WHAT'S IN YOUR POLICY? AN ANALYSIS OF THE CURRENT STATE OF INFORMATION SECURITY POLICIES IN ACADEMIC INSTITUTIONS

Complete Research

Jake Weidman, The Pennsylvania State University, State College, PA, jyw5163@ist.psu.edu
Jens Grossklags, Technical University of Munich, Munich, Germany, jens.grossklags@in.tum.de

Abstract

Colleges and universities across the United States have seen data breaches and intellectual property theft rise at a heightened rate over the past several years, partly driven by the historically open nature of academic institutions. An integral step in the first line of defense against various forms of attacks, both in the corporate and academic space, are (written) security policies designed to prescribe the construction and function of a technical system, while simultaneously guiding the actions of individuals operating within such a system. Unfortunately, policy analysis and development in the context of these security policies is an insufficiently discussed topic in many academic communities, with very little research being conducted in this space. Consequently, this work aims to assess the current state of information security policies as it exists within the top 200 universities and colleges in the United States, with the goal of identifying important features and general attributes of these documents, as well as to build a foundation for further research. To summarize high-level results, we find that only 54% of the top 200 universities had publicly accessible information security policies, and the policies that were examined lacked consistency. Additionally, we find that while shorter policies were more difficult to read, that they often contained more information, while longer policies contained significantly less practically relevant content.

Keywords: Security Policies, Qualitative Analysis, Mixed Methods, Policy Analysis, Academic Institutions

1 Introduction

Data breaches in the corporate sector have been on the rise for several years, with companies such as Yahoo (Fahey and Wells, 2016), Target (McGrath, 2014), MySpace (Perez, 2016), and many more suffering highly publicized and damaging data breaches. However, corporate institutions are not the only ones affected by this rise in security incidents. Though discussed substantially less by mainstream news sources, universities and colleges have become an increasingly popular target for cyber-attackers. Notable university data breaches include the University of Maryland (Svitek and Anderson, 2014), North Dakota University (Greenberg, 2014), UC Berkeley (Gilmore, 2015), Michigan State University (Simon, 2016), and Stanford University (Hayward, 2013), among many others. According to the Privacy Rights Clearinghouse (2017), 789 academic institutions in the United States have suffered data breaches since 2005. To put this in perspective, an estimated 5436 data breaches are estimated to have occurred across all domains (academic, corporate, government, etc.) since 2005. That is, academic data breaches have represented 14.5% of reported data breaches since 2005; a non-trivial percentage.
While data breaches have become regrettably commonplace, newer forms of cyber-attacks have begun to emerge. A prime example of this is ransomware, a specific type of malware which encrypts users' data on compromised systems, making it unusable unless a monetary ransom is paid (Laszka, Farhang,

and Grossklags, 2017). In May of 2017, a widespread ransomware attack, dubbed 'WannaCry', affected over 200,000 victims in 150+ countries. Numerous organizations across all disciplines were impacted by this attack, including several United States colleges and universities (Stephenson and Johnston, 2017). This specific ransomware attack is noteworthy from a security policy perspective, as a high number of compromised systems were found to be using outdated operating systems and equipment, accompanied by a lack of accessible backup systems within affected organizations (Brewer, 2016; Patyal et al., 2017). One of the commonalities between ever-occurring data breaches and ransomware attacks are some pre-emptive measures required to prevent a number of attack vectors used to compromise these organizations. In some cases, these problems can be solved via security technology implementations, such as two-factor authentication (Weidman and Grossklags, 2017). In other scenarios, however, deeper organizational problems may exist that can only be addressed through policies. In a recent cybercrime study by the Ponemon Institute (2016), 4 of the 7 key takeaways refer to the *construction and implementation of strong technology and information policies*.

Employees have previously been surveyed on the topic of security policies within organizations, and have noted that these policies are very important to their organizations (Carayon, Kraemer, and Bier, 2005), and therefore impact them as well. However, for these policies to be successful, they must contain actionable content and be understandable by those affected by them, as policy documents are only one component in a complex sociotechnical system within organizations. The overarching argument is that a well-formed, thorough policy has the potential to prevent or help to mitigate problems before they occur not just from a technical perspective, but from a human perspective as well. Thus, topics relating to information security (and specifically security policies) within organizations are inherently of benefit to the larger information systems community, as work in this space involves understanding how these formal, notoriously rigid policies are interpreted and acted on by human actors within a system.

A key issue in this space, however, is that literature involving implementations of modern security policy is sparse at best, possibly due to difficulties in obtaining what many organizations believe to be sensitive information (Kotulic and Clark, 2004).[1] Corporations typically present public-facing policy as it pertains to consumer rights, in particular, regarding the use of consumer data. Analyses have been provided for documents including privacy policies (Jensen and Potts, 2004), End User License Agreements (Grossklags and Good, 2007), marketing claims (Nochenson and Grossklags, 2014), and consumer-oriented fraud policies by banks (Becker et al., 2016), among others. However, (internal) corporate security policies, which guide the construction and implementation of technical systems, as well as mandate employee action, are often not publicly, or even upon request from academics, exposed to anyone who is not an employee of that organization. Thus, while organizations may permit individuals to attempt to breach their security through white hat hacking, or via other programs such as bug bounties (Laszka et al., 2018), they do not share the same degree of openness regarding their security policies.

