Shadow IT in Higher Education: Survey and Case Study for Cybersecurity

Selma Gomez Orr,[1] Cyrus Jian Bonyadi,[1] Enis Golaszewski,[1]
Alan T. Sherman,[1] Peter A. H. Peterson,[2] Richard Forno,[1]
Sydney Johns,[1] Jimmy Rodriguez[1]

[1] Cyber Defense Lab, University of Maryland, Baltimore County (UMBC), Baltimore, MD 21250, {sorr1,sherman}@umbc.edu, www.csee.umbc.edu/people/faculty/alan-t-sherman/
[2] Department of Computer Science, University of Minnesota Duluth, Duluth, MN 55812, pahp@d.umn.edu, www.d.umn.edu/~pahp/

Abstract. We explore shadow *information technology (IT)* at institutions of higher education through a two-tiered approach involving a detailed case study and comprehensive survey of IT professionals. In its many forms, *shadow IT* is the software or hardware present in a computer system or network that lies outside the typical review process of the responsible IT unit. We carry out a case study of an internally built legacy grants management system at the University of Maryland, Baltimore County that exemplifies the vulnerabilities, including cross-site scripting and SQL injection, typical of such unauthorized and ad-hoc software. We also conduct a survey of IT professionals at universities, colleges, and community colleges that reveals new and actionable information regarding the prevalence, usage patterns, types, benefits, and risks of shadow IT at their respective institutions.

Further, we propose a security-based profile of shadow IT, involving a subset of elements from existing shadow IT taxonomies, which categorizes shadow IT from a security perspective. Based on this profile, survey respondents identified the predominant form of shadow IT at their institutions, revealing close similarities to findings from our case study.

Through this work, we are the first to identify possible susceptibility factors associated with the occurrence of shadow IT related security incidents within academic institutions. Correlations of significance include the presence of certain graduate schools, the level of decentralization of the IT department, the types of shadow IT present, the percentage of security violations related to shadow IT, and the institution's overall attitude toward shadow IT. The combined elements of our case study, profile, and survey provide the first multifaceted view of shadow IT security at academic institutions, highlighting tension between its risks and benefits, and suggesting strategies for managing it successfully.

Keywords: case study · computer security · cybersecurity · DoD Cybersecurity Scholarship Program (CySP) · NSF Scholarship for Service (SFS) program · project-based learning · Shadow IT in higher education · software security · Sponsored Award Management System (SAMS) · survey of IT professionals

1 Introduction

In 2014, the Office for Civil Rights at the U.S. Department of Health and Human Services fined New York Presbyterian Hospital and Columbia University 4.8 million dollars for HIPAA violations resulting from *shadow IT*. A doctor and software developer from Columbia University placed patient data on an unauthorized server on the hospital's network. Deactivation of the server exposed personal health information for about 6,800 patients. Columbia's share of the fine was 1.5 million dollars [28].

Many computer networks include applications, system software, or hardware that is unauthorized by or outside the typical review process of the authority responsible for the network. Such shadow IT can also create potential vulnerabilities and risks involving unauthorized access, loss of data and services, and leaks of confidential information, as in the above case. People often introduce shadow IT to provide a useful functionality that does not otherwise exist, or because official channels are slow and difficult to work through. Shadow IT, however, often creates serious problems by circumventing sound security and maintenance protocols, diminishing privacy, hampering backup mechanisms, and operating outside of the awareness or control of authorized managers. Symantec's [42] study of shadow IT in the private sector surveyed 3,000 IT managers across 23 countries and found that 25 percent of those questioned knew that accounts were compromised due to shadow IT.

In comparison with managing computer networks in the private sector, managing computer networks in higher education presents several unique and daunting challenges. Institutions of higher learning serve as repositories for one of the most diverse portfolios of data, including intellectual property from research, private and financial information about donors, applicants, students, and employees, as well as medical information about students and staff. In addition, computer networks in higher education are open access and serve a large, heterogeneous, and highly collaborative population. Academic environments likely include many users with the knowledge, motivation and financial resources—available through independent research grants—to create and install shadow IT, as well as the self-sufficient and individualistic mindset to help it flourish.

Academic environments not only include several factors that facilitate the introduction of shadow IT, they also benefit from the expeditious way it satisfies an unmet IT need. Consequently, finding ways to manage shadow IT successfully rather than completely eliminating it at institutions of higher learning might serve as a practical approach for many. We argue that shadow IT at academic institutions includes specific trends and patterns related to its form, usage, and security risks that IT practitioners can incorporate to guide their efforts allocating limited resources for managing shadow IT successfully.

In this paper, we explore such shadow IT in higher education through a detailed case study and a survey of IT professionals at academic institutions. Specifically, we analyze the *Sponsored Award Management System (SAMS)*, developed circa 2010 by a team within the Chemistry Department at the *University of Maryland, Baltimore County (UMBC)* to provide functionality, not

available elsewhere, for managing research grants. By conducting a detailed security review of SAMS that identifies the substantial vulnerabilities created by the unauthorized and ad-hoc form in which it was developed, our study provides a concrete reminder of the security risks posed by shadow IT, despite the benefits and useful role it may serve. Because SAMS represents a type of shadow IT likely common within institutions of higher learning, the specific security vulnerabilities identified, especially with respect to data integrity and privacy issues, provide useful insights.

A review of SAMS' development also highlights how the involvement of UMBC's *Division of IT (DoIT)*, even after the many years of SAMS' existence outside their purview, provided meaningful benefits. These benefits include basic safeguards, and later, our detailed assessment and resulting patching of vulnerabilities. Our case study, specific to the context of an academic institution, makes a new contribution in furthering the understanding of the security risks associated with shadow IT within institutions of higher learning.

Our analysis of SAMS prompted questions regarding the form, risk, and prevalence of shadow IT within institutions of higher learning in general. To explore these broader questions, the team developed and conducted a survey of IT professionals at academic institutions. Survey results reveal connections, not previously documented in the literature, between several institutional characteristics and the occurrence of shadow IT related security incidents. Specifically, statistical analysis demonstrate significant correlations between those academic institutions experiencing an incident and the presence of a medical, engineering, or architecture school; a decentralized IT departmental structure; specific types of shadow IT, such as legacy systems; high proportions of security violations related to shadow IT; and the level of control in an institution's approach to shadow IT. Understanding how these characteristics correlate with security incidents facilitates the development of targeted preventative strategies that optimize the often limited IT resources at academic institutions. We suggest several approaches based on these findings.

In addition to reporting on these possible connections to security incidents, this study is also the first to provide a survey-based, detailed view of shadow IT at academic institutions, including a description of shadow IT along the dimensions of users, types, locations, reasons for use, impact, approach, and successful remediation strategies. In illuminating the nature of shadow IT at academic institutions and highlighting factors that potentially increase the susceptibility to a shadow IT related security incident, this study hopes to raise awareness of the potential security vulnerabilities and serves as a possible guide for developing an institutional shadow IT risk assessment, facilitating the prioritization of limited resources, and improving the efficacy of intervention strategies for dealing with security risks associated with shadow IT at academic institutions.

Drawing from existing taxonomies on shadow IT, we propose a *security profile* based on four dimensions: the source, authority, modality, and motivation for the introduction of the shadow IT into a network. We further divide each of the four dimensions into types that can provide insight into possible security implications

for a particular example of shadow IT. By asking survey respondents to rate these various components for shadow IT at their schools, we document the relative prevalence of these profile elements in the field and discuss ramifications to security.

Following initial background material on shadow IT, we present an overview of the SAMS case study with a detailed discussion available in Appendix B. Results from this analysis motivated the survey development and a complete version of the survey instrument appears in Appendix C. Based on survey findings, we discuss recommendations for managing shadow IT and identify specific vulnerability factors. A presentation of the proposed security profile for shadow IT at academic institutions concludes with a description of the resulting categorization of shadow IT by survey respondents. An interview with Jack Suess, Vice President of Information Technology at UMBC, provides additional insights by highlighting his reflections on the survey findings and the security profile, based on his many years of experience heading an IT department at an academic institution.

Our contributions include: (1) A detailed case study of the SAMS shadow IT grant management program at UMBC, focusing on its security implications. (2) Results and analysis of a survey on shadow IT filled out by a sample of 53 IT professionals at universities, colleges, and community colleges. (3) Identification of factors correlated with the occurrence of shadow IT related security incidents. (4) A comprehensive view of shadow IT at academic institutions, including users and types, that can help institutions develop sound policies and practices for dealing with shadow IT. (5) A security profile of shadow IT useful for classifying the types of shadow IT and possible associated risk factors in higher education.

2 Background on Shadow IT

IT departments can be seen as an obstacle to success, because the formal IT processes, policies, or the solutions provided through them, may be seen as too slow, expensive, restrictive, or may result in a solution not preferred by users [46]. Because of the resulting unmet need, employees with the means often choose to implement, purchase, or keep unofficial IT solutions to supplement or replace official solutions—that is, shadow IT [23, 27]. In a 2014 investigation by Silic and Back [37] at a Fortune 500 company, approximately 60% of the employees used shadow IT systems to facilitate business operations. A 2017 study by the same authors found that deterrence measures had little effect, likely because employees felt that the benefits outweighed the risks.

Shadow IT can be a simple Excel spreadsheet [31] or a sophisticated application integrated with official systems [3]. Shadow IT can exist on organization-owned hardware, personal devices [12], or cloud services [23]. For example, in a 2012 survey commissioned by Symantec [42], 83% of respondents at enterprise organizations had found unsanctioned use of cloud resources (e.g., applications or storage) for business purposes, similar to findings by Kopper and Westner [23].

Research shows that shadow IT can successfully yield benefits that may be unavailable through formal IT channels, even though most employees recognize that it is against business policy [8, 42, 46]. Shadow IT solutions can allow people to innovate in ways that may not otherwise be possible, such as with a custom-built application or one purchased from an unapproved vendor. Shadow IT provides more flexibility and agility than do formal channels, allowing users to purchase and install software the same day a need is recognized. Shadow IT can also improve efficiency or productivity through scripted automation, apps, or use of personal smartphones [46]. Additionally, shadow IT sometimes occurs because users keep previously official solutions that are no longer authorized or supported. While circumventing the formal IT process can provide benefits, they often come at a cost

Classic objections to shadow IT include duplication of data, compliance issues (e.g., HIPAA [6, 28]), lack of proper back-ups, and wasted organizational resources. In addition, there are many security-relevant risks of shadow IT, and they mirror those of unmanaged IT [8]. Shadow IT may be inadequately vetted due to the adopter's lack of experience or knowledge of sound security practices. Shadow IT systems are also often inadequately maintained, leading to vulnerabilities that may be exploited, resulting in critical system failures or security incidents. Shadow IT systems are sometimes poorly documented, leading to avoidable failures [27]. Sensitive data (e.g., personal identifying information or intellectual property) may be stored in unsanctioned or externally-controlled locations and inadvertently exposed [28, 42, 46]. Similarly, shadow IT can prevent capture of critical data when backups do not "know" about the shadow IT systems [23]. Due to these and other risks, and the projected increases in shadow IT [38], Gartner [30] predicted: "By 2020, a third of successful attacks experienced by enterprises will be on their shadow IT resources."

3 Previous and Related Work on Shadow IT

Our work is the first multidimensional study of shadow IT security in higher education, including a case study, survey, and security profile. We now briefly review the previous shadow IT literature.

3.1 Shadow IT in General

Shadow IT systems [13,27,46]—sometimes called feral systems, shadow systems, workarounds, rogue systems, or other names [23, 26]—likely have been with us since computers appeared on employee desks. The study of shadow IT, however, began only around the turn of the millennium, when organizations developed strong centralized IT departments working to manage and unify the computing environment. For example, a common backdrop for shadow IT research is the deployment of *Enterprise Resource Planning (ERP)* systems meant to integrate core computational tasks and deal with unauthorized systems users often

create [3, 4, 15, 18, 25]. While early works on shadow IT tend to focus on business or economic drawbacks (e.g., waste, duplication or risk of loss [3]), later works consider risks specific to computer security (e.g., vulnerabilities, insider threat) [12, 42, 46].

A large amount of the shadow IT literature describes shadow IT through organizational, information management, or business-centered paradigms. From these perspectives, studies report on why shadow IT arises [15,18,43], what forms it takes [24, 32], how to discourage [38] or control it [33], its social effect on the organization [3], how it fails [10, 18], and other facets [1, 4, 5, 9, 37]. Most works explicitly recognize that shadow IT can have benefits [3, 8], and some discuss ways to keep its benefits while mitigating its risks, such as through *Bring Your Own Device (BYOD)* or *App (BYOA)*, or similar policies [12, 13, 46].

3.2 Shadow IT Case Studies, Surveys, and Interviews Outside of Academe

Shadow IT papers are typically based on case studies, surveys, interviews, or meta-reviews. Case studies are extremely common, because they describe real shadow IT systems in context [3, 4, 8, 9, 14–16, 18, 19, 37, 39, 47]. Surveys are also a common source of information (either new or synthesized), where researchers asked individuals in an organization or in a community questions about their beliefs or knowledge about shadow IT [12, 37, 38, 46]. Some surveys were conducted by or for commercial purposes (e.g., [29, 42]). Interviews are also a common source of information, particularly to supplement a case study with first-hand facts or opinions [16, 22, 39, 47]. Documentation surrounding a shadow IT system is sometimes used when available [3, 4, 16, 18]. Finally, some shadow IT literature is based on a meta-review of existing literature, to summarize the field or synthesize new ideas [20, 21, 23, 24, 26, 27].

3.3 Shadow IT in Academe

Some of the earliest shadow IT papers use case studies and interviews to investigate shadow IT systems arising in response to ERP implementations in Academe. In 2004, Jones et al. [18] studied the rise and fall of a shadow IT system at the Central Queensland University (CQU) resulting from shortcomings of CQU's PeopleSoft ERP system. Around the same time, Behrens and Sadera [4] investigated CQU's of several shadow IT systems related to faculty consulting funds, reporting services, and enrollment data. In 2009, Behrens [3] revisited CQU's continued use of *Webfuse*, the shadow IT software from 2004, concluding that such a system can be beneficial and even desirable. While these works are situated in Academe, they—like other early shadow IT research—do not investigate the security risks of shadow IT, instead focusing on organizational issues, the discussion of whether shadow IT is good or bad, and classic early objections to shadow IT. One early objection is the "hit by a bus" scenario—that is, concern about a shadow IT system becoming essential but then disappearing

without warning—or related control and planning concerns from the IT department. In contrast, our work focuses specifically on the security risks of shadow IT in Academe and includes both a detailed security analysis of a particular example of shadow IT and a broader institutional view based on a survey.

3.4 Categorizing and Evaluating Shadow IT

A number of works have proposed ways to categorize shadow IT systems. Urus, Molla, and Teoh [45] created a taxonomy to organize shadow IT systems arising following an ERP deployment. Huber, Zimmerman, Rentrop, and Felden [16] developed a system to categorize shadow IT based on its dependence to a local ERP system. Furstenau, Sandner, and Anaploitis [10] organized shadow IT systems into various categories based on function and scope as part of their paper investigating why shadow IT systems fail. Lund-Jensen et al. [26] analyzed the way the terms "workarounds," "feral information systems," and "shadow systems" have been used in the literature, and classified examples along two dimensions: the extent to which a system was a process vs. a technology and whether the lifespan of the system was short term vs. long term. Rentrop and Zimmerman [32] proposed an evaluation model to determine whether or not Shadow IT should be allowed in an organization. Our security profile can be used independently or as a component of the latter method, to help understand whether the rewards of the shadow IT system outweigh its security risks.

Our security profile in Section 6 is most closely related to the 2016 work of Kopper and Westner [24]. They define a general usage taxonomy addressing 21 terms used for shadow IT and conceptualizing the roles of "... Feral Practices, Workarounds, Shadow IT, Shadow Systems, Un-enacted Projects, and Shadow Sourcing."

4 Case Study: Overview

At the request of UMBC's DoIT, a team of UMBC NSF *Scholarship for Service (SFS)* and DoD *Cybersecurity Scholarship Program (CySP)* scholars analyzed the *Sponsored Award Management System (SAMS)*, a shadow IT application built about ten years ago by the UMBC Chemistry Department to provide detailed up-to-date financial management of grants. Developed as a custom application using Microsoft Access, SAMS offered useful functionality not available elsewhere. Built without the input of UMBC's DoIT or any security guidance, SAMS represents a classic example of shadow IT. It solved important local issues, allowing the department to function more efficiently but also unwittingly exposed the department and university to potential security issues. Exploiting SAMS interfaces with other financial systems, the team identified security weaknesses in SAMS that could lead to leaks of sensitive information or unauthorized changes to the department or university budgets.

Several years after the creation of SAMS, DoIT took control of the system and began implementing a series of improvements. Notably, DoIT ported SAMS

to systems under their control, incorporated SAMS into the university's *single sign-on (SSO)* system, and in 2014, produced a web front-end for users. In spite of DoIT's improvements, a number of security issues remained. DoIT's infrastructure team did not actively maintain SAMS; the staff member in charge of patching SAMS' components retired without a replacement; and the web front-end never received a code or security review. Responding to an increasing number of researchers outside the Chemistry Department requesting access to use the system, DoIT reached out to UMBC's SFS and CySP scholars to analyze the system's security and answer questions about SAMS' long-term viability and security risks.

