Title: Their Risk is Our Risk

Subtitle: Bridging the Gap in Cybersecurity Through Shared Responsibility

Authors: Brian Kelly

Affiliation: Compass IT Compliance, LLC

Date: April 2024

The Scholarly Networks Security Initiative (SNSI) sought to identify the threats to higher education institutions and develop recommendations to protect the integrity of scientific records, scholarly systems, and the personal data of users. To achieve this, Compass IT Compliance collaborated with SNSI to produce a relevant case study.

This study adopts a mixed-methods approach to thoroughly explore the cybersecurity challenges and solutions in higher education, combining both qualitative and quantitative data for a comprehensive analysis. The methodology includes a literature review of academic and industry sources to build a theoretical base and identify knowledge gaps, along with semi-structured interviews with a wide range of international stakeholders such as CISOs, IT professionals, and students to capture diverse experiences and assess the effectiveness of current security measures. Case studies of specific cybersecurity incidents further provide practical insights. Data sources are varied, encompassing interviews with cybersecurity experts and users, academic papers with empirical studies on credential theft, and industry reports from bodies like the FBI and SNSI, highlighting the broader national and intellectual property risks associated with stolen academic credentials.

EXECUTIVE SUMMARY

Our interconnected campuses are not just a convenience but a cornerstone of higher education globally, cybersecurity risk extends beyond the confines of individual institutional concerns to become a shared responsibility. "Their Risk is Our Risk" is both a paradigm shift and a talking point for Chief Information Security Officers (CISO), especially within the higher education sector, where the often-casual use of college-issued identities (user IDs and email addresses) by students, faculty, and staff has opened floodgates to unprecedented risks. This paper delves into the intricate web of cybersecurity challenges that higher education institutions face, exploring the multifaceted nature of these risks and implications, the collaborative efforts undertaken to mitigate them, and the outcomes of such initiatives.

The evolution of cybersecurity threats has necessitated a departure from the traditional view of these risks as solely an IT department's concern. Today, an attack beginning with one compromised user can ripple through the institution impacting both the academic and research community, disrupting educational processes, compromising sensitive data, and eroding public trust. Acknowledging this, our study explores how cybersecurity is a collective issue that demands the active participation of all campus stakeholders across the higher education community.

Through an examination of shared risks and the best practices employed to counter them, this paper sheds light on the significance of fostering a culture of cybersecurity awareness. It underscores the implementation

of strategic solutions such as enhanced identity and access management protocols, multi-factor authentication, and comprehensive cybersecurity education programs. The outcomes highlighted in this study underscore the transformative power of collective action in creating a secure and resilient environment conducive to the pursuit of knowledge and innovation.

We intend for the paper to chart the course serving as a beacon, and guiding the higher education community toward a future where cybersecurity is not seen as a hurdle but as a shared responsibility that enables and safeguards the integrity of higher education in the digital age.

INTRODUCTION

BACKGROUND INFORMATION

The digital transformation[1] has empowered higher education with unparalleled opportunities for learning, research, and collaboration. However, this boon is not without its bane - the escalating threat of shared cybersecurity risks. The advent of sophisticated cyber-attacks and the increasing reliance on digital platforms for collaborative educational activities have ushered in a new era where cybersecurity is a persistent concern. We have looked at cybersecurity challenges within the higher education sector, drawing upon recent industry trends, statistics, and the collective shift towards recognizing these risks and their impacts as a communal impact rather than isolated incidents.

PROBLEM STATEMENT

At the heart of the cybersecurity conundrum in higher education lies a paradox - the core principles of academic freedom and the open exchange of information have led to the relaxed use of institution-issued identities by the very users we seek to empower. The implication of this casual attitude towards identities, encompassing user IDs and email addresses, not only exposes individuals to identity theft but also jeopardizes the integrity of academic institutions at large. The proliferation of credential theft, facilitated by phishing scams, malware attacks, and data breaches, poses a formidable challenge, threatening not just the financial and legal standing of institutions but also their reputational and the trust of their stakeholders.

Expanding on this, the theft and misuse of Institutional credentials extend beyond immediate financial losses, beginning a cascade of adverse effects that span the degradation of research integrity, the compromise of personal privacy, and the potential manipulation of academic publishing. The complexity of the impact is how stolen credentials serve as a lucrative commodity within the dark web, and the multifarious ways in which they undermine the academic and research endeavors of higher education institutions.