In contrast to corporate organizations, academic institutions often do publicly share their internal policies regarding technology and user behavior on their networks. Similar to corporate organizations, academic institutions also employ and serve a large number of users in many cases (i.e., faculty, staff, students, third-party vendors), and also produce a large amount of valuable intellectual property. Therefore, we argue that academic institutions, including colleges and universities, are an apt choice to study the current state of technical policy to determine whether or not these institutions are doing enough to protect themselves, as well as their employees and students, from cyber-attacks. More specifically, we situate this paper as the beginning of a line of research that will attempt to probe the current state of technical policy, beginning with academic institutions. To accomplish this, we assemble a corpus of information security policies (if discoverable) from the top 200 universities in the United States. To the best of our knowledge, no such corpus currently exists. Using this new resource, we conduct a series of qualitative and quantitative

[1] Following the definition from the National Institute of Standards and Technology (NIST) (1995), we refer with *security policy* or *technical policy* to (written) "documentation of computer security decisions" within an organization ranging from senior management's directives down to system-specific stipulations.

analyses on this corpus of texts to answer several research questions:

- RQ1: What is found within information security policies at universities in the United States? More specifically, what is the average length, reading complexity, and content contained within these policies?
- RQ2: Does the occurrence of certain organizational factors or items in an information security policy correlate with the appearance of other items? For example, are universities that suffered from a data breach more likely to have a CISO?

With this analysis, we aim to create an exploratory baseline work, which not only serves as a first assessment of written security policy in organizations, but also as a springboard to elicit more widespread study and attention from the academic community in this research space.

2 Related Work

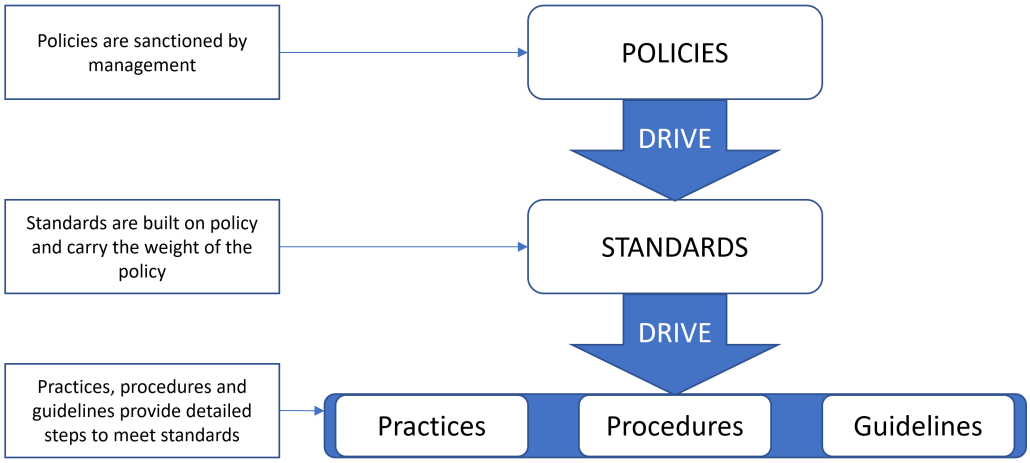
As literature in the space of security policy analysis is surprisingly sparse, we will ground readers by first providing some background on policy analysis and organizational policy design, prior to transitioning into a discussion of the general impact that strong policy has within organizations, and our strategy to address the problem space of security policy.

2.1 Organizational Policy

Policy analysis, in its simplest form, is the production and application of policy itself (Lasswell, 1971). Perhaps more concretely, it is "a process of multidisciplinary inquiry aiming at the creation, critical assessment, and communication of policy-relevant information" (Dunn, 2015). In the context of this work, we seek to provide a critical assessment of a number of policies to aid in the improvement and creation/production of new policy. Unlike many forms of science or frameworks, policy analysis is not only descriptive in nature, but is normative as well. That is, it includes judgments by the analyzer about what a particular policy or policies *should be*, as opposed to just what is (Dunn, 2015; Friedman, 1953). Although this concept may give pause to the scientific community, as one analyst's interpretation of policy could be different than another, this normative component of policy analysis is often encouraged (Robert and Zeckhauser, 2011), as dissent among analysts is believed to ultimately create more grounded and effective policy (Sabatier and Weible, 2007). As part of the policy analysis process, understanding the space in which policies exist in an organization is also important.

Our next step is to briefly discuss the textbook advice for a security policy framework. As shown in Figure 1, policies (more specifically referred to as *information security policies* or *enterprise security policies*) serve as the highest level of formal documentation and instruction within organizations. Ideally, a policy document is designed to set the strategic direction, scope, and tone for an entire organization regarding a particular topic, providing justifications for the way things are done, as well as to comply with any legal requirements. In the scope of information security policies, this would generally include the description and development of an organization's information security program, as well as detail IT operations and key individuals such as a CISO or CIO, who would be responsible for the development and maintenance of network resources. These high-level information security policies are then supported and expanded upon by standards and procedures or guidelines. In this space, standards are designed to provide specific technical requirements required for individual systems, or data access levels, and often include items such as detailed password requirements, encryption specifications, backup directives, and more. Lastly, at the lowest level, procedures and guidelines exist to provide the most detailed instructions on carrying out directives found in policies and standards. An example of a guideline in the information security space would be a step-by-step series of instructions which would show employees, students, and others, how to configure and execute a scheduled backup on their personal, or work-owned, computer.

Figure 1. Policies, Standards, and Practices (figure adopted from Whitman and Mattord, 2013).



To complicate the space, a second type of high-level policy, referred to as an *issue-specific policy* is sometimes proposed as a constituent part of a policy framework. Issue-specific policy also addresses organizational interests at a high level, but then proceeds to provide a series of detailed policy items, which may act more like a security standard or guideline. While these documents contain more details, they are perhaps more confusing to understand due to their mixed nature (Whitman and Mattord, 2013). In some organizations, issue-specific policies may be the highest-level policy documents that exist.

To the best of our knowledge, there is only limited work that examines a sizable sample of written information security policies currently in place, or explores more detailed questions such as what percentage of organizations use enterprise or issue-specific policies in the information security space, and whether either method is more effective when implemented.

