Nothing Standard About It: An Analysis of Minimum Security Standards in Organizations

Jake Weidman[1][0000−0003−4727−4271]⋆, Igor Bilogrevic[2][0000−0002−9301−3091], and Jens Grossklags[3][0000−0003−1093−1282]

[1] The Pennsylvania State University, State College, USA
jakeweidman@google.com
[2] Google, Zurich, Switzerland
ibilogrevic@google.com
[3] Technical University of Munich, Germany
jens.grossklags@in.tum.de

Abstract. Written security policies are an important part of the complex set of measures to protect organizations from adverse events. However, research detailing these policies and their effectiveness is comparatively sparse. We tackle this research gap by conducting an analysis of a specific user-oriented sub-component of a full information security policy, *the Minimum Security Standard*.
Specifically, we conduct an analysis of 29 publicly accessible minimum security standard documents from U.S. academic institutions. We study the prevalence of an extensive set of user-oriented provisions across these statements such as who is being addressed, whether the standard is considered binding and how it is being enforced, and which specific procedures and practices for users are introduced. We demonstrate significant diversity in focus, style and comprehensiveness in this sample of minimum security standards and discuss their significance within the overall security landscape of organizations.

1 Introduction

Massive data breaches within corporations such as Target, Home Depot and Yahoo have become relatively commonplace, with numerous companies suffering millions of dollars in losses (and millions of consumers having data records exposed) in a widely publicized way. Though not as predominately focused on by traditional media outlets, academic institutions have also become increasingly popular targets for cyber attackers, with numerous universities suffering damaging security incidents over the past few years. Often, within either type of organization, data breaches are at least partly related to some form of employee (in)action, whether it be intentional or inadvertent [28, 36].

To build a first line of defense against data breaches, organizations strive for an effective *Information Security Policy* [15, 47], which, in theory, can help

⋆ Jake Weidman is now with Google. The work was done while the lead author was visiting researcher at the Technical University of Munich, Germany.

educate and instruct users about how they should act on an organizational network. In reality, however, these policies can often be complex in their content and presentation, and intended audiences may struggle to identify relevant policy terms and to comprehend provisions within these policies. For instance, in our previous work we have encountered security policies in academic institutions that include dozens of individual lengthy documents covering a diverse range of technical and non-technical issues [47–49]. Further, policies need to account for diversity in the employee population [16]. Given this complexity, it is challenging to avoid non-compliance, thus placing organizational security at risk [41]. At the same time, we argue – when given a reasonable opportunity to do so – employees can be stalwart in assisting in the protection of organizational networks [6].

Our work focuses on one organizational approach, deployed in practice, which may serve to address the challenge of the overburdening complexity of security policies and resulting non-compliance. More specifically, we have observed the emergence of a user-oriented, sub-component of full information security policies: the *Minimum Security Standard*.

These minimum security standards are designed to target a specific audience, such as network administrators, or employees, and indicate clear requirements that should be followed by that individual within a technical system [24]. For example, end-users of a network may be instructed to enforce an automatic screen lock on mobile phones or computers after a certain period of time. Whereas businesses and academic organizations now almost always have some form of information security policy available within their system, minimum security standards are still less present, at least within the scope of the academic institutions we observed, which are the primary focus of this work.

Minimum (security) standards are not to be confused with separate organizational documents, referred to as procedures or guidelines. Rather, minimum security standards exist in a space between high-level, formal information security policies, and the low-level, and often simple procedures or guidelines, while simultaneously containing elements of both. For universities providing these standards, we seek to understand the general composition and formatting of these emergent documents, and to infer aspects related to their likely comprehension, implementation, and technological adequateness.

In particular, we describe our methods for obtaining and analyzing 29 minimum security standards from different universities. We evaluate these standards by first coding the documents (in seven categories) focused on end-user components, and then performing quantitative analyses on the resulting data. This included descriptive statistics, readability and tone measures, and cross-standards comparisons on features found within and across these documents. To the best of our knowledge, we provide the first analysis of the emergent policy document class of minimum security standards, and contribute to the sparse literature on the analysis of written security policies.

2 Related Work

Security Standards and Organizational Focus: Most, if not all, organizations seek to protect their digital assets primarily by following an information security policy [15], which is designed to provide mechanisms and rules to protect essential organizational data [4]. Although these information security policies are not novel, they are still regarded as difficult to construct and maintain, and thus various templates or pre-established guidelines are often used to assist administrators and policy developers in their writing of these documents [15, 22]. A major component of (or, in some cases, parent of) an information security policy is generally known as a *Security Standard*, or something of a similar nomenclature.

The first standard and guideline in this space was the BSI Group's BS 7799 (published in the United Kingdom in 1995) [24, 45]. It was designed to be a common information security framework that could be applied to many industry segments as well as to government agencies [24, 42]. Several years after its original development, BS 7799 was adopted as an international standard, and became more commonly referred to as ISO/IEC 17799[4], which was defined as a code of practice for information security management [8, 24, 37]. In what may be even more recognizable to some, standards such as these led to further focused legal frameworks and guidelines from governments, including the National Institute of Standards and Technology's (NIST) FIPS 199, or Federal Information Processing Standards [12].

Each of these different standards had a similar objective, i.e., to provide organizations across different sectors with a common baseline of information security techniques and methods for protecting their own entities from digital threats. Although these standards are effectively being used worldwide [17], they are not without issues. Due to the generalizable nature of documents intended for an international community, these various standards are often difficult for organizations to implement without modification, as a result of individual organizational security concerns and requirements [29, 39]. In particular, what aspects of ISO 17799 work for, and are compatible with the desired work flow of one organization may not be suitable for the size and scope of another organization. As a result, in many instances, organizations use these standards more as an inspiration or guiding principles, while attempting to account for their organizations' individual differences [20, 21]. Thus, while studying published international security standards can yield some conclusions about the current state of information security standards in an abstract manner [38], the extremely high number of organizations throughout the world, combined with an unclear number of individual differences in policy-making, lead to a likely highly entropic state of information security policies, and standards as a result, making the space difficult (but interesting) to study.