By framing the problem within the broader context of shared risk, impact and responsibility, this paper analyzes the strategies, solutions, and collaborative initiatives that aim to help us navigate the often-daunting cybersecurity challenge into a shared success story in the subsequent sections.

[1] i https://www.educause.edu/focus-areas-and-initiatives/digital-transformation

METHODOLOGY

RESEARCH METHODS

This study employs a mixed-methods research approach to comprehensively understand the cybersecurity challenges and solutions within higher education. By integrating qualitative data, we aim to provide a holistic view of the cybersecurity landscape, focusing on the risks associated with the carefree use of institution-issued digital identities and the strategies implemented to mitigate these risks. The research methodology encompasses:

- **Literature Review:** An review of existing academic literature, industry reports, and cybersecurity frameworks to establish a theoretical foundation and identify gaps in current knowledge.
- **Interviews:** Conduct semi-structured interviews with a diverse group of international stakeholders, including CISOs, IT professionals, faculty members, and students across several higher education institutions. These interviews aim to gather insights into personal experiences, perceived risks, and the effectiveness of implemented cybersecurity measures.
- **Case Studies:** Analyzing specific instances of cybersecurity breaches or successful implementation of security measures to draw practical insights and understand the real-world impact of various strategies.

DATA SOURCES

The data for this study was collected from a variety of sources to ensure a comprehensive analysis:

- **Interviews with Cybersecurity Experts:** Insights from CISOs in higher education and other organizations specializing in cybersecurity within academia.
- **Interviews with users:** Perspectives from student and faculty users
- **Academic Papers:** Key studies such as "Stolen Account Credentials: An Empirical Comparison of Online Dissemination on Different Platforms" by Madarie et al. (2019), and "Data breaches, phishing, or malware? Understanding the risks of stolen credentials" by Thomas et al. (2017), which provides empirical evidence and analysis of credential theft and its implications.
- **Industry Reports:** Including alerts and advisories from the Federal Bureau of Investigation (FBI) and the Scholarly Networks Security Initiative (SNSI) regarding stolen academic credentials found online, offering a perspective on the broader implications for national security and intellectual property.

LIMITATIONS

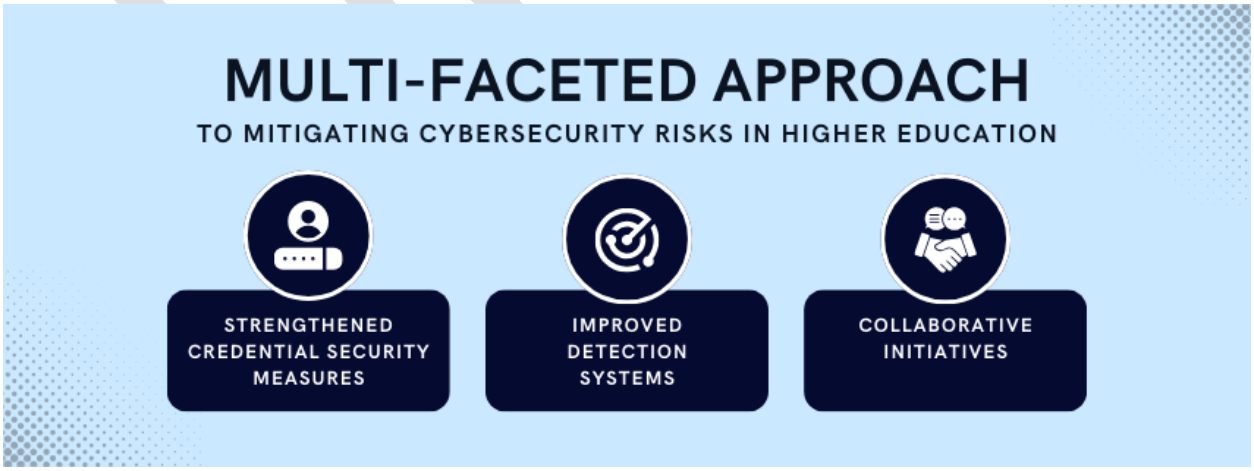
This research acknowledges several limitations, including the potential for bias in self-reported data from interviews and surveys, the rapidly evolving nature of cybersecurity threats which may outpace our analysis, which may limit the generalizability of findings to other regions or sectors.