2.2 Impact of Policy

Policy within any organization continues to be a critical component of that organization's infrastructure. When done correctly, various policies should dictate the function of an entire organization, as well as of those individuals operating within it. One of the principle goals of any organization is to protect its own assets; a topic almost entirely addressed by technical policy, which guides the technical and non-technical security operations of an organization. As a result of this, technical security and privacy issues have been a dominant concern of many administrators for years (Luftmann and Kempaiah, 2008). However, little research has been conducted by the academic community in the space of technical policy, with some authors even calling for academics to get involved in this space (Knapp et al., 2009).

Whereas very little research exists regarding the study of the design of technical policy, research has been conducted to describe the impact of policy changes on employee populations, and organizations as a whole. This work primarily exists in the space of employee compliance or deviance in regards to organizational policies. As is described in many publications (see Durgin, 2007; Gordon et al., 2006; Lee and Lee, 2002; Willison, 2006), employees are often considered one of the "weak links" in organizational policy, but can be essential assets in solidifying an organizational network (Bulgurcu, Cavusoglu, and Benbasat, 2010), if properly motivated. Often this motivation comes in the form of perceived inclusion, i.e, if an employee of an organization feels that they are a part of the solution to solidifying an organizational network, they are more likely to help protect that network (Bulgurcu, Cavusoglu, and Benbasat, 2010). Different approaches also suggest applying concepts of mandating policy strictly, e.g., evaluating employees on how well they comply with policy (Boss et al., 2009), or assigning employees to projects based on some measure of trustworthiness (Laszka et al., 2014). However, such approaches may backfire if employees believe they are being infringed upon by the organization (Kirlappos, 2016; Putri and Hovav, 2014), as has occurred in

many instances of Bring-Your-Own-Device policy implementations within organizations (Ortbach, Walter, and Öksüz, 2015; Putri and Hovav, 2014). It is clear that properly constructed policy must be able to both satisfy technical and organizational requirements dictated by senior management, while simultaneously not alienating employees of a given organization.
Most importantly, security policies should also contribute to better security outcomes (as measured, for example, by the number and severity of security incidents). However, the literature in this regard is equally scarce as argued in a recent summary of the published work (Nagle, Ransbotham, and Westerman, 2017). Those same authors contribute to this (emergent) literature with a firm-level empirical analysis of open port policy and its association with incidence figures of botnet activity, potential exploitation, and unsolicited communications. Their conclusion from the analysis is that security management indeed positively impacts security outcomes (Nagle, Ransbotham, and Westerman, 2017).

2.3 Challenges for Policy Collection

Obtaining access to internal information/technology security policies is difficult for a number of reasons. One important lesson-learned was reported by one group of researchers, who attempted to gather and analyze corporate information security policies with the intent of analysis and modeling. Ultimately, they were only left to report on the extreme difficulty of conducting this type of policy work (Kotulic and Clark, 2004). The primary stated reason for this outcome, as relayed by companies' representatives, was that analysis of policy was considered to be one of the most intrusive types of research an organization could undergo. The authors eventually determined that without having a "major supporter", policy analysis in this space would be immensely difficult (Kotulic and Clark, 2004).
As a meaningful alternative, we chose to focus on academic institutions, such as colleges and universities, to apply policy analysis. Unlike nearly every corporation, most universities post all policies guiding employees and students on their websites; including their technical policies. This same technique was also utilized by Doherty, Anastasakis, and Fulford, 2009, who conducted a similar study on the contents of information security policies for universities around the world. This work differs from ours, however, in that this paper sampled a smaller sample of international universities, while we have collected a substantially larger sample from one country, and provide deeper statistical analyses based on our coding to inform our results. Collecting the policies from universities, rather than corporations, presents an excellent opportunity to examine a large corpus of policies dictating technology usage within small and large organizations, and to collect a sample largely unaffected by selection/omission bias.

3 Methodology

3.1 Policy Selection

To conduct this study, we attempted to collect publicly available *information security policies* from the top 200 universities and colleges in the United States, based on the annual list produced by U.S. News (2017). Each of these information security policies was found and archived via a multi-step process. First, a standard search engine was utilized to locate each policy, if available, by using the university name followed by keywords including 'security policy', 'security', 'information security'. Using these different keywords was necessary, as the formal naming of policies varies across organizations. In instances where a relevant result was not returned via a search engine, we attempted to locate an IT, CISO, or other relevant internal security page, which in turn could point towards information technology policies. As an alternative, we also aimed to locate a given university's global policy page, containing several documents including security-unrelated policies, and searched for an information security policy there. We also note that there were several instances in which a given information security policy was located, but was inaccessible to us, as it had been removed from public circulation by a university. In such scenarios, we did mark that a security policy did exist, but that we were unable to access it without proper authentication.

To further ground this dataset, we were also specific about which policies, based on nomenclature, could be included. Any policy document titled 'Information Security Policy' was accepted, along with similarly named policies such as 'IT Security Policies', 'Data Security Policy', or 'Information Technology Security'. Other policy documents were excluded such as 'Access Control Policy'. Some universities had many technology-specific security policies in the absence of a higher-level security policy, and these smaller, specific policies (e.g., focused on WiFi access, BYOD etc.) were excluded from data collection as well. Lastly, in the event that a series of universities shared a common information security policy across all of them, as found in some state-sponsored universities such as the University of California system, this policy was only collected once to ensure that a given policy would not have more than one instance for data analysis purposes.

Upon locating each policy, it was downloaded, archived, and converted into plaintext format for further analysis. We did not contact universities for which we could not find a publicly accessible policy. Of the 200 surveyed institutions, 101 had publicly available information security policies that we could access, with an additional 7 universities having their security policy restricted to authorized users. Given these 101 institutions, we arrived at 90 distinct information security policies for the final analysis. The reduction in policy sample size is due to 11 cases of duplicate policies found within specific university systems (i.e., those included the university systems of Indiana University, State University of New York (SUNY), University of Alabama, University of Illinois, and University of California).