Even further, once organizations establish set security standards, they are often very protective of them, citing security by obscurity (the idea of keeping

[4] ISO 17799 is now known as ISO 27002.

something secure by camouflaging it) [1, 33], while academics continuously debate whether or not this is an effective option, with security through open sourcing being another suggested method [1, 14]. In reality, at least with corporate organizations, some degree of security through obscurity seems to be the prevalent approach, with little cooperation given to academic researchers studying the space of written security policies [25].[5] In our work, we focus on organizations which share attributes with businesses and are more open to the study of information security standards: academic organizations [46, 50]. We, thereby, also extend our previously published work on *Acceptable Use Policies* [48, 49] and *Information Security Policies* [47] to the context of minimum security standards. Likewise, Doherty et al. studied a sample of information security polices from universities [9]; their investigation does not include minimum security standards.

Like many corporations, academic organizations employ hundreds, if not thousands of people, and are also eminent producers of intellectual property that needs to be protected [43]. Again, like corporations, academic organizations are also increasingly becoming victims of data breaches, partially due to the high amount of intellectual property being generated. Unlike corporations, however, academic organizations are far more open about internal operations, and many post (or are required to post) a majority of their internal policies and procedures on the Internet, which can be publicly accessed. A report funded by the U.S. Department of Justice from 2006, which is partly based on survey responses and interviews with representatives from academic institutions, provided early insights in this problem domain [7].

Technical Components: Standards, including ISO/IEC 27002, contain specific recommendations that organizations should introduce into their infrastructure to ensure a baseline level of security with a vast majority of these provisions focusing on technical components. Specific to our study, major technical components within ISO/IEC 27002 include access control, cryptography, physical and environmental security, communications security, operation security, and compliance [19]. Each of these components breaks down into smaller items, which can be used to understand how an organization implements security. When describing access control, the standard includes items such as password creation/management, device lock or screensaver settings, and more. Cryptography and communications security primarily focus on encryption techniques used within an organization for data at-rest (stored on a computer or server) or in-transit (via email, website etc.). Physical and environment security alludes to physical premises where computer equipment or servers are stored, as well as access control to these spaces. The concept of operation security generally is focused on backups, logging, malware protection etc. Lastly, compliance does not only consider state and federal laws (where applicable), but also matters within organizations themselves, including information security reviews [19].

[5] Interestingly, the paper by Kotulic and Clark was published even though the research was incomplete due to lack of corporate cooperation. The paper ultimately became more focused on talking about the difficulties of academics working with corporations in the space of information security policies and standards.

Security Minimum Standards: As indicated in the introduction, minimum security standards are a newly emerging phenomenon constituting a subcomponent of the broader policy framework of organizations. Our initial understanding of these subcomponents is that they are introduced to reduce the complexity of existing intricate organizational policy frameworks by providing item-by-item provisions about how to act on a network. To the best of our knowledge, no theoretical or empirical research exists studying this phenomenon beyond an industry report by Braun and Stahl from 2004, which provides a useful taxonomy of suggested must-do practices for a *Minimum Security Standard of Due Care* from a legal perspective [5].

3 Methodology

Selection and Pre-Processing of Minimum Security Standards: The acquisition and analysis of the minimum security standards utilized in this study was a multi-step process. To begin our selection, we utilized the college ranking list constructed every year by U.S. News [44], which sorts and ranks the top national universities in America. Based on this list, at the time of searching for these documents, we were able to collect a sample of 30 university minimum security standards.

In searching for standards, we generally attempted to perform a Google search for the name of a given university, followed by keywords such as 'minimum security standards', 'security standards', or 'minimum standards' (e.g., "Stanford University minimum security standard"). However, in many cases, this strategy often did not yield direct results, requiring us to perform searches for the respective Office of Information Security or Information Technology, in order to locate information security policies and minimum security standards for a given university. In some instances the searches over subdivisions of university webpages provided accessible information security policies, minimum security standards, or both. In some cases, universities protected these documents behind firewalls, making them inaccessible to the public.

When ultimately identifying candidates for minimum security standards, we collected documents that were explicitly called as such, with only minor variances accepted (e.g., "Minimum Security for Computing Devices Rule" was acceptable, but "Cyberinfrastructure Standards Policy" was not). To further restrict our selection process, we only collected minimum security standards that explicitly mentioned, and were primarily focused on, end-user interactions. To clarify what we describe (or these standards describe) as an end-user, this is any individual in any capacity who connects to a given organizational network. This includes anyone from employees, students or guests. In many instances, additional parallel standards would exist for network or server administrators, and other technical administrative entities, and while these documents may also be interesting to study, our primary focus were standards that directly impacted end-users.

The minimum security standards discussed in this work were collected between July 24-25, 2017, and were archived to preserve the state of the standards

at that time. After archiving 30 such standards, we converted each one of them to plaintext formats, and removed any extra content or formatting errors that may have been introduced when extracting content from the web. This allowed us to not only review the content of these security standards ourselves, but also perform automated analyses on them. After reviewing the minimum security standards documents we had collected, we chose to remove one document, as the content within the standard was drastically different than any of the others we had collected, and generally focused on different subject matter (not related to end-users), leaving us with 29 total minimum security standards to examine.

Research Ethics: Please note that we do not intend to pass any form of judgment upon individual organizations through this work. Rather, the collection of these *publicly* available documents serves to provide us, and the research community, with a overview of the state-of-the-art with respect to minimum security standards at a given point in time.

