

2018

Standardizing Instructional Definition and Content Supporting Information Security Compliance Requirements

Theresa Curran

Nova Southeastern University, idlewellbay@gmail.com

This document is a product of extensive research conducted at the Nova Southeastern University [College of Engineering and Computing](#). For more information on research and degree programs at the NSU College of Engineering and Computing, please click [here](#).

Follow this and additional works at: https://nsuworks.nova.edu/gscis_etd

 Part of the [Computer Sciences Commons](#)

Share Feedback About This Item

NSUWorks Citation

Theresa Curran. 2018. *Standardizing Instructional Definition and Content Supporting Information Security Compliance Requirements*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (1038) https://nsuworks.nova.edu/gscis_etd/1038.

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact nsuworks@nova.edu.

Standardizing Instructional Definition and Content
Supporting Information Security Compliance Requirements

by

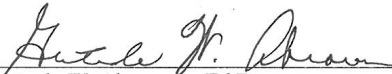
Terri (Theresa) Curran

A dissertation submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy
in
Information Systems

College of Engineering and Computing
Nova Southeastern University

2018

We hereby certify that this dissertation, submitted by Theresa Curran, conforms to acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.




Gertrude W. Abramson, Ed.D.
Chairperson of Dissertation Committee

05/16/2018
Date



Kim Round, Ph.D.
Dissertation Committee Member


5/14/18
Date



Maxine S. Cohen, Ph.D.
Dissertation Committee Member

5/16/2018
Date

Approved:



Yong X. Tao, Ph.D., P.E., FASME
Dean, College of Engineering and Computing

5/16/2018
Date

College of Engineering and Computing
Nova Southeastern University

An Abstract of a Dissertation Submitted to Nova Southeastern University
in Partial Fulfillment of the Requirements for the Degree of Doctor of Philosophy

Standardizing Instructional Definition and Content Supporting Information

Security Compliance Requirements

by
Terri (Theresa) Curran

2018

Information security (IS)-related risks affect global public and private organizations on a daily basis. These risks may be introduced through technical or human-based activities, and can include fraud, hacking, malware, insider abuse, physical loss, mobile device misconfiguration or unintended disclosure.

Numerous and diverse regulatory and contractual compliance requirements have been mandated to assist organizations proactively prevent these types of risks. Two constants are noted in these requirements. The first constant is requiring organizations to disseminate security policies addressing risk management through secure behavior. The second constant is communicating policies through IS awareness, training and education (ISATE) programs. Compliance requirements direct that these policies provide instruction about making compliant and positive security decisions to reduce risk. Policy-driven and organizationally-relevant ISATE content is understood to be foundational and critical to prevent security risk.

The problem identified for investigation is inconsistency of the terms *awareness*, *training* and *education* as found in security-related regulatory, contractual and policy compliance requirements. Organizations are mandated to manage a rapidly increasing portfolio of inconsistent ISATE compliance requirements generated from many sources. Since there is no one set of common guidance for compliance, organizations struggle to meet global, diverse and inconsistent compliance requirements. Inconsistent policy-related content and instructions, generated from differing sources, may cause incorrect security behavior that can present increased security risk. Traditionally, organizations were required to provide only internally-developed programs, with content left to business, regulatory/contractual, and cultural discretion. Updated compliance requirements now require organizations to disseminate externally-developed content in addition to internally-provided content. This real-world business requirement may cause compliance risks due to inconsistent instruction, guidance gaps and lack of organizational relevance.

The problem has been experienced by industry practitioners within the last five years due to increased regulatory and contractual compliance requirements. Prior studies have not yet identified specific impacts of multiple and differing compliance requirements on organizations. The need for organizational relevance in ISATE content has been explored in literature, but the amount of organizationally-relevant content has not been examined in balance of newer compliance mandates.

The goal of the research project was to develop a standard content definition and framework. Experienced practitioners responsible for ISATE content within their organizations participated in a survey to validate definitions, content, compliance and organizational relevance requirements imposed on their organizations. Fifty-five of 80 practitioners surveyed (68.75% participation rate) provided responses to one or more sections of the survey.

This research is believed to be the first to suggest a standardized content definition for ISATE program activities based on literature review, assessment of existing regulatory, contractual, standard and framework definitions and information obtained from specialized practitioner survey data. It is understood to be the first effort to align and synthesize cross-industry compliance requirements, security awareness topics and organizational relevance within information security awareness program content.

Findings validated that multiple and varied regulatory and contractual compliance requirements are imposed on organizations. A lower number of organizations were impacted by third party program requirements than was originally expected. Negative and positive impacts of third party compliance requirements were identified. Program titles and content definitions vary in respondent organizations and are documented in a variety of organizational methods. Respondents indicated high acceptance of a standard definition of awareness, less so for training and education. Organizationally-relevant program content is highly important and must contain traditional and contemporary topics.