3.1.1 Availability of Information Security Policies

Based on this policy search, we found that only 54% of the 200 surveyed universities had, to the best of our knowledge, an information security policy, with only 50.5% having publicly accessible policies. We believe that three possible factors may contribute to this low number: 1) More information security policies exist, but are not publicly viewable, or are very difficult to find; 2) These information security policies are named very differently across organizations; or 3) Instead of maintaining a high-level information security policy, universities instead rely on low-level technology-specific policies similar to standards and guidelines.

We want to note that even for organizations who did have an information security policy, it took a great deal of time to navigate through various search engines and web pages before reaching the security policy itself. Regarding this point, we have several takeaways. In general, this process should be streamlined to ensure all individuals are able to find relevant policy documents with relative ease, thus increasing the chance that these policy documents will be read. Second, by using non-standard nomenclature for information security policies, confusion can be created for those within and external to a given organization. Universities, and organizations in general, should strive for some level of uniformity in policy naming conventions to reduce the amount of effort to locate these documents. Lastly, while smaller, issue-specific information security policies have their place and can be beneficial, a centralized, high-level document is important to summarize an organization's information security goals, as well as provide a centralized place through which smaller issue-specific policies can be referenced.

3.2 Qualitative Coding and Further Analysis

The primary means of policy analysis for this work involved coding each of the 90 information security policies according to a series of pre-selected measures, shown in Table 1 below. We utilized five item categories, which were based on recommended policy features from information security management textbooks (see primarily Jones and Ashenden, 2005; Whitman and Mattord, 2013), as well as an iterative analysis of a sample of content found within our corpus. We note that this may not be an exhaustive list of possible features that exist across the 90 policies we examined, but the item list goes beyond high-level textbook advice for information security policy by, for example, accounting for technology features.

Item Category	Measured Items
Overview of Organizational Philosophy/Policy Structure	Provides motivation/justification; Mentions that elements are mandatory (explicit or implicit); Mentions enforcement; Mentions sanctions for violations; Has an effective date; Has a next review date; Number of sections in the policy
Information Security Structure	Clearly states who issued the policy; Clearly states who is affected by the policy; Defines organizational roles (CISO, CIO, etc.); Defines standard roles (Faculty, Students, etc.)
Responsibilities for All Network Users (Procedures)	Has *detailed* technical items; Mentions passwords; Mentions anti-virus; Mentions patching; Mentions firewalls; Mentions software licensing; Mentions patching; Mentions encryption; Mentions 2FA; Mentions backups
Responsibilities for Specific Roles	Breaks down responsibilities into different roles for different users
Supplemental Materials	Has definitions; Provides connections to other policy documents or standards; References legal/government documents or standards

Table 1. Coding metrics used for policy analysis

We coded each of the policies, based on these 25 features, in a binary fashion; that is, if a given item existed in any form, it was included. For example, a statement that 'all accounts are required to have strong passwords' would be recorded in the same way as another policy which detailed exact steps required to achieve a strong password (e.g., longer than 8 characters, must include a special character, etc.). However, we aimed to account for additional detail by capturing whether a policy 'Has *detailed* technical items', which would allow us to differentiate between policies that referred to technical requirements in a detailed way, rather than merely providing a high-level mention. In addition to these 25 features, we also captured the number of students who attend each university, as reported by each university itself.

We also conducted an exploratory statistical analysis using the measured items across all polices as input. This included running standard descriptive statistics, as well as a series of correlation analyses. This approach has been shown to be effective in the space of analyzing End-User License Agreements (EULAs) and privacy policies (Jensen and Potts, 2004; Marotta-Wurgler, 2007), allowing researchers to be able to identifying certain themes that may not have been visible through standard means of analysis. In addition to this, we also produced readability scores for each of the collected policies utilizing the Flesch-Kincaid Reading Ease metric, which has been used in a large amount of language analysis research (Feng et al., 2010; Graber, Roller, and Kaeble, 1999).

4 Results

4.1 University Information Security Policies

We can first observe that 101 universities (including duplicates at, for example, state-university systems) of the entire sample had publicly available information security policies, with an additional 7 universities that seemed to have an information security policy behind an authentication portal. Thus, we find that only 50.5-54.0% of the top 200 universities in the United States have an explicitly-named information security policy. In examining the corpus of 90 distinct information security policies, we begin by introducing the descriptive statistics for each of the 25 coded items found in Table 1. For each item, we state the occurrence of a given item, and provide examples from the policies themselves, where applicable.

4.1.1 Overview of Organizational Philosophy and General Policy Structure

At a high level, sound information security policies should include a sufficient degree of explanation or justification for why a respective policy exists. This initial section, in many policies, clearly details the goals and objectives of the policy document in the context of the organization as a whole. We found that 88.9% of the information security policies contained some amount of *motivation or justification* for the policy. Some universities, like American University, did this via a long 'Scope' section:

> American University (AU) conducts significant portions of its operations via wired and wireless computer networks [...] AU is committed to protecting its systems and data from these threats, and therefore has adopted the following objectives to achieve a reasonable degree of information technology security:
>
> –To enable all members of the University community to achieve their academic or administrative work objectives through use of a secure, efficient, and reliable technology environment.

Marquette University accomplished this via a shorter 'Overview' section:

> Marquette University relies heavily on computer systems to meet its educational, financial, and operational requirements. It is therefore imperative that computer data, hardware, networks and software be adequately protected against alteration, damage, theft, [...].

We also examined whether or not respective policies stated (explicitly or implicitly) that they were mandatory, or required to be followed. Some institutions, like the University of Rochester, explicitly stated:

> Compliance with information security procedures developed pursuant to this policy will be mandatory.

More implicitly, we argue that one could infer that a given policy is mandatory if the existence of sanctions is mentioned if a policy is violated, such as with Lehigh University:

> LTS has the responsibility to disconnect from the network any network subnet, wireless access point, server, computer, or any other network-connected device that has been identified as being the source of any action which:
>
> –Violates applicable 'conditions of use' policies [...]

