Expanding the Scope: An Empirical Approach for Identifying High-Risk Users

Corey Bolger and Tyler Moore
School of Cyber Studies
College of Engineering and Computer Science
The University of Tulsa

Abstract

Risk management is a central aspect of cybersecurity. Organizations spend ever growing sums to better understand the risk present within their systems and networks. One universally agreed upon source of risk is the user. Organizations have developed methods to determine if users are high-impact through their access and classifies these users as high-risk. This research presents an alternative method for identifying users observed to face a higher likelihood of being targeted by attacks. We collected phishing data from within an organization for thirteen months and performed analysis to identify potential factors in the likelihood that a user would receive phishing attempts. We then developed criteria based upon these factors and applied them to users in our dataset. The users identified in this way were then compared against a list of high-impact users provided by organizational IT to understand if this approach provides increased visibility into users that contribute to organizational risk. Initial results show that this approach has the potential to supplement current IT risk decision making methods.

1 Introduction

Organizations protect themselves against hackers using a combination of technologies, policies and procedures, and training [12, 3]. These efforts are typically focused on the data, processes, and personnel that are deemed to be the highest risk [12, 3]. While identifying the risk levels of specific data and processes are straightforward, determining which personnel are high-risk can be more challenging [5].

Conventional strategies often define high-risk users as those with access to sensitive data and those with administrative rights [12, 3]. In this paper, we argue such users can be more accurately considered to be high-impact.

While high-impact users certainly merit protection, there is another aspect of risk that is often overlooked when it comes to identifying users, high-likelihood. Risk is defined as the product of impact and likelihood [7]. In this paper, we explore whether individual users, specific roles, and departments can be categorized as high-likelihood.

Specifically, this research leverages more than a year's worth of incident data in a University setting. We conduct empirical analysis using odds ratios and logistic regressions to quantify how user email characteristics, work role, and department affect whether they are exposed to phishing attacks. We then leverage these results to define criteria for high-likelihood users in this environment. We apply the definition to the user base and evaluate how stable the identification of high-likelihood users remains over time. Finally, we compare the identified high-likelihood users with the University IT department's predefined list of high-impact users. We conclude that this methodology can help expand IT's understanding of phishing risk, both at the partner institution and beyond.

Research Contribution This research developed a process to identify users with a high-likelihood to experience phishing attempts based on empirically observed evidence. Additionally, this methodology was applied in a university IT setting to demonstrate the value of this approach.

Research Question Can high-likelihood users be reliably identified by using organizational cybersecurity data?

2 Background & Related Work

Done well, cybersecurity practices should follow principles of risk management [13, 2]. Organizations are forced to weigh the effectiveness of risk mitigation strategies and the cost of related cyber security controls when assessing risk. One key part of the equation that all organizations have to consider is the user [13, 12, 11]. Users are widely considered to be one of the weakest aspects of any network, and organizations are always trying to identify ways to mitigate this risk [11]. We acknowledge that users themselves should not be blamed for the risks they present to an organization, however they are frequent targets of attack which is why this research focuses on classifying this risk. Traditionally, users with administrator privileges, users with access to sensitive data, or users that are high profile such as executives are seen as the most important users to protect and monitor [12, 3]. From a risk management perspective, these users would be considered high-impact. That is, the impact of those users falling victim to a cyber security incident is much greater than that of other users. While this line of thinking is completely correct, it does fail to consider that many attackers utilize various techniques such as privilege escalation to leverage unprivileged user accounts into much greater access [14]. The intent behind this research is to take inspiration from risk management and take a look at users who may be low-impact but high-likelihood in terms of cyber security incidents. These are users that may be more exposed to cyber security incidents due to their role or department, or simply because they have more risky behaviors when it comes to computer usage. By identifying these users organizations would be able to consider additional cyber security controls such as focused training or additional protections for these users, mitigating risks that otherwise could go unchecked.