SFS and CySP scholars analyzed the sourcecode, and running an instance of SAMS in a sandboxed environment, focused on the observable security of the SAMS software stack. The scholars did not use social engineering or explore zero-day vulnerabilities. They found many security issues, including SQL injection and cross-site scripting attacks, server misconfiguration, and a lack of critical security updates. These vulnerabilities could be leveraged alone or together to modify SAMS' data or steal credentials or other information.

Due to its development as a form of shadow IT, outside the control and management of DoIT, SAMS lacked basic and critical security features. Without input validation and sanitization, no controls existed to verify input for correct type or to prevent its execution. In addition, no rate-limiting feature throttled simple exhaustive attacks. Finally, SAMS did not enforce privilege separation, allowing all SAMS accounts full privilege. Security features such as these, along with regular security updates, would solve most of the security issues with SAMS. Appendix B presents our detailed review of SAMS. After the review, DoIT followed our recommendations to mitigate the vulnerabilities we found. Other cases of shadow IT at academic institutions may share similar vulnerabilities.

This five-day UMBC case study—the fourth in a series organized by Sherman [11,35,36]—illustrates how easily shadow IT can grow and expand throughout an organization and how it can create vulnerabilities. Institutions of higher learning, with independent sources of funding available through grants and a mindset of autonomy, are especially vulnerable to the dangers of shadow IT.

5 Survey

Understanding the prevalence and impact of shadow IT within institutions of higher education presents an interesting research question. Conducting a survey of IT professionals at these organizations provides an opportunity to explore this question and investigate the security implications. Reviewing the vulnerabilities of SAMS, an internally built legacy system, prompted questions regarding the existence, nature, and security implications of shadow IT at other academic institutions. Did SAMS represent a typical example of shadow IT at colleges or universities and did it reveal common vulnerabilities? More generally, did shadow IT pose a frequent or serious security risk at academic institutions, and could providing a comprehensive view of shadow IT at colleges and universities

aid in reducing its potential threat? Motivated by these and other questions, the team conducted a survey study of shadow IT at institutions of higher education.

Survey results provide insights, not previously documented in the literature, into the relationship between several institutional characteristics and the occurrence of shadow IT related security incidents. Survey findings also provide new information regarding the users, types, locations, reasons for use, impact, approach, and successful remediation strategies for shadow IT at academic institutions. https://www.overleaf.com/project/5ee781f6772bb50001692c4e

5.1 Methodology

Interviews of IT professionals, both within and outside of academe, served as the basis for the development of survey questions. A complete version of the survey instrument appears in Appendix C and comprises 42 questions spanning topics from the demographics of respondents, to institutional characteristics, to security incidents and shadow IT usage. Most questions on the survey follow a multiple-choice or rating format, with some free response opportunities also included.

UMBC's Internal Review Board conducted an evaluation and provided approval for both the survey instrument and participation consent form. Despite the voluntary nature of the survey and consequently the possible over-representation of individuals with strong feelings toward shadow IT, only about half (53%) of respondents actually agreed that shadow IT represented one of their "top three priority concerns," a finding that alleviates some of the concerns related to response or volunteer bias.

5.1.1 Deployment and Data Collection. During October 2020, the survey appeared on listservs targeted to security professionals at institutions of higher learning—*Research Education Networking Information Sharing and Analysis Center (REN-ISAC)* and EDUCAUSE Security List. Listserv members received an invitation to participate in the survey along with a description of the survey's purpose and a link to the survey. A UMBC sponsored version of Qualtrics facilitated the anonymous collection of responses.

5.1.2 Profile of Respondents. Overall, 77 respondents agreed to take the survey, and of those, a total of 53 actually completed the survey with two others providing a partial set of answers for a substantial number of questions. Respondents to the survey came from a variety of backgrounds and experience levels, but most shared similar characteristics. A clear majority were over the age of 45 (83%), male (81%), with at least some level of graduate education (80%), and a position focused on policy and strategy (80%). In addition, almost all had more than 20 years of IT professional experience (88%) and more than five years of cybersecurity experience (84%).

5.1.3 Statistical Methods. While the limited number of survey responses does not lend itself to complex statistical analysis, the data do provide interesting insights into usage patterns of shadow IT at academic institutions and susceptibility to risk. Statistical methods to explore correlations between shadow IT security incidents and possible susceptibility factors used significance testing at the significance level of 0.05 with Fisher's Exact Test and Pearson's Chi-Square [7, 40]. The null hypothesis assumed no dependency between the susceptibility factor under study and the occurrence of a shadow IT related security incident. Analysis using R Studio provided contingency Tables and relevant statistical calculations.

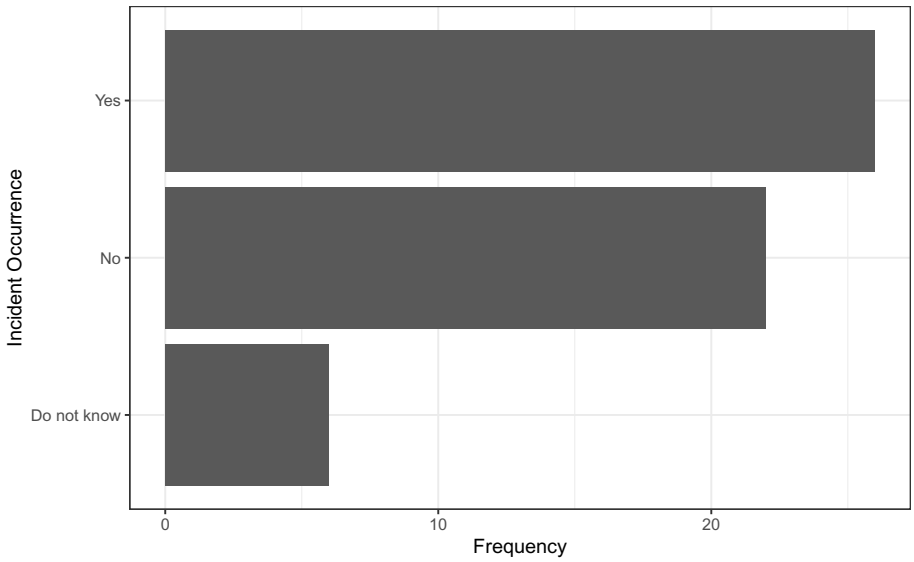

Fig. 1. Shadow IT related cybersecurity incidents in the last year. Nearly half of all respondents indicated that their institution had experienced a shadow IT related security incident in the last three years.

5.2 Susceptibility Factors

As illustrated in Figure 1, about half (48%) of the survey respondents indicated that their school had experienced a shadow IT related security incident in the last three years. By not explicitly defining what constitutes a shadow IT related security incident, the question's intentional vagueness ensured the broadest scope possible for responses. Exploring the correlation between experiencing an incident and various characteristics at the respondents' schools yielded some interesting findings. Analysis focused on five categories: 1) institutional demo-

graphics, 2) profile of graduate schools, 3) types of shadow IT, 4) profile of security violations, and 5) institutional approach to shadow IT.

5.2.1 Institutional Demographics. Figures 2, 3, and 4 summarize key features of the institutions of higher education represented by the survey respondents and include academic classification, size, and IT department structure. As seen in the graphs, a majority represented doctorate granting universities with largely centralized IT departments. In addition, with respect to the number of students enrolled, a large group of schools fell into the category of 2,000 to 10,000 students, but many also represented larger schools with more than 26,000 students.

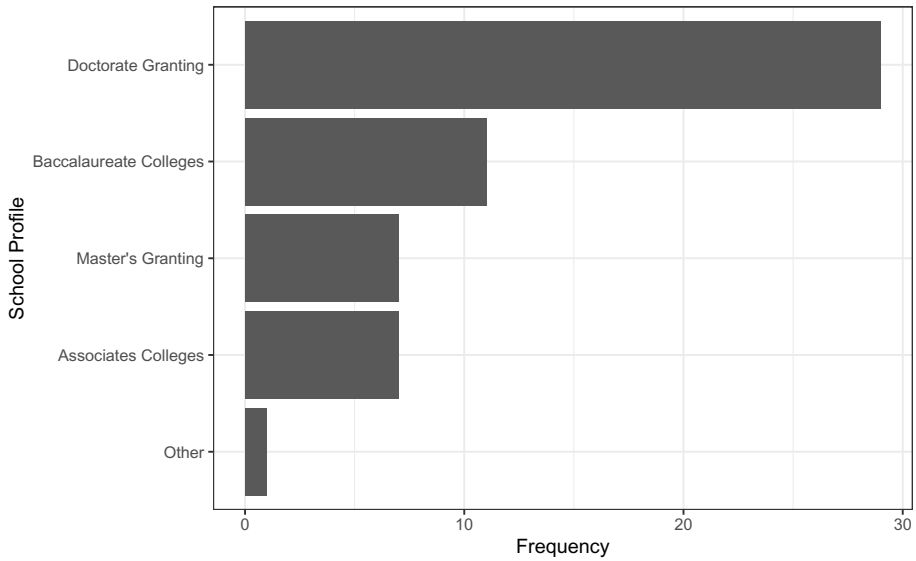

Fig. 2. Type of academic institution. The majority of schools represented in the survey were doctorate granting institutions.

Among these three variables, data indicated only a possible correlation, at the 5% level of significance, between the IT department structure and the reporting of a shadow IT related security incident. Table 1 summarizes these results.

Interestingly, the more distributed the IT department structure, the higher the rate of a reported shadow IT related security incident (centralized 25%, hybrid 63%, decentralized 100%). In describing their school's approach to managing shadow IT, one survey respondent supported the above observation with the comment that "Centralization of IT has eliminated most concerns that are addressable by the institution." If this finding holds more generally, understanding the factors which might increase susceptibility to a shadow IT related secu-

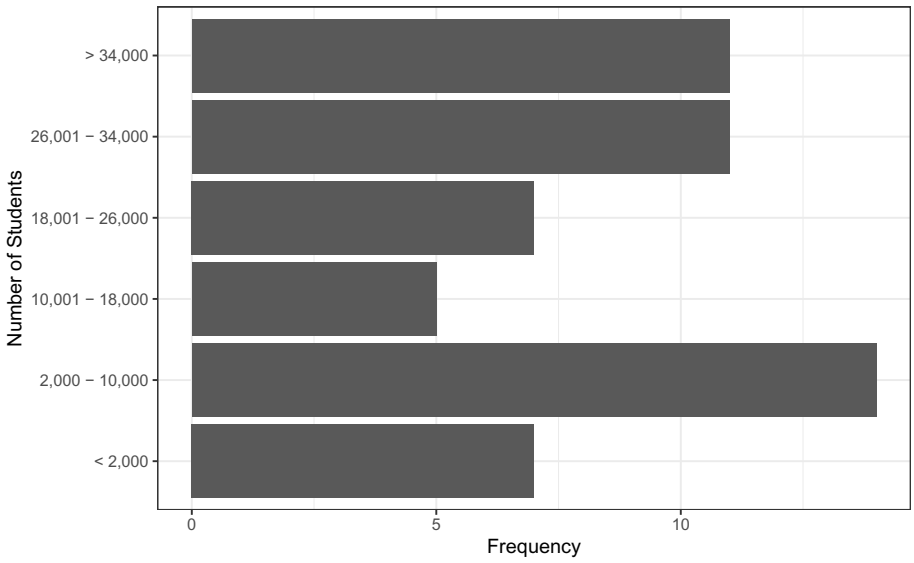

Fig. 3. Size of school by number of students. Schools represented in the survey exhibited a diversity of size according to the number of students enrolled.

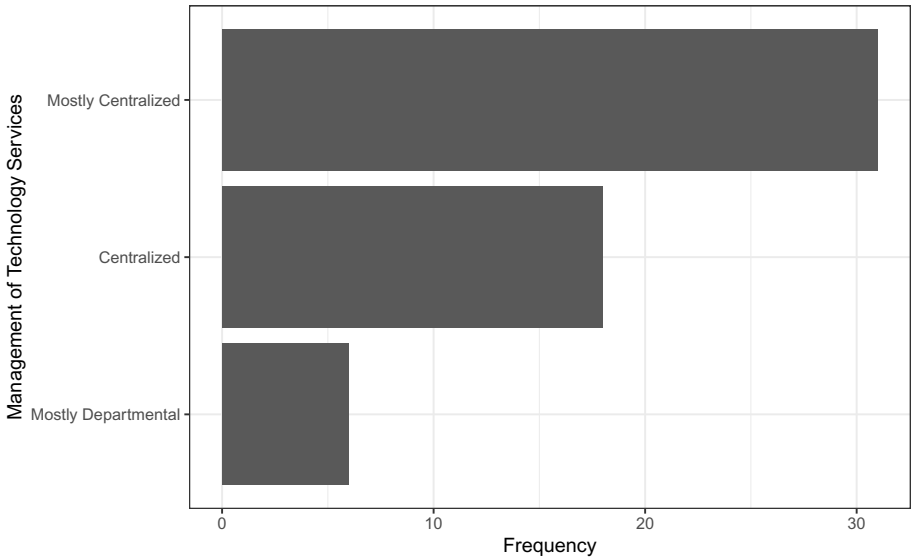

Fig. 4. Structure of technology department. The majority of schools represented in the survey had IT departments that were mostly centralized with some department focused services and resources.

Table 1. Significance of institutional characteristic.

Institutional Characteristic	Chi-Square (χ^2)	χ^2 p-value	Fisher p-value	Degrees of Freedom
Academic Classification	8.5982	0.0720	0.0511	4
IT Department Structure	10.5550	0.0051	0.0039	2
Size of Student Body	9.8684	0.0791	0.0895	5

rity incident in a more distributed IT environment, or conversely reduce it in a more centralized environment, could contribute to developing strategies to mitigate the risk of occurrence. Recognizing this potential increased susceptibility, schools with a less centralized IT structure could at least be forewarned.

While the academic classification (or institution type) did not show significance at the 5% level for a correlation with a security incident, not surprisingly, the doctorate granting institution classification, with a high degree of research activities, was the only academic classification with the rate of a reported shadow IT related security incident greater than 50 percent (73%). This finding could be explained by the availability and use of grant money to purchase IT resources outside the IT approval process. As noted by one of the survey respondents, "They're my research dollars and I need control of my research computing equipment."

5.2.2 Graduate Schools. This study represents the first to examine shadow IT usage at the granular level of the individual schools or colleges within an institution of higher education. Survey respondents first answered a question indicating all of the graduate schools or colleges present at their academic institution and then later in the survey identified all schools or colleges exhibiting a "high" level of shadow IT usage. Figures 5 and 6 illustrate these combined survey results from complementary perspectives.

Figure 5 sorts results according to the total number of respondents who identified the school or college as present at their institution. It also shows the breakdown of the number of these respondents who identified it as having "high" shadow IT usage. Not surprisingly, college of arts and sciences appeared the most often followed by business school. In contrast, Figure 6 sorts the results according to the proportion of respondents identifying the school or college as having "high" shadow IT usage. In this case, engineering school demonstrates the highest proportional level of "high" shadow IT usage followed by medical school.

In addition to identifying those graduate schools with "high" shadow IT usage, an analysis of the data also indicated a possible correlation between the presence of an Engineering School, Medical School, or Architecture School and the occurrence of a shadow IT related security incident. Table 2 summarizes these results.

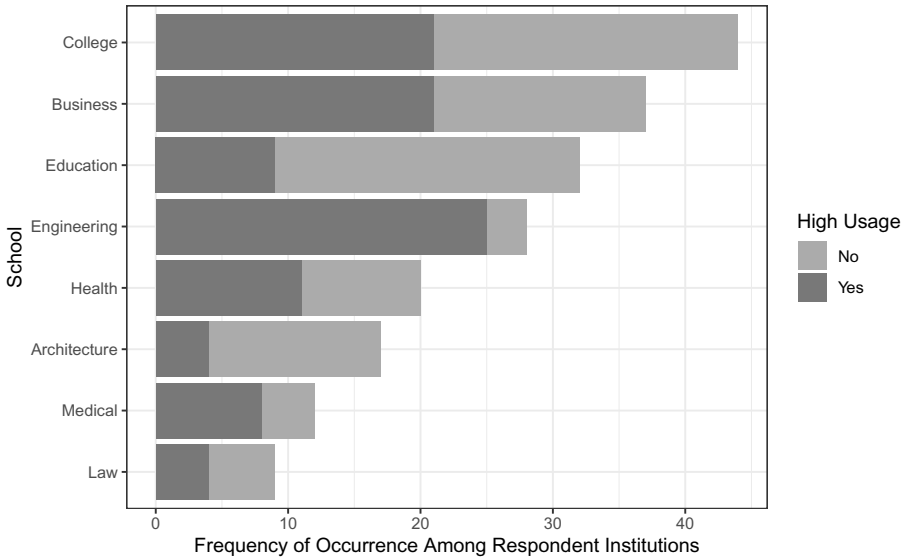

Fig. 5. Graduate schools ranked by frequency. Respondents classified different schools within their institution as having varying levels of shadow IT usage.

