



SCHOOL of
GRADUATE STUDIES
EAST TENNESSEE STATE UNIVERSITY

East Tennessee State University
**Digital Commons @ East
Tennessee State University**

Electronic Theses and Dissertations

Student Works

12-2013

Physical Security Assessment of a Regional University Computer Network

Nathan H. Timbs

East Tennessee State University

Follow this and additional works at: <https://dc.etsu.edu/etd>



Part of the [Computer Sciences Commons](#)

Recommended Citation

Timbs, Nathan H., "Physical Security Assessment of a Regional University Computer Network" (2013). *Electronic Theses and Dissertations*. Paper 2280. <https://dc.etsu.edu/etd/2280>

This Thesis - Open Access is brought to you for free and open access by the Student Works at Digital Commons @ East Tennessee State University. It has been accepted for inclusion in Electronic Theses and Dissertations by an authorized administrator of Digital Commons @ East Tennessee State University. For more information, please contact digilib@etsu.edu.

Physical Security Assessment of a Regional University Computer Network

A thesis

presented to

the faculty of the Department of Computer Science

East Tennessee State University

In partial fulfillment

of the requirements for the degree

Master of Science in Computer Science

by

Nathan Timbs

December 2013

Dr. Michael Lehrfeld, Chair

Dr. Phillip E. Pfeiffer IV

Dr. Rita M. Barrios

Keywords: Physical Security Assessment, Information Assurance, Security Requirements

ABSTRACT

Physical Security Assessment of a Regional University Computer Network

by

Nathan Timbs

Assessing a network's physical security is an essential step in securing its data. This document describes the design, implementation, and validation of PSATool, a prototype application for assessing the physical security of a network's *intermediate distribution frames*, or IDFs (a.k.a. "wiring closets"). PSATool was created to address a lack of tools for IDF assessment. It implements a checklist-based protocol for assessing compliance with 52 security requirements compiled from federal and international standards. This checklist can be extended according to organizational needs.

PSATool was validated by using it to assess physical security at 135 IDFs at East Tennessee State University. PSATool exposed 95 threats, hazards, and vulnerabilities in 82 IDFs. A control was recommended for each threat, hazard, and vulnerability discovered. The administrators of ETSU's network concluded that PSATool's results agreed with their informal sense of these IDFs' physical security, while providing documented support for improvements to IDF security.

TABLE OF CONTENTS

	Page
ABSTRACT	2
LIST OF FIGURES	6
Chapter	
1. INTRODUCTION	7
2. LITERATURE REVIEW	12
Overview.....	12
Risk Management	12
Risk Assessment	15
Vulnerability Assessment	16
Physical Protection Systems Vulnerability Assessment.....	16
The Vulnerability Assessment Team.....	18
Network Infrastructure Vulnerability Assessment	19
FEMA Vulnerability Assessment	20
Standard Practice	20
ISO/IEC 27000-Series Information Security Management Standards	20
ISO/IEC 27001.....	21
ISO/IEC 27002	23
NIST Security Controls.....	23
NIST Control Assessment	25
Legal Compliance	28
The Sarbanes-Oxley Act.....	28
The Gramm-Leach-Bliley Act	29
Best Practices for IDF Security.....	30

Chapter	Page
3. METHODOLOGY	32
Overview.....	32
Scope	32
Soundness	33
Coverage of Key Recommendations	33
Procedural Soundness	35
PSATool Practicality	35
PSATool Effectiveness	36
4. RESULTS	38
Overview.....	38
PSATool	38
PSATool Assessment Form	39
PSATool Database	40
Results Soundness.....	42
Physical Security Requirements	42
Assessment Procedure	46
PSATool Practicality	46
PSATool Effectiveness	48
Assessment Data Collection	49
Assessment Results Overview	50
Data Reporting	52
5. CONCLUSIONS.....	54
Recommendations for Future Work.....	55
Summary.....	57

Chapter	Page
WORKS CITED	62
APPENDICES	66
Appendix A: PSATool Assessment Form	66
Appendix B: Physical Security Requirements	67
Appendix C: Traceability Matrix	69
Appendix D: Database Queries	70
Appendix E: Database Table Diagram	72
Appendix F: PSATool Database Entity-Relationship Diagram	73
Appendix G: Requirement Data Summary	74
Appendix H: THV Data Summary	79
Appendix I: Assessment Recommendations	80
Appendix J: Discovered Threats, Hazards, and Vulnerabilities	82
Appendix K: Recommended Controls for Threats, Hazards, and Vulnerabilities	84
VITA	85

LIST OF FIGURES

Figure	Page
1. PSATool sample data entry screen format.....	9
2. Vulnerability Assessment Threat-System Matrix.....	19
3. PSATool Assessment Form sample.....	39
4. PSATool THV portion.....	40
5. PSATool query results format	41
6. Traceability Matrix sample	43
7. PSATool completion instructions.....	46
8. Number of requirements passed per IDF.....	51

CHAPTER 1

INTRODUCTION

The number of computer networks continues to increase as computing becomes more distributed and decentralized. Increased dependence on networked computer systems as infrastructure involves risks that continually emerge and evolve (Kairab, 2005). Security *controls* are intended to reduce these risks. These controls involve constraints on the deployment and use of equipment, policy, and procedure.

Physical security controls, security controls intended to protect material assets and operating environments, are essential to network operation and protection (Pholi, 2003). These controls include security alarms, fire alarms, and entry control systems, as well as power backup and environmental monitoring systems, including temperature and humidity control systems (Richards, 1982). Proper control implementation is essential to assure the confidentiality, integrity, and availability of information assets (Stoneburner, Goguen, & Feringa, 2002).

Physical security controls, like other mechanisms for assuring network and information security, can be difficult to implement. Defending assets from all potential threats by all conceivable attackers and means of attack is impractical (Johnston & Garcia, 2002). Justifying costs and measuring performance is difficult, due to the difficulty of identifying attempts at attacks and correlating thwarted attempts with specific defenses and potential damage. Security and support processes tend to be reactive in that system hardening is usually undertaken as a specific response to a specific security incident (Johnston & Garcia, 2002).

One common approach for securing assets uses government regulations and best practices as a basis for selecting controls. This work is concerned with the use of this approach to select and assess network-related physical security controls in university information systems.

These assets include student and employee financial, academic, and healthcare records, which universities manage as a matter of routine. The privacy and security of these records is governed by State and Federal regulations, including the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA). These regulations mandate that sensitive information that a network hosts be secured against unauthorized access.

Network-enabled services provided by universities that can expose sensitive information to unauthorized access include e-mail, Internet access, and network data storage. A typical campus network allows a university's students, administrators, and faculty to access these services via hard-wired Ethernet connections. These connections require cabling from each user's computer to a device, known as a switch, that links its users to the campus network. Switches and their support equipment are often housed in wiring closets, or *intermediate distribution frames* (IDFs). Usually found in at least one location on each floor of a building, IDFs contain equipment racks filled with networking switches, patch cables, power supplies, and fiber optics that connect to a *main distribution frame* (MDF). The MDF typically connects an entire building to a server room or data center (Cisco Systems, Inc., 2004).

Switches and other forms of network equipment are vulnerable to many modes of physical attack. Whether deliberate or unintended, physical access to network equipment can result in equipment and service loss. An attacker in close proximity to a network can record and interpret the electronic signals radiated by an operating network. Physical access to network hardware can permit electronic eavesdropping through the use of a protocol analyzer. Physical access can allow network services to be disrupted by flooding the network with traffic.

Physical security controls can reduce the risk associated with these types of attacks. These controls, however, are an often overlooked component of network and information

security (Pholi, 2003). While many well-known tools like Saint (2013), NTOSpider (2013), and Nessus (2013) support the assessment of electronic security and discovery of cyber vulnerability, there are few physical security assessment tools designed to record, evaluate, and compare the state of physical security controls of IDF's to physical security standards and best practices. Tools incorporating physical security assessment based on individual standards exist, e.g., SANS BS/ISO/IEC 17799 Checklist (Thiagarajan, 2006). However, an Internet search including the online literature databases of the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE) performed for this research returned no tools based on multiple information security standards. Likewise, a search returned no tools devoted exclusively to IDF physical security assessments.

The research described in this thesis focused on the creation of a sound, practical, and effective tool for assessing the physical security of IDFs. IDFs have historically received much less attention than MDFs, even though they are the most common type of network installation, and their compromise presents a serious risk to data security. The work's outcome, the Physical Security Assessment Tool (PSATool), is a prototype application for performing checklist-based assessments of IDF physical security.

Team	Location	Physical Security Assessment Tool	Date:		
Control Class	Requirement	Physical Security Requirements	MET	UNMET	Description of Response
Instructions: 1. Please complete the Team, Location, and Date fields above 2. Please indicate whether each requirement is Met (TRUE) or Unmet (FALSE) in the space provided below 3. Please complete the THV assessment below					
Entry Control	1	Entry control hardware shall exist to restrict entry at the IDF to authorized personnel.			
	2	More than one form of identification or information shall be required to gain entry to the IDF.			
Entry Control Type	3	A mechanical lock and key assembly is installed as entry control hardware.			
	...	Physical Security Requirements			
Surge Protection	49	A grounding electrode shall bond the building structure and IDF equipment chassis to ground.			
	50	Lightning protection shall be supplied to the incoming power.			
	51	Lightning protection shall be supplied to the communication cabling.			
Electronic Emanation	52	Electromagnetic shielding shall be used to reduce electromagnetic emanation.			
THV Assessment	Please describe any anticipated threat, hazard, or vulnerability discovered during this assessment.				
THV Assessment	Please suggest a control for any anticipated threat, hazard, or vulnerability discovered.				

Figure 1. PSATool sample data entry screen format

Figure 1 shows a fragment of a PSATool data entry screen. The tool lists 52 security requirements, compiled from NIST SP 800-53 (2009), NIST SP 800-53A (2010), and ISO/IEC 27002 (2005). Tool users determine whether each requirement is met (*TRUE*) or unmet (*FALSE*) relative to a given IDF. The tool includes fields for additional comments on each requirement, along with a supplemental area for additional concerns related to overall threat, hazard, and vulnerability (THV) data and strategies for their possible mitigation.

This data, once compiled, is entered into a *Microsoft Excel* spreadsheet linked to a *Microsoft Access* database. The current prototype includes queries that generate aggregate analyses of the data. Additional queries are provided that allow IDFs to be ranked by number of passed or failed requirements.

In fall 2012, PSATool was used to assess 135 IDF installations at East Tennessee State University (ETSU). ETSU is a regional university in northeast Tennessee with a current enrollment of more than 15,000 students. ETSU's network is managed by ETSU's Office of Information Technology (OIT), with an operating budget, excluding salaries, of \$186,030 for the 2013-2014 year (ETSU, 2013). OIT supports the network access provided to each building, classroom, and office on campus, 53 computer labs containing 1,200 computers, and all residence hall rooms (OIT, 2013).

The results of this assessment, in the view of the network's administrators, provided a realistic characterization of the IDFs' security. The assessment proper yielded 7,020 data points. A total of 95 threats, hazards, and vulnerabilities were discovered and various other concerns identified, including inaccessible IDFs located in hazardous environments, mislabeled and unidentified backup systems and power feeds, and unidentified IDF rooms. The mean and median number of passed requirements was 20 requirements. Newly constructed or recently

renovated IDF installations were found to pass more assessment requirements. Administrators also observed that the tool's Traceability Matrix will provide justification for network equipment isolation and capital investment expenditure.

CHAPTER 2

LITERATURE REVIEW

Overview

Information security is defined by U.S. Code (2002) as “protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction”. This protection is intended to assure information integrity, confidentiality, and availability. Differing perspectives on what information security should entail have yielded a large, complex literature (Bishop, 2002). Information security considerations relevant to the current work include risk management, risk assessment, vulnerability assessment, standard practice, and legal compliance. Best practices for IDF security were derived from these considerations.

Risk Management

Decisions involving security control selection and resource allocation are burdened with *risk* (Soo Hoo, 2000). Risk in the context of security is often defined as an outcome or consequence of a threat together with the likelihood of its occurrence (Henley & Kumamoto, 1996). Many organizations address risk using explicit strategies for guiding risk-related management decisions, a process known as *risk management*. Risk management processes are intended to identify a level of risk deemed organizationally acceptable and a plan for attaining that level. These processes may result in the removal, reduction, and reallocation of risk (Soo Hoo, 2000).

Early research on risk management assumed the use of highly complex, quantified models of risk. These *first-generation* strategies are typified by Soo Hoo’s framework (2000), which combines probability theory; “influence diagrams”, a type of flowchart used to analyze

organizational issues that affect decision-making; and “decision analysis”, a procedure formalizing the analysis of making decisions and outcomes. This framework attempts to accurately quantify system risk while allowing for uncertainty and fluctuating levels of model detail. Soo Hoo argues that qualitative approaches are not a long term solution to information security. He suggests that organizations might follow the best practices offered by a standard blindly, without adaptation to the specific risks within an organization (Soo Hoo, 2000). However, the standards themselves advocate ongoing assessment of risk.

Difficulties with quantitative approaches include their dependence on information that may be unavailable and questions about their effectiveness. Verendel (2009) surveyed 90 papers that comprised most of the work in information security quantification and modeling between 1981 and 2008. Papers were assessed according to their degree of support for empirical testing, their use of assumptions based on empirical testing, and the amount of direct empirical testing performed in support of the proposed model. Verendel concludes that the effectiveness of quantification for managing operational security, or the security of a system in its actual environment, has not been demonstrated by empirical means (Verendel, 2009).

The difficulties experienced in first-generation methods led to alternative strategies that sought to improve implementation, decrease complexity, and improve security. This second generation of methods includes *scenario analysis*, *integrated business*, *value-driven* and *best practice* methodologies.

In *scenario analysis*, authorities identify and then analyze scenarios in which security and services are compromised. This can involve the use of an audit team to attempt the electronic or physical penetration of a system, together with an analysis of that attempt. Scenarios presenting the greatest risk are then used to develop a risk reduction plan (Soo Hoo, 2000).

The *scenario analysis* approach simplifies assessment. Different paths leading to the same asset may be ignored and scenarios with less risk may remain unevaluated or undiscovered. The types of threats and vulnerabilities anticipated by scenario analysis are limited to the creativity of the team involved (Soo Hoo, 2000).

Value-driven methodologies focus on the economic impact of threats to subsets of assets, ignoring the probabilities associated with risk. Assets are first classified by relative value according to role and cost. A security specification is then developed for each asset class and security policies and safeguards are developed to satisfy these specifications. No mechanism for security system refinement or vulnerability assessment is provided (Soo Hoo, 2000).

Integrated business risk-management methodologies treat *information technology* (IT) risk in the same manner as any business risk. Rather than focusing on the components of risk sources such as information, software, and hardware, the approach focuses on broad, non-technical categories of risk such as financial risks, environmental risks and operating risks. Assessment is simplified in this approach as is analysis (Soo Hoo, 2000).

Best practice methodologies address security and support system concerns by implementing a given industry's standard practices and policies. These best practices are usually defined as part of public standards, e.g., British Standard 7799. This methodology's primary appeals are logistic and legal. *Best practice* methodologies avoid the need to perform intensive analysis, gather security-related information, and construct scenarios. Rather, they assume that an organization will be held harmless for implementing the same practices as the majority of an industry (Soo Hoo, 2000).