Based on these descriptions, 27.8% of universities had *explicit declarations* that following their information security policy was mandatory. An additional 50.0% of universities had *implicit declarations* that their information security policy was mandatory. This also indicates that 22.2% of university information security policies had *no explicit or implicit* statement or inference that their given policy was mandatory. We also determined whether or not universities defined some form of enforcement or sanctions, in the event that someone in a university environment would violate a component of the policy. We found that 67.8% of the information security policies had some mention of enforcement, while 64.4% explicitly mentioned sanctions that could be levied as a result of that enforcement. An example of an enforcement statement can be found in the policy snippet above of Lehigh University. An instance of a sanctions statement can be found via Auburn University:

> Deliberate violation of this policy will be considered a Group I infraction under the Auburn University Personnel Policies and Procedures Manual and is subject to disciplinary action, up to and including dismissal.

Reviewing and updating information security policies is a critical component of the policy lifecycle. As new technological threats emerge, policies must be adapted to account for these challenges. Thus, we investigated how many policies had any form of policy review protocol in place to regularly check these policies. In a similar thread, from an administrative standpoint, we also determined whether or not each university indicated an effective policy start date. We found that 88.9% of the universities we examined included an *effective date* in their policies, while only 26.7% included a *next review date*. Very few universities provided a specific review date. Generally when examining these policies, we found that

most universities had a simple statement that they would review their respective policy annually, such as with the University of Colorado: "The CIO, director of IT, the IT Advisory Council and the IT Leadership Team shall be responsible to: Review and update the security policy annually [...]."
To better understand the design of policy documents, we also counted how many individual sections each information security policy had, based on major sections only (we did not count minor subsections). The average number of sections was 7.93, with a standard deviation of 4.5 sections. The fewest number of sections found in any policy was 1 section (1 policy), while the largest was 25 sections (2 policies).

4.1.2 Information Security Structure

A critical component of any sound information security policy is understanding who the stakeholders are; that is, who is responsible for the policy, who is impacted by the policy (who must abide by it), and what the roles of organizational members are in maintaining the policy document. For the 90 information security policies, we found that 80% stated explicitly who was responsible for a given information security policy. A majority of universities stated that a Chief Information Officer (CIO) or Chief Information Security Officer (CISO) were responsible for the construction and maintenance of their information security policy. Regarding statements on who is impacted by the policy, we found that 74.4% of information security policies *clearly indicated who the target audience was*. However, some institutions like the University of the Pacific, do this in somewhat vague language:

> Any person who uses or provides information resources has a responsibility to appropriately maintain and safeguard these assets.

Others, like Virginia Tech, provide more explicit details when describing who is impacted by the policy:

> This policy applies to any technology resource or service that:
>
> –Is owned or managed by the university;
>
> –Is connected to the university network; [...]
>
> This policy applies whether the network connections are remote or campus-based. The owner of a technology resource may use it at his or her discretion; however, once that device is connected to the university network or other technology resource or service or is used to store university data, it is subject to applicable laws and regulations and to university policies.

As the last two measures in this category, we also determined whether or not these university information security policies defined specific administrative roles and responsibilities, such as a CISO or Information Steward, as well as more standard roles such as Staff or Student. We found that 45.6% of universities provided these explicit definitions for administrative roles, while only 15.6% provided similarly explicit definitions for non-administrative roles.

4.1.3 Responsibilities for All Network Users (Procedures)

In a standard enterprise information security policy, technical responsibilities and specifications are traditionally not included, and are found instead within security standards and guidelines (Whitman and Mattord, 2013). Of the 90 universities we examined, 55% of them did not contain any detailed technical features. However, a number of the information security policies we examined did contain some of these technical requirements (45%), sometimes in great detail. In fact, we found that 23.3% of information security policies contained very detailed instructions for technical systems that would be generally included in information security standards or guidelines. For example, the University of Mississippi provides an extensive list of practices as part of their information security policy, including some of the following items:

> –Mobile devices that will be used to store sensitive data must be approved by the IT Security Coordinator prior to use, and have disk-level encryption enabled. If disk-level encryption is not a viable option, the individual sensitive files may be encrypted with AES-256 encryption or equivalent instead.

Technology Feature	Percentage
Password Requirements	80.0%
Encryption	77.5%
Backups	70.0%
Patching	65.0%
Anti-Virus	60.0%
Firewalls	57.5%
Software Licensing	30.0%
Two-Factor Authentication	7.5%

Table 2. Technical features found within 40 information security policies

> –Replace un-encrypted services and protocols with encrypted equivalents. All remote-access protocols used to manage critical infrastructure and/or servers should be encrypted. Telnet should be replaced with SSH. FTP should be replaced with SFTP. X connections should be securely tunneled.

This is dissimilar from other universities which may mention some technical requirements, but do so in a more generic fashion, or reference other university standards or guidelines. An example of this is Virginia Tech: "[Users] must adhere to security standards, including, but not limited to: Maintain the operating system and application software with appropriate updates;[...] Adhere to strong password requirements in selecting a secure password." The difference to note here is that the first example showed highly detailed technical language in directing the use of technology resources, while the second example represents a more high-level statement, lacking a number of specifications. For the universities that included any form of technology procedure, we display the findings in Table 2. Note that these statistics are based on only the 45% of universities that included technical features, and exclude the 55% of universities that did not include these features.

4.1.4 Responsibilities for Specific Roles

Similar to defining roles within an organization, such as a CIO or CISO, consistent enterprise information security policies also generally contain articulated responsibilities for a number of these roles and positions from administrators, to third-party vendors (Whitman and Mattord, 2013). We found that 41.1% of the analyzed information security policies included this information, though the detail of this varied across universities. The University of Minnesota, for example, defined responsibilities for 'University Employee and University Community Member', as well as 'Compliance Officer', 'Technical Staff', 'Campus, College, and Department Administrators', 'University Chief Information Security Officer or Designate', 'University Enterprise Architect', 'Office of Information Technology (OIT) - University Information Security', and 'Security Advisory Committee'. Other universities, such as the University of Central Florida, were more general, and noted responsibilities for 'Every User', 'System Administrators', and 'Departmental Security Coordinators'.

