PULSE | IDENTITY AUTOMATION

HOW DO COLLEGES AND UNIVERSITIES PREVENT RANSOMWARE ATTACKS?

Educational institutions are frequent targets of ransomware attacks, with account takeovers being one of the largest causes. These attacks can cost institutions millions of dollars in downtime, people time, device cost, network cost, lost opportunity, and ransom paid. Plus, ransomware attacks put institutional data at risk and can cause the school to temporarily close.

Unfortunately, students and staff often re-use their institution password across dozens of other sites, platforms, and applications. If a data breach occurs at any of these entities, the college or university is now at risk. End users inadvertently become a threat vector, ultimately allowing malicious actors to perpetrate an account takeover and hold the institution hostage.

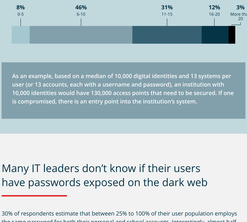
Pulse and Identity Automation surveyed 151 IT team leaders at Higher Education institutions to understand their:

- **Volume of access points**
- **Visibility into potentially compromised passwords**
- **Level of confidence that institution passwords are secure**

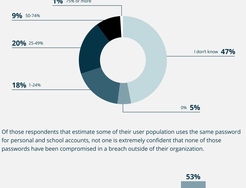
Data collection: August 12 - September 21, 2021 Respondents: 151 higher education IT and security decision-makers

50% of respondents have at least 10,000 digital identities and most users have 6+ accounts for applications

Half (50%) of respondents have at least 10,000 digital identities within their organization.



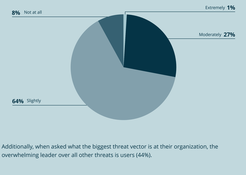
92% of respondents have 6 or more systems/applications associated with each user, and each of these accounts are access points that need to be secured.



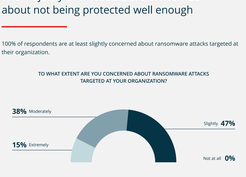
As an example, based on a median of 10,000 digital identities and 13 systems per user (or 13 accounts, each with a username and password), an institution with 10,000 identities would have 130,000 access points that need to be secured. If one is compromised, there is an entry point into the institution's system.

Many IT leaders don't know if their users have passwords exposed on the dark web

30% of respondents estimate that between 25% to 100% of their user population employs the same password for both their personal and school accounts. Interestingly, almost half (47%) of respondents don't have an estimate of what percentage of their user population uses the same password for both their personal and school accounts.

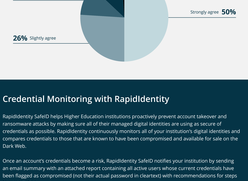


Of those respondents that estimate some of their user population uses the same password for personal and school accounts, not one is extremely confident that none of those passwords have been compromised in a breach outside of their organization.



A zero-trust security model safeguards institutions, yet 72% have not fully implemented one

Almost three-quarters (72%) of respondents have only slightly or not at all implemented a zero-trust security model.



Additionally, when asked what the biggest threat vector is at their organization, the overwhelming leader over all other threats is users (44%).

The majority of IT leaders are concerned about not being protected well enough

100% of respondents are at least slightly concerned about ransomware attacks targeted at their organization.

Despite being concerned about ransomware attacks at their organization, 76% of respondents agree that they have the appropriate funding and resources in place to effectively prevent ransomware attacks.

Credential Monitoring with RapidIdentity

RapidIdentity SafeID helps Higher Education institutions proactively prevent account takeover and ransomware attacks by making sure all of their managed digital identities are using as secure of credentials as possible. RapidIdentity continuously monitors all of your institution's digital identities and compares credentials to those that are known to have been compromised and available for sale on the Dark Web.

Once an account's credentials become a risk, RapidIdentity SafeID notifies your institution by sending an email summary with an attached report containing all active users whose current credentials have been flagged as compromised (not their actual password in cleartext) with recommendations for steps to remediation.

Even better, RapidIdentity can take it a step further to remove the threat by:

- immediately ending any active sessions,
- auto-enrolling the at-risk account in an MFA policy until the password is reset,
- auto-resetting the at-risk account's password,
- or even full-on disabling the account.

Download the eBook to learn more about how to build a foundation of automation and user security for your institution.

Respondent Breakdown

Insights powered by PULSE