Best practice methodologies are typified by Parker (2006), who advocates the use of accepted practices and standards to develop information security controls and establish a level of

due diligence. Due diligence is established by the continual application of a formal framework of security policies and procedures to an organization's information infrastructure (Tittel, Chapple, & Stewart, 2004). Establishment of a level of due diligence as promoted by Parker is intended to defend against claims of negligence in the event of litigation. Legal compliance to mandated legislation, intended to reduce penalties and liability, is also stressed by Parker as a component of security. ISO/IEC 27002 (2005) supports legal compliance as advised by Parker.

Parker (2006) advises that risk management approaches to information security offer no solutions to security control choices. He argues that security controls are ultimately selected based on *due diligence* regardless of the type of analysis involved. Stoneburner et al. (2002), Mattord (2007) and Al-Hamdani (2009) join Parker in support of standard-based security.

Risk Assessment

Risk management typically starts with *risk assessment*, a process used to discover, describe, and comprehend risk (Soo Hoo, 2000). A risk assessment is intended to “identify, prioritize, and estimate risk to organizational operations (i.e., mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation and use of information systems” (NIST, 2011).

NIST SP 800-30 (2011) divides risk assessment into three distinct phases. In the first, preparation phase, assessment scope, constraints and purpose are defined. Threat and vulnerability information sources are identified. Finally, *risk models*, used to establish key terms and risk factors, are defined. In the second, analysis phase, threats, vulnerabilities, likelihood, and outcomes are identified and analyzed. A list of prioritized information security risks is produced which is used to make risk-related decisions concerning security controls. The third and final maintenance phase includes ongoing monitoring and updating of identified risks.

Vulnerability Assessment

Garcia (2006) defines *vulnerabilities* as exploitable weaknesses in the design, implementation, and operation of asset protection systems. Once exploited, vulnerabilities can result in the interruption of services and the theft and destruction of information and assets.

Baker (2005) perceives vulnerability as driven by *threats* or *hazards*. Threats include deliberate, malicious attacks that can result in theft and destruction. Hazards involve accidental damage, often by environmental factors including floods and fires.

The objective of *vulnerability assessment* (VA) is to discover, document, and report vulnerabilities in an asset protection and support system. The vulnerabilities discovered in an assessment can be used to harden systems against those vulnerabilities and to compare the relative vulnerability among multiple installations. This assessment of relative vulnerability may be used to justify and prioritize the allocation of funds and resources (Baker, 2005).

Studies of vulnerability assessment and the anticipation of threats and hazards include DOE-related work by Garcia (2006), Whitehead, Potter, & O'Connor (2007), and Johnston et al. (2002). Related studies include guidance for VA in facilities housing critical infrastructure systems by Baker (2005); and recommendations for VA in federal buildings by Beshlin et al. (2003).

Physical Protection Systems Vulnerability Assessment

Garcia (2006) describes a highly quantified methodology for assessing the vulnerability of physical protection systems (PPS). This includes a thorough review of sensor types, construction practices, detection systems, and security forces as well as an examination of concerns related to the timing and ordering of these entities' interactions. Intrusion detection, delay, and response are quantified and analyzed, as are sensor and control performance. Garcia

indicates the usefulness of physical security checklists and surveys to establish equipment existence. She also advises that checklists do not accurately establish control effectiveness. Whitehead et al. (2007) recommend Garcia's methodology. The authors propose a higher level approach to PPS design similar to Garcia's. PPS objectives are established by identifying a facility's physical features, operations, and required level of protection. A comprehensive list of potential attackers, their tactics, and deployment speed should be compiled. Assets and potential targets should be inventoried and prioritized according to their importance. Operations, movements, or procedures vulnerable to attack should be identified. By assessing the risk of attack and gauging the loss incurred by an attack's outcome, the required level of protection should be estimated (Whitehead et al., 2007).

Attacks are usually detected with an alarm system that monitors sensors and reports alarm status through an interface for assessment by security personnel. Graphical interfaces are preferred as they can present more information for alarm assessment than other types of interfaces. Desirable characteristics of alarm systems include flexible expansion and fast reporting. Alarm communication cabling is vulnerable to attack; therefore, the alarm communication system must monitor the cabling's health (Whitehead et al., 2007).

Active alarms may be assessed by using a video system for viewing and recording. Transmission and recording systems for video cameras must be protected to prevent their compromise via the introduction of false signals or their destruction. Integrated systems that incorporate alarm signals into the video system allow recording of alarm status for forensic purposes. Alarm status can also be used to initiate video recording.

Intrusion sensors such as beam breakage, boundary penetration, and motion detection sensors may be placed on the outside or inside of a protected area or asset. PPS designers must

be aware of sensor operational characteristics, placement options, and defeat methods.

Whitehead et al. (2007) propose that PPS effectiveness be determined through the analysis of attack paths, i.e., series of actions that can compromise the assets that a PPS protects. The authors equate a PPS's overall effectiveness with the vulnerability of its critical path, i.e., that path that has the highest probability of interruption. Factors affecting effectiveness include the likelihood of detection, asset value, path length, and the access delay that can be introduced. The identification of paths is fundamental to evaluating system effectiveness. Regardless of assessment method, the PPS should be revised to include the results of the effectiveness analysis. A cycle of PPS assessment and refinement using assessment results should be maintained (Whitehead, 2007).

The Vulnerability Assessment Team

The Vulnerability Assessment Team (VAT) of Los Alamos National Laboratories (LANL) has conducted vulnerability assessments for government agencies and the Nuclear Power industry. VAT has conducted assessments on over 200 security devices. Based on these experiences, Johnston et al. (2002) propose the following recommendations for conducting vulnerability assessments.

Assessors and all levels of personnel should be encouraged to discover problems and potential solutions. Assessors must be free to consider any attack path or scenario. Each vulnerability discovered should be listed with detailed information such as the tools and time required to devise and conduct an attack. An attacker's technical sophistication level, system knowledge level, and access level should be included in the report, along with a sample of any defeated or vulnerable sensors. Controls should be suggested for any vulnerability discovered (Johnston et al., 2002).

Network Infrastructure Vulnerability Assessment

Baker (2005) proposes a general methodology for assessing physical and cyber vulnerability in facilities housing critical infrastructure systems. The methodology is intended to scale to multiple installations, thus establishing a baseline for prioritizing improvements and allocating resources. Baker suggests employees, police organizations, and the FBI as sources of threat and hazard information.

The starting point for Baker's methodology is a definition of a facility's mission. This definition is used to identify and document mission-related threats and hazards. Systems important to facility mission, mission support, and protective systems are identified and documented. A system interconnection diagram is developed to illustrate the interconnection of critical systems, demonstrating dependencies. The timing and ordering of system repair, spare parts, key personnel, emergency responders, and system changes are considered when determining the degree of dependency (Baker, 2005).

Threats	Critical Systems	Computer Work Stations	Servers, Routers	Electric Power	Heating, Ventilation, A/C	Cable & Fiber Interconnects	Security Systems, Cameras	Telephone System	Fuel, Gas Systems	Hazmat Storage	Summary
Cyber Attack	Not Vulnerable	Vulnerable	Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable
Cable Cut - Excavation	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not Vulnerable	Not Vulnerable
Fire	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not Vulnerable	Not Vulnerable
explosives	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not Vulnerable	Not Vulnerable
Sabotage	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Vulnerable	Not Vulnerable
Electric Service Outage	Scenario Dependent	Scenario Dependent	Scenario Dependent	Vulnerable	Scenario Dependent	Scenario Dependent	Scenario Dependent	Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable
Flooding	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Vulnerable	Not Vulnerable	Scenario Dependent	Not Vulnerable	Not Vulnerable
High Winds	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable	Not Vulnerable
Overall Rating by System	Vulnerable	Vulnerable	Scenario Dependent	Scenario Dependent	Not Vulnerable	Scenario Dependent	Vulnerable	Scenario Dependent	Not Vulnerable	Not Vulnerable	Not Vulnerable

	Vulnerable
	Scenario Dependent
	Not Vulnerable

Figure 2. Vulnerability Assessment Threat-System Matrix (adapted from Baker, 2005)

Vulnerabilities are analyzed according to their potential individual or combined effects on facility mission. A color coded matrix of assets vs. vulnerabilities is used to depict the degree

of perceived vulnerability in asset-vulnerability pairings (see Figure 2). Diagrams illustrating possible failure scenarios, critical system dependencies, and combinatorial failure dependencies form this stage's output. Baker suggests that diagrams be developed into a fault tree to help analyze dependencies in complex systems. Potential vulnerabilities that affect multiple critical systems from a single location should be given a higher vulnerability rating. Prior security incidents and their associated vulnerability should be included in the assessment (Baker, 2005).

FEMA Vulnerability Assessment

Beshlin et al. (2003) recommend a Federal Emergency Management Association (FEMA) methodology for assessing vulnerability in federal buildings. The methodology consists of a quantitative assessment of each asset, threat and risk, followed by a qualitative vulnerability assessment for each high-risk asset/threat pair. The authors also offer many best-practice-based recommendations regarding building HVAC, lighting, and construction.

Standard Practice

Information security standards provide organizations with security controls and assessment recommendations based on common organizational practices. These standards address cyber, procedural, physical, and environmental aspects of information security. Comprehensive assessment methods are described by NIST standards, including the ISO/IEC 27000-series and NIST SP 800-series of standards.

ISO/IEC 27000-Series Information Security Management Standards

The ISO/IEC 27000 standards for information security management are produced by a joint committee of the International Standards Organization and the International Electrotechnical Commission (ISO/IEC). These standards are based on information security standard ISO/IEC 17999, itself derived from a British information security standard, BS 7799

(Calder & Watkins, 2008).

Different 27000-series standards address different components of information security. The first two standards, ISO/IEC 27001 (2005) and ISO/IEC 27002 (2005), address security needs for Information Security Management Systems (ISMSes): holistic, integrated processes for managing the planning, implementation, and support of information security, including concerns related to system policies, procedures, and controls. ISO/IEC 27001 specifies a form for an ISMS. ISO/IEC 27002 specifies information security controls and techniques proper.

ISO/IEC 27001

ISO/IEC 27001 specifies the use of a plan-do-check-act (PDCA) model for structuring an ISMS. The *plan* stage is concerned with ISMS establishment. The *do* stage involves ISMS implementation and operation. The *check* stage involves ISMS monitoring and review. Finally, the *act* stage involves ISMS maintenance and improvement (Calder & Watkins, 2008). Each stage of the PDCA cycle acts as input to the next stage. The process is assumed to be ongoing and repetitive.

Systematic ISMS implementation is supported by ISO/IEC 27001. ISO/IEC 27001 provides guidelines for the initial planning stage through ongoing maintenance and audit phases. ISO/IEC 27001 requires an audit by a third party and certification. Monitoring is required to retain certification.

Dey (2007) and Fernández-Medina et al. (2006) advocate the implementation of an ISMS framework based on the ISO 17799 and 27001 standards. The ISMS framework begins with the establishment of information security policy boundaries, the identification of the assets to protect, and the development of scopes of protection. A formal document should be drafted requiring proof that controls have been introduced.

Once initial controls are in place, security teams should be formed for system implementation, system audit, executive approval, and technical knowledge. Officers for each team should be designated. Policy and procedures for team operations and communications should be defined (Dey, 2007).

Physical and informational assets requiring protection should be identified and then classified according to security status. Procedures regarding the proper use and disposal of assets in each security classification should be defined. After classification, security measures for specific assets should be developed. This stage's output should include a matrix illustrating the security measures for each asset (Dey, 2007).

Human Resource Department recruitment processes for employees, vendors, and contractors should be refined to include security checks and non-disclosure agreements. Job descriptions along with leave, retirement, and resignation policies should be revised to include security provisions and the consequences for violating those terms (Dey, 2007).

Physical security should include protection of computing equipment and necessary support services. Policies regarding the reporting of equipment failures and security breaches should be defined. Recovery and contingency plans should be developed to ensure rapid recovery from failures or breaches (Dey, 2007).

Entry and access control should be instituted to restrict access to sensitive areas and information. All physical and electronic information access should be logged (Dey, 2007).

Policies, responsibilities, and procedures regarding the operation, compliance, maintenance and acquisition of software and hardware should be established. Maintenance and auditing should be logged, allowing for verification of procedures (Dey, 2007).

ISMS framework implementation should conclude with an audit, associated corrections,

and ISO certification. The Information Systems Audit and Control Association (ISACA) certifies auditors in the assessment of information systems (Dey, 2007).

ISO/IEC 27001 also requires an ISMS to be audited at regular intervals with regard to processes, policies, procedures, and controls. The depth, coverage, and frequency of the audits are defined by the organization. The ISO/IEC 27000-series of standards offers no specific guidance for overall execution of an assessment.

ISO/IEC 27002

ISO/IEC 27002 provides detailed guidance on information security controls and techniques. These controls and techniques are intended to be used within the context of an ISMS. ISO/IEC 27002-specified controls include policies, procedures, and processes, systems, and devices necessary to mitigate risk associated with security; procedures related to asset management, human resources, operations management, access control, and incident management; and controls regarding legal and technical compliance.

Section 9 of the ISO/IEC 27002 standard is devoted to physical and environmental security controls. Example controls include the construction of a solid perimeter to contain system hardware and the use of entry controls to restrict egress. Controls concerned with facility location and external threat protection are provided. Additional controls dictate equipment siting, utility support, and cabling protection (Calder & Watkins, 2008).

NIST Security Controls

All Federal Information Systems except those designated as national security systems must conform to a framework of standards and guidelines for controls for information security (NIST, 2009). This framework, established by the National Institute of Standards and Technology (NIST), is intended to promote compliance with the Federal Information Security

Management Act of 2002 (FISMA). It was developed for inclusion in an organizational risk management strategy focused on assuring legal compliance with FISMA. It is designed to help an organization establish a degree of due diligence and provide asset and operational security by providing a basis for security controls (NIST, 2009).

The NIST framework assumes a six-step process for information systems risk management. In the first step, Federal Information Processing Standards Publication (FIPS PUB) 199 (NIST, 2004) is used to determine an information system's security category. A security category of low, medium, or high is assigned to a system based on the potential mission impact of a security, confidentiality, integrity, or availability breach.

In the second step, a set of security controls based on the system security category determined by FIPS PUB 199 (NIST, 2004) is selected from NIST 800-53 (2009). A risk assessment is conducted to further describe and define system vulnerability and to identify supplementary controls absent from the control set recommended by NIST 800-53. The security controls must be tailored for specific organizational needs according to scoping guidelines and then supplemented with those controls required to assure compliance to legal, federal, and institutional requirements. A control's required level of assurance is determined by the *system impact level*. Assurance requirements range from proper control function in low-impact systems to the establishment of measures for control effectiveness and improvement in high-impact systems. No preference is given regarding specific control technologies, e.g., keyed mechanical locks vs. electronic entry control. Ending the second step, the security plan is updated to include the security controls and assurance requirements (NIST, 2009).

The third step of the process is to implement the specified control set. Prior to assessment, a security plan must be drafted and approved by organization officials (NIST, 2009).