Results are believed to be an original contribution to information/cyber security practitioners, with findings of interest to academic researchers, standards/framework bodies, auditing/risk management practitioners and learning/development specialists.

Acknowledgements

This work is dedicated to my husband John, who patiently and happily supported the integration of our lives with Nova Southeastern University during this effort. Research and homework became a daily occurrence in our house. Through it all, he was the best cheerleader, travel companion, sounding board, study coach and joke teller anyone could wish for. He's my rock and a rock star at getting us both through this long process.

My sister Maureen is a constant inspiration. We both have been immersed in our studies, and I am so proud she is finishing her master's degree in nursing at the same time I am completing this doctoral work. I know Dad is very proud of us both. I also know our dear friend and "big brother" Irwin Glazier is proud of us as well. Cheers!

Mike Corby and Tom Peltier have been my best friends, mentors and colleagues for as long as I can remember. They taught me how to approach our security work with passion, common sense, humor and empathy. I am grateful they took me along with them as they defined the information security industry as we know it today.

Dr. Peter Stephenson, a long-time friend and colleague, urged me to attend Nova Southeastern University and provided wonderful insight during my studies. I would be remiss in not thanking him and my American Public University System advisors, Dr. Steven McNally and Dr. Jeffrey Fowler, for their support.

The International Association of Information Security Awareness Professionals (IASAP) made completion of my research survey possible. Pam Salaway, also a long-time friend and colleague, introduced me to IASAP. Beth Beerman, Kathy Michael, IASAP leadership and members supported my research survey, the key success factor of this work. Thank you!

I was honored to initially work with Dr. Marlyn Littman as my dissertation committee chair. She was a gracious and thoughtful advisor, and on her retirement, provided a seamless and exciting transition to Dr. Gertrude Abramson. As my dissertation chair, Dr. Abramson has been inspirational, humorous and supportive; I enjoy her company and value her guidance. I could not have imagined two better committee chairs and have been so lucky to be selected to work with them. My committee members, Dr. Maxine Cohen and Dr. Kim Round, have been wonderful. I appreciate their wisdom and support.

This work is also respectfully dedicated to the memory of Fred Howell. Fred was a gentleman, educator, sportsman, community leader, practitioner, volunteer and mentor. He is truly missed by his friends and colleagues.

And finally, to all our global friends, family and colleagues that supported us, Johnny and I thank you all

Table of Contents

Abstract	iii
Acknowledgements	v
List of Tables	viii

Chapters

1. Introduction 1

Background	1
Problem Statement	4
Goal of the Study	7
Research Questions	7
Barriers and Issues	8
Acronyms	8
Definition of Terms	10
Summary	11

2. Review of the Literature 12

Overview	12
Security Risk Management	13
Contractual and Regulatory Compliance Mandates	14
Security Policies Supporting Risk Management	15
Communicating Security Policies	17
Nonstandard Frameworks and Inconsistent Definitions	19
Nonstandard Frameworks	19
Inconsistent Definitions	20
Organizational Relevance	21
Summary	23

3. Methodology 24

Overview	24
Research Questions	25
Research Design	25
GTM Approach	27
Preparation	28
Research Participant Selection	29
Instrumentation	31
Protection of Respondent Identity and Organizational Information	31
Survey Design	32
Survey Question Design	33
Data Collection, Storage and Analysis	34
Resources	36
Summary	36

4. Results	37
Overview	37
Data Collection and Analysis	38
Survey Response Analysis	38
Section 1, Questions 1.1 and 1.2: Regulatory and Contractual Requirements	39
Section 2, Questions 2.1–2.7: Impacts of Third Party Compliance Requirements	40
Section 3, Questions 3.1 – 3.5: Definitions Used and Program Documentation	43
Section 4, Questions 4.1–4.5: Organizational Relevance /Definition Acceptance	46
Section 5, Questions 5.1–5.12: Demographic and Security Program Questions	48
Summary of Results	50
5. Conclusions, Implications, Recommendations and Summary	52
Research Problem Answered	52
Research Questions Answered	52
Benchmarking Results	57
Standard Content Definition Framework (SCDF) Recommendations	59
Pre-Planning for SCDF Deployment	60
Future Research Considerations	64
Strengths and Weaknesses	66
Limitations	67
Conclusions	68
Implications	72
Recommendations	72
Summary	73
Background	73
Problem Statement and Research Questions	74
Review of the Literature	75
Methodology	77
Research Participation Selection	78
Data Collection, Storage and Analysis	78
Research Conclusions	79
Appendices	81
A: Regulatory and Contractual ISATE Requirement Examples	81
B: Regulatory and Contractual Language Examples	82
C: IS Standards, Guidelines and Frameworks	84
D: IRB Approval 2017-308: Proceed with Study	85
E: IRB Letter to IASAP	86
F: Survey Questions, Detailed Responses and Analysis	88
References	113