ANALYSIS & FINDINGS

DRAFT

Our analysis reveals a multi-faceted approach to mitigating cybersecurity risks and their impacts to higher education, emphasizing the importance of shared responsibility across all stakeholders. Solutions implemented include:

- **Strengthened Credential Security Measures:** Use of multi-factor authentication (MFA) is a two-way street and should be required by institutions, publishers and applications, modern password policies (to include/promote Password Manager use), and regular information security awareness education for students, faculty, and staff.
- **Improved Detection Systems:** Deployment of advanced monitoring and anomaly detection tools to identify suspicious activities, such as unusual login attempts or access patterns, which could indicate compromised credentials. Websites such as HaveIBeenPwned.com were created to allow individuals to check if their personal data has been compromised by data breaches. Users can enter their email addresses or phone numbers to search against a database of known breaches.
- **Collaborative Initiatives:** Establishing partnerships between universities, publishers, and research institutions to share best practices, develop common security standards, and foster a culture of transparency and cooperation in addressing cybersecurity challenges. Entities supporting these collaborative partnerships include:
    - EDUCAUSE - A nonprofit association dedicated to pioneering the strategic application of technology and data to enhance the potential of higher education.
    - Research & Education Networks Information Sharing & Analysis Center (REN-ISAC) - Enhances cybersecurity for over 700 higher education and research institutions through protective measures, responses, threat intelligence from the Security Event System (SES), data-sharing tools, and peer assessments to elevate overall security awareness and posture.
    - Scholarly Networks Security Initiative (SNSI) - Unites publishers and institutions to address cyber-threats that compromise the scientific record, scholarly systems, and the security of personal data.



Based on the insights garnered from this research, we recommend the following strategies for higher education institutions seeking to enhance their cybersecurity posture:

- **Foster a Culture of Cybersecurity Awareness:** Regularly conduct sessions and awareness campaigns to keep all campus stakeholders informed about the latest cybersecurity threats and their support roles and best practices to mitigate those threats.
- **Strengthen Identity and Access Management (IAM) Practices:** Implement multi-factor authentication (MFA) and Single-Sign-On (SSO) access controls to protect against unauthorized access/use of institutional credentials. Services like SeamlessAccess aim to simplify online access to scholarly collaboration tools, information resources, and shared research infrastructure by promoting digital authentication using single-sign-on capabilities from a user's home institution, all while safeguarding personal data and privacy.
- **Enhance Collaboration:** Continue to build partnerships with other institutions, government agencies, and cybersecurity organizations to share resources, intelligence, and best practices.
- **Invest in Advanced Detection Tools:** Deploy state-of-the-art cybersecurity technologies that can identify and mitigate threats before they result in significant damage.
- **Promote Research on Cybersecurity in Higher Education:** Encourage academic research aimed at exploring new threats and developing innovative solutions to enhance cybersecurity in the academic sector.

IMPLEMENTATION PROCESS

The implementation of these solutions faced various challenges, including resistance to change among users accustomed to less stringent security measures, the logistical complexities of coordinating across diverse institutional systems, and the need for continuous adaptation to emerging threats. However, through an approach that prioritizes user education and engagement, institutions were able to collaboratively change their cybersecurity culture.

> *"**Mitigating risks from stolen or misused credentials demands a proactive approach:** Limit credential usage, enhance surveillance, and regularly update access protocols. By strategically managing permissions and monitoring account activity, we protect our organizational integrity and maintain trust. I urge my peers to adopt similar measures—shorten credential lifespans, align access rights tightly with resource needs, and keep a vigilant eye on all usage anomalies."*
>
> **CISO of a Chinese University**

DISCUSSION & INTERPRETATION

SIGNIFICANCE OF FINDINGS

The findings from this study illuminate the critical nature of shared responsibility in cybersecurity within higher education. By transitioning from a perspective that views cybersecurity risks as isolated IT issues to a holistic view that encompasses the entire academic community, institutions can significantly bolster their defense against cyber threats. This paradigm shift not only enhances the security of digital identities but also fosters an environment where education and research can thrive free from the disruptions of cyber-attacks.