In the fourth step, security controls are assessed using guidelines specified by NIST SP 800-53A. Assessment is intended to determine security state, effectiveness, and vulnerability (NIST, 2009).

System authorization, the fifth step, is addressed in NIST SP 800-37. Authorization is the official acceptance of system risk by organizational officials (NIST, 2009).

The last step in the NIST risk management process involves system and control monitoring with the goal of continuous improvement. In the monitoring phase, breaches of information security, e.g., loss of confidentiality, integrity, and availability, can trigger an assessment of security category and security controls. New threats and changes in mission, configuration, and risk management strategy can trigger assessment (NIST, 2009).

NIST SP 800-53 specifies cyber and physical security controls for organizational planning, policy, procedures, and training. Controls are graduated in that fewer controls are mandated for lower impact systems than for high impact systems. Controls implementation is prioritized to provide an ordering for implementation. The control set offered by NIST is very similar in organization and type to the ISO/IEC 27002 physical and environmental controls, because NIST SP 800-53A actively maps ISO/IEC controls and techniques. There are minor differences between the control sets (NIST, 2009).

NIST Control Assessment

NIST control assessment methodology is defined by NIST SP 800-53A (2010). The depth and coverage of assessment is proportional to mission risk. Assessment establishes evidence that controls are correctly implemented and properly operated. Assessment provides justification for spending capital and allocating resources. Compiling evidence by assessment is essential to building an *assurance case*: evidence in support of an assertion about a need for a

control.

Assessments may be conducted by teams composed of any number of assessors. Assessors with varying technical experience should be chosen by organizational officials as part of an overall organizational risk management strategy. Potential assessors include individual and team assessors selected from internal or external sources. Diversity in assessor experience and technical ability is expected (NIST, 2010).

A NIST assessment entails preparing for the assessment, developing a plan for assessment, conducting the assessment, and final reporting. Each of these four phases is described in detail by NIST SP 800-53A.

In the initial, preparation phase, an organization undergoing assessment must notify the appropriate officials, define the assessment team, and establish the project milestones. This organization must assemble specifications, policies, procedures and other artifacts including security plans, architectural designs, and prior assessments for inspection by the assessment team. The assessment team must establish organizational contacts and obtain the assembled artifacts. An understanding of organizational functionality, mission, and procedures must be developed, and information system architecture and security controls examined (NIST, 2010).

In the second, planning phase, the assessment team develops a *security assessment plan*. This plan outlines assessment objectives and the path by which they will be met. The assessment's scope is defined, identifying the set of controls to be assessed and the depth and coverage of the assessment (NIST, 2010).

Each assessment procedure contains *methods*, i.e., operations that *test*, *examine*, and *interview* individual controls, individuals, and policies. Methods are performed on *objects*, i.e., the entities being assessed. Objects contain *attributes* such as *depth* and *coverage* that specify the

effort required for a method's evaluation. Procedures may be tailored to an organization based on the depth and coverage required by the organization to reduce risk. Supplemental assessment procedures for controls not defined in the standard and any additional assessment procedures necessary for added assurance must be developed (NIST, 2010).

The assessment plan should include extended assessment procedures, i.e., additional assessment cases for verifying compliance with assurance requirements established in the security plan. The completed assessment plan must be reviewed for correctness, cost, and performance and then approved by organization officials (NIST, 2010).

Organizations with greater impact risk levels are required to expend greater effort in assessment depth and coverage, thereby achieving higher levels of assurance. Assessment cases range from the existence of functional controls at all impact levels to the verification of maintenance records and functionality testing in high impact systems (NIST, 2010).

In the third phase of a NIST assessment, the assessment is conducted according to the security assessment plan. During the assessment, a determination is made by applying methods to the objects specified in the assessment procedure. This determination must yield one of two values: an acceptable value of *satisfied* (S), or an unacceptable value of *other than satisfied* (O). Any unacceptable determinations are assessed for impact on information confidentiality, integrity, and availability. Assessor recommendations for vulnerability removal and corrective actions to controls are compiled into an initial draft of the security assessment report and presented to the system owner. The system owner may choose to correct issues prior to the final report. Any modified controls, policies or procedures should be reassessed prior to final report construction (NIST, 2010).

The final security assessment report characterizes the assessed set of controls from the

assessment plan. It identifies the information system, gives assessment date and impact level, and includes the determination for each assessment procedure, specifying its methods and objects. Assessor comments, including weaknesses in implementation or process, along with recommendations for corrections or enhancement, are included. Delivery of the final assessment report completes the assessment process (NIST, 2010).

Legal Compliance

Parker (2006) advises legal and regulatory compliance as an essential component of information security. This includes compliance with two key federal standards for information assurance, the Sarbanes-Oxley Act and Gramm-Leach-Bliley Act.

The Sarbanes-Oxley Act

The Sarbanes-Oxley Act (SOX) requires publicly held organizations to provide assurances that their practices have not impaired their ability to report financial information. Standards that attempt to ensure compliance with SOX are published by the American Institute of Certified Public Accountants (AICPA) (AICPA, 2011). One such standard is the Statements on Standards for Attestation Engagements (SSAE), No. 16. Section 801 of SSAE No. 16 serves as guidance for evaluating and documenting internal and outsourced organizational service provider controls. SSAE No.16, Section 801 requires that assessments be reported by a practitioner, i.e., a Certified Public Accountant (CPA).

SSAE No. 16, Section 801 defines controls as the policies and procedures planned, applied, and documented to reduce risk to financial reporting. Collectively, these controls are intended to reduce the risk of the inaccurate reporting of financial data. Outcomes that affect reporting include interruption of services and destruction of information. Information technology systems must be assessed due to the infrastructure and services they provide to financial

reporting activity (Knolmayer & Asprion, 2011).

The assessor's objective is to obtain assurance and report findings based on the criteria supplied by the organization that all of the descriptions and declarations it provided are accurate as of the date supplied in the *type 1 report*, or during the period specified in a *type 2 report*. In a *type 2 report* the auditor must also obtain assurance and report findings related to the controls' operation and the fulfillment of stated control objectives required to reduce risk. If an assessor discovers risk requiring additional controls, those controls are recommended and documented in the assessment report.

SSAE No. 16, Section 801 provides no set of controls with which to compare existing controls or establish a baseline set of controls. Control selection must be obtained by a system owner from other sources. The standard or benchmark chosen by the system owner determines the criteria by which the assessor evaluates the system. The suitability of the criteria is also assessed (AICPA, 2011).

The Gramm-Leach-Bliley Act

The Gramm-Leach-Bliley Act (GLBA) is a federal law requiring the establishment of controls for anticipated threats or hazards to the security of student customer information (1999). GLBA compliance is required by the Department of Energy (DOE) and the Tennessee Board of Regents (TBR), ETSU's governing body. GLBA (1999) requires financial service providers to insure the confidentiality and security of customer financial records. They must protect against anticipated threats or hazards to customer information security or integrity. They must also prevent unauthorized access to customer financial information that might result in customer harm or inconvenience (TBR, 2003). GLBA requirements do not specify physical security controls.

Best Practices for IDF Security

There is a lack of published research regarding IDF physical security. No prior work devoted exclusively to IDFs was found. Prior work exclusively devoted to MDFs includes Richards' (1982) work regarding data center protection. This work does not readily scale to IDFs in that IDFs represent a more numerous and exposed installation.

A characterization of an *ideal* IDF can be obtained by applying recommendations put forth by the information security standards, vulnerability assessment recommendations, and legal compliance considerations to IDFs. This ideal IDF consists of an enclosed interior area devoted exclusively to the protection of network equipment and associated support equipment, communication media, and power wiring (ISO/IEC, 2005 and NIST, 2009). Two pieces of information or identification should be required at the IDF for access, which should be authorized, monitored, and logged. No utilities, e.g., plumbing, electrical, or HVAC, should be housed in the IDF. Bulk media or supplies should not be stored in the IDF. Physical locations should be selected to avoid the possibility of flood or other hazard. No outward indications of their purpose should be given (ISO/IEC, 2005).

Protection of IDF equipment and services must include utilities such as power, environmental, and backup systems (ISO/IEC, 2005 and NIST, 2009). Power and communication wiring should be separated to prevent interference (ISO/IEC, 2005). Power should be supplied by redundant feeds that are separated physically in order to prevent a single event from damaging both (Baker, 2005 and Beshlin et al., 2003). Remote disconnects should be present, so as to allow the disconnection of power and water supplies in the event of emergency, e.g., flood, without approaching network equipment (NIST, 2009). The IDF should have dedicated HVAC systems to monitor and maintain temperature and humidity (NIST, 2009).

Power backup systems should supply enough power to allow equipment shutdown or continued operation with HVAC support (ISO/IEC, 2005). These backup systems should be located separately from the equipment being served (Baker, 2005 and Beshlin et al., 2003).

Lightning protection, including surge suppression and proper grounding, should be provided for the facility housing the IDF and equipment (ISO/IEC, 2005). Equipment should be grounded to a building grounding electrode, with surge suppression applied to incoming electrical power and communication cabling (ISO/IEC, 2005). The IDF should be shielded to prevent electronic eavesdropping. IDF cabling and equipment should be documented and identified (ISO/IEC, 2005).

Additional operational support and security should be provided by various alarm and assessment systems. Intrusion and fire detection systems should be used in addition to systems used to detect utility loss (ISO/IEC, 2005). Fire protection should include a fire suppression system, e.g., sprinkler, and extinguisher (NIST, 2009). Depending on the emergency, these systems should alert organizational security and initiate response; this may include notification of emergency personnel, activation of emergency lighting, and initiation of video recording (NIST, 2009). Cameras should be used to evaluate alarms (NIST, 2009).

CHAPTER 3

METHODOLOGY

Overview

Information security typically focuses on cyber security. As a result, few tools exist for the assessment of physical security controls. This thesis sought to address this deficiency by creating a sound, practical, and effective tool for physical security assessment. Here, soundness is equated with adherence to existing standards for physical security assurance, practicality with the tool's usability and extensibility, and effectiveness with the tool's satisfactory performance in an actual assessment.

Scope

The assessment tool, hereafter referred to as PSATool, was intended as a prototype application for gauging an IDF's physical security relative to a characterization of an ideal IDF. Prior work has concentrated on MDF physical security control selection and assessment. While facilities commonly contain one MDF, the same facility can possess multiple IDFs. These IDFs expose a university network edge to vulnerability, threat, hazard, and risk.

PSATool's design focused on concerns related to control selection and control existence. Various aspects of IDF security were excluded from consideration in order to reduce the time needed to conduct an assessment and reduce risk to the entities being assessed. Omissions include the analysis of fault trees, the effect of combined vulnerabilities, and the timing of repair and response concerns (Baker, 2005); the timeliness of attacker detection, attacker delay, and security response (Garcia, 2006); and the effect of detailed procedures and event triggers on physical security. Only simple event triggers have been considered for inclusion, e.g., the initiation of video recording once triggered by an intrusion alarm.

Other exclusions included practical constraints including capital cost and available space. Research focused exclusively on information security standards, VA recommendations, and legal compliance. In practice, political, financial, and structural aspects often affect the selection, implementation, and assessment of controls. These factors are not addressed in the standards. The PSATool aspired to characterize an ideal IDF, unconstrained by these factors.

Soundness

PSATool was intended to relate the physical security controls prescribed through its requirements to widely accepted, practice based standards and vulnerability assessment recommendations. PSATool's assessment methodology was also based on the assessment recommendations and procedures found in these standards and recommendations.

PSATool was not designed to provide an absolute measure of IDF physical security. Although the tool might be used to derive quantitative characterizations of IDF security, it was intended to support a qualitative approach to security as proposed by Parker (2006). This tool was intended to provide a system administrator with an image of IDF adherence to practice-based physical security recommendations. It was also intended to provide ordinal ranking of IDF security so that a system administrator can compare IDF physical security relative to other system IDFs in order to prioritize individual and system improvement. Tool adherence to common practice, VA recommendations, and legal compliance was intended to support the justification of capital improvement.

Coverage of Key Recommendations

PSATool's design sought to integrate recommendations from key standards and reports into a single, comprehensive set of guidelines for IDF security. The NIST SP 800-53 (2009), NIST SP 800-53A (2010), and ISO/IEC (2005) 27002 information security standards were

selected as the foundation of the physical security requirements. VA recommendations included Baker (2005), the author of a methodology for infrastructure vulnerability assessment and Federal Emergency Management Agency authors Beshlin et al. (2003). Additional literature by Department of Energy scientists Johnston & Garcia (2002), Whitehead et al. (2007), and Garcia (2006) was selected in an attempt to obtain additional requirements. DOE scientists were included because to their involvement in the atomic energy industry.

In many cases, multiple sources proposed similar or identical recommendations for controls. For example, controls for integrating intrusion system and video surveillance as described by Garcia (2006) are included in the NIST (2009) SP 800-53 standard. These common controls include the usage and monitoring of entry control systems, alarm systems, and backup systems. Again, NIST SP 800-53 and ISO/IEC 27002 specify many of the physical security controls recommended by Garcia (2006) and Whitehead et al. (2007). Baker (2005) recommends many of the same physical security controls found in FEMA guidelines and information security standards. Beshlin et al. (2003) offer many of the same physical security controls regarding alarm, fire, communication, and monitoring systems found in the NIST and ISO/IEC standards. PSATool's design sought to collapse these repeated recommendations into a single set of orthogonal recommendations that covered the original recommendations.

Some controls are found exclusively in a NIST standard, an ISO/IEC standard or a VA recommendation. ISO/IEC 27002, for example, was the lone source for a requirement for obfuscating network component rooms. Similarly, the labeling and documentation of patch cables is advised exclusively by ISO/IEC 27002.

The PSATool was also intended to support legal compliance. SOX, SSAE 16 and GLBA do not require specific controls. These laws *do* require the construction of controls for

anticipated threats, hazards, and vulnerabilities to organizational reporting structure. PSATool sought to promote GLBA compliance by providing a mechanism for promoting the discovery and recording the anticipation of threats, hazards, and vulnerabilities. This is in accordance with the recommendation by Johnston et al. (2002) that assessment teams be allowed to anticipate vulnerabilities and suggest mitigating controls.

Procedural Soundness

Design of the PSATool and its accompanying assessment aspired to be procedurally sound regarding assessment procedures. The primary standard selected for judging the tool's procedural soundness was NIST SP 800-53A, the U.S. government standard for non-security-related information systems. SSAE No. 16, Section 801 provides detailed assessment methods; however, these methods are intended to be administered by an accounting professional. NIST SP 800-53A, as described in chapter 2, prescribes a binary methodology for assessing compliance with best practices for physical security. By contrast, detailed assessment methods are not offered by ISO/IEC 27002 (2005).

PSATool Practicality

Design goals intended to assure PSATool's practicality focused on assuring its usability and extensibility. With regard to usability, the goal was to produce a tool that users with some knowledge of network equipment, a limited knowledge of computers and no knowledge of programming could use to conduct assessments. Built-in requirements for IDF security were intended to be simple, self-describing phrases stipulating the existence of a single physical security control. The assessment form was intended to be usable with little or no explanation. Additionally, the tool was to provide self-contained queries for generating reports on individual IDFs as well as overall IDF data. The tool was intended to be reusable; to support a process of

ongoing assessment, consisting of multiple, frequent, assessment events. The resulting assessment history is intended to support a claim of *due diligence*.