Researchers have been consistently working to develop better methods to protect users from threats that specifically target them, specifically phishing and spear-phishing [16, 8, 15, 1]. While there have been numerous developments in this area, there has not been as much research into how to best target these trainings and other protective measures to the users that need them the most [17]. Phishing testing is common throughout the industry, but recent research has begun to doubt the

effectiveness of this type of testing [9, 10]. Users who fall for phishing tests don't always perform worse than other users when observing real phishing incidents, and phishing training conducted as a result of failing a phishing test has not proven to consistently make users better at detecting phishing [9, 17, 18, 19]. This leaves the door open for other methods of identifying users who may need additional training or additional cyber security controls to protect them from falling for these user targeted cyber attacks.

3 Data Collection Methodology

To conduct the analysis several sources of data were collected. This study was found to be exempt by the Institutional Review Board under protocol number 24-29. To protect users from harm, all data processed was anonymized prior to analysis.

3.1 Response Variable: Incident Data

First, incident data from the email filtering system, in this case Microsoft Defender Endpoint, was collected from January 1, 2024 through February 3, 2025. As defined by Howard and Longstaff [4], we consider an incident to be "a group of attacks that can be distinguished from other attacks because of the distinctiveness of the attackers, attacks, objectives, sites, and timing." Over the course of this data collection period 4,057 unique incidents were collected. Because the focus of this research was on identifying high-likelihood users within an organization, student data was filtered so that only employee data remained. After filtering, 2,285 unique incidents remained.

This data contained information regarding investigations, both system generated and manual, into phishing attempts. These investigations did not necessarily indicate that a phishing attempt was successful, and in fact the data available did not include clear indications whether these incidents were in fact successful at any point. The data did include indications of whether malicious links or attachments were found present in the emails that were being investigated, the time of detection or report, the duration of the investigation, and the user targeted by the attempt.

3.2 Explanatory Variables

The assessed population consisted of 1,261 unique users. We consider two types of explanatory variables: (1) attributes of the email address and (2) user characteristics.

We observed two email attributes that could affect the likelihood of appearing in incidents.

Aliased The University issues email addresses to employees following the format of xxx111@university.edu. These addresses are not easily guessable and are not typically made publicly available. Users are permitted the use of an email alias, typically in the form of firstname-lastname@university.edu, though not always. The University has chosen to obfuscate email addresses to make them harder to guess for security purposes. To assess the impact that using an aliased email address has on incident likelihood we made a list of all user emails that did not follow the typical format.

Breached All users were then checked against the HaveIBeenPwned database to determine if their email was present in at least one breach [6]. Being present in this database is a strong indication that the email address is publicly accessible to cybercriminals. This criteria was included because we anticipate that many criminals sending phishing emails will source the email addresses from prior breaches. This does not indicate that the account credentials have been compromised, only that the email address is present in publicly accessible databases.

Organizational Attributes A list of all users, the *department* they belonged to, and their *role* was collected using the organizational data available in Microsoft Outlook. 799 unique roles and 128 unique departments were identified. To aid in analysis all roles were reviewed by the authors and placed into one of five categories: administration, staff, support staff, athletics staff, and faculty. Individual departments were also combined into one of 18 different categories based upon the overall organizational structure.

Additionally, we obtained a list of users marked as high-risk by the University IT department to compare against.

4 Empirical Analysis

We now analyze the collected data to illustrate how incident count varies by the characteristics identified above.

4.1 Incident Prevalence

Not all users experienced an incident during the collection period. Of the 799 roles, 420 experienced at least one incident during the collection period. The mean incident count for users over the course of one year was less than two. Over half of the users did not experience an incident during this period, resulting in a median incident count of zero. There were several outliers among the users, including one user who experienced 161 unique incidents during the data collection period. Of users who experienced an incident, 93% experienced fewer than 10. Only 29 out of 1,261 users experienced ten or more incidents. Figure 1 plots a cumulative distribution function (CDF) of incident count. Most users receive fewer than ten incidents over the course of a year, with only a small number of users likely to experience greater than ten incidents.