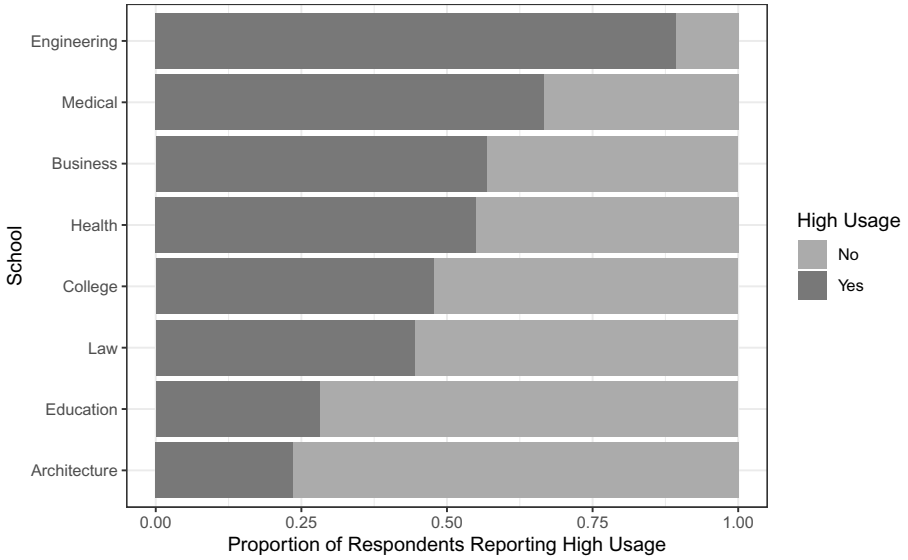

Fig. 6. Graduate schools ranked by proportion of high usage level. With respect to the proportion of users who use shadow IT at high levels, the engineering schools and medical schools received the highest ratings.

Table 2. Significance of academic unit.

College or School	Chi-Square (χ^2)	χ^2 p-value	Fisher p-value	Degrees of Freedom
Architecture	4.4491	0.0349	0.0273	1
Arts and Sciences	1.8691	0.1716	0.1523	1
Business	1.0314	0.3098	0.2227	1
Education	0.2911	0.6391	0.5570	1
Engineering	11.9370	0.0006	0.0004	1
Law	1.4545	0.2278	0.1513	1
Medical	4.0280	0.0448	0.0235	1
Public Health	0.0000	1.0000	1.0000	1

As discussed in Section 5.3.3, the single most often-cited reason for the use of shadow IT relates to the inability to get a particular IT need met by the IT department within a required timeframe. Arguably, medical schools, with their focus on saving lives, can least afford to wait for IT and have strong motivation to do what it takes to solve a problem, even if it involves shadow IT, and mirrors a high use of technology in healthcare overall. In the case of engineering and architecture schools, with their strong technical foundations, enhanced capabilities for finding their own technology solutions makes shadow IT an easy option.

While engineering schools and medical schools topped the list of the proportion of respondents identifying these graduate schools as exhibiting "high" levels of shadow IT usage, architecture schools showed the lowest proportion. This finding might indicate that, not only the preponderance of shadow IT usage, but also other factors such as the type of shadow IT might be contributing to the increased susceptibility to a security incident. Given these findings, any coordinated initiative by an IT department to address shadow IT might prioritize these three schools, whether increasing responsiveness to them or creating a more secure framework in which these schools could address their own technology needs. For example, clear policies or restricted access to certain software or data could provide helpful "guardrails." As one survey respondent put it, "'Shadow' is not the right word. 'Auxiliary systems' might be a better word and might let us understand the phenomenon better."

5.2.3 Types of Shadow IT. When asked about the types of shadow IT at their schools, survey respondents cited cloud storage and unapproved software as the most prevalent forms of shadow IT they encountered. In the survey, respondents were first asked to select as many types of shadow IT known to be present at their school in the last three years and then several questions later asked to select all types of shadow IT representing a "high" concern at their school. Figures 7 and 8 represent the combined responses to these questions from two different perspectives. Counts of "high" concern for each type of shadow IT in-

cluded only those respondents who identified it as a type of shadow IT present at some point within the last three years at their academic institution.

Figure 7 shows the identified types of shadow IT in descending order of frequency, with each bar also indicating the number of respondents identifying it as a type of shadow IT of "high" concern. To understand better the proportional degree of concern for each type of shadow IT, Figure 8 sorts the results according to the percentage of responses identifying that type of shadow IT as a "high" concern. In Figure 8, "cloud storage" remained the top answer while "unauthorized hardware" rose to the second highest proportional concern. In both graphs, legacy systems maintained a position in the top three.

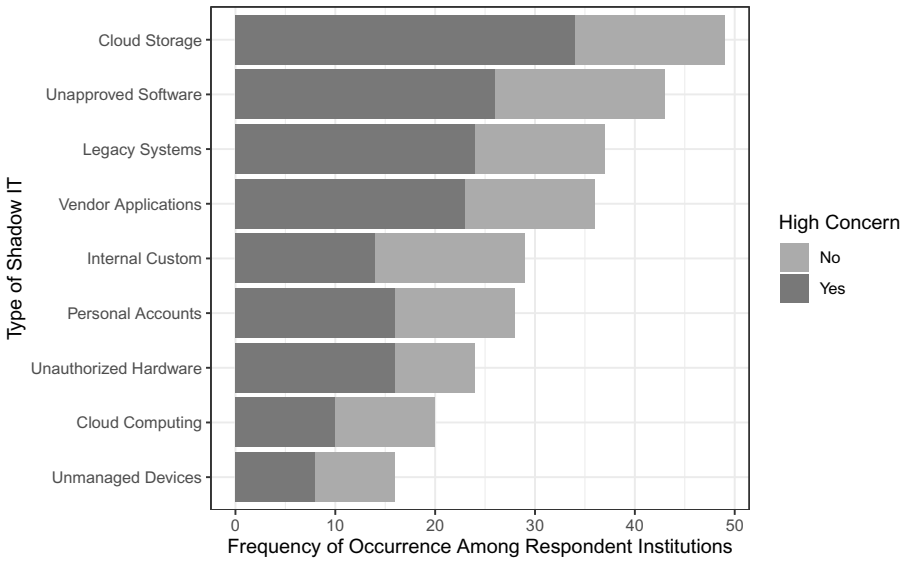

Fig. 7. Rank of existing types of shadow IT by frequency. Respondents identified the types of shadow IT present at their institution within the last three years and indicated any of high concern.

However, with respect to a possible correlation between the type of shadow IT and the occurrence of a shadow IT related security incident, only three types of shadow IT showed significance at the 5% level: legacy systems, internally custom-built applications, and unmanaged IT devices. Table 3 summarizes these results. While respondents identified other types of shadow IT as more prevalent or of higher concern, only these three types of shadow IT demonstrated a possible correlation to the reporting of a shadow IT related security incident.

SAMS represents both a legacy system and an internally custom-built application—two of the three types of shadow IT with a correlation to a security incident. Further, as Figure 9 illustrates, respondents who reported experienc-

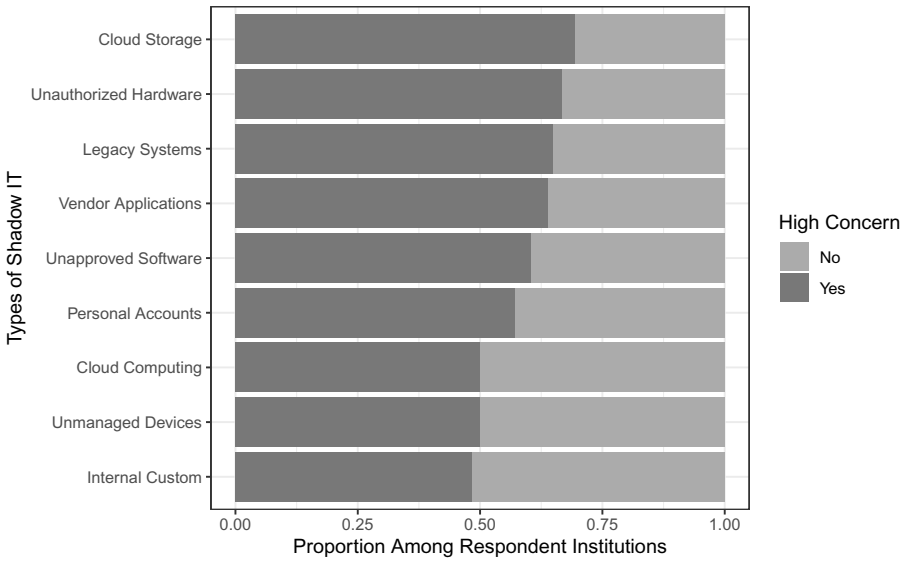

Fig. 8. Rank of types of shadow IT by proportional level of high concern. With respect to the proportion of respondents who identified a type of shadow IT as representing a high concern, cloud storage, unauthorized hardware, and legacy systems topped the list.

ing a shadow IT related security incident within the last three years most often identified legacy systems as the single dominant form of shadow IT involved in the incident.

These findings are consistent with the multidimensional vulnerabilities identified in the SAMS case study and suggest that an effective strategy might include first targeting legacy or internally custom-built systems for security upgrades or replacement—especially when limited resources constrain IT mitigation efforts related to shadow IT.

Specifically, a university-wide initiative could focus initially on identifying legacy and custom built systems on campus and then prioritizing those with access to sensitive data or networks. As the SAMS case study demonstrated, the early security enhancements made by DoIT (once DoIT learned of SAMS) contributed to a strengthened defense of the system—even as SAMS continued for several years as shadow IT, outside the oversight and direct control of DoIT. As noted in the case study, one modification included a secure password protected point of entry to the system that provided at least a basic level of protection.

5.2.4 Profile of Security Violations. Respondents were asked to estimate the proportion of all security violations related to the use of shadow IT. As seen in Figure 10, the single most common response indicated that the "majority" of IT security violations involved shadow IT. In addition, as illustrated in Table 4,

Table 3. Significance of type of shadow IT.

Type of Shadow IT	Chi-Square (χ^2)	χ^2 p-value	Fisher p-value	Degrees of Freedom
Cloud Storage	0.0390	0.8434	0.6492	1
Unapproved Software	1.8691	0.1716	0.1523	1
Vendor Applications	0.0000	1.0000	1.0000	1
Internal Custom-Built	3.9458	0.0470	0.0410	1
Legacy System	5.1326	0.0235	0.0137	1
Personal Accounts	2.8185	0.0932	0.0795	1
Unmanaged Devices	4.4491	0.0349	0.0273	1
Cloud Computing	0.9590	0.3274	0.2489	1
Unauthorized Hardware	0.4316	0.5512	0.3929	1

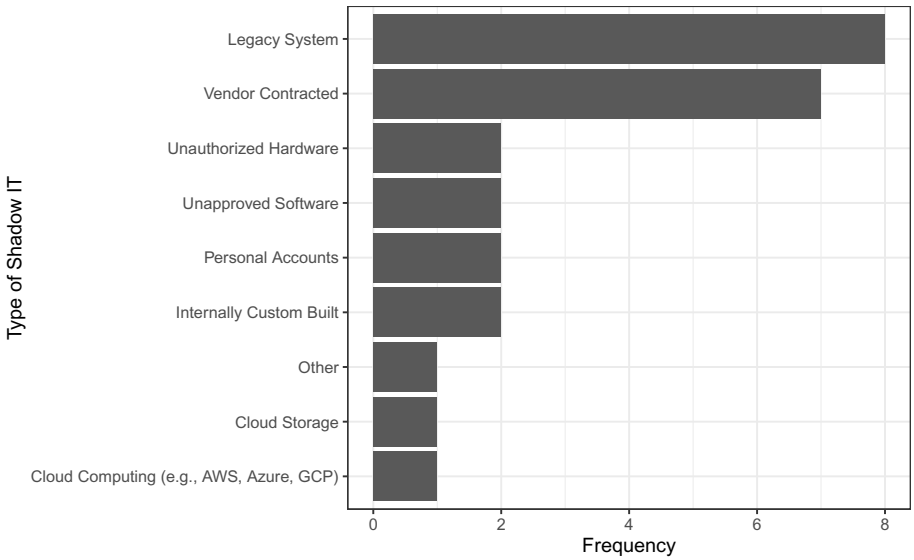

Fig. 9. Dominant type of shadow IT involved in security incidents. Legacy systems and vendor contracted products were most often cited by respondents as the single dominant type of shadow IT involved in a security incident at their school.

a correlation at the 5% level of significance resulted between the proportion of security violations related to shadow IT and the occurrence of a shadow IT related security incident. As expected, the more significant proportions resulted in a greater possibility of an incident (majority 72%, equal parts 75%, minority 30%, and none 0%). Those who "do not know" were excluded from the analysis.

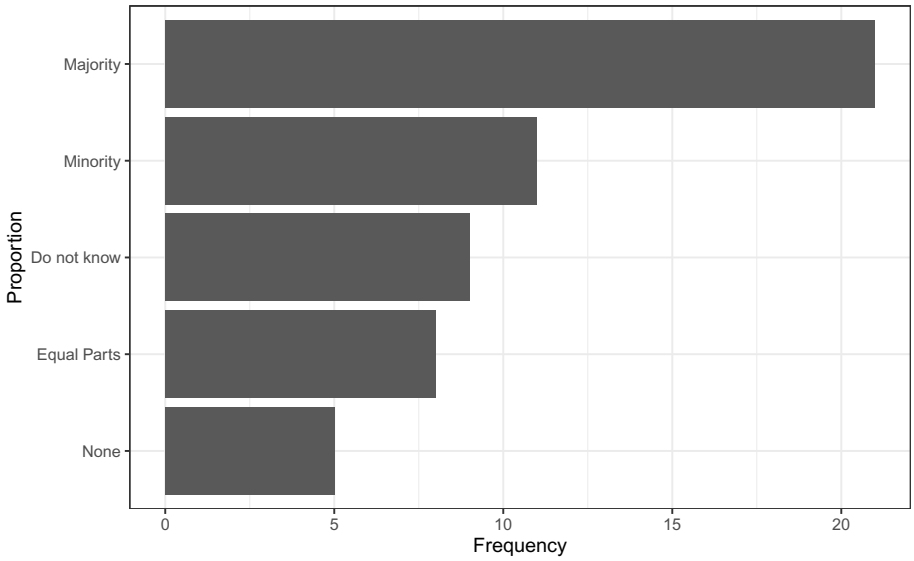

Fig. 10. Proportion of security violations related to shadow IT. Almost half of respondents indicated that the majority of security violations at their school were related to shadow IT.

Table 4. Significance of violations factor.

Violations Factor	Chi-Square (χ^2)	χ^2 p-value	Fisher p-value	Degrees of Freedom
Shadow IT Proportion	16.1690	0.0010	0.0007	3

While the relationship represents an intuitive result, given the strength of the relationship, this proportion could serve as a quick indicator for estimating the prevalence and seriousness of shadow IT at an academic institution. In addition, this metric could serve as another factor, along with IT department structure, types of graduate schools, and types of shadow IT present, in making a quick

assessment of an academic institution's risk for a shadow IT related security incident.

5.2.5 Approach to Shadow IT. In contrast to current movements within the private sector to leverage shadow IT, most respondents in the survey demonstrated a clear preference for increasing the level of control over shadow IT. The survey asked respondents to rate both their school's current approach to shadow IT and their desired approach to shadow IT on an increasing scale, with 0 representing the least level of control and 10 the most. Respondents' answers showed a statistically significant increase in rating between existing approach and desired approach. A paired t-test gave a 1.64 mean of the differences and a t-value of 4.9738 and p-value of 7.549×10^{-06}. Figure 11 summarizes the two-part responses.

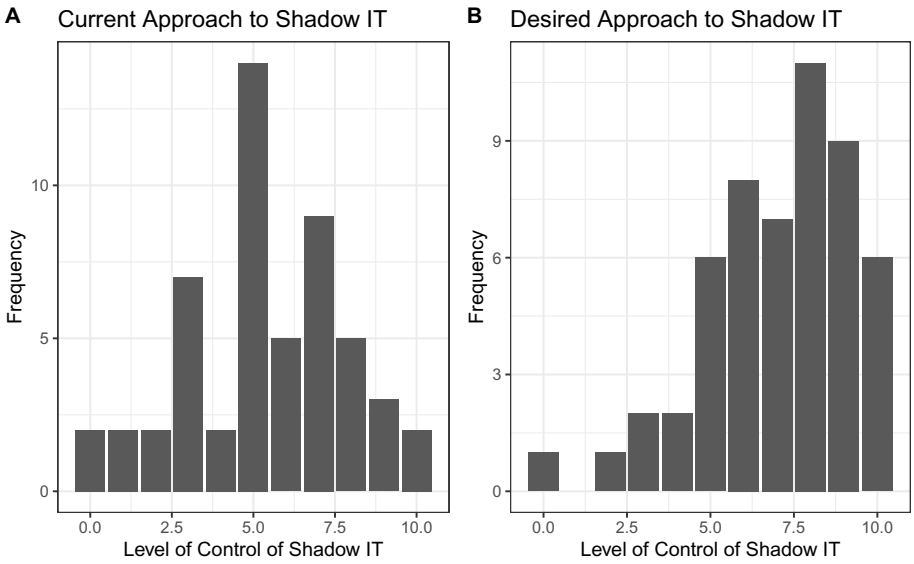

Fig. 11. Institutional approach to shadow IT. Respondents indicated both their assessment of the current approach to shadow IT by their institution and the approach they preferred. The desired approach showed less tolerance of shadow IT.