With regard to extensibility, one goal was to design an application that a computing professional with a limited knowledge of *Microsoft Access* and Structured Query Language (SQL) could extend to produce additional and tailored queries. Meeting this goal would allow organizations that required additional database tables to do so with a modest amount of programming and no changes to the tool's underlying data model. A second goal was to allow users with limited computer skills to add, tailor, and evolve requirements for several reasons. These new requirements would be required to accommodate additional, site-specific requirements for IDF security, including controls based on anticipated threats, hazards, and vulnerabilities discovered in an assessment and requirements for operational testing. Additional requirements might also be necessary due to future standards, recommendations, and analyses of security incidents. Another concern was support for adding newly commissioned IDFs to the assessment.

PSATool Effectiveness

It was determined that a case study involving the main computer network for East State Tennessee University (ETSU) be used to demonstrate PSATool's effectiveness. ETSU is a state-supported university that awards degrees in over 100 undergraduate, graduate, and professional programs (ETSU, 2012). The ETSU computing infrastructure provides network access and services to ETSU workers, students, and faculty. These services are provided at offices, classrooms, dormitories, and laboratories across the main Johnson City campus. ETSU remote sites include facilities, classrooms, and offices at the Veterans Administration Mountain Home located in Johnson City and at facilities in Kingsport, Elizabethton, and Mountain City.

Telephone service at all ETSU locations is also serviced by ETSU's Office of Information Technology (OIT).

This case study involved an initial evaluation of the tool, a meeting to plan assessment execution, and an expert review of the assessment. Review experts included ETSU OIT Associate Vice President and Chief Information Officer, Mark Bragg, and ETSU OIT Director of Telecom and Network, Beth Rutherford. These individuals were chosen as experts because of their direct involvement with OIT network installation, operation, and protection.

Assessment was restricted to IDFs in the city of Johnson City, including IDFs at the ETSU main campus, Veterans Administration, sports facilities, and student apartments. To limit the extent of the research and risks to equipment, assessment was limited to determining the existence of control hardware or simple mechanisms. These mechanisms and processes are ones that only trigger an event, e.g., intrusion system initiation of video recording. ETSU (IDF) installations vary greatly. IDF port quantities differ significantly, due to the diverse set of buildings, facilities, and departments that require network services. The areas used to house IDFs also vary. IDF installations range from multiple switch installations with primary and backup systems supplying heating, ventilation, and air conditioning (HVAC) located in a dedicated room to single switch installations with no primary or backup HVAC systems housed in a shared area. Most IDFs are installed in areas originally developed for other purposes, then adapted to host an IDF.

ETSU was deemed to be a suitable candidate for a case study for several reasons. These reasons include the large number of IDFs, the variety of diverse facilities housing these IDFs, and the frequent use of impromptu areas conscripted to host IDFs.

CHAPTER 4

RESULTS

Overview

This research sought to produce a sound, practical, and effective prototype of an application for IDF physical security assessment. The extent to which the resulting application, PSATool, met these goals was assessed using a variety of means. PSATool's soundness was assessed by checking its security model against industry standards for device and environmental security. PSATool's practicality was assessed relative to best practices for assuring the usability and extensibility of software applications. Finally, PSATool's effectiveness was assessed by using it to assess IDFs that constitute a moderate-size university WAN.

PSATool

PSATool is a software prototype composed of two architectural components, a *Microsoft Excel* spreadsheet and a *Microsoft Access* database. A separate sheet within the spreadsheet contains an assessment form for each assessed IDF. The database provides persistent storage and retrieval for assessment results. These results include assessment metadata, e.g., discrete assessment number and assessor contact information.

Assessors physically assess each IDF in the target system. This assessment is performed by completing an assessment form composed of a set of testable physical security requirements and a THV assessment. Assessors may enter requirement test results directly the assessment form using a computer. Alternatively, assessors may print a blank assessment form. In doing so, assessment data may be entered offline. No computer knowledge or skill is required of the assessor. Assessment data must be entered directly into the linked database tables. Assessment results may be generated by using the provided queries.

PSATool Assessment Form

A sample of the assessment form is shown in Figure 3. A blank assessment form is available in Appendix A. A complete listing of the requirements is provided in Appendix B.

Team	Location	Physical Security Assessment Tool	Date:		
Control Class	Requirement	Physical Security Requirements	MET	UNMET	Description of Response
Instructions: 1. Please complete the Team, Location, and Date fields above 2. Please indicate whether each requirement is Met (TRUE) or Unmet (FALSE) in the space provided below 3. Please complete the THV assessment below					
Entry Control	1	Entry control hardware shall exist to restrict entry at the IDF to authorized personnel.			
	2	More than one form of identification or information shall be required to gain entry to the IDF.			
Entry Control Type	3	A mechanical lock and key assembly is installed as entry control hardware.			
	4	An electronic keypad reader is installed as entry control hardware.			
	5	An electronic keypad/card reader is installed as entry control hardware.			
	6	An electronic card reader is installed as entry control hardware.			
	7	A biometric device is installed as entry control hardware.			
Transmission Media	8	Signal transmission media including line cabling, wiring, and fiber optics shall be protected from damage.			
	9	Power wiring shall be segregated from communication wiring.			
	10	Cabling shall be identified to minimize patching and handling errors.			
	11	Patch and connection information shall be documented and available locally.			
Access Monitoring	12	No unauthorized devices or cabling shall be connected to cabling or equipment ports.			
	13	Physical entry to the IDF shall be logged and monitored by organizational security.			
	14	Organizational security shall monitor a dedicated IDF intrusion alarm system.			
	15	The organization shall use camera surveillance systems at the IDF to assess intrusion alarms.			
	16	An IDF intrusion system shall initiate response for physical intrusion alarms.			
	17	Intrusion incidents shall trigger video recording at the IDF.			

Figure 3. PSATool Assessment Form sample

The physical security assessment form provides fields for recording assessment date, team number, and IDF location. It lists 52 physical security requirements, each of which is determined to be met (*TRUE*) or unmet (*FALSE*) relative to a given IDF. A field entitled *Description of Response* is provided next to the requirement result field. Assessment teams are urged to use this field for any additional information necessary to describe a requirement's state or justify a response.

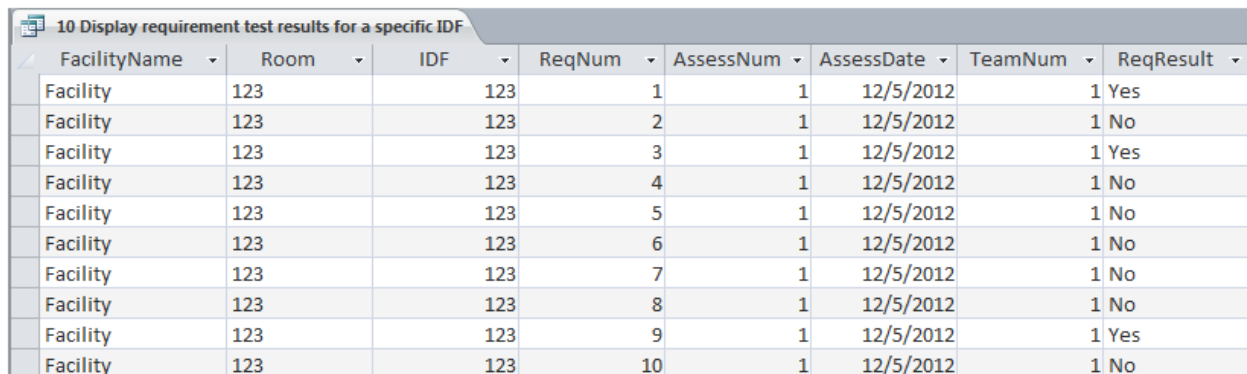
The form and tool groups related requirements into subsets called *control classes*. The *control class* allows for the grouping of requirements into subsets to aid discussion and querying. *Entry control*, *access monitoring*, and *power supply* are typical *control classes*.

NIST (2010) views assessment as information gathering. The Entry Control Type (ECT) *control class* groups information related to the type of entry control hardware used at an IDF. Because a transitional state may exist as an organization migrates to specific hardware, e.g., card

manually.

The database uses relational tables to store all requirement test and THV assessment results. An identifying number is assigned to each discrete element of THV found, as many of these elements were found in multiple locations. Definitions of all THVs and requirements are stored and assigned a unique identifier. Additionally, these tables hold each IDF's unique identifier, facility name and room number. The physical security requirement set and traceability matrix is stored; assessment team configuration and contact information is housed; and all guidance standard and reference details including the document name, author information, publication date, and applicable section is held. A diagram illustrating database tables is provided in Appendix E. A system Entity-Relationship (ER) diagram is given in Appendix F.

PSATool may be used to conduct multiple assessments with multiple assessment teams. Each assessment should be assigned a unique identifier by a user directly modifying the database table. This identifier allows for multiple assessments to be stored. Likewise, unique identifiers are assigned to each assessment team, allowing multiple assessment teams in each assessment. Queries were constructed to provide aggregate and specific IDF results. Users simply select the desired report from a list of the available queries to obtain results. Results are provided in tabular format as shown in Figure 5.



FacilityName	Room	IDF	ReqNum	AssessNum	AssessDate	TeamNum	ReqResult
Facility	123	123	1	1	12/5/2012	1	Yes
Facility	123	123	2	1	12/5/2012	1	No
Facility	123	123	3	1	12/5/2012	1	Yes
Facility	123	123	4	1	12/5/2012	1	No
Facility	123	123	5	1	12/5/2012	1	No
Facility	123	123	6	1	12/5/2012	1	No
Facility	123	123	7	1	12/5/2012	1	No
Facility	123	123	8	1	12/5/2012	1	No
Facility	123	123	9	1	12/5/2012	1	Yes
Facility	123	123	10	1	12/5/2012	1	No

Figure 5. PSATool query results format

A detailed explanation of these queries is available in Appendix D. These queries include the following reports:

1. Display all failed requirements.
2. Display all passed requirements.
3. Display IDFs that fail a specified requirement.
4. Display IDFs that pass a specified requirement.
5. Count and rank IDFs by failed requirements.
6. Count and rank IDFs by passed requirements.
7. Display IDFs with THV and controls.
8. Display all guidance documents for a specific requirement.
9. Display all IDFs with a specific THV ID.
10. Display requirement test results for a specific IDF.
11. Display negative requirement test results for a specific IDF.
12. Display positive requirement test results for a specific IDF.
13. Display all assessor information.
14. Display the total number of IDFs that fail each requirement.
15. Display the total number of IDFs that pass each requirement.
16. Display IDFs that fail a specific control class.

Results Soundness

Physical Security Requirements

PSATool was developed from multiple standards and recommendations. An explicit mapping of each requirement and THV component to its guiding reference is provided in the Traceability Matrix of Appendix C. Figure 6 shows a sample of this mapping.

Physical Security Assessment Guidance Mapping											
Control Class	Requirement	Physical Security Requirements	Guidance Document								
			NIST SP 800-53	ISO/IEC 27002	NIST SP 800-53A	GLBA	(Johnston & Garcia, 2002)	(Baker, 2005)	FISMA	Whitehead et al., 2007	(Garcia, 2006)
Entry Control	1	Entry control hardware shall exist to restrict entry at the IDF to authorized personnel.	PE-2, PE-4, PE-3(1)	9.1.2	PE-2.1, PE-3.1					SAND2007-5591.24.1.1.5	p.155
	2	More than one form of identification or information shall be required to gain entry to the IDF.	PE-3(2)	9.1.2.b	PE-2(2).1						p.155
Entry Control Type	3	A mechanical lock and key assembly is installed as entry control hardware.	PE-3		PE-2.1						p.155
	4	An electronic keypad reader is installed as entry control hardware.	PE-3		PE-2.1						p.155
	5	An electronic keypad/card reader is installed as entry control hardware.	PE-3		PE-2.1						p.155
	6	An electronic card reader is installed as entry control hardware.	PE-3		PE-2.1						p.155
	7	A biometric device is installed as entry control hardware.	PE-3								p.155
	Transmission Media	8	Signal transmission media including line cabling, wiring, and fiber optics shall be protected from damage.	PE-4	9.2.3	PE-4.1			426.2.2.4		SAND2007-5591.24.1.1.2
9		Power wiring shall be segregated from communication wiring.		9.2.3.d							
10		Cabling shall be identified to minimize patching and handling errors.		9.2.3.d							
11		Patch and connection information shall be documented and available locally.		9.2.3.e							
12		No unauthorized devices or cabling shall be connected to cabling or equipment ports.		9.2.3							
Access Monitoring	13	Physical entry to the IDF shall be logged and monitored by organizational security personnel.	PE-6	9.1.2.a	PE-6.1			426.3.8		SAND2007-5591.24.1.1.5	p.16
	14	Organizational security shall monitor a dedicated IDF intrusion alarm system.	PE-6(1)		PE-6(1).1					SAND2007-5591.24.1.1.3	p.83
	15	The organization shall use camera surveillance systems at the IDF to assess intrusion alarms.	PE-6(1)		PE-6(1).1					SAND2007-5591.24.1.1.3	p.124
	16	An IDF intrusion system shall initiate response for physical intrusion alarms.	PE-6(2)	9.1.1.f	PE-6(2).1			426.3.8		SAND2007-5591.24.1.1.3	p.123
	17	Intrusion incidents shall trigger video recording at the IDF.	PE-6(2)		PE-6(2).1					SAND2007-5591.24.1.1.3	p.123
Power Supply	18	Power equipment and cabling shall be protected from damage and destruction.	PE-9	9.2.3	PE-9.1			426.3.5		SAND2007-5591.24.1.1.2	

Figure 6. Traceability Matrix sample

Relevant information security standards include NIST SP 800-53 (2009), NIST SP 800-53A (2010), and ISO/IEC (2005) 27002. These standards form the core of the physical security requirements. The tool’s scope was expanded beyond the information security domain by including supporting recommendations on physical security from Veterans Administration (VA) and Department of Energy literature. This includes Baker (2005), Beshlin et al. (2003), Johnston & Garcia (2002), Whitehead et al. (2007), and Garcia (2006). To support legal compliance, a THV assessment was included as a component of the tool.

All physical and environmental security controls from NIST SP 800-53 and ISO 27002 deemed applicable to the assessment of IDF installations were incorporated into PSATool’s security requirements. These requirements specify controls on how entry control systems, alarm systems, and backup systems are used and monitored. Requirements were developed for controls devoted to network component location and construction. Requirements describing temperature and humidity monitoring controls were developed. A requirement was elicited for controls designed to prevent electronic information signal leakage.

Some requirements were derived from controls found exclusively in the NIST or ISO/IEC standard. These include ISO/IEC 27002 guidelines for obfuscating network component rooms, labeling and documentation of patch cables, and NIST requirements for automated emergency water shutoff valves. If any controls found in a single standard were related directly to IDF protection, they elicited an associated requirement.

Additional requirements were garnered from the domain of *vulnerability assessment*. Intrusion detection, video surveillance, and construction techniques are described in much greater depth in PPS vulnerability assessment literature than in the information security standards. A requirement for lighting that facilitates surveillance was added to the assessment tool based on recommendations by Whitehead et al. (2007), Beshlin et al. (2003) and Garcia (2006). A requirement was developed in accordance with the proposal by Beshlin et al. (2003) and Baker (2005) for the separation of redundant power supply paths and the separation of primary and backup system location.