Because over half of the users experience zero incidents, we will frequently distinguish between users who received zero incidents and those experiencing at least one.

4.2 Email Address Attributes Affecting Likelihood

We first examine how email characteristics affect the likelihood of being targeted by attackers. Table 1 shows the breakdown of incidents, split by the email address attributes of interest. It also includes odds ratios, which clearly demonstrate that both the presence of email aliases and appearing in a breached dataset are associated with experiencing incidents. In particular, having one or both of these attributes more than triples the odds of being targeted.

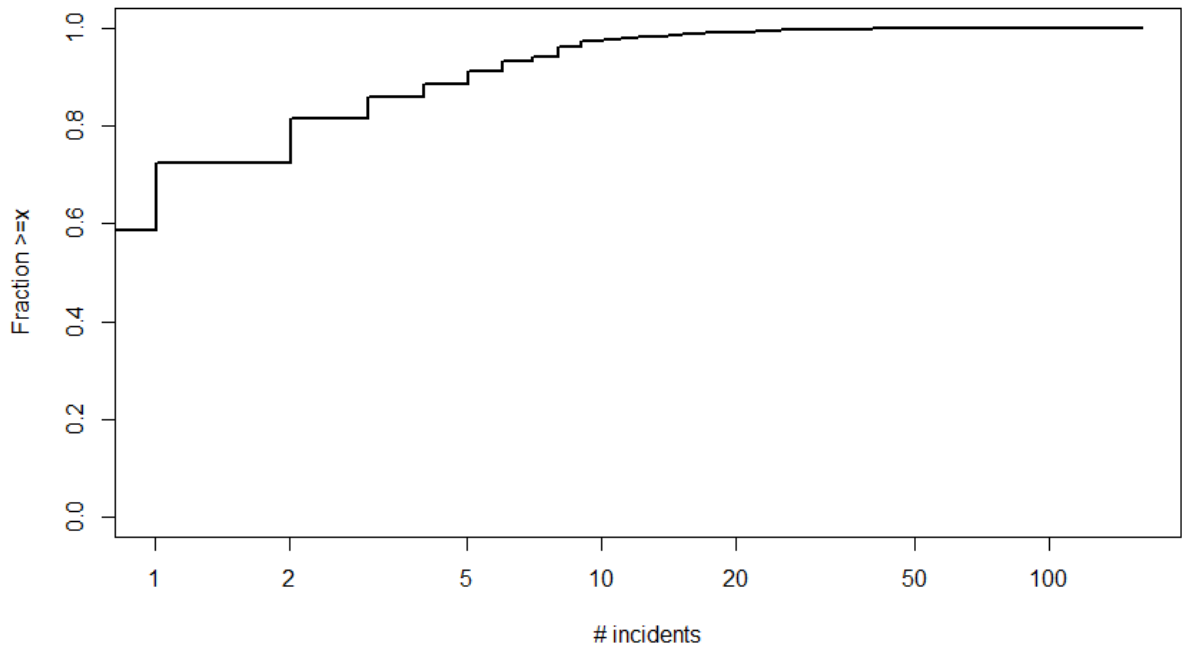

Figure 1: CDF incident count per user.

	Incidents > 0		**No Incidents**					
Attribute	**Exposed**	**Not Exposed**	**Exposed**	**Not Exposed**	**Odds Ratio**	**P-Value**	**CI Low**	**CI High**
Aliased	435	86	436	304	3.52	0.000	2.69	4.65
Breached	245	276	152	588	3.43	0.000	2.68	4.40
Aliased & Breached	237	284	137	603	3.67	0.000	2.85	4.73

Table 1: Odds ratios for aliased and breached emails.

