Proceduralization in Cybersecurity: A Socio-Technical Systems Perspective

John W. Coffey
Department of Computer Science
The University of West Florida
Pensacola, FL. 32514, USA
jcoffey@uwf.edu

ABSTRACT

Cyberdefense is a difficult, multifaceted endeavor involving humans and technology. Complex Sociotechnical Systems (CSTS) theory espouses simultaneous optimization of both human behavior and systems, and holds that optimization of one without sufficient consideration of the other leads to a suboptimal final result. Many tasks in modern society are amenable to proceduralization – the process of defining a set procedure to perform normal activities and particularly, to deal with anomalous conditions. The purpose of this work is to elaborate the concept of CSTS in the context of cybersecurity, and then to explore proceduralization of cybersecurity work in that context. It describes an ethnographic study on proceduralization in cybersecurity with the goal of defining areas where established procedures are useful and where they are less so. The work reports on a case study that was performed at a mid-sized public university in the United States.

KEYWORDS

complex socio-technical systems, cyberdefense, preventative measures, proceduralization recovery

1 INTRODUCTION

In advanced economies, we increasingly live and interact with other people in complex, evolving, technology-driven workplaces. The nature of the interactions of people and systems create work environments that are highly variable from organization to organization. The interplay of people and technology creates significant challenges for those tasked with ensuring both physical and cybersecurity in the workplace. For instance, measures that increase security often decrease convenience and therefore, decrease overall job performance efficiency.

The work environment created by people interacting with technology and each other is described in the literature as a socio-technical system. Such systems are defined by two major characteristics [1]:

- Social and technical factors interact to create an environment that is either conducive or damaging to organizational success and goal attainment.
- Attempting to optimize either social or technical aspects without consideration of the other factor leads to increases in unpredictable system behavior that can be damaging to attainment of organizational goals.

A significant body of literature regarding socio-technical systems has been produced, including the concept of varying complexity within such systems. Complex socio-technical systems have been described as having the characteristics of socio-technical systems, but additionally, a large number of variable, dynamically interacting elements, and significant propensity toward unexpected variability [2].

Socio-technical system theory has arisen from the study of socio-technical systems. Socio-technical theory addresses methods to optimize simultaneously the functioning of people, systems, and the work environment the two create. Socio-technical system theory emphasizes organizational change that leads to a more secure, productive, resilient work environment in which technology positively contributes to the productivity of people.

From the perspective of cybersecurity, the environment created by the aggregate of people and machines in an organization is a complex socio-technical system. The cybersecurity endeavor is clearly complex because system security concerns must be considered in light of impacts on productivity of the workforce, a proliferation of systems and networks in any large organization, the potential for dangerous behaviors by end users, security lapses by systems administrators and software developers, and potential insider and external malicious actors.

Most existing information and cybersecurity solutions are techno-centric. Consequently, a potentially disproportionate emphasis is placed on using technology to attempt to keep people from taking dangerous or malicious actions. Ongoing training for large cohorts is expensive and disruptive, so one can understand why organizations might choose to take a more techno-centric approach. Considering the complexity of the cybersecurity ecosystem, many decisions must be made in order to optimize both security and productivity.

This paper contains an examination of the application of socio-technical systems (STS) theory in the cybersecurity domain. STS theory recommends the equal emphasis of both the social and technical aspects of security within particular environmental contexts in an organization.

The remainder of this paper contains an examination of literature regarding Socio-technical systems and theory pertaining to their management. It provides a description of research on proceduralization in the workplace to set the stage for a case study in proceduralization of cybersecurity operations at a mid-sized public university. It will conclude with a discussion of findings.

2 SOCIO-TECHNICAL SYSTEMS

Perrow's influential book [3] was one of the early works to identify the concept of socio-technical systems. One of his basic conclusions was that significant unexpected failures inevitably occur as humans seek to manage the increasingly complex, interacting systems that approach the realm of unmanageably complex. While Perrow's work was in the context of the nuclear power industry, principles he identified apply to the complex, interacting computer systems upon which we depend and the possibility of large-scale disaster inherent in cyber attacks and dangerous end user behaviors.