The Baker methodology recommends many of the same physical security controls found in FEMA guidelines and information security standards. A requirement was established for the use of prior security incidents as a basis for control development as proposed by Baker. This control is absent from the control sets offered by the NIST or ISO/IEC standards. Prior security incidents were requested for inclusion into the assessment tool. However, no prior security incidents were recommended or provided by ETSU for inclusion as requirements in the assessment using the tool.

The inclusion of a threat, hazard, and vulnerability assessment was motivated by SSAE No. 16, Section 801 and GLBA. The former, SSAE No.16, Section 801 requires the development of controls intended to protect an organization's reporting structure. The latter, GLBA, requires

controls for anticipated threats and hazards. This inclusion of an assessment section is in keeping with a recommendation by Johnston et al. (2002) to allow assessor creativity in the anticipation of threat, hazard, and vulnerability. An area has also been provided for detailed control suggestions offered by the assessment team with which to mitigate any discovered threat, hazard, and vulnerability. The THV assessment supports legal compliance by providing a mechanism by which threats, hazards, and vulnerabilities may be anticipated, and corresponding controls devised.

Several control and VA recommendations were not used to craft requirements for various reasons. While they sacrifice completeness, these exclusions serve to reduce the time and risk incurred by assessment and to enhance the tool's usability.

In order to restrict the assessment tool and project assessment to relevant IDF physical security recommendations, recommendations related to the physically secure removal, disposal, and re-use of equipment, data, and software as advised by ISO/IEC 27002 (2005) were not used. No recommendations by ISO/IEC 27002 (2005) for facility delivery and loading areas' physical security were used. No requirements were created from the recommendations by ISO/IEC 27002 (2005) and NIST SP 800-53 (2009) for the physical security of output devices, including monitors and printers.

In order to reduce the time needed to conduct an assessment and to reduce the risk to the entities being assessed, some recommendations were omitted. Omissions include the analysis of fault trees, the effect of combined vulnerabilities, and the timing of repair and response concerns (Baker, 2005); the timeliness of attacker detection, attacker delay, and security response (Garcia, 2006); and the effect of detailed procedures and event triggers on physical security. Only simple event triggers have been considered for inclusion, e.g., the initiation of video recording once

triggered by an intrusion alarm. Requirements related to the operational testing of controls were not created.

Assessment Procedure

Like the assessment methods found in NIST SP 800-53A, the U.S. government standard for non-security-related information systems, PSATool assessment requirements elicit a binary result. Instead of the detailed assessment procedures found in NIST SP 800-53A, a set of physical security requirements was tested at each IDF.

PSATool Practicality

PSATool was designed to promote usability and extensibility, thereby increasing its practicality. The layout of the assessment form and the language used in the security requirements is self-describing. To assist this self-description, the assessment form contains instructions related to its proper completion, as shown in Figure 7. The assessment form is divided into two easily discernible sections, a requirement test and a THV assessment. Instructions on the assessment form guide assessors in the use of the THV assessment. The binary requirement test result is designed to elicit an unambiguous response from the assessor. Requirement structure follows the intentional sentence structure commonly used in software requirements engineering as promoted by Kandt (2003).

Team	Location	Physical Security Assessment Tool			Date:
Control Class	Requirement	Physical Security Requirements	MET	UNMET	Description of Response
Instructions: 1. Please complete the Team, Location, and Date fields above 2. Please indicate whether each requirement is Met (TRUE) or Unmet (FALSE) in the space provided below 3. Please complete the THV assessment below					
Entry Control	1	Entry control hardware shall exist to restrict entry at the IDF to authorized personnel.			
	2	More than one form of identification or information shall be required to gain entry to the IDF.			

Figure 7. PSATool completion instructions

A user’s computer skill level determines the extent to which PSATool is usable and extensible. This includes users with no computer skills or limited computer skills, to computing professionals having programming knowledge.

Users with no computer skills may perform assessments using a printed assessment form. The use of assessors possessing varying skill sets and experiences to conduct vulnerability assessments is recommended by Johnston et al. (2002). Additionally, users with no computer skills may develop additional or tailored requirements by following the language structure found in the assessment physical security requirements (Kandt, 2003).

Users possessing basic computer skills may display assessment results by using the provided queries. These queries require users to simply select a report and enter no more than one operand to obtain query results. These results provide network support personnel with detailed data useful for prioritization of physical security improvement.

Users with intermediate computer skills can extend PSATool. They may add new and modified requirements into the assessment form, insert additional IDFs into an assessment, and insert data directly into the database tables. This modification may be performed by copying a row containing any requirement, then inserting this copied row into the appropriate control class. This duplicate row may then be modified to reflect the new requirement. The updated assessment form is then linked to the database. Intermediate skill users may also extend PSATool by adding IDFs to an assessment. This is performed by copying and inserting an additional blank assessment form into the PSATool spreadsheet, then linking this new sheet to the database. Intermediate skill users can insert assessment data directly to the database tables by locating and navigating to the appropriate table, then populating the appropriate cell.

Users who can program in SQL can extend PSATool by constructing new queries, e.g., a new query that counts and ranks IDFs by number of THV elements. This user would also be able to tailor existing queries to suit organizational need. A programmer with knowledge of relational database theory can extend PSATool's data model by adding new tables or altering existing

tables. New table attributes could also be added or modified by this level of user. This change might be necessary if an additional persistent attribute were required, e.g., the addition of a field to record the date that a requirement was incorporated into the assessment form.

Reusability is another practical feature of PSATool. The spreadsheet and database may be used to conduct multiple assessments, thereby developing a history of physical security assessment. While the date of an assessment is logged, assessments are assigned an identifier that indicates the assessment set to which an individual assessment belongs.

PSATool Effectiveness

An assessment team composed of George Peters, OIT Network Support Specialist, and Nathan Timbs, a graduate student, evaluated PSATool by using it to assess physical security at 135 IDF locations on the ETSU campus in autumn 2012. A printed version of PSATool's assessment form was used to evaluate 52 physical security requirements and complete the included threat, hazard, and vulnerability assessment by visually inspecting each IDF interior and exterior. These IDF locations were evaluated during a span of 50 hours over a period of 6 weeks from mid-October through early December. Each assessment required an average time of roughly 22 minutes. Some requirements tests were incomplete due to insufficient power and backup system labeling and documentation. As a result, the data collected at the IDF locations was augmented with supplemental data in the form of facility generator information obtained from ETSU's Facilities Department in January 2013. The requirements tests yielded 7,020 data points. The threat, hazard, and vulnerability assessment yielded 95 elements of THV. Controls were recommended for each element. All data garnered during the assessment was entered into PSATool during December 2012 and January 2013. Detailed assessment results and reports were provided to ETSU in late January 2013.

To protect ETSU's security, the following discussion of the assessment's results characterizes the findings in relatively broad terms. All characterizations of specific assessment results and vulnerabilities will be withheld until they have been addressed. All references to the identity and location of specific IDFs have been obfuscated.

Assessment Data Collection

The ETSU OIT network contains 158 IDFs located in Johnson City and surrounding areas. Johnson City locations include 147 IDFs. PSATool was used to audit 135 of the IDFs located in Johnson City.

Approximately 100 assessments were successfully completed in the first attempt. The remaining locations required additional information and investigation regarding power supply and backup capability. Ultimately, all assessed IDFs yielded complete data sets.

Three Johnson City campus IDFs were not assessed. The Reece Museum IDF was undergoing construction; therefore, any assessment would have been incomplete. One installation containing a single switch was not assessed due to difficulty in gaining equipment access. One installation slated for removal was not assessed. This installation has since been eliminated.

Five types of obstacles were encountered during data collection. Nine Veterans Administration IDFs were not assessed due to their location. These IDFs were in buildings considered to be hazardous environments. Gaining authorized entry to these IDFs was therefore considered difficult. A recommendation to relocate these IDF's to more easily accessible locations or separate sites with network cable being pulled to the locations with restricted access was offered to the system administrators in the final report and in the final meeting.

Backup system capabilities were not clearly identified at each IDF. This lack of

identification increased assessment difficulty and decreased accuracy. Several IDF installations that appear to have backup systems had no visible indication of such, e.g., signage or labeling, of their backup capability. Only those IDF locations with a backup system located inside the IDF, or those with a visual indication of a backup system, e.g., uninterrupted power supply circuits designated with orange receptacles, met the requirements for a backup power supply.

Additionally, the location of a generator on the immediate facility grounds capable of supplying power to the facility main power service produced a positive response for a long-term backup system. A recommendation for proper labeling was submitted in the final report.

Generator information for various ETSU facilities was obtained from the Facilities Department. Facilities personnel did not know how well these generators would support their respective subgrids during an outage, including the resident IDFs. A recommendation for careful investigation followed by documentation was given in the final report.

Inconsistent labeling of redundant power feeds increased assessment difficulty and decreased accuracy. Several IDF installations had parallel redundant power wiring that was unlabeled or ambiguously labeled. Only those IDF locations with clearly labeled and readily identifiable power feeds passed the requirements for physically separated redundant power feeds. A recommendation for careful investigation followed by documentation was given in the final report.

Several IDFs had no room number. This lack of identification may impede location of the IDF by department personnel and emergency responders. A recommendation to label all unidentified rooms was supplied in the final report.

Assessment Results Overview

Assessed IDFs vary greatly in construction, protection, and location. Assessment results

reflect this variation.

Figure 8 presents a graph displaying the total requirements passed at each IDF. At least 10 requirements were passed by all IDFs. Five IDFs passed the most requirements, at 27. Newly constructed or recently renovated IDF installations passed more assessment requirements. The mean and median number of passed requirements was 20 requirements. Eleven IDFs passed at least half of the requirements. Almost all IDFs failed requirement 10, which was concerned with the labeling of IDF cables.

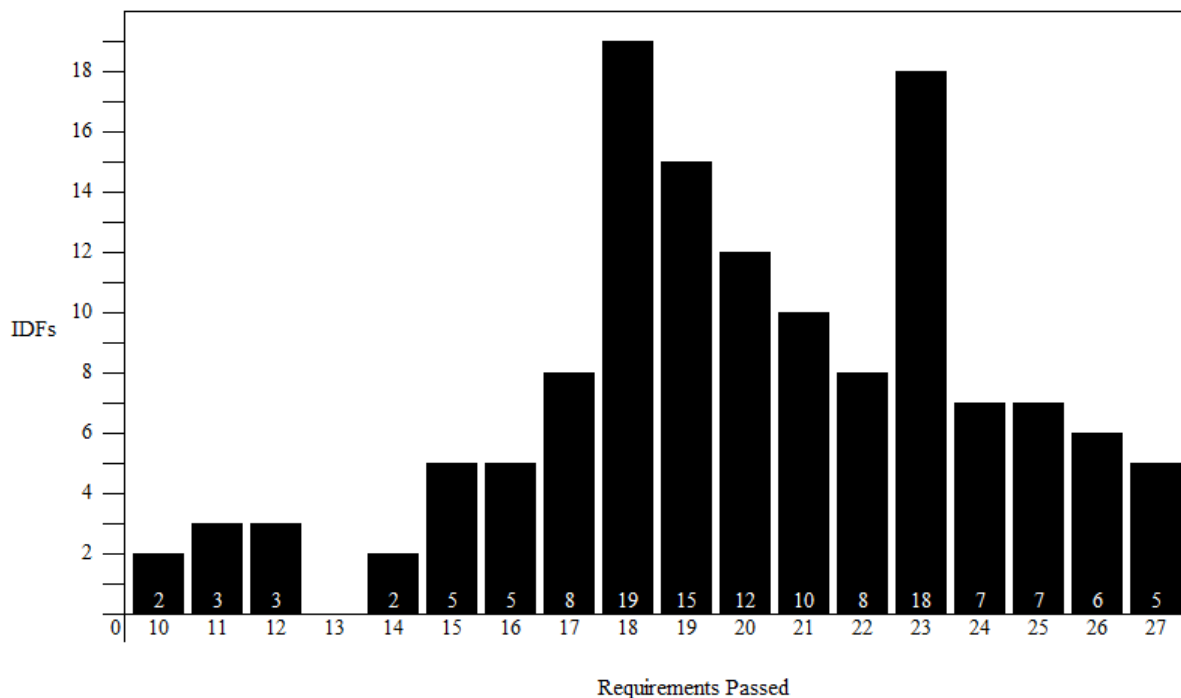


Figure 8. Number of requirements passed per IDF

Of 135 IDFs assessed, 82 IDFs exhibited a total of 95 threats, hazards, and vulnerabilities. Thirty-one distinct elements of THV were found. Nineteen IDFs were found to have no room number. This was considered to be hazardous to network operations due to the inability of service and emergency personnel to locate the IDF using the room number. Eleven IDFs had no lighting. This was considered hazardous in that service personnel might

unintentionally endanger network operations by accident while maneuvering around in a dimly lit IDF. Nine IDFs had a vent located in the IDF door. This was considered vulnerability because the vent could be easily removed, thereby gaining unauthorized IDF access. Each THV element triggered a control recommendation by the assessment team. Some recommended controls covered multiple threats, hazards, and vulnerabilities. This overlap resulted in 26 distinct control recommendations. Appendix J contains the individual elements of discovered THV. Appendix K lists the control recommendations offered by the assessment team for each element of discovered THV.

Data Reporting

The five documents that comprise the detailed assessment results were provided to ETSU (OIT) in January of 2013. The assessment report *Requirement Data Summary* and *THV Data Summary* sections have been included in Appendices G and H, respectively. The assessment report *Recommendations* section has been included in Appendix I.

In April 2013, a final meeting was held with ETSU (OIT) to review the assessment. Additional assessment results were collected as a result of this meeting concerning the validity, usefulness, and completeness of the assessment requirements. The meeting results are as follows:

1. When ranked by requirements passed, IDF rank corresponded to the system owner's estimation of IDF physical security, i.e., IDFs considered more secure by the system owner ranked higher.
2. The Traceability Matrix provides justification for isolation of network equipment.
3. The Traceability Matrix provides justification for capital investment.
4. Assessment coverage and depth exceeded system owner expectation.
5. All IDFs failed Requirement 10, which states that "cabling shall be identified to

minimize patching and handling errors”. ETSU (OIT) practice is to label ports rather than cables. It was recommended that this departure from requirements (and standard practice) be justified and documented as part of a system risk assessment. Once justified, Requirement 10 could be tailored to organizational practice to prefer the labeling of switch ports, e.g., “switch ports shall be identified to minimize patching and handling errors”.

CHAPTER 5

CONCLUSIONS

The goal of creating a sound, practical, and effective tool for physical security assessment was achieved. The goal of soundness was met by reviewing key standards of the information security domain and reviewing literature from the vulnerability assessment domain. The goal of practicality was met by demonstrating the relation between the standards and the information collected, while allowing for expansion through a THV assessment. The tool's effectiveness was demonstrated by validating its use in a university network setting.

Assessment tool implementation provided an image of IDF state that corresponded to the system owner's preconceived estimation of IDF state, i.e., IDFs that owners viewed as more physically secure met more requirements than IDFs that were viewed as less secure. When ranked by the number of passed requirements, rooms perceived by the system owner to be more physically secure ranked higher. Rooms expected to be less physically secure ranked lower. This correlation between assessment results and owner estimation of security attests to the tool's validity.