4.3 Organizational Attributes Affecting Likelihood

Next we looked at the impact of role and department on a user's likelihood to receive phishing emails. This is displayed in Table 2 where we can see several stand out roles and departments. Administration has three times greater odds of being targeted than others, while faculty experience a 46% increase. On the other hand, athletics staff were much less likely to be targeted. Among departments IT and Admissions are more likely to be targeted, while Law, the College of Health and Natural Sciences, and Athletics are less likely.

While this analysis does not give us explicit reasons for these roles and departments that stand out, there are some plausible reasons for the increased odds. For the roles, it is unsurprising that users with an administrative role experience higher likelihood of receiving phishing attacks. These users likely have some type of access or position that makes it more attractive for attackers to compromise their accounts. For faculty, it is much more likely that users in these roles have emails that are publicly available.

Category	Incidents per User	Users with Incidents	Total Users	%	Odds Ratio	95% CI
Role						
Administration	2.50	106	165	64%	**2.94**	**(2.10-4.16)**
Faculty	1.44	210	577	36%	**1.46**	**(1.16-1.83)**
Staff	2.17	138	329	42%	0.96	(0.75-1.25)
Support Staff	1.98	40	84	48%	0.76	(0.49-1.19)
Athletics Staff	0.95	27	106	25%	**0.46**	**(0.29-0.71)**
Department						
Human Resources	2.80	7	10	70%	3.25	(0.87-15.97)
Finance	2.67	10	15	67%	2.83	(0.98-9.36)
IT	3.31	20	32	63%	**2.41**	**(1.18-5.15)**
Admissions	2.29	20	34	59%	**2.06**	**(1.03-4.23)**
Risk Management	1.21	15	44	34%	1.37	(0.73-2.66)
Arts & Sciences	1.85	81	185	44%	1.13	(0.82-1.54)
College of Business	1.79	31	71	44%	1.11	(0.68-1.79)
Eng. & Comp. Sci.	1.94	62	146	42%	1.05	(0.74-1.50)
Campus Safety	1.60	4	10	40%	0.96	(0.23-3.47)
President	2.04	57	125	46%	0.82	(0.57-1.20)
Marketing & Comm.	4.07	5	14	36%	0.80	(0.24-2.37)
Univ. Adv. & Alumni	1.67	16	33	48%	0.74	(0.37-1.50)
Provost	1.20	67	137	49%	0.71	(0.50-1.01)
Law	1.01	28	92	30%	**0.60**	**(0.38-0.94)**
Health & Nat. Sci.	1.00	58	190	31%	**0.58**	**(0.41-0.80)**
Athletics	1.02	28	100	28%	**0.53**	**(0.33-0.82)**
Inst. Research	1.00	1	4	25%	0.52	0.02-4.45)
Research & Econ. Dev.	12.11	11	19	58%	0.51	(0.19-1.28)

Table 2: Incident rates, percentages, and odds ratios by role and department.

For the departments, IT being more targeted than other departments is also unsurprising due to the nature of those roles. Admissions being more targeted is harder to understand, though it may also be due to users in those roles being more public facing. It is difficult to get a complete picture of all the information without looking at role, department, alias, and breach together, so in the next section we will look at a regression that includes all factors to better understand these interactions.

4.4 Regression Analysis

The odds ratios presented above indicate which attributes correlate with incident prevalence. To disentangle the effects of these explanatory variables, we constructed a series of logistic regressions. The dependent variable is a Boolean that is true if a user experienced at least one phishing incident and false otherwise.

Table 6 presents the results. Regression 1 uses a single explanatory variable, *Aliased*. With a

Definition: High likelihood
A user is considered high-likelihood if they meet one of the following criteria:
Criteria 1: **At least 4 of the following 5:** - A raw incident count in the top 10%. - Present in a breach. - An aliased email. - A department with a significant risk factor in the regression. - A role with a significant risk factor in the regression.
OR
Criteria 2: - A raw incident count at least two standard deviations above the mean.