Coding of Minimum Security Standards and Analysis: The analysis we conduct in this work is based on the coding of these 29 minimum security standards. In developing our coding schema, we first referenced ISO/IEC 27002 [19], and then followed more focused work by Braun and Stahl [5], which provides seven key information security elements that should be contained in a minimum security standard (from a legal perspective). This list included executive management responsibility, information security policies, user awareness training, computer and network security, third-party information security assurance, physical and personal security, and periodic risk assessment. We based our coding on these seven primary categories, with certain relevant subcategories that were added for completeness. During the coding phase, a major issue we encountered was the appearance – in some of the 29 standards – of additional content beyond the scope of our current study. Specifically, a share of the minimum security standards that we collected contained standards not just for end-users, but for "Servers" and "Data/Applications" in the same document. As our focus for this work was primarily on end-users, any information focused on servers or data/applications found within any section was left for future study. In summary, our coding was based on 7 categories, with a total of 29 items across these categories for our analysis.

To analyze the minimum security standards we collected, we begin by performing descriptive statistics across all 29 universities and coded items. Frequencies, distributions, and examples for each item are provided. We then continue our analysis by reporting the Flesch-Kincaid readability scores of each minimum security standard document, which has been previously used to analyze consumer-oriented, online privacy policies [32] or End User License Agreements [13]. Continuing this theme of text analysis, we also conduct a language tone analysis utilizing IBM's Watson Tone Analyzer [18]. Specifically, we used the 2016 variant of the Tone Analyzer API (2017 is the most recent), as it breaks down analyzed text among a wider number of dimensions. At the highest level, these dimensions are based on three tonal categories: Emotion, Language, and Social tone(s). Within each of these categories are sub-items, which include:

anger, disgust, fear, joy, and sadness (Emotional tones); analytical, confident, and tentative (Language tones); and openness, conscientiousness, extraversion, agreeableness, and finally emotional range (Social tones). Each of the Social Tones are based entirely on the Big-Five personality model, which has been used by psychologists for many years [3], while the Emotional Tones are self-explanatory. The additional Language Tones are based on the following: Analytical tones are intended to describe a writer's analytical and reasoning attitude and ability; Tentativeness is intended to show the attitude of inhibition; and Confidence is designed to show the degree of certainty exhibited by the author of any text [18]. While a relatively straightforward series of metrics, demonstrating readability scores and tones is a necessary, albeit basic, foundational process of analyzing these documents. Next, we perform a simple cross-document text comparison to determine any similar language patterns, common phrases, or possible duplication of document text across university standards.

4 Results

We begin presenting the results by showing descriptive statistics and examples of each of the 29 coded measures.

Executive Management Responsibility The role of Executive Management Responsibility is to define who, or what organization, in management has responsibility for the content of a minimum security standards document. To begin our analysis of this primary component, we determined whether or not each minimum security standards document clearly stated a person or entity who issued the standard, thus declaring ownership and responsibility. We found that 34.5% of the security standards contained this information. For example, Boston University provides this information through a statement at the top of their standard, which reads "Responsible Office: Information Services and Technology". This also contains a hyperlink which directs individuals to this respective office's webpage. In another example, UC Merced provides a responsible official and responsible office, which are referred to as "Responsible Official: Chief Information Officer" and "Responsible Office: Information Technology", respectively.

A second component of this category is whether the security standards clearly state who is affected or impacted by the standard. 82.8% provided such information. The University of Cincinnati, for example, provided a statement indicating:

> "This standard outlines the responsibility of all university community members, including students, faculty, staff, agents, guests, or employees of affiliated entities. This includes (a) individuals who connect a device, either directly or indirectly, to the university data network or support infrastructure, (b) individuals who install, maintain, or support a critical server, and (c) individuals who develop, deploy, or maintain an application that resides or runs on a critical server."

Another example is found via Rochester Institute of Technology, which states: "This standard applies to any computers that access RIT information resources."

A third component we measured was whether or not our collected standards had an effective date, or a next review date, which would indicate when these policies were made active, and when they may be updated. In regards to the latter, only one university did so (UC San Francisco). Within the scope of effective dates, UC Merced provided two dates; an issuance and effective date, June 8th, 2015, and July 1st, 2015, respectively. Other universities, such as Iowa State, also provided effective dates in the format of "Effective: August 1, 2015".

Within the component "Executive Management Responsibility", we examined whether documents provided users with some form of high-level justification or purpose. We found that 69% contained such information. Boston University, for example, begins their security standard with a "Purpose and Overview" section, which states:

> "Protecting University Data is a shared effort. Individuals with access to University Data are responsible for accessing, storing, and processing data on systems that have appropriate security controls in place for the class of data."

Information Security Policies The main goal of the information security policies component is to determine how management in an organization approaches compliance with security responsibilities by members of the network. We first briefly comment on the naming conventions of these minimum security standards. Due to our search and selection criteria, we only observe minor or subtle variations. For example, at Iowa State University the title of the document is "Minimum Security Standards and Guidance".

The next components that we measured were whether or not each minimum security standard classified itself as a mandatory document, including whether content within these standards can be enforced, and if sanctions for violators are provided. We found that 62.1% stated that the minimum standards were mandatory. For instance, Colorado State University stated the mandatory nature of its standard in a preamble: "The requirements in this section are mandatory, minimum requirements that shall be implemented on all IT systems associated with the University." Other universities, such as UT Austin, would specify further systems on which the standards should be mandatory, but – in this case – in less strict language: "This section lists the minimum standards that should be applied and enabled in Confidential, Controlled, Published data systems that are connected to the university network. Standards for Confidential are generally required." In the area of enforcement, 34.5% of the documents included some reference to rule enforcement. Similarly, 24.1% included some mention of sanctions for those who violated the standards. The University of Georgia, for example, included a "Consequences and Sanctions" section in their standard:

> "Non-compliance with these standards may incur the same types of disciplinary measures and consequences as violations of other University policies, including progressive discipline up to and including termination of employment, or, in the cases where students are involved, reporting

> of a Student Code of Conduct violation. Any device that does not meet the minimum security requirements outlined in this standard may be removed from the UGA network, disabled, etc. as appropriate until the device can comply with this standard."