The Traceability Matrix found in Appendix C addresses several system owner concerns. Encroachment of building utilities, hardware, and systems into space ideally relegated to network equipment is an increasing problem. In the system owner's experience, building designers are concerned primarily with building codes. They are not typically concerned with information security standards and practices that attempt to provide a protected, dedicated space for network equipment as described by the *comparison IDF*. The Traceability Matrix provides standard and practice support for the system owner related to providing an isolated space for network equipment. Justification of capital expenditure is another owner concern. Unlike the *comparison*

IDF, system owners have limited funding with which to select controls. System owners must also justify security concerns and related control choices to administrative entities to secure funding. Through the use of PSATool's Traceability Matrix, capital expenditure can be prioritized and justified based on practices, standards, and legislative support.

When the system owner was asked how the assessment might be improved upon, no suggestions for improvement were offered. Assessment coverage and depth exceeded system owner expectation.

Assessment requirements were developed with no prior knowledge of existing system controls; however, no existing system controls were found to be missing from assessment requirements, i.e., existing *IDF* controls were contained within the set of assessment requirements. This finding implies that assessment requirements were sufficient to assess existing controls. Additionally, this finding implies that all existing controls were deemed necessary for physical security, supporting the validation of the individual assessment requirements.

Additional *THV* was discovered in several *IDFs*. This new *THV* could represent significant risk. It should be reviewed by system owners. If determined to be significant, this *THV* should be treated with appropriate controls. Any new controls should trigger new requirements for inclusion in future assessments. If the *THV* is deemed insignificant, justification as to its insignificance should be formally documented.

Recommendations for Future Work

Requirements for operational testing should be developed and incorporated into future assessments. Currently, PSATool's requirements are limited to establishing that recommended controls are in place. These expanded requirements should increase testing depth. Increased

testing depth, however, will incur increased risk, i.e., a failed operational test may result in system and service failure.

Requirements that specify these complex sequences of events should be developed as needed. Assessment tool requirements currently specify simple event triggers. Complex sequences of actions may be required to provide a proper alarm response. Complex action sequences triggered by system input constitute controls and should be tested by a formal requirement as such.

Additional requirements should be developed that guarantee the evolution of requirements to meet current practice and conditions. Assessment tool requirements reflect current standards and practice. To adequately assess control choice, requirements must be based on current industry practices and environmental conditions. These requirements would require the use of the latest best-practice standards and vulnerability literature. Additional corollary requirements might trigger the review of foundation documents on a periodic basis.

Requirements should be developed that stipulate ongoing, periodic assessment. These temporal requirements might be met only if an assessment has been performed within a specified time limit.

The project assessment contains compound requirements. Unless specifying detailed sequences of action, compound requirements should be decomposed into simple requirements. For example, requirement 27 stipulates that “Fire detection shall be automatically activated and emergency responders automatically notified”. This requirement could be decomposed into two constituent requirements, one specifying automatically activated fire detection and another specifying the automated notification of emergency response personnel upon fire detection.

Requirements should be developed for newly-discovered THV and related, recommended

controls reviewed by system owners. Ideally, the control suggestions collected by the THV assessment will result in new system controls and accompanying requirements. Additional table attributes might be required to log the incorporation date of new and modified requirements.

Additional queries should be developed and tailored to suit organizational need. These queries might count and rank IDFs by the number of THV elements they possess. Future queries should exploit the ability of PSATool to store multiple assessments with multiple teams, allowing searches based on assessment date, assessment number, and team configuration.

Summary

Security assessments for computer networks, increasingly used as system infrastructure and service provider, primarily focus on cyber security. As a result, few tools exist for network physical security assessment. To help address this need, PSATool, a sound, practical, and effective physical security assessment tool was designed, implemented, and evaluated at ETSU, a regional university. This tool is devoted to the physical security assessment of IDFs.

To promote soundness, PSATool was designed to support standard-based security as endorsed by Parker (2006). The tool is composed of a spreadsheet and linked database. The tool's spreadsheet interface contains an assessment form with requirements developed from physical security controls used to mitigate risk provided in National Institute of Standards and Technology (NIST) SP 800-53 (2009), NIST SP 800-53A (2010) and International Standards Organization and the International Electrotechnical Commission (ISO/IEC) 27002 (2005) information security standards. Additional requirements were derived from vulnerability assessment recommendations by Department of Energy scientists, Federal Emergency Management Agency authors, and vulnerability assessment authors. Legislative compliance was addressed with the inclusion of Tennessee Board of Regents guideline B-090 (2003)

requirements which stipulate Graham-Leach-Bliley Act compliance.

To promote practicality, PSATool was designed to be easily used, extended, and reused. PSATool provides a spreadsheet interface for entering the requirements tests. Threat, hazard, and vulnerability (THV) data must be entered directly into the database. A printed version of the assessment form allows users with no computing skills to act as assessors. Users with basic skills can produce assessment results with the use of provided queries. Users with intermediate skills can extend PSATool by adding and modifying physical requirements; they can also add new IDFs to an assessment. Advanced users with programming knowledge can alter or add queries. These users can also modify PSATool's data model by adding or altering tables. PSATool supports a program of ongoing assessments using multiple assessment teams.

To demonstrate its effectiveness, PSATool was used at East Tennessee State University (ETSU) to assess physical security at 135 intermediate distribution frame (IDF) installations. 52 physical security requirements were used to compare the existence of IDF network physical security controls to controls recommended by information security standards and *vulnerability assessment* recommendations. A threat, hazard, and vulnerability assessment was conducted at each IDF.

Four types of obstacles were encountered during the assessment. Several Veterans Administration IDFs were not assessed due to access difficulty. This obstacle led to a recommendation for IDF relocation. Backup system capabilities were not identified at each IDF. This obstacle led to a recommendation for careful investigation and documentation of power sources. Facility and IDF generator capability was unknown by facilities personnel. This obstacle led to a recommendation for careful investigation and documentation. Inconsistent labeling decreased assessment accuracy. This obstacle led to a recommendation for proper labeling.

The assessment yielded 7,020 data points. The mean and median of passed requirements was 20. At least 10 requirements were passed by all IDFs. At least half of the requirements were passed by 11 IDFs. Five IDFs passed the most requirements, at 27. Almost all IDFs failed requirement 10. Eighty-two IDFs were found to contain 95 additional threats, hazards, and vulnerabilities. A control was recommended for each THV element discovered. Newly constructed or recently renovated IDF installations passed more requirements.

Raw data, data analysis, and improvement recommendations based on assessment results were provided to the system owner in a report and database. The database provided queries that allowed the ranking of IDFs by quantity of passed or failed requirements. Additional queries allowed system owners to display all requirements passed or failed by a specific IDF. Conversely, all IDFs passing or failing a specific requirement could be displayed.

Recommendations for improvement include the following:

1. Perform a risk assessment to justify and document deviation (including supplementary and unneeded controls) from assessment requirements.
2. Prioritize and implement any required controls specified by failed requirements.
3. Label unidentified IDFs.
4. Use redundant power feeds effectively.
5. Label power feed sources.
6. Perform operational testing to prove the existence and operation of backup systems.
7. Install humidity monitoring sensors.
8. Label backup system components.
9. Install shunt trip hardware in locations where sprinklers could damage equipment or create a hazard for electrical shock.

10. Tailor the requirements in this assessment to ETSU practices.
11. Perform an assessment with the tailored requirements.
12. Make assessment a continuous procedure.

A final assessment meeting was held to discuss assessment results and elicit additional feedback. System owners advised that when ranked according to the quantity of passed requirements, the relative rank of individual IDFs corresponded to their preconceived ideas of IDF physical security. This correlation between assessment results and system owner estimation of IDF physical security supports the tool's validity. System owners noted the usefulness of the Traceability Matrix in providing justification for isolation of network equipment. This result should provide defense against encroaching building systems into space allocated for network equipment. System owners noted the usefulness of the Traceability Matrix in justifying capital investment. This result should help system owners, faced with finite funding, prioritize and support specific control investment. Assessment coverage and depth was found to have exceeded system owner expectation. More controls were specified by requirements than were found in the assessed IDFs. Requirement 10 was examined for relevance to organizational practice. It was recommended that Requirement 10 be modified to reflect organizational practice after being justified and documented as part of a risk assessment.

Future work based on this assessment includes the following recommendations:

1. Develop requirements that specify operational testing and incorporate those requirements into future assessments.
2. Develop requirements for controls that specify complex sequences of events.
3. Develop requirements that guarantee that assessment requirements are based on current practice and conditions.

4. Develop requirements that stipulate ongoing, periodic assessment.
5. Decompose compound requirements into simple requirements.
6. Develop requirements to stipulate the controls recommended for newly-discovered THV be reviewed by system owners.

WORKS CITED

- AICPA. (2011, June 1). *SSAE No. 16 -AT Section 801*. Retrieved May 27, 2012, from American Institute of CPAs:
<http://www.aicpa.org/research/standards/auditattest/downloadabledocuments/at-00801.pdf>
- Al-Hamdani, W. A. (2009). Non Risk Assessment Information Security Assurance Model. *InfoSecCD '09* (pp. 84-90). New York: ACM.
- Baker, G. H. (2005, April). *A Vulnerability Assessment Methodology for Critical Infrastructure Sites*. Retrieved February 1, 2012, from The Berkeley Electronic Press:
http://works.bepress.com/george_h_baker/2
- Beshlin, D., Chipley, M., Hester, M., Kaminskis, M., & Lyon, W. (2003, December). *Resource Record Details: Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*. Retrieved February 2, 2012, from FEMA:
<http://www.fema.gov/library/viewRecord.do?id=1559>
- Bishop, M.A. (2002). *The Art and Science of Computer Security*. Boston, MA: Addison-Wesley Longman Publishing Co., Inc.
- Calder, A., & Watkins, S. (2008). *IT Governance: A manager's guide to data security and ISO27001/ISO 27002*, 4th edition. London, Philadelphia: Kogan Page.
- Cisco Systems, Inc. (2004). *Power and Cooling for VoIP and IP Telephony Applications*. Retrieved May 15, 2012, from www.apcmedia.com:
www.apcmedia.com/salestools/RMEN-65ZRMF_R0_EN.pdf
- Dey, M. (2007). Information Security Management — A Practical Approach. *AFRICON 2007* (pp. 1-6). Windhoek: IEEE.
- ETSU (2012). *ETSU Fact Book*. Retrieved June 24, 2013, from
<http://www.etsu.edu/opa/factbooks/Fact%20Book%202012%20PDF/Section%2001%20University%20Information/1.02%20University%20Profile.pdf>
- ETSU (2013). *ETSU Budget*. Retrieved September 9, 2013, from
http://www.etsu.edu/budget/budget_docs/ETSU_July2013_2014.pdf
- Fernández-Medina, E., Sanchez, L. E., Villafranca, D., & Piattini, M. (2006). Practical Approach of a Secure Management System based on ISO/IEC 17799. *ARES '06: Proceedings of the First International Conference on Availability, Reliability and Security* (pp. 585-592). Washington: IEEE Computer Society.
- Garcia, M. L. (2006). *Vulnerability Assessment of Physical Protection Systems*. Burlington, MA: Elsevier Butterworth-Heinemann.

- GLBA. (1999, November) *Graham-Leach-Bliley Act*. Retrieved from <http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/pdf/PLAW-106publ102.pdf>
- Henley, E. J., & Kumamoto, H. (1996). *Probabilistic Risk Assessment and Management for Engineers*. New York: New York: Institute of Electrical and Electronics Engineers, Inc.
- ISO/IEC 27001. (2005). *ISO/IEC 27001:2005*. Information technology—Security techniques—Information security management systems—Requirements.
- ISO/IEC 27002. (2005). *ISO/IEC 27002:2005*. Information technology—Security techniques—Code of practice for information security management.
- Johnston, R. G. & Garcia, A. R., (2002, September 03). *Effective Vulnerability Assessments for Physical Security Devices, Systems, and Programs*. Retrieved October 9, 2011, from Los Alamos National Laboratory: <http://library.lanl.gov/cgi-bin/getfile?00852052.pdf>
- Kairab, S. (2005). *A practical guide to security assessments*. Boca Raton: CRC Press LLC.
- Kandt, R.K. (2003). *Software Requirements Engineering: Practices and Techniques*. Retrieved July 22, 2013, from http://whalen.ws/index_files/JPL_SW_Reqmts_Engr_D-24994%5B1%5D.pdf
- Knolmayer, G. F., & Asprion, P. (2011, June). Assuring Compliance in IT Subcontracting and Cloud Computing. (Working Paper No. 236). Retrieved May 22, 2012, from Institute of Information Systems at the University of Bern: http://www.iwi.unibe.ch/content/e6050/e6133/e10078/e10080/e10081/AB236_ger.pdf236_ger.pdf&ei=Qyr
- Mattord, H. J. (2007). Rethinking risk-based information security. *Proceedings of the 4th annual conference on information security curriculum development* (pp. 28-29). New York: ACM.
- Nessus. (2013). Nessus Vulnerability Scanner. *Tenable Network Security*. Retrieved July 18, 2013, from <http://www.tenable.com/products/nessus>
- NIST. (2004, February). *Federal Information Processing Standards Publication*. Retrieved from National Institute of Standards and Technology Information Technology Laboratory: Retrieved May 27, 2012, from <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>
- NIST. (2009, August 14). *NIST Special Publication 800-53 Revision 3*. Retrieved from National Institute of Standards and Technology Information Technology Laboratory: Retrieved May 27, 2012, from http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf

- NIST. (2010, June). *NIST Special Publication 800-53A Revision 1*. Retrieved from National Institute of Standards and Technology Information Technology Laboratory: Retrieved May 27, 2012, from <http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf>
- NIST. (2011, September). *NIST Special Publication 800-30 Revision 1*. Retrieved from National Institute of Standards and Technology Information Technology Laboratory: Retrieved June 25, 2012, from http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
- NTOSpider. (2013). *World Class Web Application Security Testing and Scanning. NTObjectives*. Retrieved July 18, 2013, from <http://www.ntobjectives.com>
- OIT (2013). *Office of Information Technology*. Retrieved August 27, 2013, from <http://www.etsu.edu/oit/>
- Parker, D. (2006, May). Making the case for replacing risk-based security. *ISSA Journal*, pp. 6-10.
- Pholi, L. (2003, April). Security in Practice – Reducing the Effort. Retrieved June 24, 2013, from http://www.sans.org/reading_room/whitepapers/bestprac/security-practice-reducing-effort_1106
- Rakers, J. (2010). Managing Professional and Personal Sensitive Information. *SIGUCCS '10 Proceedings of the 38th annual fall conference on SIGUCCS* (pp. 9-13). New York, NY: ACM.
- Richards, T. C. (1982). Improving Computer Security Through Environmental Controls. *ACM SIGSAC Review* , 18-24.
- Soo Hoo, K. J. (2000). *How Much Is Enough? A Risk-Management Approach to Computer Security*. Stanford, CA: Consortium for Research on Information Security Policy (CRISP) Working Paper.
- Saint. (2013). Integrated Vulnerability Assessment and Penetration testing. *Saint Vulnerability Management Title, Penetration Testing & Compliance*. Retrieved July 18, 2013, from <http://www.saintcorporation.com/>
- Stoneburner, G., Goguen, A., & Feringa, A., (2002, July). Risk Management Guide for Information Technology Systems. *Special Publication 800-30* . Gaithersburg, MD, USA: National Institute of Standards and Technology.
- TBR. (2003, November). *TBR Guideline B-090*. Retrieved from <http://www.tbr.edu/policies/default.aspx?id=1712>

- Thiagarajan, V. (2006). BS ISO IEC 17799 SANS Checklist. Retrieved July 18, 2013, from http://www.sans.org/score/checklists/ISO_17799_2005.pdf
- Tittel, E., Chapple, M., & Stewart, J. M. (2004). *CISSP: Certified Information Systems Security Professional Study Guide*. Alameda: SYBEX.
- U.S. Code (2002). Cornell University Law School. *44 USC 3542 Definitions*. Retrieved June 25, 2013, from <http://www.law.cornell.edu/uscode/text/44/3542>
- Verendel, V. (2009). Quantified Security is a Weak Hypothesis. *NSPW '09 Proceedings of the 2009 workshop on new security paradigms workshop*. New York: ACM.
- Whitehead, D. W., Potter, C. S., & O'Connor, S. L. (2007). *Nuclear Power Plant Security Assessment Technical Manual*. Albuquerque, NM: Sandia National Laboratories.