Table 3: High-likelihood user definition.

pseudo R^2 of 0.0937, this simple regression does explain some of the variance. Regression 2 adds *In Breach*, which is also highly significant. Adding this variable increases the explained variance by 50% to 0.1419. Regression 3 adds departments, while the final regression 4 also adds role. This final regression has a pseudo-R^2 of 0.1999.

It is worth noting that in all four regressions *Aliased* and *In Breach* remain significant. In the final regression, *In Breach* has an odds ratio of 2.6 and *Aliased* has 2.32, which means that the odds more than double with the addition of each characteristic, regardless of role or department.

In the final regression 4, the departments of IT and Finance both experience statistically significantly higher odds of attack. The odds increase by 182% for IT employees and by 237% for workers in the Finance department. Meanwhile, employees in the College of Business face 21% lower odds.

Among roles, workers in Administration are much more likely to be targeted, with an odds ratio of 12.1. Similarly, the odds that support staff will be targeted increase by 745%.

The particular results found here, which may not generalize beyond the University under study, are interesting but of limited direct importance. Instead, what is noteworthy is that the process we have developed illustrates how data can be collected and analyzed in an enterprise to identify what employee attributes are associated with higher targeting by attackers. This information can then be utilized to inform rules to proactively identify high-likelihood users that may require additional oversight, training and protection. We next describe a process for doing precisely that.

5 Method for Identifying High-Likelihood Users

Following the analysis, we developed a definition of *high-likelihood*, examined the stability of the definition over time, and compared these users to externally identified high-impact users.

Appearances	User Count	Percentage
0	1,149	91.1%
1	82	6.5%
2	16	1.3%
3	9	0.7%
4	5	0.4%

Table 4: High-likelihood user counts by number of quarters.

Quarter	Number of Users
Q1	72
Q2	38
Q3	22
Q4	29
2 or more quarters	30

Table 5: Quarterly high-likelihood user analysis.

5.1 Defining High Likelihood

Table 3 specifies criteria for defining high likelihood that directly follows from the results of the empirical analysis that identify characteristics associated with receiving phishing emails. The roles and departments found to significantly impact the likelihood of experiencing a phishing attempt were included, as well as the aliased email and presence in a breach risk factor. We also included a second criteria to account for users that receive a large number of incidents, regardless of the other characteristics.

For the definition to be helpful, it should identify some users, but not so many that all are deemed high-risk. Requiring 4 out of 5 categories to be met helps limit the number of users falling into the category. The second criteria was added because it was observed that a small number of users experience many more phishing attacks than the rest of the population.

5.2 High-Likelihood Users over Time

To test the effectiveness of these criteria we applied them to users on a quarterly basis. We then categorize users as high likelihood and compared the users present in each quarter. Table 4 shows the number of times users were found to appear in a quarter. The vast majority of users (91%) did not meet the definition. 82, or 6.5%, met the criteria exactly once, while 30 users (2.4%) appeared in two or more quarters. We focus on these users in particular.

Table 5 shows the number of users appearing in each quarter, along with the count of users who appeared in two or more quarters. A full list of the users who qualified to be labeled as high-likelihood is available in Table 7.

These results indicate that the criteria used are sufficient to identify a reasonably sized number of users who are more likely to experience phishing attempts throughout the year.

5.3 Comparison to High-Impact Users

To further determine if this approach could aid the IT department in identifying high-risk users, we compared our list of 30 high-likelihood users against a list of 29 high-impact users provided by the IT department. The list of high-impact users is available in Table 8.

We can apply the definition of risk to identify different risk levels for users. Users present in both the high-likelihood list and the high-impact list were truly *high* risk, whereas users present in either the high-likelihood list or the high-impact list (but not both) can be thought of as *medium* risk. Finally, users present in neither list can be labeled *low* risk. Six users were found to be high risk, 53 users were found to be medium risk, and the remaining 1,196 users were found to be low risk. High-risk users are identified in Tables 7 and 8.