Given that the respondents represent IT professionals who must contend with what one respondent called the "You break it. I fix it." syndrome, their desire for increased control over shadow IT is not surprising. This finding complements the observed relationship between an institution's approach to shadow IT and the existence of security incidents related to shadow IT. Specifically, consolidating the rating for the current level of control of shadow IT into two categories—"controlled" and "flexible"—by splitting the numerical range in half provides

an opportunity to examine this relationship. As summarized in Table 5, a correlation at the 5% level of significance resulted between an institution's current level of control of shadow IT and the occurrence of a shadow IT related security incident, with a more flexible approach resulting in a higher possibility of a security incident (flexible 73% and controlled 32%). Consequently, before adopting a more flexible policy toward shadow IT, an academic institution might want to put specific safeguards in place.

Table 5. Significance of approach factor.

Approach Factor	Chi-Square (χ^2)	χ^2 p-value	Fisher p-value	Degrees of Freedom
Current Level of Control	6.5936	0.0142	0.0143	1

5.3 An Institutional Profile of Shadow IT

In addition to exploring susceptibility factors related to shadow IT and security incidents, this study also provides a comprehensive view of shadow IT at academic institutions with respect to the people using it, their reasons for doing so, the institutional impact of its use, those responsible for dealing with any problems, and successful strategies for managing shadow IT. We hope this window into shadow IT at academic institutions combined with the possible susceptibility factors provides practitioners with valuable information in developing efficient and effective programs for managing shadow IT at their schools.

5.3.1 Who is Using Shadow IT? In addition to considering what types of shadow IT prevail and where, the survey focused on developing a better understanding of the individual users of shadow IT within academic institutions, including the respondents themselves. Not surprisingly, over 90 percent of respondents indicated that they did not personally use shadow IT in their daily work. As IT professionals, respondents might feel less comfortable admitting to shadow IT use, or in the alternative, this result might reflect a genuine trend. However, when asked a possibly less sensitive question about the proportion of their immediate co-workers using shadow IT in their daily work, a combined 77.3 percent of respondents indicated either "none" or a "minority" but the remainder of responses roughly split between "equal parts" and "majority".

While this finding might imply a generally low to moderate level of shadow IT usage within IT departments, survey respondents identified several groups and departments at their schools with "high" shadow IT usage. In response to questions about the groups and departments that exhibit a "high" level of shadow IT usage within their institutions, respondents overwhelmingly answered "faculty" and the "academics" department, respectively. A designation of "faculty,"

whether involved in research or not, topped the list. Even though "administrative staff" followed as a close third, these results might indicate that successful strategies for dealing with shadow IT within institutions of higher education will likely need to focus on faculty members first. Figures 12 and 13 depict the full range of responses.

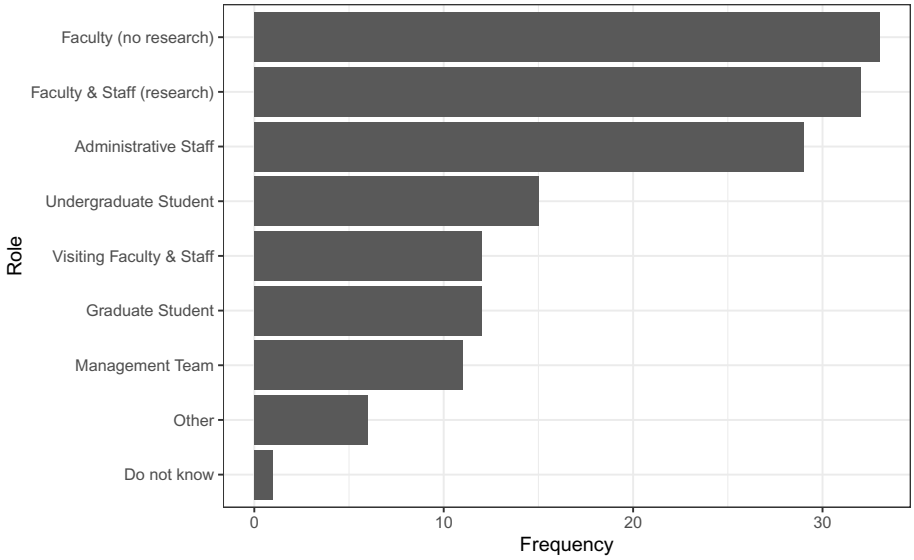

Fig. 12. High shadow IT usage by role. In trying to understand who is using shadow IT at academic institutions, respondents identified the roles with high usage. Faculty, whether involved in research or not, ranked highest.

Presumably, respondents based their answers on direct experience—e.g., with tracking security violations, incident reports, audits, or service tickets—rather than on perception. Interestingly, apart from the academics department, the next two departments with "high" levels of shadow IT usage, marketing and development, represent two of the more business-oriented departments.

In terms of discovering users of shadow IT, respondents identified the "procurement process" as the most common method, followed by an "internal review," and an "IT support request." Working collaboratively with departmental purchasing offices, IT departments could use historical procurement data to identify significant IT purchases made outside the IT review process that might benefit from additional security guidance.

5.3.2 What is the Institutional Impact of Shadow IT? About half of the respondents indicated that they had experienced some form of security incident in the last three years that could be traced to shadow IT. Of those, almost half

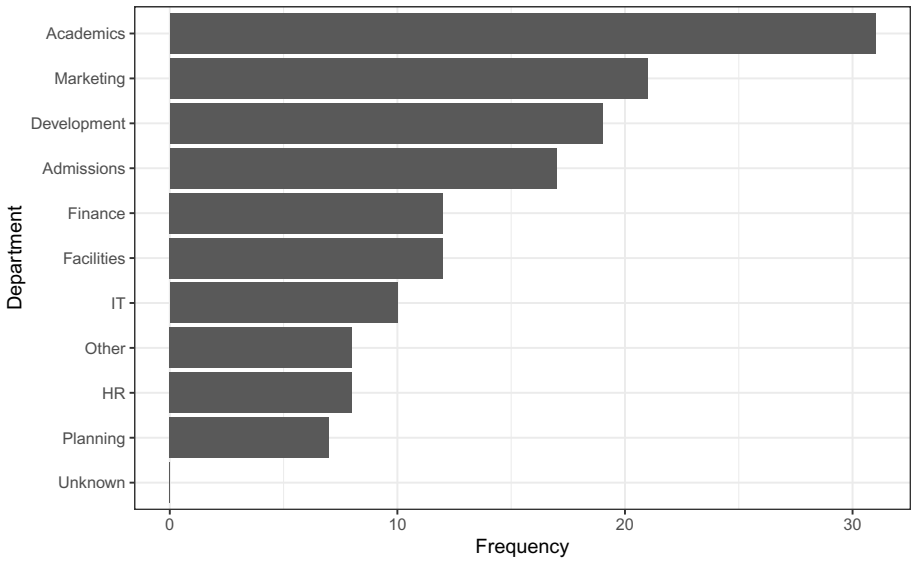

Fig. 13. High shadow IT usage by department. Respondents were asked to identify the departments in which high shadow IT usage occurred. Consistent with the finding of high shadow IT usage by faculty, academic departments ranked highest.

indicated that the "majority" of all cybersecurity incidents in the last three years had in fact involved shadow IT. Further, if considering only security incidents within the last year, respondents indicated that this proportion would "increase" or stay the same.

As seen in Figure 14, when comparing the cost of dealing with a shadow IT related security violation versus other employee security violations, most respondents considered the cost "greater than." Both of these results would seem to imply a critical problem. However, when asked whether the majority of overall IT dollars spent and IT staff resources used focused on shadow IT, respondents overwhelmingly said "no" (87%).

In addition, when asked if the majority of their time was spent dealing with shadow IT related issues, the vast majority (85%) again said "no." As noted earlier, about half of the respondents considered shadow IT to be among their "top 3 priority concerns." These responses exemplify some variability among respondents with as many as half identifying it as a serious issue and almost fifteen percent of respondents seeing it as the dominant one in terms of their time.

Significantly, most do agree that the compromise of data represents one of the most negative potential consequences of shadow IT, as seen in Figure 15 below where respondents were asked to rank order negative impacts. Given this finding, a targeted mitigation strategy might be to prioritize for a security upgrade those cases of shadow IT that deal with or access sensitive data, especially given that

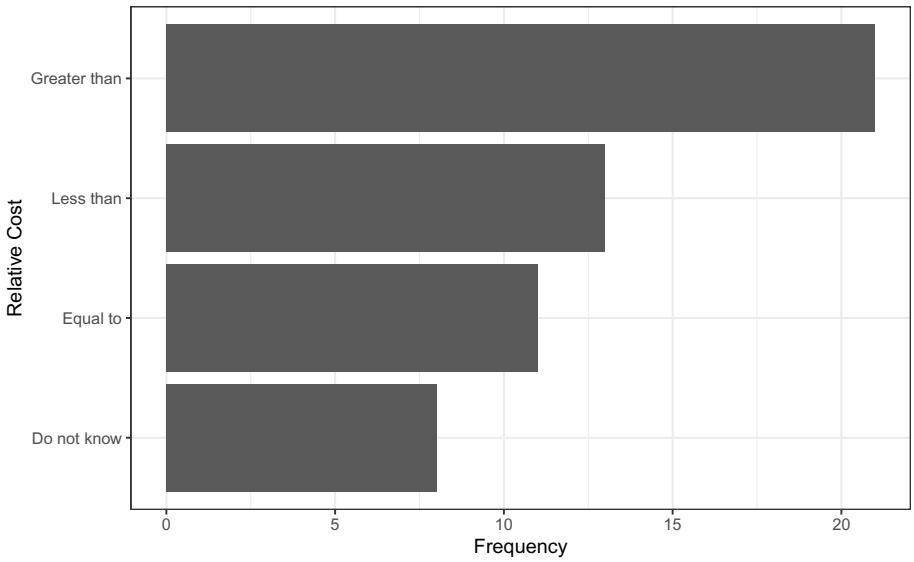

Fig. 14. Relative cost of security violations related to shadow IT. Respondents were asked to determine the relative cost of security violations related to shadow IT and most said that it was greater.

as shadow IT, they may contain predictable vulnerabilities as described in the case study.

5.3.3 Why do People Use Shadow IT? Typical of shadow IT, SAMS' ability to meet an unfilled need quickly expanded its use to other teams within the Chemistry Department at UMBC and generated requests from researchers in other departments for access to SAMS. Similar to the motivation observed in the case of SAMS, respondents from the survey overwhelmingly selected "Trying to get work done and did not want to wait for IT." as the single most often cited justification they hear from those using shadow IT. Figure 16 lists the other responses selected. Notably, a few of the responses under "other" had to do with issues of control, but several also reinforced the inability of the IT department to understand or meet a particular need.

Any attempt to address shadow IT within an academic institution would ultimately need to take account of this common underlying cause in some form. As one respondent noted, "Shadow IT exists because a need isn't being fulfilled." Both the private sector and the public sector reflect this finding to some extent. As discussed in Section 5.2.2, an IT department can employ strategies to increase responsiveness to user needs or provide a secure framework for solutions outside its purview (or a combination of both). For example, by screening, approving, and making available popular technology solutions that users can implement themselves, IT departments can at least ensure some level of security protection.

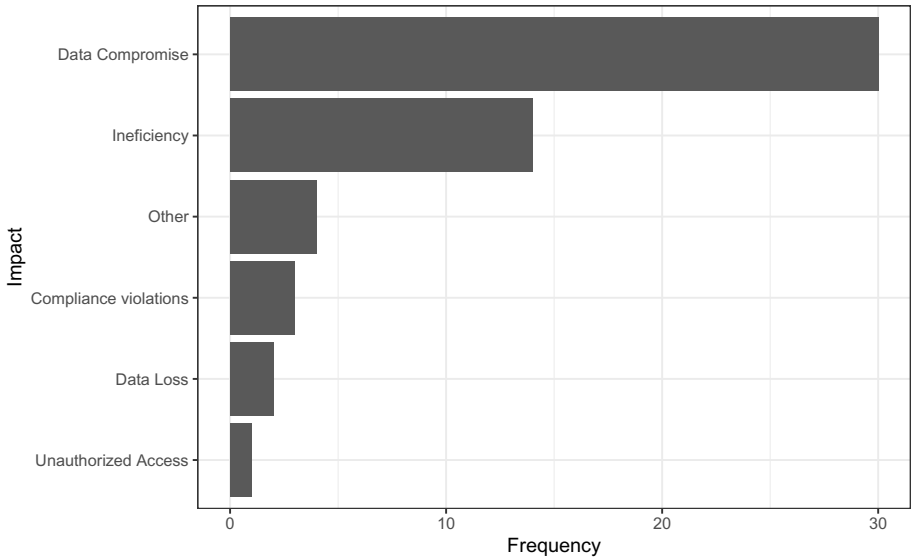

Fig. 15. Rank order of potential negative impacts of shadow IT. When asked to rank order the potential negative impacts of shadow IT, most respondents selected data compromise as the most negative impact.

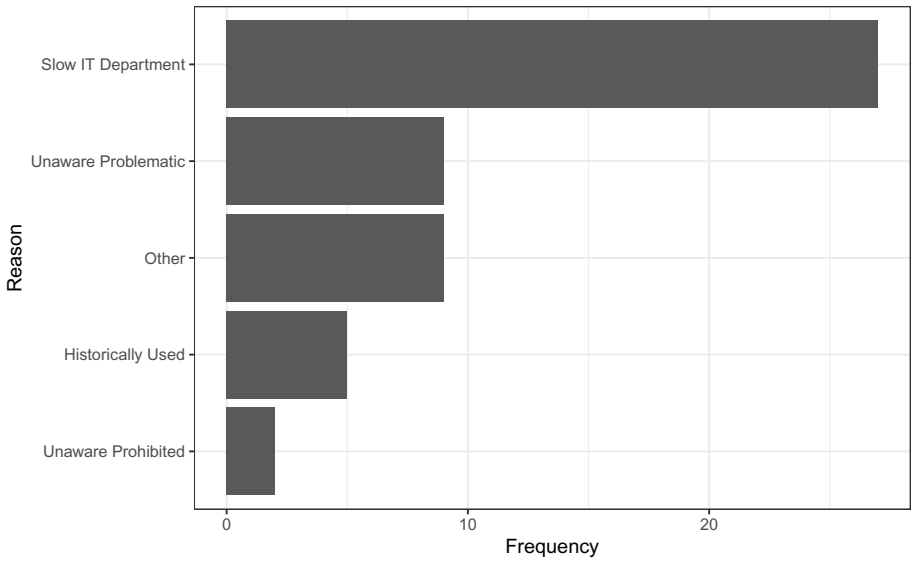

Fig. 16. Reasons for using shadow IT. Overwhelmingly, respondents cited an unresponsive or slow IT department as the reason for using shadow IT.

5.3.4 Who is Responsible for Solving Shadow IT Problems? When asked to select all groups with a "High" level of responsibility for handling any shadow IT related problems at their institution, respondents most often selected the individuals who set it up, as seen in Figure 17 part A. However, combining responses for "distributed IT" and "central IT" for a combined IT department total exceeds this value, which seems more consistent with what one would normally expect, given that IT departments often take the lead in solving problems created by shadow IT. When respondents were asked to select the single group that they believed should be most responsible, 43 percent selected the managers who approved it, as in Figure 17, Part B.

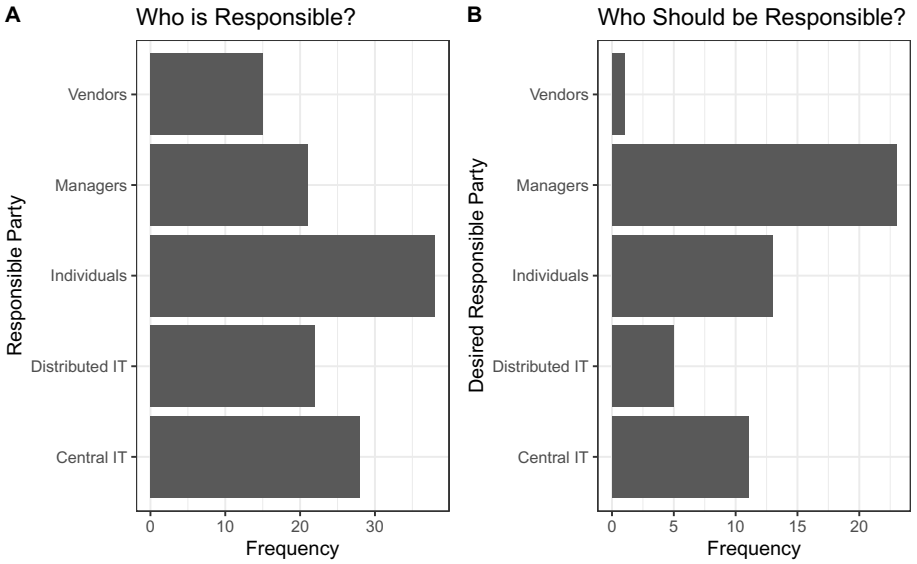

Fig. 17. Responsibility for fixing issues due to shadow IT. Respondents were asked to identify who is currently responsible and who should be responsible for dealing with problems related to shadow IT. Managers received the most votes. However, when combining the responses for both centralized and decentralized, the IT department most frequently occurs as the responsible entity followed by the individuals who introduce it.