Cooper and Foster [1] state that humans interact with technology and each other in ways that either bode relatively well or poorly for system performance. Interactions can include cause and effect relationships that in some cases can be enumerated, but they also involve unexpected and essentially unpredictable interactions leading to unexpected and potentially highly negative results.

Saurin and Gonzalez [2] state that it is likely that all socio-technical systems (STS) have at least some characteristics of complexity. Computers are so pervasive in modern society that even historically "low tech" industries have evolved into socio-technical systems. The authors go on to suggest that some industries including the power generation industry, air travel, healthcare, computer security, and petrochemical industries might be regarded as "strongly complex," and that incompatibilities might exist between the basic nature of the system and the way it is managed.

Saurin and Gonzalez identify the following characteristics of complex socio-technical systems:

1. a large number of dynamically interacting elements. They state that, while some systems might have many parts, the complexity arises out of the changing nature of interactions among elements of the system.
2. unpredictable, non-linear behaviors with sensitive dependency to small changes in initial conditions, akin to chaotic systems.
3. a wide diversity of elements, both human and technical, that comprise the system. Interactions among these many elements are difficult to characterize.
4. unanticipated variability. The people and technology that comprise the system can interact in ways that cause outcomes that are difficult to predict without the benefit of hindsight.

5. resilience. While the first features of STS complicate management, complex systems might have resilience (ability to recover from damage) that is not found in simpler systems.

Saurin and Gonzalez present a case study regarding how to assess the compatibility of a complex system with the way it is being managed. Like Suarin and Gonzalez, others have suggested that management of a CSTS is often out of step with its nature, since those who work in such systems have a tendency to treat working situations simplistically [4].

Although a number of studies have proposed generic characteristics of CSTS [2, 5], they normally do not show, based on primary empirical data, how an actual STS can be described according to the enumerated characteristics.

There are many reasons to view cybersecurity from a CSTS perspective [6, 7]. Technological solutions cannot guarantee security, as there will always be security vulnerabilities in software. Reducing vulnerabilities in code is expensive and not ultimately successful. Malicious insiders with privileged access do damage even with the most secure software. Interestingly, with regard to human factors, procedures such as requiring frequent password changes may cause unanticipated problems when end users cannot remember all their passwords, write them down, and store them in unsecure places.

A focus on technological aspects of security may lead to a narrow view such as improving methods of detecting intrusion signatures. While highly focused work is obviously beneficial, there are so many different systems and problems to be addressed that a narrow approach is not the final answer. A more broad, global view of the problem is important as well.

Organizers of the Socio-technical Cybersecurity Workshop [7] set as a goal “taking a socio-technical approach identifying human, social, organizational, economic and technical factors that must be considered, techniques for understanding the interactions among them, and positive steps that can be taken to better protect and defend our information and critical infrastructure.” This goal illustrates the strong interconnectedness of cybersecurity systems and the potential for rapid evolution in the cybersecurity vulnerability landscape.

MoorKamp [16] describes the concept of "temporary design" within organizations, whereby more static, bureaucratic building blocks are "mixed and matched" in order to achieve agility. He cites potential vulnerabilities that emerge out of such approaches due to suboptimal coordination in crises and the possibility of system failure as a result. In the Cybersecurity context, the book is of importance when a breach has occurred and a crisis ensues.

Möller et al [17] provide a comprehensive, practical view of risk analysis and safety engineering in CSTS. Their book includes chapters on human factors engineering, communication of risk in organizations, safety automation, and principles for developing good procedures. While aimed very broadly at safety engineering across organization type, their principles have good applicability in Cybersecurity.

3 PROCEDURALIZATION OF WORK

This section contains descriptions of work on proceduralization. Research pertaining to proceduralization of digital forensics is discussed first, followed by an in-depth examination of a case study illustrating research methods that might be employed to examine congruence of proceduralization with organizational goals.

3.1 Proceduralization in Digital Forensics

Significant attempts have been made to proceduralize the digital forensics process. Sudyana et al [8] describe the need to adhere to a well-defined digital forensics procedure such as that specified in ISO 27037:2012. Reasons to follow a well defined forensics procedure are to

- adhere to the rule of law
- avoid contamination of the evidence
- ultimately provide convincing proof regarding what happened

They describe various frameworks [9, 10]. These frameworks often cull elements from a standard that the framers consider to be the most important for a certain application. Sudyana et all state that, while the frameworks might be useful, due to their complexity, investigators might omit elements of the standard, weakening the final result of the investigation.