6 Concluding Remarks

Users are frequently the target of cyber criminals seeking to gain access to enterprises. In order to better protect against these cyber threats, it is imperative that we expand our understanding of which users are most at risk of experiencing a cyber attack within our organizations. In this paper, we have constructed and analyzed a dataset of phishing incidents spanning more than a year at a University. Through empirical analysis, we identified factors associated with higher incidence. This includes attributes of email addresses that make it more likely to be attacked, such as guessability and whether the address had previously been leaked. It also includes attributes of the employee's place in the organization, namely department and role.

The evidence shows, for the organization under study at least, that users in specific roles and departments do have increased likelihood of experiencing phishing attempts beyond those roles considered high-impact through conventional means. It is reasonable to expect that while the details could vary, analysis following a similar approach in different organizations could also find characteristics associated with greater attack likelihood. Hence, we advocate identifying these high-likelihood users based upon the characteristics identified in the empirical analysis. We demonstrate the value of doing so for the data at hand.

There are several limitations with this study. The data that was used for the analysis was limited to only the output of what is available in Microsoft Defender Endpoint. While this data was helpful, certain details like the determination of whether a phishing incident was legitimate or benign was unavailable. A more robust dataset, notably one that considers additional forms of attack, could further bolster the results in this study. Future research in this area should be conducted by utilizing the methods outlined in this paper against other organizations.

Additionally, more investigation is required into the presence of drift when identifying high-likelihood users. The method to identify high-risk users is considerably more valuable if an identified user remains at an elevated likelihood of attack for some time.

The methodology outlined in this paper shows that it could be worthwhile for IT departments to consider not just high-impact users but also high-likelihood users when developing additional security controls and targeted security training. By expanding the internal definition of high-risk, IT departments may be able to better protect the organization by utilizing the controls already in place to protect high-impact users for high-likelihood users as well. In addition, the identification of users who are both high-impact and high-likelihood may provide incentive for IT departments

to add additional security measures to these accounts. Expanding the understanding of user risk in this way could benefit IT departments in protecting the organization.

Acknowledgments

The authors acknowledge support from Tulsa Innovation Labs via the Cyber Fellows initiative, the University of Tulsa, the University of Tulsa IT personnel, and Logan Quirk.

References

[1] Luca Allodi, Tzouliano Chotza, Ekaterina Panina, and Nicola Zannone. The need for new antiphishing measures against spear-phishing attacks. *IEEE Security & Privacy*, 18(2):23–34, 2019.

[2] CompTIA. What is information technology risk management? `https://www.comptia.org/content/guides/what-is-information-technology-risk-management`, 2022. Accessed: 2/12/2025.

[3] International Organization for Standardization (ISO). Iso/iec 27001:2022 - information security, cybersecurity, and privacy protection — information security management systems — requirements. `https://www.iso.org/standard/82875.html`, 2022.

[4] John D Howard and Thomas A Longstaff. A common language for computer security incidents. Technical report, Sandia National Lab.(SNL-NM), Albuquerque, NM (United States); Sandia, 1998.

[5] Wenjing Huang, Sasha Romanosky, and Joe Uchill. Beyond technicalities: Assessing cyber risk by incorporating human factors. *WEIS 2024 Proceedings*, 2024.

[6] Troy Hunt. Have I been pwned: Pwned websites. `https://haveibeenpwned.com/`, 2025. Accessed: 10/15/2024.

[7] ISACA. IT asset valuation, risk assessment, and control implementation model. *ISACA Journal*, 3, 2017. Accessed: 02/13/2025.

[8] Daniel Jampen, Gürkan Gür, Thomas Sutter, and Bernhard Tellenbach. Don't click: towards an effective anti-phishing training. A comparative literature review. *Human-centric Computing and Information Sciences*, 10(1):33, December 2020.

[9] Daniele Lain, Kari Kostiainen, and Srdjan Čapkun. Phishing in organizations: Findings from a large-scale and long-term study. In *2022 IEEE Symposium on Security and Privacy (SP)*, pages 842–859. IEEE, 2022.