4.1.5 Supplemental Materials

While perhaps not technically part of a given information security policy, supplemental materials can be helpful in understanding a policy, or by providing additional resources referenced within a policy. For the sake of this analysis, we determined whether or not the collected university information security policies contained definitions, made references to external documents or standards (within the university), or made references to legal requirements or documentation (NIST Recommendations, HIPAA Requirements, etc.). We found that 62.2% of universities *provided some level of definitions* within their security policies. As an example, Cornell University provided these definitions within the document itself:

> These definitions apply to terms as they are used in this policy:
>
> –Custodian: An individual with access to institutional information, or who uses that information in the legitimate course of university business.
>
> –Handheld Device: An electronic, hand-held computing device such as a smartphone, cellphone, tablet, or personal digital assistant (PDA) used to conduct university business. [...]

Other universities, like Georgetown University, provided a section entitled 'Definitions', but this section only contained a list of terms used in the policy, not the actual definitions:

> For clarification on the terms used in this document, please refer to the Office of Information Services Policy Definitions, Roles, and Responsibilities. Terms used in this policy include:
>
> –Data Extract [...]
>
> –Data User [...]

As noted in the previous example, a number of additional documents related to information security policies are often found at other locations. We found that 70% of the policies *referenced other documents* within the context of each respective university, whether they be definitions, security standards, guidelines, or procedures. We also found that 40% of all analyzed universities also *referenced state and federal laws, or guidelines*, citing or linking to HIPAA requirements, or NIST standards that may be applicable to the policy document at the university.

4.2 Readability Analysis

Following the qualitative coding of the policy corpus, we conducted a series of readability analyses on each policy to determine respective Flesch Reading Ease scores, as well as a general word count. We found that the information security policies we examined had an average Flesch Reading Ease score of 12.54 (SD=8.66), indicating that the average readability of these documents is extremely low. For reference, a score of 50.0-30.0 is generally considered to be a college-level difficulty reading, while 30.0-0.0 is suitable for college graduates. An average score of 12.54 shows that these policies are generally very difficult to parse and understand, even for college graduates. Considering that the student population of universities is quite diverse, not including staff or third-party affiliates, this may pose a significant problem.
Further, we found that 8 universities, or 8.9% of the policy corpus, had a Flesch Reading Ease score of 0, the lowest achievable readability score. The highest reading score we found was 40.20. In total, only 3 universities (3.3%) had a reading ease score above 30.0.

4.3 Policy Correlations

Based on the classification of items across all policies, we conducted bivariate correlation analysis across all measured items, as well as student population size, readability score, and word count. Selected results are reported here, with implications discussed further in the following section. Beginning with the determined readability scores and word count, we found that there was a mild, positive correlation between the word count and readability score, which was statistically significant ($r = .312$, $n = 90$, $p<.03$). Perhaps unsurprisingly, we also found that word count was positively correlated with the number of sections found in a given policy, and was statistically significant ($r = .458$, $n = 90$, $p<.001$). However unexpectedly, readability and word count were negatively correlated with nearly all technical items. At a high level, word count was negatively correlated with having specific technical details ($r = -.361$, $n = 90$, $p=.001$). The detailed technical item correlations are shown in Table 3. These correlations were similar for reading ease as well. These results seem to indicate two things: 1) Longer policy documents disclosed technical specifications significantly less often compared to shorter policy documents, and 2) Policy documents were easier to read if they did not contain technical details.
Regarding any correlations involving student enrollment, we first found that student body size was negatively correlated with a given policy clearly defining who is impacted by a policy, and was statistically

	Password Rules	Anti-virus	Patching	Firewalls	Encryption	Backups
Word Count	-0.348**	-0.381**	-0.394**	-0.409**	-0.357**	-0.327*

*Table 3. Technology Item Correlations to Word Count (Note *p<0.01; **p<0.001).*

	Policy Justifications	Defined Organizational Roles	Policy Definitions	State/Federal Law Compliance
External References to standards or policies	0.231*	0.209*	0.340**	0.238*

*Table 4. External Policy Reference Correlations (Note *p<0.05; **p<0.01)*

significant (r = -.211, n = 90, p<.05). Similarly, we found that the size of a given student population was negatively correlated with policies detailing responsibilities across roles within a university (r = -.236, n = 90, p<.05). This is a critical organizational issue that should be addressed. Without clearly articulated policy statements indicating what groups a given policy is targeting, it is not unlikely for some groups to believe that a policy may not apply to them, and thus, they may not comply with it. This opens an organization up to greater non-compliance issues through this obfuscation of a target audience.

For each of the measured technical items (presence of anti-virus, patching, firewalls, etc.), we found strong, positive correlations for each item with all other technical items, with the exception of two-factor authentication. This generally indicates that if a policy had one of these technical items, it would often have many of them, with the exception of two-factor authentication. For non-technical items, we also found correlations between supplementary materials and overview of organizational philosophy. For policies that provide external references to security standards or other institutional policies, there were positive correlations found with policies that provide justifications, define organizational roles, provide definitions, and provide links to state or federal laws and requirements. These are shown in Table 4.

5 Discussion

With this work, we collect and analyze in-practice information security policies by using a sizable sample of universities in the United States. We position this paper as an initial work in this space, which seeks to inspire additional needed research in this area. The research questions of this work focused on what content is included within information security policies at universities, as well as how certain factors within these policies may or may not relate to each other. The simple answer is that information security policies across organizations are anything but standardized, with a wide variety of covered features included (or not included) in each.