Yeboah-Ofori et al [11] study cybersecurity threats to Cyber Physical systems. They are interested the role of decision trees in cybersecurity for Cyber Physical systems. Decision trees encode definitive processes for dealing with various contingencies and are a form of proceduralization.

In [12], Nowduri describes several best practices for cybersecurity including many that are subject to proceduralization. For instance, he advocates for a proceduralized incident and reporting structure, well-specified and mandatory training procedures, and many other practices such as having a policy of forcing browsers to use https.

3.2 Studying Efficacy of Proceduralization

Saurin's case study [2] seeks to assess the compatibility between a CSTS and the management of standard procedures (SPs). His group performed a study on operations in an oil refinery that had highly proceduralized processes. Saurin laid groundwork for the study by stating that some procedures are explicitly specified and some are tacit – not documented or verbalized. Saurin states that the literature is particularly ambiguous concerning recommendations about the level of detail and prescription of SPs in CSTS.

In the study, the researchers culled seven basic principles regarding use of SPs in CSTS from the literature:

1. Differences between what is prescribed in the SPs and the real work may be frequent, legitimate and normal.
2. Non-compliance to a SP is not necessarily regarded as a human error or something that should result in disciplinary actions.
3. The SPs should be designed, reviewed and monitored by a team of representatives from all the areas affected by them.
4. The content of SPs should state their relationships with other elements of the socio-technical system, stressing the underlying reasons and impacts of these relationships.
5. The content of SPs should state possible triggering factors that may indicate the need to adjust them.
6. The gap between a SP and real work should be monitored to approximate the prescribed work to the actual work.
7. Workers should be trained in order to realize when and how to adapt the procedures.

They then assessed the degree to which employees agreed with the principle (the degree to which the principle is how it *should* be) and the degree to which the principle is actually upheld (how it *actually is*). They cited a variety of results including low or high overall agreement with the principle and either a consistent level of agreement or a relative lack of agreement between how valid the participants in the study thought the principle to be and the degree to which it was actually enforced in practice.

Generally, agreement that the principle was valid and should be in place was higher than perceptions of how adequately the principle was enforced. Suarin et al conclude that the literature is not clear on whether it is preferable to have extensive SPs or not.

Clearly, a continuum exists from minimal specification, which allows for judgment and experience to play a significant role in decision-making, to highly specified, which reduces variability in prescribed methods, but not necessarily in outcomes.

Aviation and nuclear power plants have relied on highly proceduralized systems with success. However, considering the ongoing evolution of threats in the cybersecurity environment, it is likely that identified practices might well become sub-optimal in light of a rapidly evolving threat. Others might simply become obsolete. Maintaining currency in SP descriptions and documentation entails an entirely separate challenge.

4 A CASE STUDY IN CYBERSECCURITY PROCEDURALIZATION

This section contains a description of a study of proceduralization of cybersecurity activities at a medium-sized regional comprehensive university in the United States. The following sections first provide descriptions of the organization’s information technology infrastructure, the IT support structure, technical staff organization, and security capabilities. It then presents a description of the implementation of security procedures as well as awareness of and adherence to specified procedures.

4.1 Information Technology Infrastructure and Support

The university’s IT infrastructure includes many computer systems for both academic and administrative purposes. Major software includes an ERP system for both student and administrative records. A popular LMS is used for online and face-to-face class resources. Several online synchronous meeting software programs are available for the conduct of online class delivery. Video recording software is widely used.

A large suite of Microsoft productivity tools, and many discipline-specific hardware and software capabilities are also employed. Student records are subject to FERPA privacy regulations that raise the stakes in protecting sensitive information. Student health services have HIPPA-regulated private information. Employee records contain significant amounts of sensitive, personally identifiable information. Consequently, security concerns loom large.

Two groups support the IT infrastructure: Information Technology Services (ITS), a centralized capability for all academic and administrative systems, and Local Service Providers (LSPs) who work for the various administrative units including the five colleges, Academic Affairs, Veterans Services, etc. While their numbers vary, there are approximately 34 IT employees who are listed as having LSP responsibilites. Some in that cohort are responsible for other support besides information technology.