[10] Matt Linton. On Fire Drills and Phishing Tests, 2024. `https://security.googleblog.com/2024/05/on-fire-drills-and-phishing-tests.html`.

[11] Kevin D Mitnick and William L Simon. *The art of deception: Controlling the human element of security*. John Wiley & Sons, 2003.

[12] National Institute of Standards and Technology (NIST). Cybersecurity framework (CSF) 2.0. https://www.nist.gov/cyberframework, 2024. Framework for Improving Critical Infrastructure Cybersecurity, Version 2.0.

[13] National Institute of Standards and Technology. Risk management framework (RMF). https://csrc.nist.gov/projects/risk-management/about-rmf, 2020. 2/12/2025.

[14] Praveen. What are privilege escalations? attacks, understanding its types & mitigating them. https://www.eccouncil.org/cybersecurity-exchange/penetration-testing/privilege-escalations-attacks/, 2023. Cybersecurity Exchange.

[15] Antonio San Martino and Xavier Perramon. Phishing secrets: History, effects, countermeasures. *Int. J. Netw. Secur.*, 11(3):163–171, 2010.

[16] Orvila Sarker, Asangi Jayatilaka, Sherif Haggag, Chelsea Liu, and M. Ali Babar. A Multivocal Literature Review on challenges and critical success factors of phishing education, training and awareness. *Journal of Systems and Software*, 208:111899, February 2024.

[17] Steve Sheng, Mandy Holbrook, Ponnurangam Kumaraguru, Lorrie Faith Cranor, and Julie Downs. Who falls for phish? a demographic analysis of phishing susceptibility and effectiveness of interventions. In *Proceedings of the SIGCHI conference on human factors in computing systems*, pages 373–382, 2010.

[18] David Shipley. (25) The hard truths about phishing simulation click rates | LinkedIn, 2020. https://www.linkedin.com/pulse/hard-truths-phishing-simulation-click-rates-david-shipley/.

[19] Omer Taran. Assessing Your Phishing Risks: More Than Just Click Rate, 2018. https://cyberready.com/phishing-attacks/phishing-simulation-training-right-metrics.

A Appendix

	Incidents Occurred			
	(1)	(2)	(3)	(4)
Aliased	1.260***	0.929***	0.858***	0.845***
	(0.140)	(0.148)	(0.154)	(0.156)
In Breach		0.935***	0.967***	0.957***
		(0.134)	(0.141)	(0.143)
Engineering & Computer Science			0.109	0.496
			(0.384)	(0.427)
College of Business			0.308	0.793*
			(0.421)	(0.481)
Law			−0.283	0.050
			(0.414)	(0.449)
University Adv. & Alumni			0.472	0.026
			(0.500)	(0.521)
Admissions			0.670	0.502
			(0.495)	(0.508)
Arts & Sciences			0.055	0.533
			(0.373)	(0.431)
Provost			0.460	0.501
			(0.383)	(0.388)
Health & Natural Sciences			−0.147	0.320
			(0.377)	(0.437)
President			0.516	0.537
			(0.388)	(0.396)
Information Technology			0.933*	1.037**
			(0.509)	(0.515)
Human Resources			1.292*	1.228
			(0.778)	(0.790)
Inst. Research & Data Analytics			−0.493	−0.504
			(1.206)	(1.221)
Finance			1.156*	1.217*
			(0.668)	(0.672)
Campus Safety			0.314	0.234
			(0.760)	(0.775)
Marketing & Communications			0.119	0.210
			(0.680)	(0.682)
Research & Economic Development			0.776	0.701
			(0.610)	(0.620)
Athletics			−0.329	1.538
			(0.410)	(1.141)
Administration				2.493**
				(1.083)
Faculty				1.373
				(1.100)
Support Staff				2.135*
				(1.106)
Staff				1.714
				(1.085)
Constant	−1.263***	−1.330***	−1.463***	−3.376***
	(0.122)	(0.123)	(0.352)	(1.135)
Observations	1,261	1,261	1,261	1,261
Log Likelihood	−809.478	−784.745	−767.724	−753.651
Pseudo R^2	0.0937	0.1419	0.174	0.1999