The collaborative initiatives identified in this study underscore the power of the community in addressing cybersecurity challenges. These efforts not only mitigate the immediate risks associated with credential theft and cyber-attacks but also contribute to a culture of cybersecurity awareness and vigilance that extends beyond the boundaries of individual institutions.

RELATION TO EXISTING RESEARCH AND THEORY

Our analysis aligns with and expands upon existing research that emphasizes the importance of community engagement and shared responsibility in cybersecurity. The findings support theories in social and organizational psychology that stress the role of collective action and shared norms in overcoming communal challenges. By applying these theories within the context of higher education cybersecurity, this study contributes to a deeper understanding of how collaborative efforts can effectively address complex, systemic issues.

LINK TO PROBLEM STATEMENT

The combination of implementing multi-faceted cybersecurity measures and the emphasis on shared responsibility can directly address the carefree use of institution-issued digital identities by higher education users. The positive outcomes observed in this study - including reduced instances of credential theft, enhanced detection of suspicious activities, and improved security awareness among stakeholders - demonstrate a significant step forward in mitigating the risks posed by this carefree attitude.

CONCLUSION & RECOMMENDATIONS

SUMMARY OF KEY FINDINGS

This study highlights the transformative impact of adopting a shared responsibility model for cybersecurity in higher education. Through collaborative efforts, strengthened security measures, and a collective shift in attitudes toward digital identity protection, institutions can effectively reduce their vulnerability to cyber

threats. The key findings underscore the importance of community engagement, the implementation of robust security protocols, and the cultivation of a pervasive cybersecurity culture.

CONCLUDING REMARKS

To summarize, the phrase "Their Risk is Our Risk" aptly captures the intertwined risks of cybersecurity in higher education and signals a clear call for collaboration and communication. The urgency of this challenge demands a concerted response from all departments of the academic community: from Chief Information Officers and Chief Information Security Officers, to librarians, students, faculty, and staff. By raising awareness of the need for a unified model of shared responsibility and proactive cooperation, we can fortify and unify our defenses against these advancing threats. This collective effort is crucial in preserving the integrity of our educational and research environments, ensuring they remain resilient and secure against disruptions caused by cyberattacks. In this way, we not only protect individual stakeholders, but also uphold the broader educational mission against the ever-evolving landscape of cyber risks.

DRAFT

RESOURCES

- https://moldstud.com/articles/p-the-art-of-cyber-security-communication-engaging-with-university-stakeholders
  - The Art of Cyber Security Communication: Engaging with University Stakeholders
- https://rems.ed.gov/Cyber?AspxAutoDetectCookieSupport=1
  - CYBERSECURITY PREPAREDNESS FOR K-12 SCHOOLS AND INSTITUTIONS OF HIGHER EDUCATION
- https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2022-06-28/fbi-alert-about-login-credentials-us-education-institutions-found-compromised-dark-web
  - (GENERAL-22-38) FBI ALERT about Login Credentials from US Education Institutions Found Compromised on Dark Web
- https://edtechmagazine.com/higher/article/2022/07/fbi-issues-new-alert-about-stolen-academic-credentials-found-online
  - FBI Issues New Alert About Stolen Academic Credentials Found Online
- https://www.researchgate.net/publication/337892534_Stolen_account_credentials_an_empirical_comparison_of_online_dissemination_on_different_platforms
  - Stolen account credentials: an empirical comparison of online dissemination on different platforms
- https://www.academia.edu/59406647/Data_Breaches_Phishing_or_Malware
  - Data Breaches, Phishing, or Malware?
- https://www.sciencedirect.com/science/article/pii/S157401372300059X
  - A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises
- https://oertx.highered.texas.gov/courseware/lesson/4779/student/?section=10
  - Mastering Cybersecurity Policy: Analysis and Implementation
- https://www.forbes.com/sites/forbestechcouncil/2023/09/12/the-cybersecurity-risks-in-education-cannot-be-ignored/?sh=7cb480474566
  - The Cybersecurity Risks In Education Cannot Be Ignored
- https://www.ey.com/en_us/insights/consulting/why-cybersecurity-should-be-required-reading-for-higher-education
  - Why cybersecurity should be required reading for higher education
- https://www.upguard.com/blog/top-cybersecurity-problems-for-universities-colleges
  - The State of University Cybersecurity: 3 Major Problems in 2024

DRAFT