Security concerns pervade operations within ITS. ITS has both a significant role in hardware and software systems acquisition and in-house software development and maintenance. Unlike in larger organizations where they would often be separate positions, the Director of Infrastructure Services also has responsibilities as the Chief Information Security Officer (CISO). A second ITS employee's work responsibilities are largely cybersecurity-related. All ITS employees are made conscious of cybersecurity concerns in an ongoing fashion through regular briefings and periodic updates on policy changes.

Communication and coordination between ITS and the LSPs occur through a variety of channels and at varying times throughout the year. Three scheduled meetings recur via policy and may be deemed as standard operating procedure. In those meetings, ITS creates an agenda of informational items to disseminate to the LSPs. ITS encourages the LSPs to bring issues for discussion. Any significant system changes are tracked by JIRA tickets and therefore, viewable on both ends. A dedicated Slack channel is available to foster communication between ITS and LSPs, and it is monitored by ITS personnel and LSPs. ITS has an LSP group in email.

The security infrastructure has evolved over time by picking and choosing best practices from the NIST Cybersecurity Framework [13] and from Center for Internet Security (CIS) [14] guidelines. The university has a Security Incident and Response Team (SIRT) that handles security issues. The SIRT is comprised of four permanent members with additional members added as needed, determined by the nature of the event. Examples of issues the team has addressed include passwords that have been compromised, malware that has been installed on end user machines, a bitcoin mining operation that was being carried out on university machines, a ransomware attack on the university, etc.

4.2 Goals and Methods of the Study

The goals of the current study are to explore various issues surrounding the proceduralization of the cybersecurity effort at the university, including the degree of proceduralization to be found, where and when procedures originate, how they are updated, and how they are communicated to interested parties.

For the study, two sets of questions were developed, one for security people within ITS (see Appendix A) and one for the LSPs (Appendix B). Pre-study interviews with ITS personnel and the author's departmental LSPs helped identify differences in the viewpoints of those two groups that suggested the need for two different sets of questions. After acquiring IRB approval, an ethnographic study was carried out with two focus groups, one involving ITS personnel and the other with a group of LSPs

The ITS CISO convened a meeting for discussion of the questions that were to be answered from the ITS perspective. Given the large number of LSPs, a standard recruitment effort for this study involved contacting the most senior LSP within each organizational unit to set up the meeting for the LSP interview. Interviews were conducted, and results of the interviews were determined by employing a textual content analysis approach [15].

4.3. Study Results

The following sections report on the results of interviews with ITS personnel and LSPs regarding proceduralization of the cyber defense and recovery endeavor. Additionally, the following section addresses the evolution of the conceptualization of the nature of a procedure as the idea is applied to cybersecurity. A broadening of the notion appeared necessary in order to encompass operations that, while not officially codified as standard procedure (SP), are so enmeshed in the operating culture as to take on that status de facto. Commentary on implications of the de facto nature of policies and procedures that might be more rigorously codified is also described.

Proceduralization had originally been couched in quite strict, narrow terms as “step-by-step practices, formalized in organizational documentation, promulgated by formalized training of relevant employees, and assessed for compliance” (author’s definition). One basic result of the current study was appreciation of the fact that proceduralization constitutes a range from the aforementioned strict definition to best practices engrained in the culture of the organization and promulgated by less formal means such as on-the-job training. Under such a definition, assessment of compliance is ad-hoc, typically after the fact of a substantive evolution in operations or a procedure-triggering event.

4.3.1 Standard Procedures (SPs) From the ITS Perspective

Numerous SPs were identified in interviews with ITS personnel. The most extensively proceduralized administrative division is the ITS Help Desk. SPs were in place for virtually all aspects of the end user support function including those that pertain to security. The ITS Help Desk function has specified procedures for dealing with deviations from SPs.

Several factors led to the extensive proceduralization of Help Desk operations including the fact that frontline support personnel are among the most junior employees and high turnover occurs in those positions. The need to maintain currency of support for deployed systems, software, and adverse event response dictate a high degree of proceduralization. Also, the perceived need to present a consistent public face dictates extensive use of SPs by frontline support personnel. Second and third tier support personnel have more agency and hence, more discretion in how to handle security issues.