Iowa State followed a similar pattern by including a "Compliance" section in their standard, which read: "Non-compliance with these standards will result in revocation of access to the data, system, and/or network, as well as notification of superiors. All Iowa State University employees are required to comply with all applicable policies, standards, rules, regulations and laws."

As we were examining technical documents dictating how end-users should act on an organizational network, we measured whether universities included any form of technical definitions for content that may be discussed within a minimum security standard (e.g., what a firewall or anti-virus is). We found that 24.1% of universities provided terminology within the minimum standards themselves to assist in the reading of these standards[6]. Finally, we measured the percentage of universities that provided data (sensitivity) classifications. In some instances, we noted that a few institutions not only provided minimum standards for all devices, but also broke down the standards by how sensitive information stored on certain devices would be. In our sample, 34.5% of the universities provided this breakdown of information sensitivity, which was generally expressed in three categories, such as Public, Non-Public, and Confidential as with the University of Nebraska, but also Low Risk, Moderate Risk, and High Risk, such as at Stanford University.

User Awareness and Education As one of the seven components of our analysis, we sought to determine which documents explicitly mentioned any form of user awareness training or education in regards to operating correctly on an organizational network. It should be noted here that it is very possible that these universities do offer training on these topics. However, for the sake of this work, we are only focused on what is contained in the collected minimum security standards. We found that 17.2% mentioned training for network administrators, while 10.3% mentioned anything about training for end-users. For instance, the University of South Carolina included a section on end-user training, which included: "Option(s): Security awareness videos recommended and available at no additional cost through Securing The Human". Iowa State University presented a section on "Training and Compliance", and provided two requirements: 1) "All system users must be notified of what protected data exists on a system and its protection requirements.", and 2) "At least annually all system users must sign the Protected Data Confidentiality Agreement."

[6] We do note that some standards included hyperlinks to other pages which contained technical definitions. However, as they were not explicitly mentioned in the documents themselves, they are not counted here.

Table 1: Technologies discussed in university minimum security standards.

Technology Name	Universities that detail the technology (in %)
Patching	93.1%
Encryption	89.7%
Anti-Virus	79.3%
Firewalls	79.3%
Passwords	75.9%
Access Control	75.9%
Physical Security	72.4%
Device Locking	58.6%
System Logging	51.7%
Backups	48.3%
Anti-Malware	48.3%
System Integrity	37.9%
VPN Access	34.5%
University-Provided Security Tools	24.1%
Two-Factor Authentication	20.7%
Third-Party Tools/Access	13.8%

Computer and Network Security and Third-Party Roles Much of the information we collected for this study dealt with the computer and network security component of these minimum security standards. Specifically, we were seeking to understand the technical makeup of these documents; which features and technologies are discussed, and which ones are not. We break down the various technologies, and what percentage of universities explicitly mentioned those, in Table 1. We also include the percentage of universities which include any statements of third-party information security assurances or discussions.

Physical and Personnel Security Within the physical and personnel security aspect, we sought to determine if physical device security or device locking policies were discussed. In the area of physical device security (e.g., keeping devices stored in locked offices), we found that 55.2% mentioned this topic. Duke University's minimum security standards document states, for example: "Locate workstations in an access-controlled environment. Keep laptops with you at all times or stored in a secured location. Use a lock to prevent laptop theft." Somewhat less comprehensively, Mississippi State University states the following about physical security: "Systems must be physically secure or encrypted with restricted access". For device locking (e.g., passcode requirements on a mobile device), we found that 58.6% mandated some form of additional security. The University of Alabama requires devices to be auto-locked, stating: "Devices shall be configured to automatically lock and require a logon, pin, or other means of authentication after being unattended or inactive for a predefined period of time." UCLA provides the following explanation and rule-set: "Unauthorized

physical access to an unattended Device can result in harmful or fraudulent modification of data, fraudulent email use, or any number of other potentially dangerous situations. In light of this, where possible and appropriate, Devices must be configured to 'lock' and require a user to re-authenticate if left unattended for more than 20 minutes."

Periodic Risk Assessment The final component we explored was the concept of Periodic Risk Assessment, or whether or not universities clearly specify their intention to continually review and update their pre-existing security documentation. In our data corpus, we found that only 6.9% clearly stated something reflecting this aspect in their security standards. The University of Cincinnati states: "OIS must review this document and must update or modify the standard requirements as necessary on at least an annual cycle." Similarly, UC San Francisco also mandates reviews on an (at minimum) annual cycle, stating: "The minimum standards in this document are reviewed, updated for applicability, and approved by the Information Security Committee (ISC) at least once a year or more often as determined by Security & Policy (S&P)."

Readability Analysis: Beyond the categorizations and quantifications of information from these minimum security standards, we also conducted readability analyses on these documents to be able to quantitatively discuss the makeup of these texts from a human-centered aspect. Utilizing the Flesch-Kincaid readability tests, we show the resulting readability scores for each university, along with the number of words in each standard to describe these documents.

We found that the mean readability score was 28.34 ($SD = 4.91$). According to the Flesch-Kincaid analysis, this places the average minimum security, plus or minus one standard deviation, at above a level of complexity necessitating a college degree (scores between 0 and 30). Mississippi State held the score for the most complex text, at 17.7 (college graduate or higher level), and Yale contained the most readable text at 38.1 (some college education). The average length of the minimum security standards was 1256.89 ($SD = 718.55$) words, with Duke University issuing the shortest minimum security standard, and UC San Diego publishing the longest.