Because respondents represent IT professionals, who often have nothing to do with introducing shadow IT yet must solve its associated problems, they would naturally want another group to take on this responsibility. A possible approach could examine whether placing greater responsibility on the managers who approve shadow IT—as recommended by many of the survey respondents—might deter its introduction.

5.3.5 What are Successful Strategies for Managing Shadow IT? When asked to select all successful strategies from a list for dealing with shadow IT based on their experience, most respondents identified "educate and train," followed by some policy focused approaches, and then finally a series of technical solutions, as seen in Figure 18 below. By selecting most often a strategy that centers on people rather than technology, respondents reinforced the importance of involving users in any approach to managing shadow IT. However, as one respondent bluntly stated, "None of these 'strategies' addresses the core problem," or simply put, unmet IT needs.

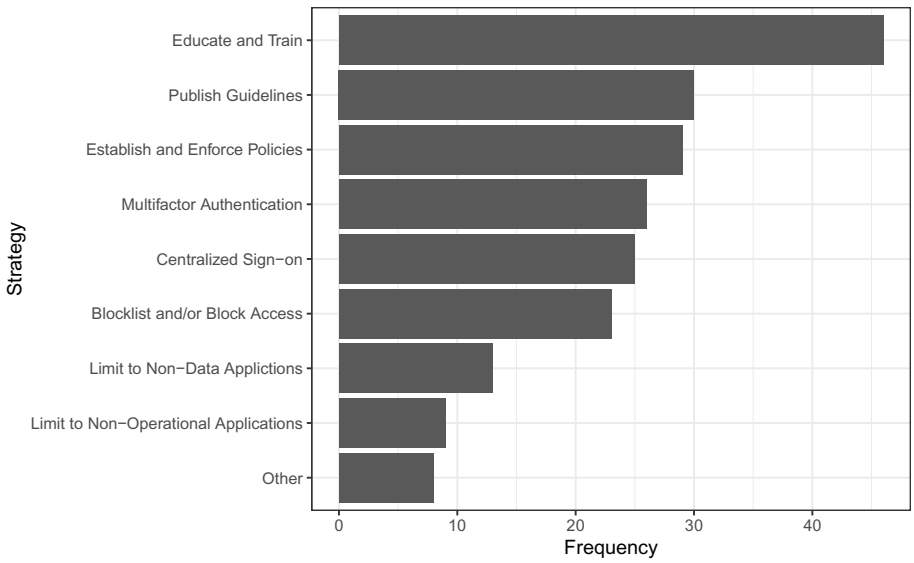

Fig. 18. Successful strategies for dealing with shadow IT. Respondents were asked to identify any strategies they had found to be successful in dealing with shadow IT. Education and training, a strong strategy for dealing with cybersecurity in general, was selected by just about all respondents.

6 A Security Profile of Shadow IT

To understand the types of shadow IT in higher education, to find their vulnerabilities, and to facilitate their analysis, we developed a *profile* of security-relevant features of shadow IT. We categorize shadow IT according to its source or origin, the authority by which it was introduced, its modality or nature, and the motivation for its introduction. Inspired and informed by our study of SAMS, and drawing from existing taxonomies, we developed our profile with the distinguishing focus of detecting vulnerabilities and making policy decisions. When

analyzing a system, identifying the type of shadow IT may help guide a security analyst to discover vulnerabilities. For example, a system developed in-house might have common vulnerabilities owing to its amateur creation and absence of a security review.

Our security profile shares several elements with, and establishes some distinctive features from, a shadow IT taxonomy developed by Kopper [24]. Common elements include labels of authority, modality, and motivation. Kopper's taxonomy categorizes infrastructure and scale, which speak to risk and who is capable of exploiting potential vulnerabilities, but are less indicative of the existence of vulnerabilities. Unlike Kopper, we include source, which may indicate the level of security review at implementation.

After explaining our profile's elements and applications, using our survey data, we examine the prevalence of profile elements in higher education. These data paint a portrait of the security profile of shadow IT at the survey respondents' academic institutions. We then suggest some implications of this portrait.

6.1 Profile Elements

Building on our experience with SAMS and directing the focus on security, our profile of shadow IT further categorizes the elements of source, authority, modality, and motivation into types (see Table 6). A shadow IT's *source* may come from an external supply, internal development, or as the result of internal modification (or potentially a legacy-induced abandonment) of an existing IT solution. With respect to its *authority*, shadow IT is not always unsanctioned, even though it is outside the typical review process. In some cases, the authority of the IT department may have sanctioned or even been involved with its introduction, or involved with an upgrade, as in the case of SAMS.

Shadow IT may be found in a multitude of *modalities*, including physical system hardware, software, network infrastructure, a collection of data, or an operational procedure to use existing IT infrastructure in a method uncontrolled by the IT authority. Common *motivations* for shadow IT include that it is legacy in nature (often introduced from a previous project or organization), a replacement for a former infrastructure, a duplicate for preference or backup, significant customization of a component of IT infrastructure, or simply a fix or patch.

6.2 Applications

Through categorizing and contextualizing shadow IT, our security profile helps analysts identify potential vulnerabilities. For example, in our case study, the legacy SAMS is an internally developed, sanctioned, data storage and software system, which played a role in the operational procedure of handling grant-spending requests. Labeling these attributes helps detect vulnerabilities: operational software for data storage often exposes cross-site scripting, and internally developed components often lack security reviews by third parties.

In our subsequent January 2021 research study at UMBC, our profile helped us to analyze and assess potential vulnerabilities in an IT ticket management

Table 6. A profile of security-related features of shadow IT. Each element is categorized into types, listed with generally increasing risk.

Element	**Type**
Source	Externally produced
	Internally developed
	Abandoned or altered official IT solution
Authority	Sanctioned by IT (though not directly managed by IT)
	Unsanctioned by IT
Modality (one or more)	Operational procedure
	System hardware
	Network infrastructure
	Data storage
	Software
Motivation	Fix
	Customization
	Duplication
	Replacement
	Legacy (personal or organizational)

system under development at UMBC. The modality of operational procedure suggested possible social-engineering attacks; the data storage suggested possible database-interface attacks; and software suggested possible program interface attacks. Additionally, the authority of a sanctioned product suggested the possibility of elevating permissions. The source of an internally developed product suggested lack of review, increasing the likelihood of common coding errors. Finally, the motivation of replacing a product suggested the possibility of allowing arbitrary interface interactions, increasing the likelihood of an input-validation vulnerability. Using these characterizations, we narrowed the scope of our investigation and quickly found a database upload race condition exploit and an effective combination of other vulnerabilities necessary to exploit it.

6.3 Prevalence of Profile Element Types from Survey

Figures 19–22 summarize responses from the survey questions about the prevalence of shadow IT types within each profile element. For each element, the survey asked respondents to identify the single type under the element for which shadow IT at their institution most frequently occurs. For the element of modality, shadow IT might display multiple types, as is true for SAMS.

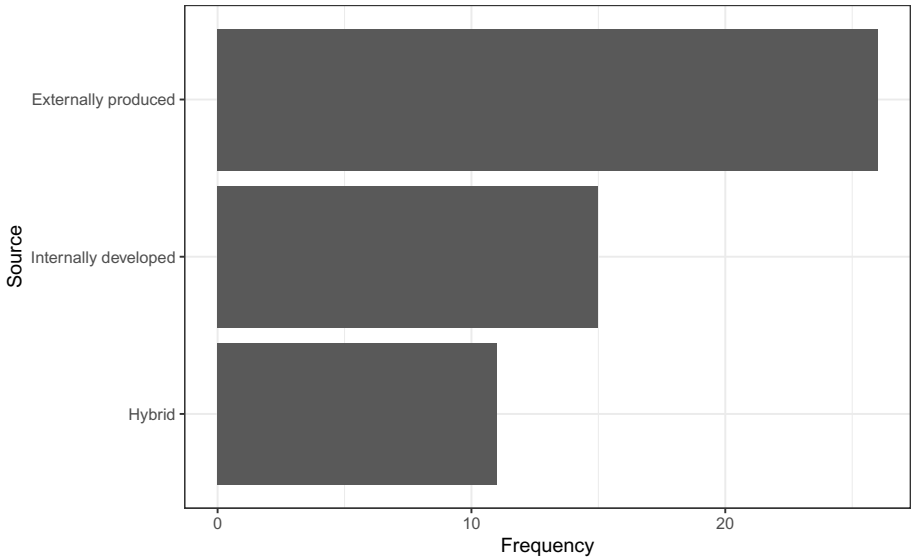

Fig. 19. Prevalence of shadow IT profile element source. Most respondents indicated "externally produced."

Figure 19 shows that the most prevalent source of shadow IT in higher education is externally produced, such as a vendor solution. Externally produced items

may tend to have greater security than internally built ones, since security professionals may more likely help create externally produced items. In the survey results, vendor-contracted solutions represent the second most cited dominant form of shadow IT involved in security incidents. Such applications, however, did not demonstrate a correlation to a security incident at the 5% significance level, supporting a possible security benefit. Externally produced shadow IT, including vendor-contracted solutions, might be easier to detect, for example, via purchasing.

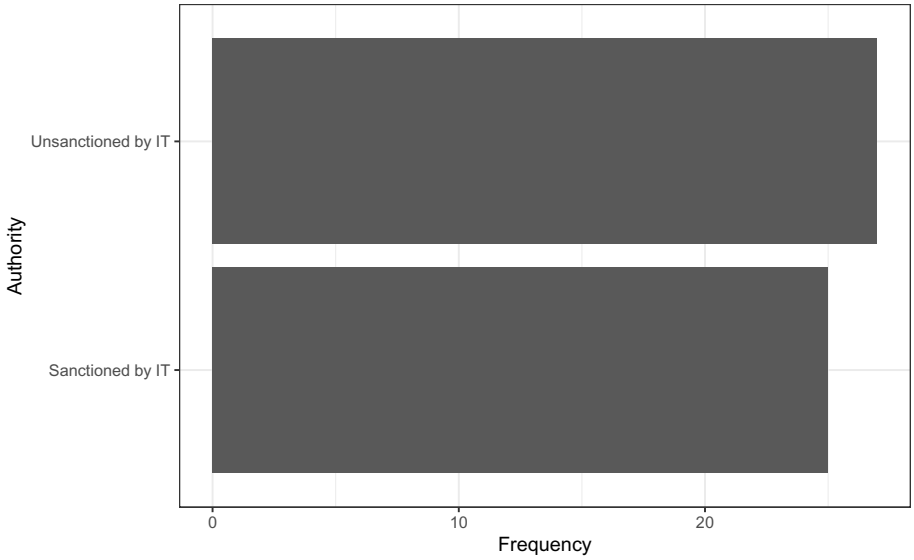

Fig. 20. Prevalence of shadow IT profile element authority. A slight majority indicated "unsanctioned by IT."

Figure 20 shows that only a slight majority of known shadow IT in higher education is unsanctioned. Therefore, almost half of known shadow IT is sanctioned. For mitigation efforts, this finding should be somewhat reassuring given that it is likely easier to identify and address sanctioned shadow IT than unsanctioned shadow IT. From a security perspective, sanctioned shadow IT may also benefit from the involvement of an IT department to ensure at least basic security standards, as in the case of SAMS.

As shown in Figure 21, the most common modality of shadow IT in higher education is software, closely followed by cloud solutions; these two modalities dominate all others. This finding is consistent with Figure 7, which reveals that unapproved software and cloud storage are the two most common forms of shadow IT.

Figure 22 shows that the most common motivation for shadow IT in higher education is customization, closely followed by legacy. Legacy systems and internally custom-built solutions displayed a correlation to shadow IT security incidents at the 5% significance level. Thus, SAMS, which is a custom system with vulnerabilities, represents a typical example of shadow IT in higher education.

Our profile provides a shorthand way to categorize shadow IT and identify possible security vulnerabilities common to certain types. While intended neither as a comprehensive nor exhaustive framework, the profile may serve to aid security practitioners in developing a preliminary view of the shadow IT at their academic institutions and guide them in their policy decisions. While our profile is a work in progress, the profile has already shown that it can add structure to what is often an amorphous problem. Future use in practice could serve to inform and further refine this profile and enhance its applicability.

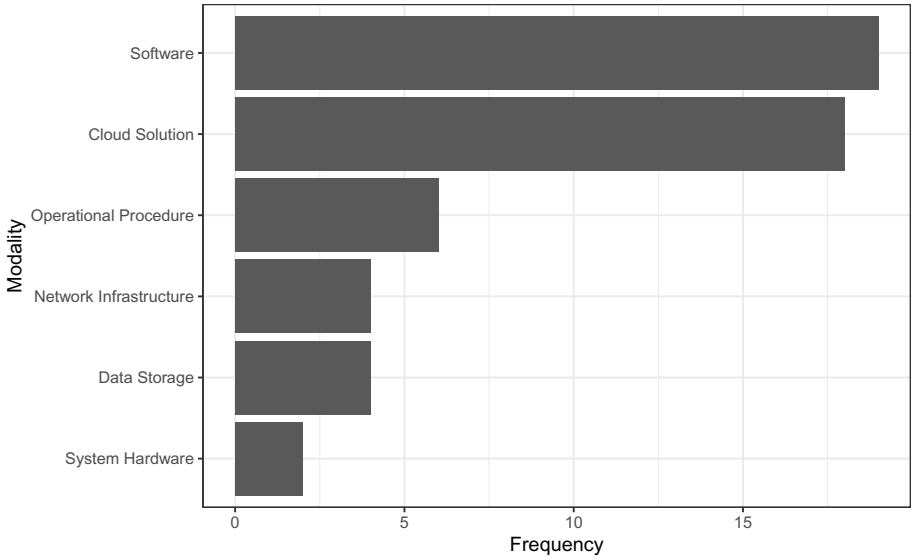

Fig. 21. Prevalence of shadow IT profile element modality. A clear majority indicated "software" or "cloud solution."

In reviewing the security profile, Jack Suess of UMBC suggests adding two elements: *level of adoption* and *data classification* as follows: "For Level of Adoption, I want to know if an application is something used by a single research group or multiple faculty across colleges. An application with a small well defined population is different than something hundreds of people may use. For Data Classification, this would be a summarized classification of the type of data used/created/manipulated. For central IT, the type of data this used/created/

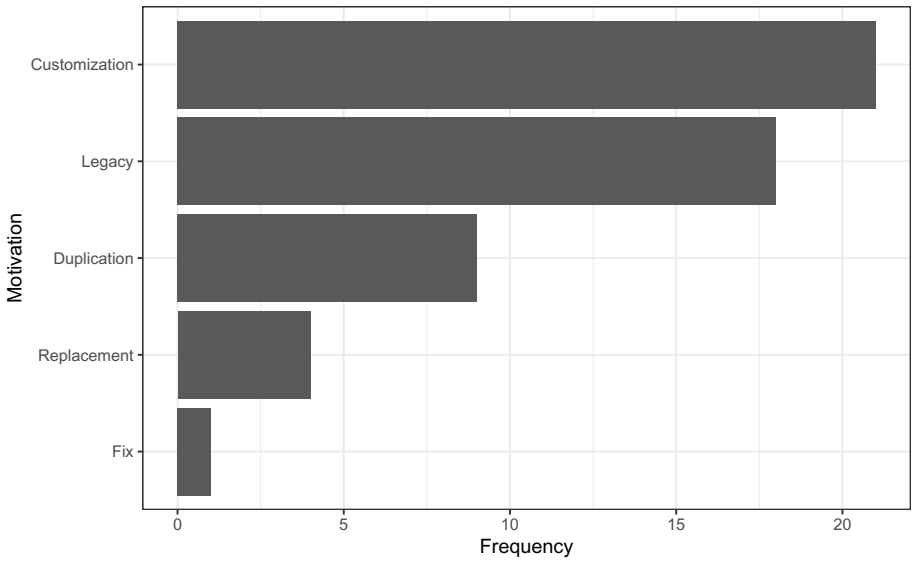

Fig. 22. Prevalence of shadow IT profile element motivation. A clear majority indicated "customization" or "legacy."

manipulated is the driving factor in how we assign risk." Suess goes on to recommend aligning the security profile with "security controls based on controlled unclassified information (CUI), as noted in NIST 800-171" [34].

We agree with his suggestions. We excluded level of adoption because initially we were more focused on vulnerability than risk. Based on valuable input from practitioners such as Suess, the security profile will continue to evolve as a work in progress.