Nevertheless, higher level support personnel have SPs for handling security incidents. Two security-related procedures were identified:

- How to convene the Security Incident Response Team
- Notifying top-level administration so they are not blindsided by (for instance) the press seeking information about a potentially damaging incident

Within ITS, procedure development arises proactively and reactively. Proactive procedure development arises from keeping abreast of current events including publicized exploits and vulnerabilities. Evolutions of NIST and CIS standards lead to implementation of new SPs. Ongoing surveillance of problems others have had leads to preemptive efforts to evolve policies and procedures to prevent similar problems. New procedures also arise reactively from responses ITS has had to make to security problems that have arisen.

With regard to the balance between security procedures pertaining to humans vs technologies, some interesting results were found. It was the perception of ITS that somewhat more effort is directed to the technological side since ITS has better control over technologies than over the actions of people.

ITS has implemented multiple systems that provide ongoing security monitoring. An Intrusion Detection System scans devices looking for command and control codes in a package, specific signatures, or other anomalies. Procedures are in place to handle anomalous conditions. A second system crawls university computers looking for endpoints where sensitive information is stored. Procedures have been formalized regarding how to handle situations in which end users have sensitive information in places that might present security vulnerabilities. The university also retains the services of an external organization that scans open ports in the university firewall to find public web applications that might have issues such as SQL injections, cross-scripting vulnerabilities, etc.

In addition to restrictive firewall rules, ITS uses micro-segmentation strategies to gain more fine-grained control over sensitive data, all made possible by software-defined networks. ITS has evolved the current configuration of network segments over years. Segmentation policies are enforced, rising to the level of procedures.

On the human side, ITS has a policy of having users agree to a standard "Computing Resources Agreement" every time they log onto any university computer. The agreement includes two statements regarding security:

- Computing users shall adhere to established security procedures and shall not access resources to which they are not entitled, including but not limited to, representing themselves as someone else and altering or fabricating of records.
- Computing users will not connect personal computing devices to the UWF wired network. Only UWF Information Technology staff may connect computing devices to the UWF wired network.

ITS has a policy that LSPs must present a clear reason to ITS in order for an end user to have administrative privileges on their systems. By SP, no one but LSPs and ITS personnel have administrative privileges. The case must be made that the prospective grantee of administrative privileges both has clear need and the capability to avoid behaviors that are dangerous from a security perspective.

Policies and procedures are documented in Confluence pages. New policies and procedures are continually being added. ITS personnel suggest that the documentation on the “well-traveled paths” tends to be more current than less commonly invoked items. As in all cases, documentation currency and maintenance can be problematic with ongoing pressure to maintain operations in a rapidly evolving environment. The communication channels previously described are used to notify interested parties, including those who must adhere to the procedures and those who enforce them.

4.3.2. Standard Procedures From the LSP Perspective

LSPs function in surprisingly diverse contexts across the university community, and, while sharing many of the same basic concerns as ITS personnel, all tend to have issues specific to their particular constituencies. For instance, public facing administrative units that have large numbers of casual, external visitors needing guest access to computers and the Internet have concerns above and beyond more cloistered administrative units and academic units with specified user populations.

Among academic departments, those such as Computer Science and Computer Engineering and technically oriented departments in the College of Education and Professional Studies have additional concerns with maximizing student access to and use of technology while attempting to minimize the likelihood that such use creates vulnerabilities.

The LSPs consistently reported (in a fashion similar to ITS folks) that, while procedures are in place to manage risks stemming from both technology and people, more emphasis has been placed on technological controls than on security awareness and training for people. The prevailing view was that both ITS and LSPs have control over technology in a way that they do not have over humans.

LSPs stated that it is a challenge to keep users attentive to security threats spanning a wide range, from covering computers when severe weather threatens to the presence of phishing attacks. Some LSPs expressed the viewpoint that it can be difficult to keep members of the tech support community attentive to cybersecurity concerns because of a broadly held view that technically-oriented cybersecurity operations are primarily the responsibility of ITS.

Several years ago, a university-wide policy was put in place that all university employees would need to undergo cybersecurity training. ITS created the plan, but it fell to LSPs via designated security officers in the various academic and administrative units, to enforce training requirements. The original plan was to revoke access privileges of those who did not complete the training. While nearly 90% of all employees completed the training successfully, the university ultimately did not rescind access for those who did not. Results of that initiative, while ultimatedly deemed successful, likely helped create a more techno-centric focus to the overall cybersecurity effort.

