creating balanced policies that enforce security in areas where needed without being overly restrictive.

- **Using context for granular policies:** Analyzing user behavior can provide valuable information about the different types of risks associated with data loss. Seeing anomalous behavior can indicate a compromised account or a malicious employee. This is essential for implementing effective policies, enforcement measures, and training without hindering user performance.
- **Implementing data security technologies:** Data loss prevention (DLP) technologies can detect violations and enforce policy measures for the unacceptable use of information. These enforcement tools can be adjusted to protect the most valuable data from being lost to risky user behaviors, such as misdirected emails or inappropriate data sharing.
- **Training users in real time:** Implementing in-the-moment training by using documented activities and policy violations clarifies what is and is not acceptable.

Benefits of Using Human-Centric Security Tools to Manage Insider Risk

In a data-centric digital business, people are a tremendous risk to information security and privacy. By focusing security enforcement on user activity and behavior, organizations can fine-tune control over the most critical data without sacrificing the usability and value of that information. By looking at who attackers are targeting, as well as what those individuals are involved in or have access to, protection can be customized down to an individual user, based on risk. This allows for the free flow and use of data that higher education organizations want, while remaining confident in the security of their most important assets.

Implementing a sound data security strategy to manage insider risk offers a number of benefits to higher education:

- **Easier/faster adherence to compliance/privacy regulations:** Demonstrating compliance is often a time- and resource-intensive endeavor — luxuries that most education institutions do not have. By focusing efforts on high-risk users and data, organizations can simplify the process of not only securing sensitive data but also demonstrating its protection for compliance and/or privacy audits.
- **Flexible control for diverse populations:** Data security cannot involve a blanket approach, especially in organizations that have multiple types of users, such as in higher education. For these groups, a people- and risk-centric approach to data security offers the right level of control necessary to protect the organization's most sensitive/confidential information.
- **Improved security, privacy, and compliance:** Beyond stopping data from leaving the organization, on-the-spot notification and training for users can extend the effectiveness of security tools.

Considering Proofpoint

Founded in 2002, Proofpoint Inc. is a leading human-centric cybersecurity company serving more than 510,000 customers worldwide. On average, Proofpoint reports that it scans and analyzes 3.1 trillion emails, 21 trillion URLs, and 0.8 trillion attachments and monitors 45 million cloud accounts for takeover detection per year using advanced AI and ML. It uses these insights to improve its clients' security posture.

Proofpoint offers end-to-end email protection across the entire predelivery, click time, and postdelivery email attack chain. Its core email security packages include advanced AI-based predelivery detection and comprehensive protection powered by NexusAI, Proofpoint's proprietary AI engine built on trillions of data points, capable of stopping various payloadless social engineering threats like advanced email fraud and malicious links. In addition, Proofpoint offers adaptive email security with behavioral AI defense postdelivery to counter targeted threats like internal phishing, specifically for high-risk employees, with seamless API integration with Microsoft 365. Proofpoint organizes its product portfolio into four families: people protection, information protection, human risk mitigation, and premium services. Under people protection, the focus of this Spotlight, are the product packages shown in Figure 1. Each package builds on the company's Core P0/P1 solution and subsequently each other to provide comprehensive protection:

- **Core P0/P1 delivers essential email threat protection:** There are multiple modules within Core P0/P1. Targeted Attack Protection (TAP) detects, analyzes, and blocks advanced email threats involving social engineering such as BEC, phishing emails, malware and ransomware, and spam. Threat Response Auto-Pull works with TAP to protect users from incoming malicious emails. Closed-Loop Email Analysis and Response streamlines the evaluation of emails users report as potentially malicious to an abuse mailbox. People Risk Explorer analyzes and segments the risks that internal and external users pose to identify the users most likely to pose a threat.

- **Core Plus provides impersonation protection:** Impersonation targets can be internal employees or third parties such as customers and suppliers with whom employees would typically communicate but who may have been compromised or spoofed. Email Fraud Defense secures email channels, mitigates email fraud, provides visibility into fraud risks posted by external parties, and simplifies domain-based message authentication, reporting, and conformance (DMARC) authentication. Secure Email Relay protects application-generated email and supports the migration of on-premises email relays to the cloud. Supplier Threat Protection looks for suspicious emails from suppliers and third-party accounts to detect potential phishing, malware, and business email account compromise attacks. Analysis of patterns across Proofpoint's customer base enables alert notification before threat actors launch their email attacks.

- **Advanced offers adaptive email data loss protection:** Building off the capabilities of Core and Core Plus, the Advanced package uses behavioral AI to detect anomalies, prevent email from being delivered to the wrong recipient or the right recipient but with the incorrect email attachment, and detect data infiltration in real time. Email Data Loss Prevention detects sensitive or confidential data within an email so that it can be further tracked and safeguarded. Email Encryption automatically encrypts emails and attachments, thus ensuring more secure email communications. The Advanced package mitigates the risk of data loss at the hands of the careless, compromised, or malicious user.