At the highest level, the policies within this collected corpus varied in length substantially. The shortest information security policy we reviewed was 172 words, while the longest was 27,425 words; the average security policy was 2639 words. When factoring in readability scores, we found an interesting correlation; namely, that the longer an information security policy is, the easier it is to read. Many of the shortest security policies we reviewed had readability scores of 0, the lowest possible score. It seems evident that in the attempt to be more concise with the construction of information security policies, some policy authors have effectively made the document inaccessible to a wider audience. A takeaway from this is that even though the shorter policy documents may at first seem appealing to implement and might encourage readership, the opposite may actually be true. While having a 27,425 word policy may be not read by members of an organization for length reasons, it is clear that simply crafting shorter policies will not solve this issue, and in many cases will further complicate it.

Another high-level finding is that these deployed policies are relatively evenly divided between enterprise

information security policies, similar to issue-specific information security polices. The primary differentiating factor between the two policy types is the inclusion of specific technical details in issue-specific policies, which was the case for 45% of the policies examined in this study. This seems to indicate that policy authors are split on what type of policy design is most effective when crafting an information security policy. To the best of our knowledge, with the exception of providing textbook examples (Whitman and Mattord, 2013), we are unaware of any work that has been done to determine how individuals actually perceive these two document types, and which they find to be more useful or generally beneficial. We suggest this as a critical next step in this research space.

Concerning document features, we do note that a majority of information security policies contain appropriate justifications (88.9%), effective policy dates (88.9%), and a clear indication of policy ownership (80%). However, we also found that a majority of policies did not have any plan for reviewing and updating their information security policy after it had been issued. In one extreme example, we found that one university had an information security policy with an origination date of July 1993, with the most recent noted revision having taken place in October 2005. Considering the constantly shifting technological landscape, it seems unreasonable to not have a formal plan in place to review an information security policy at least annually. This is especially true for issue-specific information security policies, which would need to be updated more readily than an enterprise information security policy, due to their concrete technical details for protecting against threats.

Regarding other components of these information security polices such as whether or not a given policy provided definitions, provided breakdowns of role responsibilities, and more, we found that these items were more difficult to analyze at a higher level due to the sheer amount of differentiation between them. As an example, some universities provided detailed changelogs for their policies, noting each time a revision was made, and what was changed. Other universities simply noted a singular date which signified the last date that a revision was made. Do more detailed changelogs help or hinder readability and comprehension? If these changelogs are a hindrance, how should universities best account for revision history? A great deal of variance between policy documents we examined stemmed from these individual differences, and was generally more difficult to quantify or categorize. In general, we can say that only 12 total policies contained all of the elements generally recommended for enterprise information security polices (see Table 1). As all of policies we examined were titled as an Information Security Policy, we argue that each of these policies should, at a minimum, meet the standard recommendations for enterprise information security policies, even if issue-specific items are included as well. The need to meet standard recommendations becomes even more important in countries outside of the United States. This is especially true for all countries within the European Union which will be adopting the General Data Protection Regulation (GDPR) in May 2018, forcing all organizations to ensure that their policies are compliant with the new rules. While it is not initially clear how such regulations may impact internal information security policies specifically, it may still be worth comparing US-based and EU-based information security policies after the GDPR has been implemented.

6 Conclusion

In this paper, we collected and analyzed a corpus of 90 distinct information security policies from universities within the United States. We find that the prevalence of these high-level policies across the sampled population is modest at best, with a 54% policy existence rate. For those universities that maintain these policies, we find that the high-level policy types are evenly split between what would be traditionally-called enterprise information security policies, which focus more on organizational details, and issue-specific information security policies, which may include organizational details, but also technical ones. Future work should determine which of these strategies is more appropriate. While textbook examples and generic advice for policy design have existed for some time, we argue that there have been few successful attempts to study information security policies on a wide scale. Further work in this space is necessary to understand how these documents are designed, implemented, and enforced to ensure that universities, and

other organizations are more effectively protected from rising external security threats.

Acknowledgments
We want to thank the anonymous reviewers and editors for their constructive comments and feedback. The research activities of Jake Weidman and Jens Grossklags are supported by the German Institute for Trust and Safety on the Internet (DIVSI).

References

Becker, I., A. Hutchings, R. Abu-Salma, R. Anderson, N. Bohm, S. Murdoch, A. Sasse, and G. Stringhini (2016). "International comparison of bank fraud reimbursement: Customer perceptions and contractual terms." In: *Workshop on the Economics of Information Security (WEIS)*.

Boss, S., L. Kirsch, I. Angermeier, R. Shingler, and W. Boss (2009). "If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security." *European Journal of Information Systems* 18 (2), 151–164.

Brewer, R. (2016). "Ransomware attacks: Detection, prevention and cure." *Network Security* 2016 (9), 5–9.

Bulgurcu, B., H. Cavusoglu, and I. Benbasat (2010). "Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness." *MIS Quarterly* 34 (3), 523–548.

Carayon, P., S. Kraemer, and V. Bier (2005). "Human factors issues in computer and e-business security." *Handbook of integrated risk management for e-business: measuring, modeling and managing risk*, 63–85.

Doherty, N. F., L. Anastasakis, and H. Fulford (2009). "The information security policy unpacked: A critical study of the content of university policies." *International Journal of Information Management* 29 (6), 449–457. ISSN: 02684012. DOI: 10.1016/j.ijinfomgt.2009.05.003.

Dunn, W. (2015). *Public policy analysis*. Routledge.

Durgin, M. (2007). "Understanding the importance of and implementing internal security measures." *SANS Institute Reading Room (https://www2. sans. org/reading_room/whitepapers/policyissues/1901. php)*.

Fahey, M. and N. Wells (2016). "Yahoo data breach is among the biggest in history." *CNBC*.

Feng, L., M. Jansche, M. Huenerfauth, and N. Elhadad (2010). "A comparison of features for automatic readability assessment." In: *Proceedings of the 23rd International Conference on Computational Linguistics: Posters*. Association for Computational Linguistics, pp. 276–284.