LSPs expressed varying degrees of concern and identified varying policies and procedures for physical security, network security and systems security. With regard to physical security of computing assets, many issues were identified including management of room keys, record keeping for enabled and disabled wired ports, physical access to desktop computers and physically securing machines that are available to the public. While many policies and procedures were in place for these concerns, consistent enforcement was characterized as difficult.

Network security raises many issues including policy on port management and firewalls, and potential (mis)uses to which networked computers might be subjected by end users. Systems security concerns that were specified included how to ensure that timely software updates are enforced, and how to manage userids and passwords. A centralized system that tracks all employees' access privileges and procedures to manage that system have improved access management. Significant mention was made regarding the handling of machines that are thought to have been infected or that were used by departing people.

Some LSPs stated that they did not try to do much with machines that were identified as having malware; such machines are re-imaged from the bottom up. Similarly when personnel leave, their machines are re-imaged to remove any potentially sensitive information on the machine.

An interesting finding from the LSP perspective was that many de-facto SPs exist but they are not codified. Without codification, they are essentially unenforceable. The university has a SP regarding the inclusion of verbiage in the login screen of all university computers. The verbiage is essentially a mini-acceptable use policy statement. LSPs expressed the opinion that it would be beneficial to have more extensive end-user policies and procedures so that enforcement would have more teeth.

LSPs also discussed the concern that they are often called upon to perform "soft" collateral duties for which no SP or policy exists. In such situations, it can be difficult to know for sure how to carry out the task in a way that does not compromise security. More collateral duties also impact the amount of time available to carry out the core activities (including those that are security-related) of the LSPs' positions.

LSPs interviewed consistently stated that ITS takes the lead in originating new operating procedures. They generally felt that sufficient

Table 1. Top-level proactive and reactive procedures identified in the study.

	Proactive Procedures	**Reactive Procedures**
ITS	Security System Maintenance - Maintain IDS - Maintain university firewall - Maintain/evolve segmentation policy - Grant/rescind administrative privileges Communication - Convene LSP meetings - Maintain procedure documentation Research - Review CIS/NIST guidelines - Evaluate external security failures - Originate mew procedures Monitor user compliance Monitor moving data	Convene SIRT - Select additional members - Create plan to handle event - Run forensic procedures Inform upper level administration
LSP	Physical Security - Manage access to rooms - Enable access for visitors - Control software/hardware inventory Network Security - Manage ports and firewalls - manage access privileges System Security - manage new user setup - manage decommission of machines - manage software updates - group management/privilege control Monitor user compliance	Take emergency control measures Escalate event to ITS

channels of communication were open between ITS and LSPs and that LSPs could originate university-wide security policies and procedures if they came upon a compelling need for such. The university has had an initiative to encourage two-factor authentication but has not, so far, made it a requirement. Table 1 provides high-level summary of proactive and reactive responsibilities of ITS and LSPs identified in the study.

5. DISCUSSION

Results of the surveys indicate that there is broad perception of good communication of security issues between ITS and LSPs. Generally, ITS is perceived to have primary responsibility for global technological security operations such as administration of the university-wide malware protection software, firewall policy and control, monitoring of sensitive data movement, etc. LSPs have more of the human-centric concerns such as group management and privilege control, enforcing users' work on training materials, managing machines that are to be deployed to new users or wiped when current users relinquish them.

There are many standardized practices for carrying out the myriad tasks of both ITS personnel and LSPs, but many generally accepted practices are not strictly written as enforceable procedures. Some LSPs expressed the opinion that more codified procedures would aid in compliance by making sanctions for lack of compliance more enforceable.

While extensive proceduralization of preventative and remedial security measures was found in this organization, higher level security personnel still have significant agency when making security decisions. Ongoing research ensures that policies and procedures continue to evolve and change, usually under ITS' lead. The continually evolving threat landscape necessitates affording some freedom of action and the ability to improvise, particularly among higher level personnel.