- **Complete ensures identity protection:** There are two modules in the Complete package. Identity Threat Defense and Response continuously scans for identity threats to stop privilege escalation and lateral movements of threat actors to their ultimate target of extremely sensitive — and lucrative on the dark market — data assets. TAP Account Takeover identifies the diverse types of threats targeting email accounts, including business email compromise, brute-force attacks, and data exfiltration. It automates alerts for them and accelerates email threat investigation and account remediation.

Cloud Email Security Use Cases

Deployed together, Proofpoint's extensive offerings address the following use cases:

- **Increased prevalence of human social engineering:** Threat actors are taking advantage of AI to launch more sophisticated attacks involving human social engineering. They use GenAI to quickly generate phishing emails that mirror the targeted organization's communication style or translate effective phishing emails into other languages to attack targets in other countries. The Core P0/P1 package protects against BEC, ATO, credential theft, and financial fraud attacks.
- **Increased reliance on third-party vendors:** Healthcare organizations are leaning on third-party email services to send emails on their behalf for marketing campaigns, customer support, and other administrative workflows. The Core Plus package protects against vendor email compromise through its Supplier Threat Detection module.
- **Data loss:** Misdirected email by careless users is as much a problem as data exfiltration, if not more so, because users have logged in with legitimate credentials and may be misdirecting email to validated recipients (e.g., wrong customer or colleague). Proofpoint's inaugural edition of its *2024 Data Loss Landscape Report* (January 2024) revealed that more than 70% of respondents across industries identified "careless users" as a cause of their data loss, while fewer than 50% cited technical issues. The Advanced package offers protection against both forms of data loss.
- **Identity compromise:** Active Directory (AD) identities are a common target for theft. Once AD has been compromised, threat actors can use legitimate credentials to move laterally through the network or escalate privileges to gain access to more sensitive information. The Complete package offers identity threat defense and detection and identifies potential account takeover events.

Challenges

Data volume will only continue to grow, and the shift to more digital operations will make the spread of information easier. Organizations — particularly those in higher ed — will have to continue adjusting data security programs to accommodate new applications, formats, and initiatives. Trying to protect data from malicious insiders will be a constant challenge. Further, major market initiatives, such as generative AI, will make data security even harder to implement. Attackers will be capable of polishing their methods and techniques, making compromised credentials more of a concern. The creation of new AI models for business optimization will create an even bigger challenge for detecting anomalous users/attackers and controlling the flow of data.

The growing cybersecurity skills gap is likely to disproportionately affect higher education organizations, which may struggle with the budgets necessary to attract top talent.

The market for DLP and messaging security solutions is very crowded, and many vendors struggle to demonstrate high value, especially for organizations with limited budgets. Human-centric security offers clear benefits for protecting data

> Higher education institutions need to protect their valuable data assets by analyzing risks to users and monitoring users' activities to make intentional enforcement decisions that keep information secure without hindering collaboration.

within higher education. To the extent that Proofpoint can demonstrate how its solutions address the challenges identified in this paper, the company has ample opportunity for success.

Conclusion

IDC believes that incidents that compromise data will continue to grow in volume and frequency. These incidents — whether a result of trusted insiders' behavior or external factors such as ransomware — will be a significant source of risk for all organizations. Higher education institutions need to protect their valuable data assets by limiting the opportunities for malicious activity to occur. This includes analyzing risks to users and monitoring users' activities to make intentional enforcement decisions that secure information without hindering collaboration. Institutions must also educate and train users to recognize risky behavior to reduce future incidents.

About the Analyst

***Jennifer Glenn,** Research Director, Security and Trust*

Jennifer Glenn is research director for the IDC Security and Trust Group and responsible for the information and data security practice. Ms. Glenn's core coverage includes a broad range of technologies, such as messaging security, sensitive data management, encryption, tokenization, rights management, key management, and certificates.

MESSAGE FROM THE SPONSOR

About Proofpoint

Proofpoint, Inc. is a leading cybersecurity and compliance company that protects organizations' greatest assets and biggest risks: their people. With an integrated suite of cloud-based solutions, Proofpoint helps companies around the world stop targeted threats, safeguard their data, and make their users more resilient against cyber attacks. Leading organizations of all sizes, including more than half of the Fortune 1000, rely on Proofpoint for human-centric security and compliance solutions that mitigate their most critical risks across email, the cloud, social media, and the web.

More information is available at proofpoint.com.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
140 Kendrick Street
Building B
Needham, MA 02494, USA
T 508.872.8200
F 508.935.4015
Twitter @IDC
idc-insights-community.com
www.idc.com

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.