Note: *p<0.1; **p<0.05; ***p<0.01

Table 6: Regression Model

Role	Department	# Quarters	# Incidents	In Breach	Aliased
	High-Likelihood Only				
Faculty	Engineering & Computer Science	4	70	✓	✓
Administration	Information Technology	4	25	✓	✓
Staff	Research & Economic Development	4	161	✓	✓
Support Staff	Admissions	3	16	✓	✓
Staff	President	3	38	✗	✓
Administration	University Advancement & Alumni Engagement	3	10	✓	✓
Faculty	Arts & Sciences	3	19	✓	✓
Administration	Provost	3	6	✓	✓
Support Staff	Arts & Sciences	3	19	✗	✓
Staff	Marketing & Communications	3	24	✗	✓
Administration	President	3	23	✗	✓
Administration	Research & Economic Development	2	6	✓	✓
Administration	Human Resources	2	4	✓	✓
Staff	Research & Economic Development	2	17	✗	✓
Faculty	Engineering & Computer Science	2	9	✓	✓
Support Staff	President	2	7	✓	✓
Support Staff	Engineering & Computer Science	2	7	✓	✓
Support Staff	Arts & Sciences	2	10	✗	✓
Administration	Risk Management	2	17	✓	✓
Administration	College of Business	2	4	✓	✓
Faculty	Arts & Sciences	2	13	✓	✓
Staff	Information Technology	2	11	✗	✓
Staff	President	2	13	✗	✓
Staff	Information Technology	2	8	✓	✓
	High-Likelihood & High-Impact				
Administration	Finance	4	5	✓	✓
Administration	Information Technology	4	0	✓	✓
Administration	Campus Safety	3	11	✓	✓
Administration	University Advancement & Alumni Engagement	2	7	✓	✓
Administration	Information Technology	2	6	✗	✓
Staff	Finance	2	5	✓	✓

Table 7: High-likelihood users appearing in two or more quarters.

Role	Department	# Quarters	# Incidents	In Breach	Aliased
	High-Impact Only				
Administration	Provost	0	0	✓	✓
Administration	Institutional Research & Data Analytics	0	4	✗	✓
Administration	Research & Economic Development	0	3	✓	✓
Administration	President	1	4	✓	✓
Administration	President	0	4	✗	✓
Administration	Finance	1	6	✗	✓
Administration	President	0	3	✓	✓
Administration	President	0	0	✗	✓
Administration	Arts & Sciences	0	0	✓	✓
Administration	Admissions	0	3	✓	✓
Faculty	Provost	0	1	✗	✓
Administration	Provost	0	0	✗	✓
Administration	President	0	1	✓	✓
Administration	Marketing & Communications	0	0	✗	✓
Administration	Human Resources	0	1	✗	✓
Administration	Provost	0	1	✓	✓
Faculty	Arts & Sciences	0	1	✓	✓
Administration	President	0	2	✗	✓
Administration	Health & Natural Sciences	1	9	✓	✓
Administration	Law	0	0	✗	✓
Support Staff	President	0	1	✓	✓
Administration	Engineering & Computer Science	0	2	✗	✓
Administration	President	0	1	✗	✓
	High-Likelihood & High-Impact				
Administration	Finance	4	5	✓	✓
Administration	Information Technology	4	0	✓	✓
Administration	Campus Safety	3	11	✓	✓
Administration	University Advancement & Alumni Engagement	2	7	✓	✓
Administration	Information Technology	2	6	✗	✓
Staff	Finance	2	5	✓	✓

Table 8: High-Impact Users provided by IT