Proceduralization is extensive in terms of specified security settings defined by organizations such as CIS that are used by the organization studied here. For example, a download of the CIS Benchmarks for Android 1.2.0 proscribes 27 security settings, 10 privacy settings and 6 Android Chrome Browser settings. Enumerating such settings creates a procedure for assessing security and privacy in a device. SPs would specify that users employ such settings and technical professionals would need to check that such specifications are followed.

However, adherence to SPs enumerated by NIST and CIS present their own challenges since such standards are extensive and evolve with technology. For instance, CIS currently publishes five versions of the benchmarks for Android between 6/28/2012 and 8/6/2018. Each version represents a significant evolution from the prior one, typically with a longer specification.

CIS provides multiple revisions of standards for 11 separate flavors of Linux/UNIX, Windows, Windows Server, VMWare, Apache, Tomcat, PostgreSQL, Cassandra, Oracle, MySQL, Kerberos, etc. Although destined to be challenging because of the sheer volume of such standards, organizations with limited approved products lists can more readily ensure adherence to benchmarks such as these. Academic institutions that must employ a great many disparate technologies might arguably have a more difficult time confirming adherence, since many disparate technologies are used in their operations.

As cited in the literature pertaining to proceduralization of cybersecurity operations, standards such as ISO 27037:2012 provide detailed procedures for crime scene investigation after an incident has occurred. However, implementation of the entire standard is time-consuming, costly, and not always feasible in the chaos following a data breach. The current study illustrates the inherent difficulties in specifying actionable procedures in rapidly evolving complex socio-technical systems, and ensuring that all the proper actions are taken.

The current study also illustrates that many SPs are clearly specified and others are essentially tacit. It would be expected that, if this is the case in an industry such as oil refining or nuclear power (where operations do not change and evolve rapidly day by day), it could only be expected in a rapidly evolving ecosystem such as cybersecurity. The current study finds a truly "mixed bag" of codified SPs, tacit or implicit SPs, and areas where human judgment is still foremost in determining a course of action in the University setting.

The complex interplay of humans and technology in the case study presented here make clear how multi-faceted the cybersecurity effort is. It is also clear that the people in charge of security tend to have a more technology-focused approach to their work due to the fact that technology is more controllable than people. Complex Socio-technical Systems theory would suggest that, even though it is expensive, to some degree disruptive to work lives, and sometimes not well-received, the human aspects of cybersecurity must remain a central focus.

6. CONCLUSIONS

Proceduralization takes out some of the uncertainty regarding how humans will perform in complex socio-technical systems. Proceduralization is extensive in many such systems including power plants, manufacturing facilities and airline operations and maintenance. The cybersecurity effort seems less amenable to proceduralization than other complex socio-technical systems for a variety of reasons.

Overall, it is evident that, while many aspects of cybersecurity defense and recovery after an attack are susceptible to proceduralization, many are not. Given the rapidly evolving nature of cybersecurity threats and defenses, identification, development, and documentation of SPs occurs at a more rapid rate than in highly proceduralized settings such as oil refineries or nuclear power plants. Such rapid evolution suggests that procedure creation and maintenance, while critical, are difficult. Judgements of procedure obsolescence and their removal is an entirely separate issue.

REFERENCES

[1] Cooper, R., Foster, M. Sociotechnical systems. American Psychologist, 26, pp 467--474. (1971).

[2] Saurin, T. A., Gonzalez, S. S. Assessing the compatibility of the management of standardized procedures with the complexity of a sociotechnical system: Case study of a control room in an oil refinery. Applied Ergonomics. 44. pp 811--823. (2013).

[3] Perrow, C. Normal Accidents: Living with High-risk Technologies. Princeton University Press, Princeton, NJ. (1984).

[4] Blakstad, H., Hovden, J., Rosness, R. Reverse invention: an inductive bottom-up strategy for safety rule development. A case study of safety rule modification in the Norwegian railway system. Safety Science 48, pp 382--394. (2010).

[5] Cilliers, P. Complexity, deconstruction and relativism. Theory, Culture & Society. 22 (5). pp. 255--267. (2005).

[6] Sociotechnical Cybersecurity Workshop, December 12-13, 2016. Hyattsville, MD 20783, United States, Online, Available: https://cra.org/ccc/events/sociotechnical-cybersecurity/

[7] National Cyber Security Center. A Sociotechnical Approach to Cybersecurity. Online, Available: https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1513173793.pdf

[8] Sudyana, D., Prayudi, Y., Sugiantoro, B. Analysis and Evaluation Digital Forensic Investigation Framework Using ISO 27037:2012. International Journal of Cybersecurity and Digital Forensics. 8(1). pp. 1--14. (2019).