Tonal Analysis: While readability scores can be one means of analytically describing text, we chose to analyze the tones of each minimum security standard to determine how these documents might be perceived by readers. The Watson Tone Analyzer tool allows for a tonal analysis across 13 dimensions, organized into three categories of high-level tones (Emotion, Language, and Social). The visualized results of this analysis can be found in Figure 1. Beginning with Emotional tones, we found that the majority of the standards did not convey a significant degree of emotion. However, there were 6 individual standards documents which portrayed a distinct level of emotion (between 40% and 52%); specifically, Joy (2 standards) and Sadness (4 standards). For example, standards that were perceived as having sad language included the use of words such as 'failures', 'discouraged', and 'vulnerable'.

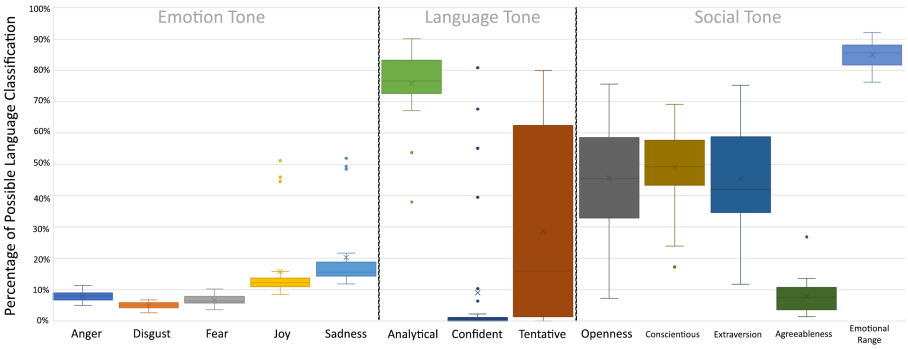
Although most of the examined minimum security standards were not inherently emotional, we found that the documents were very analytical in their nature. Only one standard was classified as being less than 40% analytical. Examples of statements classified as Analytical are: "Category I data is protected specifically by" or "Information Security Program Minimum Security Standards for Computer Systems". Within the Language Tone category, the concept of Confidence was the most disparate measure. In many instances, standards would be found to be 0% confident. In contrast, one standard was found to be highly confident at 80.85%. Examples of Confidence within this document included items such as: "Firewall rule changes must be documented and tracked." and "All vulnerabilities must be remediated within 30 calendar days.", among others. A number of standards also contained Tentative language. Generally, these classifications dealt with language that deflected responsibility away from a given standards document, and on to another authority. Examples of such language use included: "If you have questions, ask your supervisor, Departmental Security Administrator, or Information Security." or "Other countries may have requirements concerning access to data stored in or crossing their borders."

The third tonal category, Social Tone, was moderately applicable to nearly all examined standards. Concepts of Openness, Conscientious, and Extraversion were throughout well-represented. Examples of Openness included phrases like "The following standards apply to the use of Cloud Services provided by or arranged for by, the University:", while Conscientious concepts were extracted from phrases such as "You must read and understand the terms of use, including whether the provider has access to your data and what it can do with the data." Extraversion was also a predominant feature, represented by phrases such as the following: "Set up your system and applications to receive updates automatically except where specific business requirements prevent doing so." Many of the sentences classified as various Social Tones tended to show a certain directness in language, without being overly emotional or negative. Moreover, nearly all of the documents had a very low degree of Agreeableness. Lastly, based on the common occurrence of various Social tones through the examined security standards, we found that the documents had a high amount of Emotional Range, which is to say that the documents often expressed multiple sentiments throughout.

Standards Cross-Comparison: After determining the tone(s) and readability of each minimum security standard individually, we also compared each of the collected standards to each other. This ultimately yielded 807 document comparisons in total. Understanding potential commonalities between these documents can potentially provide insights about how these documents may have been created or where they might have drawn inspiration from.

We found that 86% of the compared standards shared less than 2% of content similarity between them. Examples of this would include simple, and common, phrase duplication such as "[...] the minimum security standards [...]". 7.8% of universities shared between 2% and 10% similar content to other documents. In these instances, longer, though still common phrases were duplicated including: "[...] may be made for patches that compromise the use of critical applications

Fig. 1: Tonal Analysis of Minimum Security Standards



[...]", or "[...] devices must not provide an active SMTP service that allows unauthorized third parties [...]".

Only 3.45% of documents shared a high level of similarity with other security standards (>10%). In these cases, sentences and sections were very related, only distinct from others via additional or redacted components of sentences. We demonstrate this via the two text blocks below:

[...] apply high severity security patches within seven days of publish, medium severity within 14 days, and low severity within 28 days. Use a supported version of the application.

[...] apply critical and high severity security patches within seven days of publish and all other security patches within 90 days. Use a supported version of the application.

In this example, we can most likely see some form of duplication occurring, with certain words or phrases omitted or added to separate the two sentences slightly and to account for different requirements. We also find that in these instances, visual styles duplicated as well. Within this dataset, we found that a number of standards seem to be designed in a similar fashion to that of Stanford University, which structures its document via a series of tables. For example, the documents of Stanford University and Virginia Tech share 56% of their content with each other, and appear to be based on the same visual design. We also encountered highly similar documents from universities within the same school systems. Examples of this included UC Berkeley and UC Merced sharing 70% of their standards, as well as UT Dallas and UT Austin, which shared 80%.

5 Discussion and Concluding Remarks

As has been remarked in other works [25], creating a dataset of information security policies, including minimum security standards, is a daunting task. When beginning this work, we attempted to acquire minimum security standards from corporations, but did not succeed. While universities are a seemingly suitable substitute, these documents are also not particularly easy to locate, and often

buried within much broader policy document repositories (e.g., including employment policies) that may even be distributed across various websites of a university network. This raises a concern with the authors. Namely, if we as researchers struggle to locate these security-relevant documents, how are regular users of these networks expected to 1) find these documents, and 2) follow these standards while using their devices on a given network. Rethinking the placement and accessibility of policies should be considered a contributing factor for improved organizational information security [2], and for increased involvement of employees and staff within an organization as valuable security assets [35].