7 Discussion

Our detailed analysis of the vulnerabilities associated with SAMS, a specific example of shadow IT at an academic institution, reveals some potential commonalities and broader lessons. Our survey of technology professionals at institutions of higher learning provides a broader view of shadow IT at academic institutions and identifies institutional factors with a possible relationship to the occurrence of shadow IT related security incidents. Further, our work may provide useful guidance in helping academic institutions to assess their own shadow IT risk level and to consider how best to allocate limited resources for mitigating it. Our development of a security based profile for classifying specific examples of shadow IT at academic institutions serves as a practical tool for security practitioners by providing a context in which to categorize security risk factors. Our multidimensional approach to studying shadow IT at academic institutions yields lessons learned for this unique methodology, and highlights opportunities

for future work. An interview with Jack Suess, VP of IT at UMBC, provides additional context and insight for this paper's findings.

7.1 Main Findings from Case Study

Our detailed examination of SAMS, a particular example of shadow IT, yields lessons that might prove more generally applicable, including conditions that contribute to its existence, the value of IT department involvement, and data-related dangers. Lab staff with technical know-how and financial resources first developed SAMS to fit a specific need of a lab team in the Chemistry Department, completely by-passing the IT department. What began as one team's grant-tracking system pervaded throughout the Chemistry Department and at the time of our case study, other departments had requested access to SAMS for their own grant-tracking activities.

SAMS illustrates how the technical knowledge, independent financial resources, and intra- and inter-departmental cooperation typical of academic institutions might facilitate the development and easy spread of shadow IT. In addition, IT departments with limited resources at academic institutions might be more structured to prioritize institution-wide or departmental needs over team or individual requirements, leading to a proliferation of unauthorized ad-hoc systems such as SAMS that satisfy the needs of individuals or smaller groups.

The addition by DoIT of a secure password-protected point of entry served as a basic security safeguard, although not an impenetrable one. Even though SAMS remained as shadow IT, outside the control of DoIT, their involvement ensured a basic level of protection for SAMS, allowed DoIT to intervene when other departments requested access to SAMS, and made possible the detailed security review of SAMS. By analogy, IT departments at academic institutions could directly appeal to and enlist the help of users of these types of unauthorized, ad-hoc applications to cooperate in making important security upgrades that at a minimum could provide basic safeguards, such as security updates, or enable a detailed security analysis. As Jack Suess notes on the important lesson of the case study, "This is an example that highlights that shadow IT systems can, with minimal effort, have a significant number of risks mitigated when the application is reviewed."

SAMS also demonstrates that within an academic environment, even a simple grant-tracking system directly accesses protected data. Legacy systems, like SAMS, might house university data not backed up elsewhere or left relatively unsecured, thus opening an institution up to legal and financial consequences. To date, high-profile cases with severe penalties related to these types of data violations have not been reported. With time, however, the potential for increased targeting by malicious actors of these unprotected systems and the resulting risk of data compromise grow.

By describing in depth the security vulnerabilities identified in SAMS, our case study highlights for IT professionals at academic institutions the many risks common to similar examples of shadow IT. This micro-level analysis of shadow IT complements the macro-analysis provided in our survey where the type of

legacy system embodied by SAMS not only represents the most common type of shadow IT identified by survey respondents, but also one with a possible correlation to security incidents.

7.2 Survey Findings

While the limited number of survey responses does not lend itself to complex statistical analysis, a basic statistical analysis of the data does provide interesting insights into susceptibility to risk, as well as usage patterns of shadow IT at academic institutions.

Findings from the survey highlight a potential correlation between the occurrence of a shadow IT related security incident and the presence of a medical school, an architecture school, or an engineering school. Suess concurs, "I think it is clear that shadow IT is most common in departments with faculty that have significant research that requires programming." Not only does the presence of these schools warn of potential shadow IT security risks, but by narrowing their focus to these specific schools, mitigation efforts could be targeted for highest impact.

In addition, a correlation also exists between experiencing an incident and the presence of one of three types of shadow IT: legacy systems, internally custom-built applications, or "unmanaged" devices. Especially relevant to this study, respondents identify legacy systems, such as SAMS, as the dominant type of shadow IT involved with security incidents at their schools. Focus on legacy or custom-built systems lends an additional dimension for targeting preventive efforts. A correlation with IT department structure show a predominantly decentralized IT department more likely to experience a shadow IT related cybersecurity incident. Reflecting on this finding and the impact of legacy systems, Suess observes that, as a result of the strong relationships built by the central university IT unit with UMBC's colleges and research faculty, the central IT unit is "more likely to be 1) pulled in when decisions are being made, and 2) more likely to be aware and take responsibility for fixing issues when risks are identified that shouldn't be ignored."

Further, both the proportion of security violations related to shadow IT, and the academic institution's approach to shadow IT with respect to level of control, also exhibit a correlation with the occurrence of a shadow IT related security incident. Potentially, these vulnerability factors could serve as indicators of increased risk. For example, an institution's current proportion of security violations related to shadow IT could provide a quick, numerical score for shadow IT risk and an early warning of potential problems.

In addition to identifying susceptibility factors, survey responses provide insight into the profile of users, with those exhibiting the highest use coming from "faculty" and from within the "academics" department. While not a surprising finding, it offers another way to target mitigation efforts, by focusing on the specific groups most involved in its use.

According to the survey, motivations for using shadow IT centered on unfulfilled needs by the IT department. Looking at ways that an IT department could

respond more quickly to the needs of the individuals, departments, or schools that predominantly use shadow IT, might be one way to address this root cause. Another involves security upgrades or development of frameworks which provide a safer environment for the existence of shadow IT, as in the case of SAMS. Respondents also identified the purchasing process as the most common method for detecting shadow IT and highlighted education and training as the most successful strategy for managing it.

In addition to these strategies from the survey, Suess adds that regular risk assessments associated with shadow IT applications provide a "key element that could help address these issues." He elaborates, "Where we know that shadow IT is using protected data elements, we will take that into considerations when doing risk assessments and address that risk; otherwise that shadow system is of lower priority." Suess also emphasizes the limitations that IT departments naturally face due to the faculty-centric nature of research universities, where "asking faculty to review all the things they want to do with security staff could be viewed by faculty as impeding research, and these reviews are more useful with research in highly regulated areas, such as medical research."

7.3 Significance of a Security-Focused Profile

Not all shadow IT presents equal security risks. Given that completely eliminating shadow IT within most academic environments presents an insurmountable challenge, finding ways to identify and address those cases with the greatest potential for harm gives security practitioners a valuable tool. Analysis of SAMS prompted the development of a security-focused profile of shadow IT, providing four key dimensions with types of varying risk levels based on existing taxonomies of shadow IT. By looking at the source, authority, modality and motivation for the introduction of a shadow IT system, IT professionals may perform a preliminary risk assessment.

According to our security-focused profile of shadow IT, the following is among the riskiest forms of shadow IT: an internally developed or modified system, unsanctioned by the IT department, with data storage or software elements, introduced as a legacy system. While possessing most of these elements, SAMS benefited from an intervention by the IT department, transforming its status to "sanctioned." With that came important security enhancements, including our detailed security review.

Respondents in the survey categorized shadow IT at their respective schools by identifying the most common types in the security-focused profile. Doing so revealed that most shadow IT at the survey respondents' schools is characterized as externally provided by a vendor, equally split between sanctioned and unsanctioned, involving software, and with some form of customization. The security-focused profile's possible rating of risk for these types suggests that the forms of shadow IT most commonly found at academic institutions, at least in our sample, might reflect a relatively low risk profile overall. As the security profile continues to evolve, practitioners' experiences will provide possible enhancements, such as Suess's recommendation of adding the elements of level

of adoption and data classification, as well as aligning the profile with security controls noted in NIST 800-171.

7.4 Lessons Learned Conducting our Studies

Our study's two-tiered approach—SAMS case study and survey—introduced unique benefits and challenges in ensuring a cohesive framework throughout the study. While it required extra effort to maintain integration of the study's two components, their reinforcing elements strengthened the individual findings and proved especially revealing for this relatively unexplored area of shadow IT at institutions of higher learning.

Involving IT practitioners, both from within and outside of academe, in all aspects of our analysis proved critical for developing instructive survey questions, a practicable security-focused profile, and targeted review of SAMS. Participation by practitioners also contributed to making our study's analysis focused on actionable results.

While placement of the survey invitation on listservs targeted to IT professionals at institutions of higher learning ensured a wide audience and low-cost methodology, it also created the potential for response or voluntary bias and low response rates. In addition, given the sensitivity of the issue under study, IT professionals might naturally exhibit reticence in answering a survey related to their institution's IT security practices, regardless of the survey's anonymous format. Connecting the study with some trusted group for institutions of higher learning and sending personalized invitations to institutions selected through stratified sampling might generate a higher and more representative response.

7.5 Open Problems

Due to the limited number of respondents completing the survey, our preliminary findings highlight opportunities for further validation and research. Remarkably, even this small number of survey responses resulted in highly intuitive results. Future work could involve a larger-scale survey effort to confirm the findings of this study, identifying the susceptibility or vulnerability factors. In addition, including in the survey stakeholders who are most responsible for managing overall institutional risk could provide an overarching perspective with respect to the perceived security risks that shadow IT systems present to an institution of higher education. Collecting additional information and statistics regarding all security related incidents as compared to shadow IT related security incidents could provide valuable insights into the unique vulnerabilities of the shadow IT systems. This effort could also explore and validate the formalization of an institution-wide risk assessment tool with respect to shadow IT by incorporating these factors into some weighted calculation, thereby providing academic institutions with a metric for estimating their overall risk level associated with shadow IT.

With respect to specific instances of shadow IT, our security-focused profile requires further refinement and elaboration through additional case studies and

research to formalize better the common vulnerabilities of each archetype. We hope his work will lead to a set of strategies, mitigation techniques, and policies for dealing with shadow IT.

Further, incorporating the security-focused profile into the "detect" phase of the *NIST Cyber Security Framework (CSF)* [2] would enable the use of the *NIST Enterprise Risk Management (ERM)* tool [41]. Through such placement, shadow IT may eventually be recognized within a national risk register for future evaluation, highlighting the systemic risks and benefits of shadow IT in cybersecurity.

8 Conclusion

From a cybersecurity risk management perspective, shadow IT necessarily introduces unreviewed and unmitigated risks for IT departments, opening the door to incidents such as ransomware attacks or theft of proprietary assets. The impacts of shadow IT can be as much legal as they are financial. Universities have the unique responsibility of *Family Educational Rights and Privacy Act (FERPA)* and *Protection of Pupil Rights Amendment (PPRA)* requirements, U.S. federal laws which discuss how student data should be handled. If the institution does not comply with these standards, penalties could result in termination of funds or suspension of operations.

Academe's extensive and diverse data stores make the consequences of keeping "unofficial" databases or allowing access to data through "unmanaged" IT systems especially problematic. Despite these substantial consequences, survey respondents exhibited a mixed response with respect to the frequency and severity of shadow IT concerns at their schools. While overall they identified it as a real concern, only about half of the respondents indicated some sense of urgency.

Academic institutions reflect conditions, such as widespread technical expertise, financial independence through grants, an open learning environment, and high levels of collaboration, that allow shadow IT to flourish. Likely, it will grow as an IT security problem with increasing financial and legal consequences. Because of its nature, shadow IT often resides hidden in pockets throughout an academic institution, potentially attracting limited interest by malicious actors and thereby masking a true measure of the problem. Ironically, this obscurity has possibly provided a relative measure of security, but one easily circumvented by determined attackers.

Given the unmet needs shadow IT satisfies, and potential difficulties in eliminating it completely, finding ways to mitigate its risk provides a more practical solution. Our study's unique, two-pronged approach to study shadow IT at institutions of higher education provides a multidimensional view of this phenomenon, from a specific case study to an institution-wide perspective. By exploring these mutually-reinforcing elements, this paper identifies several consistent features of shadow IT at academic institutions and proposes specific strategies for reducing its security risks.

Not only is it possible to identify factors that potentially increase an institution's susceptibility to experiencing a shadow IT related security incident, but vulnerabilities may be identified and addressed by categorizing types of shadow IT through a security-related profile. Providing a lens that highlights usage patterns and types of shadow IT allows for a targeted risk mitigation approach, for highest impact with limited resources at institutions of higher learning.

As long as university IT authorities do not provide desired user functionality in a timely fashion, cybersecurity risks involving shadow IT will continue to arise. Given evolving user expectations and ongoing developments in technology and organizational workflows, higher education needs to address shadow IT in a way that wisely balances its potential benefits and vulnerabilities. We hope that our work highlights and expands the understanding of this challenge and presents practical approaches to managing shadow IT in higher education.

Phenomena underlying the issues exposed in our study transcend shadow IT in higher education and underscore a broader concern. When a need exists and authorized solutions are unavailable, cumbersome, expensive, time-consuming, or lacking in desired functionality, ad-hoc, unauthorized solutions flourish. Such solutions often circumvent important security and safety considerations. Devised to address an immediate need, these solutions generally lack many important design elements for long-term use and success. Notably, ad-doc solutions frequently depend critically on the knowledge and skills of a single person, creating a single point of failure. Also, they often lack appropriate security and safety features. Placing shadow IT in this broader context—as a consequence of the failure to provide adequate authorized solutions in a timely fashion or with the desired level of user control—highlights a security issue beyond information technology and the opportunity for a new approach.

Acknowledgments

We thank UMBC CIO Jack Suess for suggesting that we analyze SAMS, for granting us access to do so, and for his insights on the survey findings. Thanks to Damian Doyle and UMBC CSO Mark Cather for providing technical support for the case study. Suess and Doyle also helped shape the content of the survey instrument.

The following students also participated in the case study: Richard Baldwin, Alex Bassford, Scott Bohon, Casey Borror, Daniel Dominguez, Elias Enamorado, Maksim Eren, Akshita Gorti, Gabriel Onana, Cabel Pinkney, Mykah Rather, Firew Shafi, Ken Studley, Johnny Truong, Charles Varga, Ryan Wnuk-Fink, and Armand Yonkeu.

Thanks also to Glenn Mains of the Prince George's County Office of Information Technology for his valuable contributions in the development of our security profile and for his helpful comments on the survey instrument. Thomas Penniston of UMBC's Department of Information Technology provided valuable assistance for the survey deployment in Qualtrics, as well as feedback on the survey instrument. Linda Oliva led the design and assessment of the educational

aspects of the student research study. We thank Ming Chow, Josiah Dykstra, and Oliva for helpful comments.

This work was supported in part by the National Science Foundation under SFS grants DGE-1241576, 1753681, and 1819521. Sherman, Bassford, and Johns were also supported in part by the U.S. Department of Defense under CySP grants H98230-17-1-0387, H98230-18-1-0321, and H98230-19-1-0308.