[9] Yusoff,Y., Ismail, R., Hassan, Z. Common Phases of Computer Forensics Investigation Models. Int. J. Comput. Sci. Inf. Technol., 3(3). pp. 17--31. (2011).

[10] Kohn, M.D., Eloff, M.M., Eloff, J. Integrated digital forensic process model, Computer Security, 38. pp. 103--115. (2013).

[11] Yeboah-Ofori, A., Abdulai, J-D., Katsriku, F. Cybercrime and Risks for Cyber Physical Systems. International Journal of Cybersecurity and Digital Forensics. 8(1). pp. 43--57. (2019).

[12] Nowduri, S. Critical Thinking Skills and Best Practices for Cyber Security. International Journal of Cybersecurity and Digital Forensics. 7(4). pp. 391--409. (2018).

[13] NIST. NIST Cybersecurity Framework. Online. Available: https://www.nist.gov/cyberframework

[14] Center for Internet Security. Cybersecurity Best Practices. Online. Available: https://www.cisecurity.org/cybersecurity-best-practices/

[15] Neuendorf, K. A. The Content Analysis Guidebook, 2nd ed. Thousand Oaks, CA: Sage. ISBN 978-1412979474. (2017).

[16] Moorkamp, M. Operating Under High-Risk Conditions in Temporary Organizations: A Sociotechnical Systems Perspective. Routledge. ISBN: 9780815395027. (2018).

[17] Möller, N., Hansson, S. O., Holmberg, J. E., Rollenhagen, C. (Eds.). Handbook of safety principles (Vol. 9). John Wiley & Sons. (2018).

Appendix A.

Proceduralization in Cyber Defense and Remediation

ITS Cybersecurity Questionaire

General Cybersecurity-related questions

1. Does UWF have staff (ITS or LSP) whose only job is security related?

If so, how many?

If not, do you view this as a problem? Elaborate.

2. What is your perception of current top-level administration support for cybersecurity?

3. How does ITS strike the balance between the level of resources dedicated to security and the level dedicated to other functions?

4. Do you base the cybersecurity effort on a specific framework such as the NIST Cybersecurity Framework?

5. Is cybersecurity support at UWF appropriately balanced between expenditures for technology and for human factors (training)?

6. Do we have university-wide standard procedures for Cyber defense?

Proceduralization

1. What preventive procedures does ITS employ?

2. What is the mix of technological vs human-focused preventative procedures? How do you strike this balance?

3. What detection and response procedures has ITS specified? Has ITS had to use any of them? If so, how was their perceived effectiveness?

4. Who determines ITS standard cybersecurity procedures, and how is that achieved?

5. To what degree and how are standard procedures communicated to LSPs?

5. Can LSPs originate new practices that become standard procedures? If so, has that happened?

6. What steps are taken to ensure that ITS security specialists and LSPs follow procedures/best practices?

7. Does ITS have standard procedures that pertain to in-house software development?

8. Is it generally held that systems specialists or software developers might sometimes diverge from standard procedures with proper cause?

9. How and how often are procedures updated?

10. How are changes in procedures promulgated within ITS and to LSPs?

Appendix B

Proceduralization in Cyber Defense and Remediation

LSP Questionnaire

1. Are you aware of university-wide standard procedures for Cyber defense?

If yes:

2. What preventive procedures are you aware of?

3. What is the mix of technological vs human-focused preventative procedures? Do you perceive a proper balance?

4. What detection and response procedures do we have? Have you had to use any of them? How was their perceived effectiveness?

5. Who determines standard cybersecurity procedures?

6. Can LSPs originate new cybersecurity practices that become standard procedures? If so, has that happened?

7. What steps are taken to ensure that LSPs follow procedures/best practices?

8. How are procedures updated?

9. How often are procedures updated?

10. How are changes in procedures promulgated to LSPs?

If No:

11. Would you favor having Cybersecurity-related standard procedures for cyberdefense and/or attack recovery in place?

If yes:

12. What procedures would you like to have in place?