In the event that an individual finds these standards, there is still a persistent issue of readability that seemingly plagues many policy-type documents [34] considering the average Flesch-Kincaid score of 28.34. Lessons that have been learned in studies on consumer-facing policies still seem to be seldom implemented, questioning the cross-cutting impact that this literature generally has in practical environments. An additional problem that we find in this space is the lack of definitions or terminology within many of these technical documents, with less than 25% of standards containing this information. Knowing that end-users generally struggle with technical jargon [11], including these technical definitions could be a way to increase readability for those who are less technically inclined. This is consistent with other literature in the legal space, which suggests that simplified sentence structure and terminology lead to higher comprehension among non-experts [31].

How Do Similar Standards Differ? The cross-document comparison shows that most documents do not share common phrases, which could be considered somewhat surprising given the specific focus of the document corpus. However, there are also several pairs of documents with a high degree of consistency across standards. For example, based on an exact language comparison, Stanford University and Virginia Tech are 56.10% similar to each other; a significant overlap. Specifically, Virginia Tech shares 56.10% of its content with Stanford's minimum security standard, while Stanford shares 44.10% of its content within the Virginia Tech standard. However, these direct language comparisons alone offer an incomplete picture of what is within these standards.

Finally, we can explicitly compare the individual factors occurring within a set of security standards. In our example, we find for our 29 measured items, that Stanford University contains 2 items that Virginia Tech does not include, and Virginia Tech lists 4 items that Stanford does not capture. More specifically, Virginia Tech has an effective start date, definitions for data sensitivity levels, a device-locking standard, and a password construction/maintenance standard; Stanford does not. Inversely, Stanford presents definitions for technical terms within the standard, and mentions system integrity, which Virginia Tech does not. What is perhaps surprising about this result is that Virginia Tech has the shorter standard based on word count (i.e., 1004 vs. 1314 words), but contains more items that we measured, at least at a high level, than Stanford.

A further key difference between documents relates to details and actionability (i.e., the ability given to a user to take action on a given item). In our

example, though these two university minimum security standards are very similar at a high level, Stanford's standard generally provided more comprehensive descriptions for each item within its standard, and often provided actionable instructions or hyperlinks that would allow anyone reading the document to learn more, or take immediate action to follow a given standard item. An example of this can be found regarding whole disk encryption, something both universities covered. Virginia Tech provided the following statement regarding whole disk encryption: "Use FileVault2 for Mac. Use BitLocker for Windows. Consider using Veracrypt if applicable." Stanford, for the same standard item, provided the following statement: "Enable FileVault2 for Mac, BitLocker for Windows. SWDE is recommended, option to use VLRE instead. Install MDM on mobile devices.", but also provided embedded hyperlinks for FileVault2, BitLocker, SWDE, VLRE, and MDM. Following any of these hyperlinks would display a highly detailed page describing how to implement each of these given technologies.

Actionability is an aspect that we did not consider in depth when running this initial document study. However, it is clear that even for similar standards, this hard-to-measure concept could be a critical factor in determining the effectiveness of these standards documents in practice. Standards that are able to provide immediate, actionable information should allow for a higher degree of understanding by readers of such a document, and ideally, of compliance as well.

How Different Are Dissimilar Standards? In the following, we discuss an example of low overlap according to our initial metrics. When directly comparing Boston University and the University of South Carolina based on text similarity, we observed a 0% match for each other; that is to say, that no exact duplicate sentences, statements, or short phrases were shared between the two documents. Again, beginning at a high level we analyzed the readability and length of both standards. The University of South Carolina was found to be 818 words long, while Boston University was 2,666 words long; a significant difference. In terms of readability, Boston University had a Flesch Reading Ease score of 31.3, while the University of South Carolina had a score of 24.6 (lower scores indicate a higher reading difficulty).

Focusing on the content found within the two standards, we also see a large number of differences between the two, with Boston University containing many more components than the University of South Carolina. Specifically, Boston University contained 14 measured items that South Carolina did not, while the University of South Carolina contained 4 measured items that Boston University did not include. Many of the similar items shared between the two universities were administrative features, such as including an effective date, and certain technical features, including logging, software patching, backups, 2FA, encryption, and anti-virus. Beyond this, however, a majority of the items were different from each other.

The differences continued when analyzing the visual format of the two standards. Boston University, for example, presented its standard in a semi-structured outline format, with large section headers and bullet points, with each point

containing one or more sentences describing the elements of the standard. The University of South Carolina opted for a table-based design, organized with each standard as a row item, with goals and options for meeting those goals displayed in a corresponding column. Both of these formats were seen frequently when examining standards, so these differences are not unusual. However, similar to the example above, the main difference between these two documents in terms of presentation is that of added details. Boston University provides more content, not only in the items included in their standard, but with the explanations detailing the standard as well. While intuition might suggest that these added details might lead to readability problems, our results suggest the opposite, showing that the lengthier, more detailed standard was easier to read than the shorter standard. This presents an interesting outcome for standards authors, as this shows that brevity may not always be the best action when writing technical documents.

2020 Updates. As the sample of minimum security standards was accessed in July 2017, and at the time of publication, it is 2020, we decided to "check in" on the standards to see what, if anything had changed. In short, the magnitude and comprehensiveness of changes was rather limited: only 11 of the 29 minimum security standards had been updated since we had last accessed them. In many instances, these changes were small. For example, Virginia State's standard had been updated twice with only minor revisions. For example, we observed the following change (Policy: June 16, 2020 - Endpoints section): "Install antivirus (e.g. Windows Defender) and configure to automatically update and run scheduled scans" was changed to "install antivirus software if possible and configure to automatically update and run scheduled scans."