References

1. Alter, S.: Theory of workarounds. Communications of the Association for Information Systems **34**(1), 55 (2014)
2. Barrett, M.P.: Framework for improving critical infrastructure cybersecurity. National Institute of Standards and Technology, Gaithersburg, MD, USA, Tech. Rep (2018)
3. Behrens, S.: Shadow systems: The good, the bad and the ugly. Communications of the ACM **52**(2), 124–129 (2009)
4. Behrens, S., Sedera, W.: Why do shadow systems exist after an ERP implementation? Lessons from a case study. PACIS 2004 proceedings p. 136 (2004)
5. Chua, C., Storey, V., Chen, L.: Central IT or shadow IT? Factors shaping users' decision to go rogue with IT. In: Thirty-Fifth International Conference on Information Systems (2014)
6. Feder, J.: The Family Educational Rights and Privacy Act (FERPA): A legal overview (2013)
7. Fisher, R.A.: Statistical methods for research workers. In: Breakthroughs in statistics, pp. 66–70. Springer (1992)
8. Fuerstenau, D., Rothe, H.: Shadow IT systems: Discerning the good and the evil. In: Proceedings of the European Conference on Information Systems (ECIS) 2014 (2014)
9. Fuerstenau, D., Rothe, H., Sandner, M., Anapliotis, D.: Shadow IT, risk, and shifting power relations in organizations. In: Americas Conference on Information Systems (AMCIS) (2016)
10. Fuerstenau, D., Sandner, M., Anapliotis, D.: Why do shadow systems fail?: An expert study on Determinants of Discontinuation. In: 24th European Conference on Information Systems, ECIS 2016. p. 1159. Association for Information Systems. AIS Electronic Library (AISeL) (2016)
11. Golaszewski, E., Sherman, A.T., Oliva, L., Peterson, P.A.H., Bailey, M.R., Bohon, S., Bonyadi, C., Borror, C., Coleman, R., Flenner, J., Enamorado, E., Eren, M.E., Khan, M., Larbi, E., Marshall, K., Morgan, W., Mundy, L., Onana, G., Orr, S.G., Parker, L., Pinkney, C., Rather, M., Rodriguez, J., Solis, B., Tete, W., Tsega, T.B., Valdez, E., Varga, C.K., Weber, B., Wnuk-Fink, R., Yonkeu, A., Zetlmeisl, L., Doyle, D., O'Brien, C., Roundy, J., Suess, J.: Project-Based learning continues to inspire cybersecurity students: The 2018–2019 SFS research studies at UMBC. ACM Inroads **11**(2), 46–54 (May 2020). https://doi.org/10.1145/3386363, place: New York, NY, USA Publisher: Association for Computing Machinery
12. Györy, A., Cleven, A., Uebernickel, F., Brenner, W.: Exploring the shadows: IT governance approaches to user-driven innovation (2012)
13. Haag, S., Eckhardt, A.: Shadow IT. Business & Information Systems Engineering **59**(6), 469–473 (2017)
14. Houghton, L., Kerr, D.V.: A study into the creation of feral information systems as a response to an ERP implementation within the supply chain of a large government-owned corporation. International Journal of Internet and Enterprise Management **4**(2), 135–147 (2006)
15. Houghton, L., Kerr, D.: Understanding feral systems in organisations: A case study of a SAP implementation that led to the creation of ad-hoc and unplanned systems in a large corporation. In: 9th Asia-Pacific Decision Sciences Institute Conference (2004)

16. Huber, M., Zimmermann, S., Rentrop, C., Felden, C.: The relation of shadow systems and ERP systems — Insights from a multiple-case study. Systems **4**(1), 11 (2016)
17. Johns, S.: Shadow IT and the Shadow IT Security Assessment Tool (SITSAT) (2020)
18. Jones, D., Behrens, S., Jamieson, K., Tansley, E.: The rise and fall of a shadow system: Lessons for enterprise system implementation. ACIS 2004 proceedings p. 96 (2004)
19. Kerr, D.V., Houghton, L., Kevin Burgess, e.a.: Power relationships that lead to the development of feral systems. Australasian Journal of Information Systems **14**(2) (2007)
20. Klotz, S.: Shadow IT and business-managed IT: Where is the theory? In: 2019 IEEE 21st Conference on Business Informatics (CBI). vol. 1, pp. 286–295. IEEE (2019)
21. Klotz, S., Kopper, A., Westner, M., Strahringer, S.: Causing factors, outcomes, and governance of shadow IT and business-managed IT: A systematic literature review. International Journal of Information Systems and Project Management **7**(1), 15–43 (2019)
22. Kopper, A.: Perceptions of IT managers on shadow IT (2017)
23. Kopper, A., Westner, M.: Deriving a framework for causes, consequences, and governance of shadow IT from literature. MKWI 2016 proceedings pp. 1687–1698 (2016)
24. Kopper, A., Westner, M.: Towards a taxonomy for shadow IT. In: 2016 Americas Conference on Information Systems (AMCIS) (08 2016)
25. Lee, J.: A grounded theory: Integration and internalization in ERP adoption and use. The University of Nebraska-Lincoln (2001)
26. Lund-Jensen, R., Azaria, C., Permien, F.H., Sawari, J., Bækgaard, L.: Feral information systems, shadow systems, and workarounds–a drift in is terminology. Procedia Computer Science **100**, 1056–1063 (2016)
27. Magunduni, J., Chigona, W.: Revisiting shadow IT research: What we already know, what we still need to know, and how do we get there? In: 2018 Conference on Information Communications Technology and Society (ICTAS). pp. 1–6. IEEE (2018)
28. McCann, E.: Groups hit with record $4.8M HIPAA fine (May 2014), `https://www.healthcareitnews.com/news/group-slapped-record-hipaa-fine`
29. Nasuni: Survey: Nearly half of employees that use file sharing services at work do so despite knowing employer bans their use, `https://www.nasuni.com/news/65-survey_nearly_half_of_employees_that_use_file/`, accessed 6-4-2021
30. Panetta, K.: Gartner's top 10 security predictions 2016, `https://www.gartner.com/smarterwithgartner/top-10-security-predictions-2016/`
31. Raden, N.: Shedding light on shadow IT: Is Excel running your business? DSSResources. com **26** (2005)
32. Rentrop, C., Zimmermann, S.: Shadow IT evaluation model. In: 2012 Federated Conference on Computer Science and Information Systems (FedCSIS). pp. 1023–1027. IEEE (2012)
33. Rentrop, C., Zimmermann, S.: Shadow IT: Management and control of unofficial IT. Proceedings of the 6th International Conference on Digital Society pp. 98–102 (01 2012)
34. Ross, R., Pillitteri, V., Dempsey, K., Riddle, M., Guissanie, G.: Protecting controlled unclassified information in nonfederal systems and organizations. Tech. Rep.

NIST Special Publication (SP) 800-171, Rev. 2, National Institute of Standards and Technology, Gaithersburg, MD (2020). https://doi.org/10.6028/NIST.SP.800-53r4
35. Sherman, A.T., Golaszewski, E., LaFemina, E., Goldschen, E., Khan, M., Mundy, L., Rather, M., Solis, B., Tete, W., Valdez, E., Weber, B., Doyle, D., O'Brien, C., Oliva, L., Roundy, J., Suess, J.: The SFS summer research study at UMBC: Project-Based learning inspires cybersecurity students. Cryptologia **32**(4), 293–312 (Mar 2019). https://doi.org/10.1080/01611194.2018.1557298
36. Sherman, A.T., Peterson, P.A.H., Golaszewski, E., LaFemina, E., Goldschen, E., Khan, M., Mundy, L., Rather, M., Solis, B., Tete, W., Valdez, E., Weber, B., Doyle, D., O'Brien, C., Oliva, L., Roundy, J., Suess, J.: Project-Based learning inspires cybersecurity students: A scholarship-for-service research study. IEEE Security & Privacy **17**(3), 82–88 (Jun 2017). https://doi.org/10.1109/MSEC.2019.2900595
37. Silic, M., Back, A.: Shadow IT–A view from behind the curtain. Computers & Security **45**, 274–283 (2014)
38. Silic, M., Barlow, J.B., Back, A.: A new perspective on neutralization and deterrence: Predicting shadow IT usage. Information & management **54**(8), 1023–1037 (2017)
39. Silic, M., Silic, D., Oblakovic, G.: Influence of shadow IT on innovation in organizations. Complex Systems Informatics and Modeling Quarterly CSIMQ pp. 68–80 (2016)
40. Starnes, D.S., Yates, D., Moore, D.S.: The practice of statistics. Macmillan (2010)
41. Stine, K., Quinn, S., Witte, G., Gardner, R.: Integrating cybersecurity and enterprise risk management (ERM). Tech. rep., National Institute of Standards and Technology (2020)
42. Symantec Corporation: Internet security threat report (2013)
43. Thatte, S., Grainger, N., McKay, J.: Feral practices. In: Proceedings of the 23rd Australasian Conference on Information Systems 2012. pp. 1–10. ACIS (2012)
44. Tischer, M., Durumeric, Z., Bursztein, E., Bailey, M.: The danger of USB drives. IEEE Security & Privacy **15**(2), 62–69 (2017)
45. Urus, S.T., Molla, A., Teoh, S.Y.: Post-ERP feral system taxonomy: A manifestation from multiple case studies. In: The European Conference on Information Systems Management. p. 458. Academic Conferences International Limited (2011)
46. Walters, R.: Bringing IT out of the shadows. Network Security **2013**(4), 5–11 (2013)
47. Zimmermann, S., Rentrop, C., Felden, C.: A multiple case study on the nature and management of shadow information technology. Journal of Information Systems **31**(1), 79–101 (2017)

A Acronyms and Abbreviations

BYOA	Bring Your Own App
BYOD	Bring Your Own Device
CAE	National Center of Academic Excellence in Cyber Defense Education
CSF	NIST Cyber Security Framework
CUI	Controlled Unclassified Information
CySP	Cybersecurity Scholarship Program
DoIT	Division of Information Technology
ERM	NIST Enterprise Risk Management
ERP	Enterprise Resource Planning
FERPA	Family Educational Rights and Privacy Act
IT	Information Technology
PII	Personally Identifiable Information
PPRA	Protection of Pupil Rights Amendment
SAMS	Sponsored Award Management System
SFS	CyberCorps: Scholarship for Service
SSO	Single Sign-On
UMBC	University of Maryland, Baltimore County
VPN	Virtual Private Network
XSS	Cross-Site Scripting

B Case Study: Technical Details

For our technical readers, we present details of our case study analyzing a typical example of shadow IT in higher education: the *Sponsored Award Management System (SAMS)*. Readers uninterested in these details should feel free to skip this section.

Over five days in January 2020, NSF *CyberCorps: Scholarship for Service (SFS)* and DoD *Cybersecurity Scholarship Program (CySP)* scholars at UMBC analyzed the security of SAMS. The students uncovered numerous potential security vulnerabilities and risks that we commonly associate with unauthorized, ad-hoc applications. The failures of SAMS illustrate how shadow IT can introduce serious vulnerabilities. The study also illustrates how shadow IT arises to satisfy an unmet need. This research study was the fourth in a series organized by Sherman [11,35,36] to inspire students through authentic project-based learning.

We present our research problem, an overview of SAMS, our study scope and adversarial model, details on how we analyzed the system, potential issues we uncovered, our own struggles with shadow IT during the study, and recommended mitigations. UMBC's *Division of Information Technology (DoIT)*, followed our recommendations and mitigated the vulnerabilities we found.

B.1 Problem

The problem was to analyze the security of SAMS. Specific questions included: How vulnerable is the SAMS application to unauthorized access? How well does SAMS protect the privacy of its grants data? What possible vulnerabilities does SAMS introduce as a stepping stone into other aspects of the UMBC network? Does inspection of SAMS reveal any interesting findings (e.g., undocumented connections or permissions; evidence of prior malicious activity)?

B.2 The Sponsored Award Management System (SAMS)

Built circa 2010 by the Chemistry Department to track up-to-date spending on grants, SAMS enables authorized users to create, view, modify, and approve purchases. SAMS sends monthly expense reports to the business manager. SAMS exports approved budgets into the university budget system. Innovative and created with good intentions, SAMS helped the university function more effectively. The Chemistry Department, however, developed SAMS without oversight from DoIT, bypassing critical security review.

Originally written in Microsoft Access before being ported to a Microsoft SQL Server, SAMS holds and modifies detailed financial data. SAMS links to the Chemistry Department's budget, user accounts, account numbers, vendors, and other *personally identifiable information (PII)*. A trusted user manages data flows between SAMS and a central UMBC administrative database.

SAMS is a web application with two components: a *web server* that provides a web-based interface for users, and a *database server* that stores the application's data. The web server (SAMS-Web) serves a SAMS PHP-based web application

using Apache HTTP 2.4.34 and PHP 7.3.2 and uses UMBC's WebAuth instance to authenticate users. The database server (SAMS-DB) hosts an instance of Microsoft SQL Server 2012. Both the web and database servers run the Microsoft Windows Server 2016 operating system. Users interact with SAMS via Internet browsers running on machines connected to the UMBC network.

SAMS is a prime example of Shadow IT: a sanctioned, abandoned, legacy, data storage and software solution. Several properties of SAMS make it an appealing target: SAMS contains PII (telephone numbers, email addresses); it provides functions for viewing, modifying, and approving purchase requests; and it likely contains common security flaws. Vulnerabilities in SAMS leading to fraudulent budgets could impact the university budget. Its creators, however, seemed unaware of its security risks, and our analysis of SAMS found many security vulnerabilities.

B.3 Scope and Adversarial Model

DoIT gave students access to a secure network containing a copy of the SAMS frontend (*sandbox-Web*) and backend (*sandbox-DB*), and root access to a workstation (*cyberbox*) that could connect to either server for reconnaissance and attacks. DoIT also provided sourcecode for SAMS, allowing students to search the sourcecode for potential exploits. Before accessing this copy of SAMS, students signed a non-disclosure agreement pledging that they would not misuse any information found during their investigation.

Students assumed an adversary skilled in network reconnaissance, web exploitation, and implementing known attacks on vulnerable software. They also assumed the adversary had access to a legitimate UMBC user account with a SAMS account authorized to create purchase requests and modify account-related fields in SAMS (e.g., email, phone number, password). Finally, they assumed the adversary had access to the UMBC network from the cyberbox host and was able to reach the SAMS web-application and database.

We assumed that the adversary cannot defeat standard cryptographic functions and protocols. We did not consider any zero-day vulnerabilities targeting any of the software running on SAMS-related systems. We also declared as out-of-scope any social engineering or physical attacks on UMBC systems, students, faculty, or staff.

B.4 How We Analyzed the System

Students analyzed SAMS by meeting daily, organizing themselves into small groups tasked with different aspects of the system: reconnaissance, SQL injection, static code analysis, and XSS scripting.

Figure 23 shows how the research team team connected to the frontend and backend of their copy of SAMS in the sandboxed environment used during the study. This figure also shows how users would connect to SAMS, and it shows the attack paths for certain attacks.

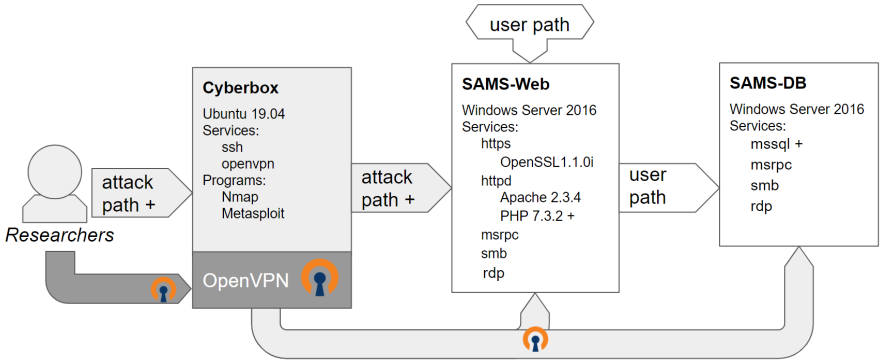

Fig. 23. How the researchers, users, and attackers can access SAMS. During the study, researchers accessed a copy of SAMS via the cyberbox virtual workstation. The unshaded area denotes the existing environment, including the sandbox-Web frontend and the sandbox-DB backend. Light shading denotes infrastructure provided to the researchers, and dark shading denotes infrastructure created by the researchers. The plus icon (+) denotes an attack path; the OpenVPN logo denotes access provided by additional infrastructure created by the researchers. Certain attacks can be performed through Cyberbox and over OpenVPN, which has access to SAMS-DB.

B.5 Potential Vulnerabilities, Attacks, and Risks

We summarize major vulnerabilities in SAMS and discuss each of their associated potential attacks and risks. SAMS exhibited many flaws common in web-applications: SQL injection, improper server configuration, poor programming practices, *cross-site scripting (XSS)*, vulnerable user management, and inadequate patching. We present each of these flaws, beginning with the most severe, and explore their potential consequences. For additional details, see Johns et al. [17].

B.5.1 SQL Injection. SAMS was extremely vulnerable to SQL injection. Once any user logged into SAMS, they could inject SQL into the update password field, allowing arbitrary modifications to the database. SQL injections allowed an attacker to see database names, which could be used to find SAMS users with elevated privileges, or to identify SAMS accounts suitable for targeted phishing. SQL injection can also modify database contents, enabling a hacker to do such things as change the amount of money that a person is receiving, or delete the user information altogether.

B.5.2 Apache Misconfiguration. Configuration issues could be exploited to reveal information about SAMS without access to a legitimate UMBC or SAMS user. For example, certain URLs on the SAMS server revealed directory listings, providing information about how SAMS works that should not be available,

including the SAMS sourcecode. Sourcecode analysis revealed an operational backdoor that was built into the code for development purposes and described in comments.

B.5.3 Sourcecode Vulnerabilities Detected by Grabber. Students used Grabber, an application scanner available in Kali Linux, to search the sourcecode for vulnerabilities, such as opportunities for XSS scripting, SQL injection and file inclusion. The report generated by Grabber found 29 possible XSS scripting vulnerabilities and one header injection vulnerability. Automated security scanning could have resulted in improved software security.

B.5.4 Cross-Site Scripting. SAMS accepts input without input validation or sanitization. This vulnerability allows an attacker to inject Javascript payloads into the SAMS database through input fields. When the attacker's browser displays such a payload, the code is executed as if it were part of the SAMS website, giving the attacker access to SAMS data while appearing to be a legitimate SAMS user. Students implemented a proof-of-concept attack that injected a malicious login form on pages viewed by SAMS users (see Figure 24). The form sent any entered credential to the attacker. Students also implemented a clickjacking attack using XSS scripting: clicking on a target link downloaded malware.

B.5.5 Login Issues. The SAMS authentication system lacked basic security features. There was no limit on the number of failed authentication attempts, enabling an exhaustive search attack. Also, SAMS does not separate privileges; all users have equal privileges.

B.5.6 Patches and Software Updates. Although the Chemistry Department occasionally modified SAMS (e.g., to add new features), they did not regularly maintain the software from a security perspective. Numerous updates to software components had not been applied. For example, no one updated the Apache web server since 2018 and it was missing six recent patches. Similarly, no one updated the Microsoft SQL Server 2012 software since 2018, exposing the server to several known vulnerabilities.

B.6 Insider Attack

To teach study participants about the dangers of insider attacks, organizer Sherman (for the second year in a row) secretly recruited a student, Bonyadi, to carry out a benign insider attack against the other study participants. Bonyadi requested the assistance of another student, Golaszewski, who served as a "plant;" Golaszewski's role was simply to go along with Bonyadi's suggestion, lending it credibility in the eyes of the other participants.