APPENDIX B

Physical Security Requirements

1. Entry control hardware shall exist to restrict entry at the IDF to authorized personnel.
2. More than one form of identification or information shall be required to gain entry to the IDF.
3. A mechanical lock and key assembly is installed as entry control hardware.
4. An electronic keypad reader is installed as entry control hardware.
5. An electronic keypad/card reader is installed as entry control hardware.
6. An electronic card reader is installed as entry control hardware.
7. A biometric device is installed as entry control hardware.
8. Signal transmission media including line cabling, wiring, and fiber optics shall be protected from damage.
9. Power wiring shall be segregated from communication wiring.
10. Cabling shall be identified to minimize patching and handling errors.
11. Patch and connection information shall be documented and available locally.
12. No unauthorized devices or cabling shall be connected to cabling or equipment ports.
13. Physical entry to the IDF shall be logged and monitored by organizational security.
14. Organizational security shall monitor a dedicated IDF intrusion alarm system.
15. The organization shall use camera surveillance systems at the IDF to assess intrusion alarms.
16. An IDF intrusion system shall initiate response for physical intrusion alarms.
17. Intrusion incidents shall trigger video recording at the IDF.
18. Power equipment and cabling shall be protected from damage and destruction.
19. Any parallel power supply paths provided shall be separated physically.
20. Redundant parallel cabling paths shall be used to provide power to the IDF.
21. A power service disconnect shall be provided with which to remove equipment power remotely.
22. Any remote power service disconnect provided shall be protected from unapproved activation.
23. Automatically activated emergency lighting shall be provided for emergency egress.
24. Lighting shall be designed to assist surveillance using a camera system.
25. A fire detection system shall be installed.
26. A fire suppression system shall be installed.
27. Fire detection shall be automatically activated and emergency responders automatically notified.
28. Fire suppression shall be automatically activated and emergency responders automatically notified.
29. A fire extinguisher shall be provided at the IDF.
30. A dedicated HVAC system shall be used exclusively for IDF temperature control.
31. Temperature shall be monitored and maintained within the IDF.
32. Humidity shall be monitored and maintained within the IDF.
33. Alarm systems shall be installed in the IDF to detect disruption in any supporting utility.

34. Water supply shutoff valves shall be provided in the event of water leakage adjacent to the IDF.
35. Water supply shutoff valves shall be accessible.
36. Automated water supply shutoff valves shall be provided to protect against adjacent area water leakage.
37. The IDF shall be located above the first floor to minimize flood impact.
38. Equipment shall be protected from HVAC utility disruption.
39. A short-term uninterruptable power supply shall be provided for equipment shutdown.
40. A long-term uninterruptable power supply shall be provided for continuous equipment operation.
41. Any utility backup systems provided shall be located separately from the equipment to be served.
42. The IDF shall have its purpose obscured, with no external indication as to use.
43. The IDF shall be built in a solid and continuous manner with no gaps in construction.
44. The IDF shall have no windows installed.
45. The IDF shall have no drop ceiling installed.
46. The IDF shall be located on a wall other than an exterior wall to minimize vulnerability.
47. Facility utilities shall be located outside the IDF.
48. Spare equipment including backup media and bulk supplies shall be stored outside the IDF.
49. A grounding electrode shall bond the building structure and IDF equipment chassis to ground.
50. Lightning protection shall be supplied to the incoming power.
51. Lightning protection shall be supplied to the communication cabling.
52. Electromagnetic shielding shall be used to reduce electromagnetic emanation.

APPENDIX C

Traceability Matrix

Physical Security Assessment Guidance Mapping											
Control Class	Requirement	Physical Security Requirements	Guidance Document								
			NIST SP 800-53	ISO/IEC 27002	NIST SP 800-53A	GLBA	(Johnson & Garcia, 2002)	(Baker, 2005)	FEMA	Whiteland et al., 2007	(Garcia, 2006)
Entry Control	1	Entry control hardware shall exist to restrict entry at the IDF to authorized personnel.	PE-2, PE-4, PE-3(1)	9.1.2	PE-2.1, PE-3.1					SANS2007-5591.24.1.1.5	p.155
	2	More than one form of identification or information shall be required to gain entry to the IDF.	PE-2(2)	9.1.2b	PE-2(2).1						p.155
Entry Control Type	3	A mechanical lock and key assembly is installed as entry control hardware.	PE-3		PE-2.1						p.155
	4	An electronic keypad reader is installed as entry control hardware.	PE-3		PE-2.1						p.155
	5	An electronic keypad/card reader is installed as entry control hardware.	PE-3		PE-2.1						p.155
	6	An electronic card reader is installed as entry control hardware.	PE-3		PE-2.1						p.155
	7	A biometric device is installed as entry control hardware.	PE-3		PE-2.1						p.155
Transmission Media	8	Signal transmission media including line cabling, wiring, and fiber optics shall be protected from damage.	PE-4	9.2.3	PE-4.1			426.2.2.4		SANS2007-5591.24.1.1.2	p.163
	9	Power wiring shall be segregated from communication wiring.		9.2.3.a							
	10	Cabling shall be identified to minimize patching and handling errors.		9.2.3.d							
	11	Patch and connection information shall be documented and available locally.		9.2.3.e							
	12	No unauthorized devices or cabling shall be connected to cabling or equipment ports.		9.2.3							
Access Monitoring	13	Physical entry to the IDF shall be logged and monitored by organizational security personnel.	PE-6	9.1.2.a	PE-6.1			426.3.8		SANS2007-5591.24.1.1.5	p.16
	14	Organizational security shall monitor a dedicated IDF intrusion alarm system.	PE-6(1)		PE-6(1).1					SANS2007-5591.24.1.1.3	p.83
	15	The organization shall use camera surveillance systems at the IDF to assess intrusion alarms.	PE-6(1)		PE-6(1).1					SANS2007-5591.24.1.1.3	p.124
	16	An IDF intrusion system shall initiate response for physical intrusion alarms.	PE-6(2)	9.1.1.f	PE-6(2).1			426.3.8		SANS2007-5591.24.1.1.3	p.123
	17	Intrusion incidents shall trigger video recording at the IDF.	PE-6(2)		PE-6(2).1					SANS2007-5591.24.1.1.3	p.123
Power Supply	18	Power equipment and cabling shall be protected from damage and destruction.	PE-9	9.2.3	PE-9.1			426.3.5		SANS2007-5591.24.1.1.2	
	19	Any parallel power supply paths provided shall be separated physically.						(Baker, 2005)	426.2.10		
	20	Redundant parallel cabling paths shall be used to provide power to the IDF.	PE-9(1)	9.2.2	PE-9(1).1			426.2.10			
	21	A power service disconnect shall be provided with which to remove equipment power remotely.	PE-10	9.2.2	PE-10.1						
	22	Any remote power service disconnect provided shall be protected from unapproved activation.	PE-10		PE-10.1						
Emergency Lighting	23	Automatically activated emergency lighting shall be provided for emergency egress.	PE-12	9.2.2	PE-12.1						
	24	Lighting shall be designed to assist surveillance using a camera system.						426.3.5		SANS2007-5591.24.1.1.3	p.136
Fire Protection	25	A fire detection system shall be installed.	PE-13	9.1.4.e	PE-13.1			(Baker, 2005)	426.3.6		
	26	A fire suppression system shall be installed.	PE-13	9.1.4.e	PE-13.1			(Baker, 2005)	426.3.6		
	27	Fire detection shall be automatically activated and emergency responders automatically notified.	PE-13(1), PE-13(3)	9.1.4	PE-13(1).1, PE-13(3).1						
	28	Fire suppression shall be automatically activated and emergency responders automatically notified.	PE-13(2), PE-13(3)	9.1.4	PE-13(2).1, PE-13(3).1						
	29	A fire extinguisher shall be provided at the IDF.	PE-13	9.1.4.e							
Environmental Protection	30	A dedicated HVAC system shall be used exclusively for IDF temperature control.	PE-14(1)		PE-14.1						
	31	Temperature shall be monitored and maintained within the IDF.	PE-14	9.2.1.f	PE-14(1).1, PE-14(2).1						
	32	Humidity shall be monitored and maintained within the IDF.	PE-14(1)	9.2.1.f	PE-14(1).1, PE-14(2).1						
	33	Alarm systems shall be installed in the IDF to detect disruption in any supporting utility.		9.2.2							
Flood Protection	34	Water supply shutoff valves shall be provided in the event of water leakage adjacent to the IDF.	PE-15		PE-15.1						
	35	Water supply shutoff valves shall be accessible.	PE-15		PE-15.1						
	36	Automated water supply shutoff valves shall be provided to protect against adjacent area water leakage.	PE-15(1)		PE-15(1).1						
	37	The IDF shall be located above the bottom floor to minimize flood impact.	PE-18	9.1.4	PE-18.1						
Backup Systems	38	Equipment shall be protected from HVAC utility disruption.		9.1.4							
	39	A short-term uninterruptable power supply shall be provided for equipment shutdown.	PE-11	9.2.2	PE-11.1						
	40	A long-term uninterruptable power supply shall be provided for continuous equipment operation.	PE-11(1), PE-11(2)	9.2.2	PE-11(1).1, PE-11(2).1						
	41	Any utility backup systems provided shall be located separately from the equipment to be served.						(Baker, 2005)	426.2.10		
IDF Construction	42	The IDF shall have its purpose obscured, with no external indication as to use.		9.1.3.a				426.2.10			
	43	The IDF shall be built in a solid and continuous manner with no gaps in construction.		9.1.1				426.2.10			
	44	The IDF shall have no windows installed.		9.1.1.b							
	45	The IDF shall have no drop ceiling installed.		9.1.1				426.3.1.3			
	46	The IDF shall be located on a wall other than an exterior wall to minimize vulnerability.		9.1.1, 9.2.1.4				426.3.1.2			
	47	Facility utilities shall be located outside the IDF.		9.2.1.4				(Baker, 2005)			
General Vulnerability	48	Spare equipment including backup media and bulk supplies shall be stored outside the IDF.	PE-18	9.1.4	PE-18.1						
Surge Protection	49	A grounding electrode shall bond the building structure and IDF equipment chassis to ground.		9.1.4							
	50	Lightning protection shall be supplied to the incoming power.	PE-9(2)	9.2.1.g							
	51	Lightning protection shall be supplied to the communication cabling.		9.2.1.g							
Electronic Emanation	52	Electromagnetic shielding shall be used to reduce electromagnetic emanation.	PE-19	9.2.1.i	PE-19.1, PE-19(1).1			(Baker, 2005)			
	53	Requirement(s) garnered from prior security incident(s).						(Baker, 2005)			
THV Assessment		Please describe any anticipated threat, hazard, or vulnerability discovered during this assessment.				15 USC 6801 80C.501(2)	LAUR-62-5545.3	(Baker, 2005)		SANS2007-5591.24.2.1.1	
THV Assessment		Please suggest a control for any anticipated threat, hazard, or vulnerability discovered.				15 USC 6801 80C.501(2)	LAUR-62-5545.3	(Baker, 2005)		SANS2007-5591.24.2.1.1	

APPENDIX D

Database Queries

1. Display all failed requirements.

This query displays all failed requirements ordered alphabetically by the facility name.

2. Display all passed requirements.

This query displays all passed requirements ordered alphabetically by the facility name.

3. Display IDFs which fail a specified requirement.

This query displays all IDFs that failed a requirement specified by the user.

4. Display IDFs which pass a specified requirement.

This query displays all IDFs that passed a requirement specified by the user.

5. Count and rank IDFs by failed requirements.

This query ranks the IDFs by the number of failed requirements. The number of failed requirements is displayed.

6. Count and rank IDFs by passed requirements.

This query ranks the IDFs by the number of passed requirements. The number of passed requirements is displayed.

7. Display IDFs with THV and controls.

This query displays IDFs with additional threats, hazards, and vulnerabilities and their recommended controls ordered by facility name.

8. Display all guidance documents for a specific requirement.

This query displays all guidance documents for a requirement specified by the user.

9. Display all IDFs with a specific THV ID.

This query displays all IDFs that contain a THV ID specified by the user.

10. Display requirement test results for a specific IDF.

This query displays all requirement test results for an IDF specified by the user.

11. Display negative requirement test results for a specific IDF.

This query displays all negative requirement test results for an IDF specified by the user.

12. Display positive requirement test results for a specific IDF.

This query displays all positive requirement test results for an IDF specified by the user.

13. Display all assessor information.

This query displays all assessor information.

14. Display the total number of IDFs that fail each requirement.

This query counts and displays the total number of IDFs passing each requirement, ordered by requirement.

15. Display the total number of IDFs that pass each requirement.

This query counts and displays the total number of IDFs passing each requirement, ordered by requirement.

16. Display IDFs that fail a specific control class.

This query displays all IDFs which have failed a requirement in the control class specified by the user.