For other standards, although they had been "updated", this did not necessarily mean that they contained up-to-date information or standards. In one such instance, at the University of Colorado, the minimum security standard (last updated on February 20, 2018) still noted that devices on the network should "Enable Windows XP or 2003 firewall". Considering that end-of-life occurred for Windows XP in 2014, this standard is woefully out of date [10]. In most other instances, it was not inherently clear as to what changes had been made to the security standards, and they appeared to be nearly identical to their predecessors. Only two security standards had undergone any significant changes. In one instance, at the University of Wisconsin, a previously singular security standard was now found to be broken up into several smaller components. In a second instance, the University of South Carolina had removed public access to their minimum security standard, placing it behind a single sign-on service. In summary, while some updates to these security standards have been made over recent years, they are *minimal*, and for a majority of security standards that we analyzed in the study, they have not changed or been updated in comparison to our sample from 2017.

Concluding Remarks Through our analyses, we find the key contribution of this paper: a very clear lack of consistency in the construction of minimum security standards, across a number of dimensions. Considering that these are all

organizations within one business sector (i.e., higher level education institutions), we should expect to find a reasonable amount of similarity between security standards, as the issues and threats faced by each organization are related.

We also find that while university standards contained technical items with a degree of consistency, covering topics such as patching, encryption, anti-virus, and more, we still found several that were severely lacking in this area. This is an issue that should be addressed; namely, that all standards should be required to meet at least a base specification of technical requirements. This disparity is more clear when it comes to the lesser-discussed administrative components of these standards; specifically, who writes/is responsible for them, when their effective dates are, when they were last updated, and when they will be updated again. This, however, becomes especially important, as technological threats develop rapidly. To illustrate this point, only 48.8% of the universities we sampled discuss backups. Over the past years, ransomware attacks have crippled numerous computing systems, including transportation systems and hospitals [26, 30]. One of the key defenses again ransomware attacks are consistent, secure backups [27, 40]. However, without a standards group who regularly reviews and updates these standards, these potential gaps in security could be left unchecked for a long period of time, making organizations (in our case, universities) a softer target for cyber attacks. This combination of modest technological comprehensiveness, and a slower re-evaluation of standards, is a clear issue that should be addressed by many organizations.

Finally, we noted the largest amount of dissimilarity across all of the universities in the areas of technological comprehensiveness, readability, and managerial aspects, and it is worth highlighting that *no* two universities shared exactly the same items in their minimum security standards. In this vein, we also wish to briefly discuss the presentation of these standards. In some instances, the security standards we viewed came in the form of a formal outline, detailing categories, sub-categories, and then items. Others present their minimum security standards in a very visual way, utilizing tables with technical rules, with check-marks indicating which systems, and types of data, are affected by a specific rule. Work is needed in this area to determine which methods are most suitable to visualize and present this information, similar to research previously conducted on privacy policies [23]. Another set of inconsistencies we encountered involved the intended target audience of a given standard. A number of security standards not only focused on end-users, but also servers, and a third category which was generally titled data/applications. Some standards had all of these target audiences, while others only had end-user information. Inversely, others may only have standards for servers, or administrators, but not end-users. This lack of consistency in the addressed audience of these standards is yet another issue worth noting, and hearkens back to the general theme of this section, and the title of the paper: the minimum security standards that we analyzed are not standardized.

Acknowledgements: We thank the reviewers and the participants of the Second Workshop on Security, Privacy, Organizations, and Systems Engineering for their feedback.

References

1. Anderson, R.: Security in open versus closed systems - The dance of Boltzmann, Coase and Moore. Tech. rep., Cambridge University, England (2002)
2. Ashenden, D., Sasse, A.: CISOs and organisational culture: Their own worst enemy? Computers & Security **39**, 396–405 (2013)
3. Barrick, M., Mount, M.: The big five personality dimensions and job performance: A meta-analysis. Personnel Psychology **44**(1), 1–26 (1991)
4. Baskerville, R., Siponen, M.: An information security meta-policy for emergent organizations. Logistics Information Management **15**(5/6), 337–346 (2002)
5. Braun, R., Stahl, S.: An emerging information security minimum standard of due care. Citadel Information Group, Inc (2004)
6. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. MIS Quarterly **34**(3), 523–548 (2010)
7. Burd, S., et al.: The impact of information security in academic institutions on public safety and security: Assessing the impact and developing solutions for policy and practice. Tech. rep., Project funded by National Institute of Justice, Office of Justice Programs, U.S. Department of Justice (2006)
8. Disterer, G.: ISO/IEC 27000, 27001 and 27002 for information security management. Journal of Information Security **4**(2), 92–100 (April 2013)
9. Doherty, N.F., Anastasakis, L., Fulford, H.: The information security policy unpacked: A critical study of the content of university policies. International Journal of Information Management **29**(6), 449–457 (2009)
10. Farhang, S., Weidman, J., Kamani, M.M., Grossklags, J., Liu, P.: Take it or leave it: A survey study on operating system upgrade practices. In: Proceedings of the 34th Annual Computer Security Applications Conference (ACSAC). pp. 490–504 (2018)
11. Felt, A.P., Ha, E., Egelman, S., Haney, A., Chin, E., Wagner, D.: Android permissions: User attention, comprehension, and behavior. In: Proceedings of the Eighth Symposium on Usable Privacy and Security (SOUPS). ACM (2012)
12. Grance, T., Stevens, M., Myers, M.: Guide to selecting information technology security products. NIST Special Publication 800-36 (2003), `https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-36.pdf`
13. Grossklags, J., Good, N.: Empirical studies on software notices to inform policy makers and usability designers. Financial Cryptography and Data Security pp. 341–355 (2007)
14. Hoepman, J.H., Jacobs, B.: Increased security through open source. Communications of the ACM **50**(1), 79–83 (2007)
15. Höne, K., Eloff, J.: Information security policy - What do international information security standards say? Computers & Security **21**(5), 402–409 (2002)
16. Hudock, A., Weidman, J., Grossklags, J.: Security onboarding: An interview study on security training for temporary employees. In: Proceedings of Mensch und Computer (MuC). pp. 183–194 (2020)