To carry out the main project, students needed a way to connect to the sandbox via a *virtual private network (VPN)*. Bonyadi helpfully volunteered to

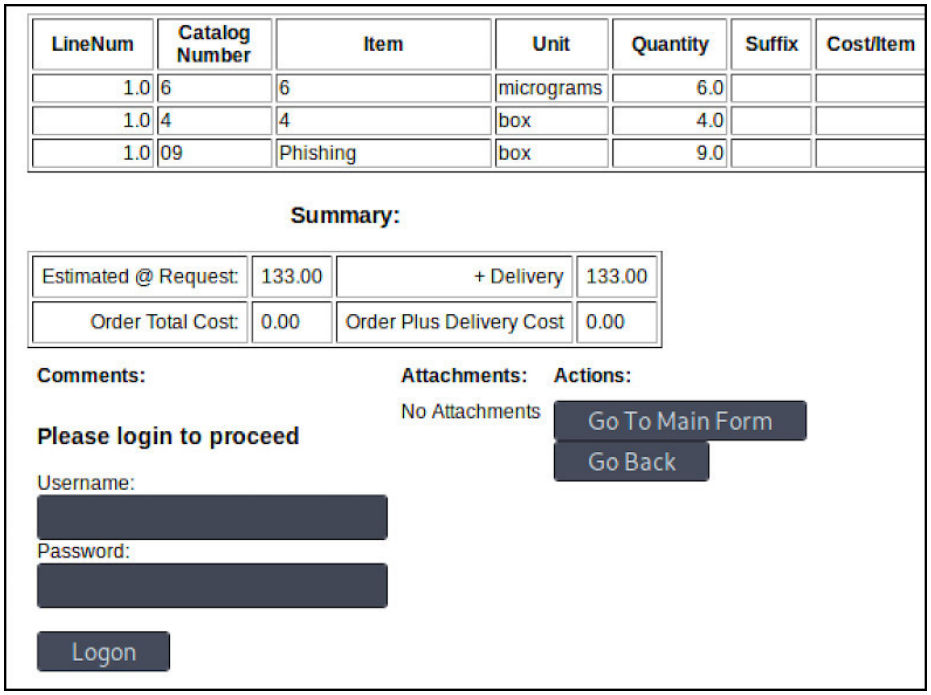

Fig. 24. A cross-site scripting attack on SAMS. The attack inserts a malicious login form into the comment section (lower left) that prompts the user to enter their username and password. The form may execute on SAMS-Web.

write a script to facilitate this connection, making the legitimate script available to participants on a *gold* USB stick. He announced that he had prepared the script and instructed students to use the script on the *gold* stick. In doing so, Bonyadi never overtly lied or mislead anyone.

Later, without explanation, a *pink* stick that contained obfuscated malware appeared next to the *gold* stick. USB sticks are a classic delivery mechanism for malware [44]. This pink stick contained the legitimate script, as well as obfuscated malware that opened a command shell and—in lieu of a truly malicious payload—sent the victim's hostname to a remote server.

Most students used either stick without hesitation. One suspicious student announced their intent to compare the two sticks. Hearing of this plan, Bonyadi secretly sanitized the pink stick before it could be analyzed. After the student found the two sticks to be identical, Bonyadi restored the malware to the pink stick, and the skeptical participant proceeded to use the *pink* stick.

Although participants were elite cybersecurity scholars who expected some type of insider attack, this year's attack compromised 84% of the study participants, 61% of the hosts, and 23% of the virtual machines.

Notably, the two versions of the script created by our insider are, themselves, Shadow IT! Bonyadi's scripts provided useful functionality that was not otherwise easily available, and the scripts were written and deployed without involvement from UMBC's DoIT, and without any oversight from the other stakeholders. The script was helpful and worked well, providing value to the team. One version also intentionally included hidden malicious functionality supporting our insider's task. A truly malicious insider, however, could have inserted a genuinely harmful payload. Furthermore, the script might have contained unintentional vulnerabilities with security ramifications.

Because the exercise was carried out solely for educational purposes within an educational activity, no IRB approval was needed.

B.7 Recommendations

Our highest-priority recommendation is to sanitize and validate all user inputs, ensuring that only relevant and safe inputs are processed. This practice would prevent SQL injection and XSS scripting. For example, when filling a field meant for a purchase amount, a user should be limited to entering numbers. Similarly, all fields should be updated so that data are never interpreted as SQL, Javascript, or any other kind of instructions. All SAMS software and SAMS-supporting components should be kept up-to-date, especially in terms of security patches.

C Survey Instrument

Informed Consent Block

INFORMED CONSENT FOR PARTICIPATION IN RESEARCH ACTIVITIES
DRAFT FOR REVIEW

Thank you for agreeing to participate in our brief survey. Before beginning, please read the informed consent information below. Informed consent refers to the voluntary choice of an individual to participate in research based on an accurate and complete understanding of its purposes, procedures, risks, benefits, and alternatives.

The survey will be completely anonymous and voluntary. We do not collect nor ask for personally identifiable information of any individual who participates in this survey. If you have any questions before completing this survey, please contact the investigator Dr. Selma Gomez Orr by e-mail at sorr1@umbc.edu.

Informed consent:

You must be of 18 years or older to participate in this survey.

This study aims to investigate the extent, source, and type of shadow information technology ("IT") at institutions of higher learning. In addition, the study explores the impact of shadow IT with respect to security vulnerabilities and use of resources, as well as best practices for dealing with shadow IT.

You are being asked to volunteer because of your position in information technology at an institution of higher learning and will be asked to share

information about shadow IT at your institution. It will take approximately 10 minutes to complete this survey.

There are no known risks involved in completing the survey. There are no tangible benefits for completing the survey, but you will have access to all results once the data has been tabulated and analyzed.

Participation is entirely voluntary; you may withdraw from participation at any time.

All data obtained will be anonymous and no personally identifiable information will be collected.

This study has been reviewed and approved by the UMBC Institutional Review Board (IRB). A representative of that Board, from the Office for Research Protections and Compliance, is available to discuss the review process or your rights as a research participant. Contact information of the Office is (410) 455-2737 or compliance@umbc.edu.

After reading the above consent items, please proceed to the questionnaire by selecting your response below acknowledging your consent.

- ◯ Yes
- ◯ No

Survey Questions Block

Institutional Background

Thank you for agreeing to take part in this anonymous survey designed to investigate the impact of shadow Information Technology (“IT”) at institutions of higher learning. Before you begin the technology specific questions, please answer a few institutional background questions to help us understand our respondents.

Which classification of institutions of higher education best applies to your school?

- ○ Doctorate-granting Universities (high level of research activities)
- ○ Master's Colleges and Universities
- ○ Baccalaureate Colleges
- ○ Associates Colleges
- ○ Other

Select all Colleges and Schools at your institution.

- ☐ Architecture School
- ☐ Business School
- ☐ College of Arts and Sciences
- ☐ Education School
- ☐ Engineering School
- ☐ Law School
- ☐ Medical School
- ☐ Public Health School
- ☐ Other (please specify)
- ☐ Do not know

Using headcount, what is the approximate range of the number of students (undergraduate and graduate) enrolled at your institution? Data reported to the Integrated Postsecondary Education Data System provides a helpful reference with detailed enrollment numbers (https://nces.ed.gov/collegenavigator/).

- ○ < 2,000
- ○ 2,000 - 10,000
- ○ 10,001 - 18,000
- ○ 18,001 - 26,000
- ○ 26,001 - 34,000
- ○ > 34,000

Informed Consent Block

INFORMED CONSENT FOR PARTICIPATION IN RESEARCH ACTIVITIES
DRAFT FOR REVIEW

Thank you for agreeing to participate in our brief survey. Before beginning, please read the informed consent information below. Informed consent refers to the voluntary choice of an individual to participate in research based on an accurate and complete understanding of its purposes, procedures, risks, benefits, and alternatives.

The survey will be completely anonymous and voluntary. We do not collect nor ask for personally identifiable information of any individual who participates in this survey. If you have any questions before completing this survey, please contact the investigator Dr. Selma Gomez Orr by e-mail at sorr1@umbc.edu.

Informed consent:

You must be of 18 years or older to participate in this survey.

This study aims to investigate the extent, source, and type of shadow information technology ("IT") at institutions of higher learning. In addition, the study explores the impact of shadow IT with respect to security vulnerabilities and use of resources, as well as best practices for dealing with shadow IT.

You are being asked to volunteer because of your position in information technology at an institution of higher learning and will be asked to share

- [ ] Other (please specify) _____
- [ ] Do not know

Select all Colleges and Schools that you estimate exhibit a **HIGH** level of shadow IT usage at your institution.

- [ ] Architecture School
- [ ] Business School
- [ ] College of Arts and Sciences
- [ ] Education School
- [ ] Engineering School
- [ ] Law School
- [ ] Medical School
- [ ] Public Health School
- [ ] Other (please specify) _____
- [ ] Do not know

Based on the following general departmental categories, select all those that you estimate exhibit a **HIGH** level of shadow IT usage at your institution.

- [ ] Academics
- [ ] Admissions
- [ ] Communications/Marketing
- [ ] Development
- [ ] Facilities and Maintenance
- [ ] Finance
- [ ] Human Resources
- [ ] Information Technology
- [ ] Strategy and Planning
- [ ] Other (please specify) _____
- [ ] Do not know

Of the total number of employee **IT security violations,** approximately what proportion are related to the use of shadow IT?

- ○ Majority
- ○ Equal Parts
- ○ Minority
- ○ None
- ○ Do not know

Generally, how would you compare your institution's cost of dealing with a **shadow IT related security violation** versus other employee security violations?

- ○ Greater than
- ○ Equal to
- ○ Less than
- ○ Do not know

Identify the **single** most often cited justification for using Shadow IT.

- ○ Did not know that it could cause a problem.
- ○ Unaware that it was prohibited.
- ○ Trying to get work done and did not want to wait for IT.
- ○ It is a system we have always used.
- ○ Other (please specify) _____

The below list includes examples of shadow IT used by individuals in their work. Select all that you are aware exist or existed at your institution within the **last three years**.

- ☐ Cloud storage (e.g., DropBox, Google Drive)

- [ ] Unapproved software downloaded by individual users
- [ ] Vendor contracted applications
- [ ] Internal custom-built applications
- [ ] Legacy systems (e.g., obsolete hardware, software, OS, DBMS, etc.)
- [ ] Personal email or social media accounts used for conducting business
- [ ] Unmanaged devices in violation of Bring Your Own Device policies
- [ ] Cloud Computing (e.g., AWS, Azure, GCP)
- [ ] Unauthorized hardware/network infrastructure (e.g., servers, switches, wifi)
- [ ] Other (please specify)

The following four questions look at different ways of categorizing shadow IT. For each category, select the **single choice** under which shadow IT at your institution **most frequently** occurs.

Source: Origin of the shadow IT.

- ○ Externally produced (originating out of house, for example from a vendor)
- ○ Internally developed
- ○ Hybrid - Internally altered or customized external solution

Authority: Level of sanction by IT department for the shadow IT.

- ○ Sanctioned by IT (IT does not manage/maintain/control but is aware of its existence)
- ○ Unsanctioned by IT

Modality: Facet of information technology involved in the shadow IT.

- ○ System Hardware
- ○ Software
- ○ Network Infrastructure
- ○ Data Storage

- ○ Operational Procedure
- ○ Cloud Solution

Motivation: Reason that the shadow IT was introduced into the organization.

- ○ Legacy (either personal or organizational)
- ○ Replacement
- ○ Duplication
- ○ Customization
- ○ Fix (patch, etc.)

From a security perspective, which of the following types of shadow IT represent a **HIGH priority concern** at your institution? Check all that apply.

- ☐ Cloud storage (e.g., DropBox, Google Drive)
- ☐ Unapproved software downloaded by individual users
- ☐ Vendor contracted applications
- ☐ Internal custom-built applications
- ☐ Legacy systems (e.g., obsolete hardware, software, OS, DBMS, etc.)
- ☐ Personal email or social media accounts used for conducting business
- ☐ Unmanaged devices in violation of Bring Your Own Device policies
- ☐ Cloud Computing (e.g., AWS, Azure, GCP)
- ☐ Unauthorized hardware/network infrastructure (e.g., servers, switches, wifi)
- ☐ Other (please specify) _____

Select your greatest concern related to shadow IT.

- ○ Inefficient use of IT staff and resources
- ○ Compromise of data that has not been properly secured
- ○ Unauthorized access to the network

- ◯ Compliance violations
- ◯ Loss of data that has not been properly backed up
- ◯ Other (please specify) _____

In the **last three years**, has there been a cybersecurity incident at your institution that could be traced to shadow IT?

- ◯ Yes
- ◯ No
- ◯ Do not know

Please mark the **dominant** type of shadow IT involved in any security incidents.

- ◯ Cloud storage (e.g., DropBox, Google Drive)
- ◯ Unapproved software downloaded by individual users
- ◯ Vendor contracted applications
- ◯ Internal custom-built applications
- ◯ Legacy systems (e.g., obsolete hardware, software, OS, DBMS, etc.)
- ◯ Personal email or social media accounts used for conducting business
- ◯ Unmanaged devices in violation of Bring Your Own Device policies
- ◯ Cloud Computing (e.g., AWS, Azure, GCP)
- ◯ Unauthorized hardware/network infrastructure (e.g., servers, switches, wifi)
- ◯ Other (please specify) _____

What proportion of all **security incidents** at your institution in the **last three years** would you estimate could be traced to shadow IT?

- ◯ Majority
- ◯ Equal Parts
- ◯ Minority
- ◯ None

If you consider **security incidents** only within the **last year**, how does that proportion change?

- ○ Increases
- ○ Decreases
- ○ No change

Do you spend the majority of your time dealing with shadow IT related issues?

- ○ Yes
- ○ No

Taking into consideration the overall dollars spent and staff resources used on IT at your institution, would you estimate the majority to be related to shadow IT?

- ○ Yes
- ○ No

What is the most effective method for discovering shadow IT at your institution? Choose up to three responses.

- ☐ Procurement process
- ☐ Request for IT support
- ☐ Violation reporting by colleagues/peers
- ☐ Internal review
- ☐ External audit
- ☐ Other

Select all groups with a **HIGH** level of responsibility for handling any shadow IT related problems within your institution.

- ☐ Individual users who set it up
- ☐ Managers who approve it
- ☐ Central IT department
- ☐ Distributed IT departments/groups
- ☐ Product vendors who supplied it

What group do you believe should be **most** responsible?

- ○ Individual users who set it up
- ○ Managers who approve it
- ○ Central IT department
- ○ Distributed IT departments/groups
- ○ Product vendors who supplied it

Many different approaches to shadow IT have been proposed, ranging from embracing it to eliminating it. Choose the rating that **best** describes the current approach at your institution.

Freely Embrace — Strictly Prohibit

0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 ○ 8 ○ 9 ○ 10 ○

Choose the rating that **best** describes your desired approach at your institution.

Freely Embrace — Strictly Prohibit

0 ○ 1 ○ 2 ○ 3 ○ 4 ○ 5 ○ 6 ○ 7 ○ 8 ○ 9 ○ 10 ○

Do you use shadow IT in your daily work?

- ○ Yes

- ○ No

What proportion of your immediate co-workers would you estimate use shadow IT in their daily work?

- ○ Majority
- ○ Equal Parts
- ○ Minority
- ○ None

Based on your personal experience, identify any **highly effective** strategies for dealing with shadow IT. Select all that apply.

- ☐ Establish identity-level control versus device-level control/centralized sign-on
- ☐ Blocklist and/or block access of insecure devices, applications, and cloud services
- ☐ Publish guidelines for devices, cloud services, and third-party applications
- ☐ Create and enforce shadow IT specific policies
- ☐ Offer multi-factor authentication for SaaS applications
- ☐ Limit use of shadow IT to non-data related applications
- ☐ Limit use of shadow IT to non-operational applications
- ☐ Educate/Train the workforce, especially management, on the possible dangers of shadow IT
- ☐ Other (please specify) _____

How do you feel about the following statement related to your job priorities? *"Shadow IT represents one of my top three concerns."*

- ○ Agree
- ○ Disagree

Overall, my concern for shadow IT is best represented by the following word(s):

Additional Comments:

Demographics

Just a few final questions on demographics.

What is your age?

- ◯ < 25
- ◯ 25 - 34
- ◯ 35 - 44
- ◯ 45 - 55
- ◯ > 55

What is your sex?

- ◯ Male
- ◯ Female
- ◯ Non-binary

What is your highest educational level?

- ◯ High School degree
- ◯ Associate degree
- ◯ Bachelor degree
- ◯ Graduate degree

How many years of general IT professional experience do you have?

- ◯ < 5
- ◯ 5 - 10
- ◯ 11 - 20
- ◯ 21 - 30
- ◯ > 30

How many years of cybersecurity-specific professional experience do you have?

- ◯ < 5
- ◯ 5 - 10
- ◯ 11 - 20
- ◯ > 20

What is the predominant focus of your current IT position?

- ◯ Policy and Strategy
- ◯ Operations
- ◯ Do not have an IT related position