Friedman, M. (1953). "The methodology of positive economics." *The Philosophy of Economics: An Anthology* 2, 180–213.

Gilmore, J. (2015). "Campus announces data breach." *Berkeley News, University of California at Berkeley*.

Gordon, L., M. Loeb, W. Lucyshyn, and R. Richardson (2006). "2006 CSI/FBI computer crime and security survey." *Computer Security Journal* 22 (3).

Graber, M. A., C. M. Roller, and B. Kaeble (1999). "Readability levels of patient education material on the World Wide Web." *Journal of Family Practice* 48 (1), 58–59.

Greenberg, A. (2014). "North Dakota University System hacked, roughly 300K impacted." *SC Magazine*.

Grossklags, J. and N. Good (2007). "Empirical studies on software notices to inform policy makers and usability designers." In: *International Conference on Financial Cryptography and Data Security*, pp. 341–355.

Hayward, B. (2013). "Investigating apparent IT breach, Stanford urges users to update passwords." *Stanford University*.

Jensen, C. and C. Potts (2004). "Privacy policies as decision-making tools: An evaluation of online privacy notices." In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 471–478.

Jones, A. and D. Ashenden (2005). *Risk management for computer security*. Butterworth-Heinemann.

Kirlappos, I. (2016). "Learning from "shadow security": Understanding non-compliant behaviours to improve information security management." PhD thesis. University College London.

Knapp, K., F. Morris, T. Marshall, and T. Byrd (2009). "Information security policy: An organizational-level process model." *Computers & Security* 28 (7), 493–508.

Kotulic, A. G. and J. G. Clark (2004). "Why there aren't more information security research studies." *Information & Management* 41 (5), 597–607.

Lasswell, H. D. (1971). *A Pre-view of Policy Sciences*. Elsevier.

Laszka, A., S. Farhang, and J. Grossklags (2017). "On the Economics of Ransomware." In: *International Conference on Decision and Game Theory for Security*, pp. 397–417.

Laszka, A., B. Johnson, P. Schöttle, J. Grossklags, and R. Böhme (2014). "Secure Team Composition to Thwart Insider Threats and Cyberespionage." *ACM Transactions on Internet Technology* 14 (2-3).

Laszka, A., M. Zhao, A. Malbari, and J. Grossklags (2018). "The Rules of Engagement for Bug Bounty Programs." In: *International Conference on Financial Cryptography and Data Security*.

Lee, J. and Y. Lee (2002). "A holistic model of computer abuse within organizations." *Information Management & Computer Security* 10 (2), 57–63.

Luftmann, J. and R. Kempaiah (2008). "Key issues for IT executives 2007." *MIS Quarterly Executive* 7 (2).

Marotta-Wurgler, F. (2007). "What's in a standard form contract? an empirical analysis of software license agreements." *Journal of Empirical Legal Studies* 4 (4), 677–713.

McGrath, M. (2014). "Target data breach spilled info on as many as 70 million customers." *Forbes.com*.

Nagle, F., S. Ransbotham, and G. Westerman (2017). "The Effects of Security Management on Security Events." In: *Workshop on the Economics of Information Security (WEIS)*.

National Institute of Standards and Technology (1995). *An Introduction to Computer Security: The NIST Handbook (Chapter 5: Computer Security Policy)*. NIST.

Nochenson, A. and J. Grossklags (2014). "An Online Experiment on Consumers' Susceptibility to Fall for Post-Transaction Marketing Scams." In: *European Conference on Information Systems (ECIS)*.

Ortbach, K., N. Walter, and A. Öksüz (2015). "Are you ready to lose control? A theory on the role of trust and risk perception on bring-your-own-device policy and information system service quality." *European Conference on Information Systems (ECIS)*, 1–10.

Patyal, M., S. Sampalli, Q. Ye, and M. Rahman (2017). "Multi-layered defense architecture against ransomware." *International Journal of Business & Cyber Security* 2 (1), 52–64.

Perez, S. (2016). "Recently confirmed Myspace hack could be the largest yet." *TechCrunch*.

Ponemon Institute (2016). *Cost of cyber crime study & the risk of business innovation*.

Privacy Rights Clearinghouse (2017). *Data Breaches*. Continuously updated database. Last accessed on June 7, 2017. URL: `https://www.privacyrights.org/data-breaches`.

Putri, F. and A. Hovav (2014). "Employees' compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory." *European Conference on Information Systems (ECIS)*, 1–17.

Robert, C. and R. Zeckhauser (2011). "The methodology of normative policy analysis." *Journal of Policy Analysis and Management* 30 (3), 613–643.

Sabatier, P. A. and C. M. Weible (2007). "The advocacy coalition framework: Innovations and clarifications." *In: Sabatier, PA (ed.). Theories of the Policy Process, Second Edition, 189-217*.

Simon, L. A. (2016). "Information on Data Security Incident." *Michigan State University*.

Stephenson, C. and R. Johnston (2017). "U.S. universities race to contain WannaCry ransomware, officials say." *CyberScoop.com*.

Svitek, P. and N. Anderson (2014). "University of Maryland computer security breach exposes 300,000 records." *Washington Post*.

U.S. News & World Report (2017). *The 10 Best Universities in America*. URL: `https://www.usnews.com/best-colleges/rankings/national-universities`.

Weidman, J. and J. Grossklags (2017). "I Like It, but I Hate It: Employee Perceptions Towards an Institutional Transition to BYOD Second-Factor Authentication." In: *Proceedings of the 33rd Annual Computer Security Applications Conference*. ACM, pp. 212–224.

Whitman, M. and H. Mattord (2013). *Management of Information Security*. Nelson Education.

Willison, R. (2006). "Understanding the perpetration of employee computer crime in the organisational context." *Information and Organization* 16 (4), 304–324.