APPENDIX E

Database Table Diagram

IDF							
ID	FacilityName	Room					
Number	Text	Text					
Required	Required	Required					
Unique IDF Number	Facility in which IDF is housed	Room where IDF is housed					
REQASSESSMENT							
IDF <small>fk to IDF.ID</small>	ReqNum <small>fk to REQUIREMENT.ID</small>	AssessNum	AssessDate	TeamNum <small>fk to TEAM.TeamID</small>	ReqResult		
Number	Number	Number	Text	Number	Text		
Required	Required	Required	Required	Required	Required		
Unique IDF Number	Requirement Number	Assessment Number	Assessment Date	Team Number	Requirement Test Result		
THVASSESSMENT							
IDF <small>fk to IDF.ID</small>	THV <small>fk to THV.ID</small>	Control <small>fk to Control.ID</small>	AssessNum	AssessDate	TeamNum <small>fk to TEAM.TeamID</small>		
Number	Number	Number	Number	Text	Number		
Required	Required	Required	Required	Required	Required		
Unique IDF Number	Unique THV Number	Unique Control Number	Assessment Number	Assessment Date	Team Number		
THV							
ID	Definition						
Number	Text						
Required	Required						
Unique THV Number	THV Definition						
CONTROL							
ID	Definition						
Number	Text						
Required	Required						
Unique Control Number	Control Definition						
REQUIREMENT							
ID	Definition	ControlClass					
Number	Text	Text					
Required	Required	Required					
Unique Requirement Number	Requirement Definition	Control Class					
TEAM							
TeamID	AssessorID <small>fk to ASSESSORS.AssessorID</small>	AssessmentNum					
Number	Number	Number					
Required	Required	Required					
Unique Team Number	Assessor ID	Assessment Number					
ASSESSORS							
AssessorID	HomePhone	CellPhone	EmailAddr	Given	Middle	Surname	Role
Number	Text	Text	Text	Text	Text	Text	Text
Required	Null Accepted	Null Accepted	Null Accepted	Required	Null Accepted	Required	Required
Unique Assessor Number	Home Phone Number	Cell Phone Number	Assessor Email Address	Given Name	Middle Name	Last Name	Assessor Role
TRACEABILITY							
ReqNumber <small>fk to REQUIREMENT.ID</small>	GuidNum <small>fk to GUIDANCE.ID</small>						
Number	Number						
Required	Required						
Requirement Number	Guidance Number						
GUIDANCE							
ID	Publisher	Document	RelevantSection	Authors	Year		
Number	Text	Text	Text	Text	Number		
Required	Required	Required	Null Accepted	Null Accepted	Required		
Unique Guidance Number	Guidance Publisher	Document Name	Relevant Section	Author Names	Year Published		

APPENDIX G

Requirement Data Summary

An overview of assessment results is described below. Results have been organized into the *control classes* found in the assessment tool then summarized.

The Entry Control *control classes* list requirements for IDF entry control systems. An entry control system is required to restrict IDF physical access to authorized personnel. Guidance documents show no preference for the specific entry control technology used; e.g., lock and key assemblies are not preferred over biometrics.

No entry control system is installed in several IDFs. These unprotected IDFs are located in a particular type of IDF. Two or more pieces of information or identification to gain entry are advised by NIST (2009) and ISO/IEC (2005). This control exists in IDF located at various locations.

The Entry Control Type *control classes* list requirements for specific hardware type information. ETSU IDFs use mechanical lock and key assemblies exclusively to restrict access. If multiple types of entry control hardware existed, these requirements would be used to inventory the quantities of each type.

The Transmission Media *control class* lists requirements for protecting, identifying, and installing communication wiring. Communication wiring susceptible to damage from electrical conduits without grommets, wall penetrations without sleeves, or ceiling grids without sleeves can be found at multiple IDFs. One IDF failed the requirement for separation of communication and power wiring. Its communication wiring was installed along long parallel incoming power feeds, increasing the possibility of electrical noise introduction through induction.

ISO/IEC (2005) recommends the identification and documentation of communication

cables to prevent misconnection. ETSU practice is to label switch ports and patch panels instead of cables. Because the ISO/TEC requirement explicitly states that the cabling shall be labeled, no IDFs passed the requirement for labeled cabling. However, a change in this requirement might be justified using risk assessment, then the requirement evolved to the ETSU practice of labeling ports instead of cables. All IDFs passed the requirement for locally available connection documentation because documentation of network connection information is provided online to network technicians.

No unauthorized devices were found connected to any IDF switches. ETSU disables unused ports to discourage the connection of unauthorized devices. This practice lessens the possibility that an intruder can interface with a port to gain network access undetected, as network access would require disconnecting an authorized connection.

The Access Monitoring *control class* lists requirements for distributing, observing, recording, and assessing IDF intrusion detection and entry control systems. Intrusion detection or entry control systems are not installed at multiple IDFs. Without intrusion detection, assessment requirements for alarm triggered video recording and camera assisted alarm assessment failed for multiple IDFs. Without entry control systems, the requirement for security personnel to monitor and log IDF entry through the use of electronic entry control systems failed in multiple instances.

The Power Supply *control class* lists requirements for installing, protecting and disconnecting IDF power supply circuits. ETSU power circuits are well protected from mechanical damage, with multiple IDF locations having power circuits susceptible to damage. Redundant power supplies were installed at multiple IDFs; of those, several had separated cable paths.

A remote means of power disconnection is recommended by NIST (2010) for emergency

use to allow authorized personnel to disconnect power remotely without requiring them to approach equipment, e.g., a service disconnect located near the IDF door. A power disconnection means of this type is installed at several locations.

The Emergency Lighting *control class* requirements mandate the automatic activation of IDF lighting to assist emergency egress. Lighting should also be designed to assist camera surveillance. These types of lighting are not found at multiple assessed IDFs.

The Fire Protection *control class* lists requirements for installing fire detection, suppression, and notification equipment. All ETSU fire protection systems are assumed to be monitored systems with automated emergency responder notification. Fire detection and suppression is installed at multiple IDFs. Fire detection is installed at multiple IDFs, while multiple IDFs have fire suppression installed. Fire extinguishers are installed at multiple IDFs.

The Environmental Protection *control class* lists requirements for installing, observing, and operating HVAC systems. Alarm systems are recommended to detect and signal the loss of utilities and systems that support an IDF. No sensors are installed in multiple IDF support systems or utilities. ETSU uses switches with temperature sensors to monitor the temperature at the IDF.

The HVAC systems installed at IDFs vary. Several IDFs lacked HVAC systems. Dedicated systems are found in multiple IDFs. Facility HVAC supplies provide temperature control at several IDFs.

Air conditioning equipment removes humidity from the air. Humidity may be added by installing separate humidification equipment. None of the systems at ETSU were observed to contain hardware capable of monitoring and maintaining a specified humidity. Thus the requirement to maintain and monitor equipment was failed by several IDFs without a

dehumidification system, devoted exclusively to humidity control.

The Flood Protection *control class* lists requirements for flood related controls. Control valves are specified for piping systems located near an IDF. Manual valves or automated valves to shut off adjacent water supply or plumbing were not found at several assessed IDFs. Ground floor installations are found at multiple IDFs. These ground-floor locations can be more susceptible to flood.

The Backup System *control class* lists requirements for electrical and HVAC backup systems. The required redundant or backup HVAC systems are found at several IDFs. Short-term backup systems for equipment shutdown are found at multiple IDFs. Long-term generator power supplies are provided at several IDFs. The separation of primary and backup equipment is recommended by Baker (2005) and Beshlin et al. (2003). A battery backup system may be found in close proximity to the supported IDF equipment at several IDFs.

The IDF Construction *control class* lists requirements for constructing, locating, and obfuscating the enclosure that houses the IDF. Several IDFs have incomplete or nonexistent structures for containing and isolating IDF equipment. Windows are present in multiple IDFs. Drop ceilings are present in some IDFs. Exterior wall installations, which can be susceptible to hazard or blast damage, are found at several IDFs. Extraneous equipment, piping, or systems unrelated to IDF operation are found in many IDFs. ISO/IEC (2005) recommends the obfuscation of equipment areas. Signage that could indicate an IDF's purpose exists at several locations.

The General Vulnerability *control class* contains a single requirement stipulating that no bulk supplies should be stored in the IDF. Only equipment and supplies related to network operation should be stored in equipment rooms. Such equipment and supplies were found at

several locations.

ISO/IEC (2005) recommends electrical surge and lightning protection to include electrical grounding of the building structure, surge suppression on incoming power, and surge suppression on communication cabling. The Surge Protection *control class* lists requirements for lightning protection and surge suppression. Grounded equipment racks bonded to the building grounding electrode exist at multiple installations. Surge suppression is applied to incoming power at multiple IDFs. The requirement for surge suppression to be used on communication cabling failed multiple times.

The Electronic Emanation *control class* contains a single requirement which stipulates that an IDF shall be protected from electronic eavesdropping by the use of shielding. The requirement for shielding failed multiple times.

APPENDIX H

THV Data Summary

Threats, hazards, and vulnerabilities not covered explicitly by the physical security requirements were found in several IDFs. These THVs range from IDF doors that were found to be propped open to light switches that were located on an opposite wall from the IDF entrance. THV is also detailed in the assessment database, ETSU Physical Security Database.accdb. All THV information may be accessed through the use of database Query 7. Controls have been recommended for each instance of THV.

APPENDIX I

Assessment Recommendations

The following recommendations for hardware and system assessment are based on the assessment recommendations found in the requirement guidance literature.

1. Perform a risk assessment. NIST (2009) and ISO/IEC 27002 (2005) promote the use of risk assessment to formalize and document control selection based on institutional need. Deviations from assessment requirements should be justified and commented. Controls for the THV presented by this assessment should be evaluated and deviation documented. Document any required supplementary controls and unneeded recommended controls in the risk assessment.
2. Prioritize and implement controls for failed requirements. Risk assessment should determine the required controls and implementation priorities.
3. Label unidentified rooms. Several IDFs had no room number. This lack of identification may impede location of the IDF by department personnel and emergency responders.
4. Use redundant power feeds effectively. Several IDFs have redundant power feeds that do not take advantage of the redundant feed.
5. Label power feed sources. Visual indication, e.g., signage or labels, that denote the supply circuit breaker on the receptacle or power strip, would clarify a feed's power source so that a redundant supply may be used effectively, or that a single supply may be known as such.
6. Do operational testing to prove the existence and operation of backup systems. Systems should be labeled appropriately with testing results.
7. Install humidity monitoring sensors. ETSU uses switches that monitor temperature but

not humidity. NIST and ISO/IEC recommendations advise that humidity and temperature be monitored and maintained within a range defined by the system owner.

8. Label backup system components. Because no operational testing was conducted in this assessment, the documentation and labeling of system elements increases in importance. Searching for proof that a system contains a backup system without operational testing requires investigation of the wiring and connected equipment. A system may be embellished with multiple backup systems, redundant power feeds, and remote utility disconnects. If these system elements are not labeled as such, they are not easily assessed or inventoried.
9. Install shunt trip hardware in locations where sprinklers could damage equipment or create a hazard for electrical shock. IDF sprinklers are typically located above network equipment. The installation of a shunt trip switch to disconnect network equipment from electrical supply power upon activation of the sprinkler system or remote signal will lessen the chance of electrical shock and equipment damage.
10. Tailor the requirements in this assessment to ETSU practices. The requirements used in this assessment were designed with no prior knowledge of ETSU hardware or practices. Document the reasons for deviation from established standards and practices.
11. Perform an assessment with the tailored requirements. Tailored assessment requirements should produce a more meaningful assessment.
12. Make assessment a continuous procedure. Incorporate assessment results into the next requirement evolution and assessment.

APPENDIX J

Discovered Threats, Hazards, and Vulnerabilities

ID	THV Definition
1	Equipment is visible through window.
2	No room number on door. This is potential impedance to emergency personnel.
3	No lighting installed in IDF.
4	Enclosure requires ladder for access.
5	A louver is installed in the door. There is concern that the louver could be used as entry. The louver also decreases HVAC efficiency.
6	This IDF is in a high traffic area.
7	A spigot is located on the sprinkler system in IDF.
8	IDF room has no ventilation and is therefore very warm.
9	Ongoing construction in adjacent area.
10	Inside unit is located directly above equipment rack. There is a concern that the condensate drain could block, causing condensate to build up and release onto equipment.
11	Drawing on Internet of building. This drawing shows a room labeled "Communic.".
12	Switch and network components are housed on wall in telecommunications room with no enclosure.
13	IDF is in a shared area.
14	This IDF is located inside of a restroom. Flooding is a possible hazard.
15	Light switch is located behind equipment rack opposite room entrance requiring walking through unlit room to activate switch.
16	The sprinkler is located above the rack gear.
17	No blinds on window. Sunlight entering the IDF through the window decreases HVAC efficiency and increases component visibility.
18	Plumbing located above equipment.
19	IDF Door propped open.
20	Redundant power systems are provided, but not used.
21	The IDF room is used as an HVAC plenum. The HVAC unit is located directly above the switching equipment rack. The filters will require changing, endangering switches and cabling.
22	A bushing is missing on a conduit in IDF. This could cause wear on wire jacket.
23	Lighting insufficient.
24	This switch is housed in a lockable rack enclosure in a room housing utilities serving the Minidome. Room exists for a separate room to house the IDF.
25	A map at the building stairwell identifies the IDF as room X-XXXCOMM. There is concern that this identification may betray its use as a communications room.
26	The designation for this room is X-XXXCOMM. There is concern that the "COMM"

ID	THV Definition
	designation may betray its use as a communication center.
27	This area provides roof access.
28	Visible signs of previous flooding.
29	There is a flood risk due to location.
30	A cover is missing from a communication wiring conduit outside of the IDF. Wire is exposed.
31	A ladder is required to access rack.

APPENDIX K

Recommended Controls for Threats, Hazards, and Vulnerabilities

ID	Recommended THV Control Definition
1	Cover window with blinds or otherwise obscure window.
2	Number Door.
3	Install lighting.
4	Install dedicated space and lower rack.
5	Cover louver or replace door.
6	Enclose IDF area.
7	Provide an appropriate outside drain on sprinkler system.
8	Increase AC supply or install dedicated system.
9	Advise contractors of OIT emergency contact information in case of emergency.
10	Place a pan under the inside unit evaporation coils to collect and deposit condensate to a drain. Alternatively, move inside unit to a different location.
11	Obscure drawing on Internet.
12	Segregate IDF in dedicated area.
13	Segregate IDF in dedicated area.
14	Relocate restroom entry door wall approximately 5 feet will relocate the IDF outside of the restroom and decrease the probability of flood hazard.
15	Relocate light switch closer to door.
16	Install a shunt trip switch to remove power upon sprinkler activation or flood.
17	Install blinds or cover window.
18	Install drip pan.
19	A supervisory entry control system could have alarmed on the door being held open. Install monitored entry control.
20	Install additional power strip to take advantage of redundant feed.
21	Relocate HVAC unit or move the filter housing to the outside of the IDF wall.
22	Replace bushing.
23	Install lighting.
24	Enclose IDF area.
25	Change room designation such that no indication of usage is given, e.g. X-XXXXA.
26	Change room designation such that no indication of usage is given, e.g. X-XXXXA.
27	Enclose IDF area.
28	Install drip pan.
29	Enclose IDF area.
30	Replace cover.
31	Move rack to a lower position in a dedicated space.

VITA

NATHAN TIMBS

Personal Data: Date of Birth: July 10, 1968

 Place of Birth: Elizabethton, Tennessee

 Marital Status: Married

Education: David Crockett High School, Jonesborough, Tennessee

 Honors

 B.S. Electronics Engineering Technology, East Tennessee State
 University, Johnson City, Tennessee, 1991

 M.S. Computer Science, East Tennessee State University, Johnson
 City, Tennessee, 2014

Professional Experience: Process Engineer, Tex-Tenn Corporation,
 Gray, Tennessee, 1993-2005

 Facilities Engineer, Superior Industries International,
 Johnson City, Tennessee, 2005-2006

 Manufacturing Engineer, A.O. Smith Corporation,
 Johnson City, Tennessee, 2006-Present

Honors and Awards: Upsilon Pi Epsilon International Honor Society for the Computing
 and Information Disciplines