17. Humphreys, E.: Information security management standards: Compliance, governance and risk management. Information Sec. Tech. Report **13**(4), 247–255 (2008)
18. IBM: Watson Tone Analyzer - New service now available. IBM Cloud Blog (Dec 2016), information available at: `https://web.archive.org/web/20181206170813/https://www.ibm.com/blogs/bluemix/2015/07/ibm-watson-tone-analyzer/`
19. International Organization for Standardization (ISO): ISO/IEC 27002:2013 - Information technology - Security techniques - Code of practice for information security management (2013)
20. Johnson, M., Karat, J., Karat, C.M., Grueneberg, K.: Optimizing a policy authoring framework for security and privacy policies. In: Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS) (2010)
21. Johnson, M., Karat, J., Karat, C.M., Grueneberg, K.: Usable policy template authoring for iterative policy refinement. In: Proceedings of the IEEE International Symposium on Policies for Distributed Systems and Networks. pp. 18–21 (2010)
22. Karat, J., Karat, C.M., Bertino, E., Li, N., Ni, Q., Brodie, C., Lobo, J., Calo, S.B., Cranor, L.F., Kumaraguru, P., et al.: Policy framework for security and privacy management. IBM Journal of Research and Development **53**(2), 4–1 (2009)
23. Kelley, P.G., Bresee, J., Cranor, L.F., Reeder, R.: A nutrition label for privacy. In: Proceedings of the Fifth Symposium on Usable Privacy and Security (SOUPS). ACM (2009)
24. Kenning, M.J.: Security management standard - ISO 17799/BS 7799. BT Technology Journal **19**(3), 132–136 (2001)
25. Kotulic, A.G., Clark, J.G.: Why there aren't more information security research studies. Information & Management **41**(5), 597–607 (2004)
26. Krebs, B.: Hospital declares 'internal state of emergency' after ransomware infection. Krebs on Security (2016)
27. Laszka, A., Farhang, S., Grossklags, J.: On the economics of ransomware. In: International Conference on Decision and Game Theory for Security. pp. 397–417. Springer (2017)
28. Liginlal, D., Sim, I., Khansa, L.: How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management. Computers and Security **28**(3-4), 215–228 (2009)
29. Ma, Q., Pearson, M.: ISO 17799 :"Best practices" in information security management? Communications of the Association for Information Systems **15**, 577–591 (2005)
30. Mansfield-Devine, S.: Ransomware: Taking businesses hostage. Network Security **2016**(10), 8–17 (2016)
31. Masson, M., Waldron, M.A.: Comprehension of legal contracts by non-experts: Effectiveness of plain language redrafting. Applied Cognitive Psychology **8**(1), 67–85 (1994)
32. Mcdonald, A., Reeder, R., Kelley, P.G., Cranor, L.F.: A comparative study of online privacy policies and formats. In: International Symposium on Privacy Enhancing Technologies. pp. 37–55. Springer (2009)
33. Mercuri, R., Neumann, P.: Security by obscurity. Communications of the ACM **46**(11), 160 (2003)
34. Milne, G., Culnan, M., Greene, H.: A longitudinal assessment of online privacy notice readability. Journal of Public Policy & Marketing **25**(2), 238–249 (2006)
35. Pfleeger, S.L., Sasse, A., Furnham, A.: From weakest link to security hero: Transforming staff security behavior. Journal of Homeland Security and Emergency Management **11**(4), 489–510 (2014)

36. Richardson, R.: CSI computer crime and security survey. Computer Security Institute (2008), http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf
37. Saint-Germain, R.: Information security management best practice based on ISO/IEC 17799. Information Management **39**(4), 60 (2005)
38. Siponen, M.: Information security standards focus on the existence of process, not its content. Communications of the ACM **49**(8), 97–100 (2006)
39. Siponen, M., Willison, R.: Information security management standards: Problems and solutions. Information and Management **46**(5), 267–270 (2009)
40. Sittig, D., Singh, H.: A socio-technical approach to preventing, mitigating, and recovering from ransomware attacks. Applied Clinical Informatics **7**(2), 624–632 (2016)
41. Sohrabi Safa, N., von Solms, R., Furnell, S.: Information security policy compliance model in organizations. Computers and Security **56**, 1–13 (2016)
42. Susanto, H., Almunawar, M.N., Tuan, Y.C.: Information security management system standards: A comparative study of the big five. International Journal of Electrical Computer Sciences **11**(5), 23–29 (2011)
43. Thursby, J., Kemp, S.: Growth and productive efficiency of university intellectual property licensing. Research Policy **31**(1), 109–124 (2002)
44. U.S. News: National university rankings (2017), https://www.usnews.com/best-colleges/rankings/national-universities
45. von Solms, R.: Information security management: Why standards are important. Information Management & Computer Security **7**(1), 50–58 (1999)
46. Weidman, J.: Policies, Standards, and Practices: An Analysis of the Current State of Organizational Security at Universities and Corporations. Ph.D. thesis, Pennsylvania State University (2018)
47. Weidman, J., Grossklags, J.: What's in your policy? An analysis of the current state of information security policies in academic institutions. In: Proceedings of the European Conference on Information Systems (ECIS) (2018)
48. Weidman, J., Grossklags, J.: The acceptable state: An analysis of the current state of acceptable use policies in academic institutions. In: Proceedings of the European Conference on Information Systems (ECIS) (2019)
49. Weidman, J., Grossklags, J.: Assessing the current state of information security policies in academic organizations. Information & Computer Security **28**(3), 423–444 (2020)
50. Willinsky, J., Alperin, J.P.: The academic ethics of open access to research and scholarship. Ethics and Education **6**(3), 217–223 (2011)