List of Tables

1. Qualitative Research Characteristic and Research Application 26
2. Perceived Impact of Third Party Requirements 41

Chapter 1

Introduction

Background

Information security (IS) risks affect global organizations on a daily basis as a result of insecure global, interactive electronic connectivity among public and private organizations (Biener, Eling & Wirfs, 2015). Security risks are introduced through technical, physical or human-based activities and have increased significantly due to availability and exploitation of web-based applications, mobile devices, cloud-based computing, social media and Internet of Things (IoT)-connected devices (Safa et al., 2015).

Types of risks include fraud, hacking, malware, insider abuse, physical loss, human error, mobile device misconfiguration or unintended disclosure. Risks, once fully realized, can result in data security breaches (Ponemon, 2016). Data security breaches affect personal health or financial information, information availability, trade secrets, financial confidentiality or intellectual property (IP) (Romanosky, 2016). Security risks resulting in breaches have increased over time (Ponemon, 2016; Sen & Borle, 2015) and are projected to remain an ongoing threat to individuals and organizations (Edwards, Hofmeyr & Forrest, 2015).

In response to these risks and threats, layers of regulatory and contractual compliance mandates have emerged. Governments have imposed new regulations and business partners increasingly include specific contract language requiring responsible security practices (Haeussinger & Kranz, 2017). Organizations must understand not only how to

protect information but also how to comply with regulations and contracts to demonstrate regulatory and contractual compliance (Dunlap, Cummings & Janicki, 2017).

From a *regulatory* perspective, global governments and industries have mandated compliance requirements intended to help organizations proactively manage risk and prevent breaches (Kam, Katerattanakul & Gogolin, 2013; Fagade & Tryfonas, 2017). Examples of regulatory and contractual ISATE requirements are contained in Appendix A. Non-compliance may result in monetary fines, negative publicity, brand reputation impact and possible business stoppage (Chaudhry et al., 2013). A sampling of overarching United States (US) Federal requirements that may affect organizations based on business conducted includes the US Cybersecurity Framework (The White House, 2014) and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 (NIST, 2014). In a more granular example, US interstate bulk electricity transmission providers are required to adhere to North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) reliability standards (Collinson, Massacci, Ruprai & Williams, 2016) having specific inclusion of awareness, training, risk assessment and access control program requirements (NERC, 2018).

At least nineteen US states have enacted data privacy and breach notification laws that require a statewide and comprehensive approach to security and security oversight (NCSL, 2018). Over 170 new cybersecurity laws were introduced by 37 state legislatures in 2015-2016. While many state laws do not receive final approval, organizations must track legislative compliance requirements and assess organizational relevance and impact (Dunlap, Cummings & Janicki, 2017).

Adding *contractual* complexity, organizations may also be required to comply with

industry-specific compliance requirements. A well-known example is the Payment Card Industry Data Security Standard (PCI DSS), applicable to organizations that manage, issue, process or access credit card information (PCI DSS, 2014). Critical infrastructure (CI) mandates such as NERC CIP reliability standards (Collinson, Massacci, Ruprai & Williams, 2016) also present both contractual and regulatory considerations.

Regular, formal and measured contractual compliance reporting may be required within an organization's value chain. Value chains are relationships among businesses, vendors, contractors or local, state and Federal government agencies. Organizations may be uninformed and at risk because of insecure activities of others in their value chain (Patnayakuni & Patnayakuni, 2014). For example, provisions of the US Consumer Protection Finance Board (CFPB) mandate financial institutions (FIs) to reduce or eliminate risk through contractual interrelationships among FIs and others in their value chain (FFIEC, 2014). Similar examples of third party risk management mandates appear in PCI DSS (PCI DSS, 2014), the National Association of Insurance Commissioners (NAIC) Principles for Effective Cybersecurity (NAIC, 2015) and the Cruise Line Industry Association (CLIA) Cybersecurity Guidelines (CLIA, 2016).

Security-related compliance requirements vary in length, detail, scope, direction, guidance, consistency and language (Yimam & Fernandez, 2016). New, updated or differing regulations and requirements enlarge effort of achieving and maintaining internal and external regulatory and contractual compliance (Thalmann et. al., 2012). Little research has been done to assess organizational impact of new, imprecise and variable security compliance requirements. Regulated organizations are confused about measuring compliance (Bamberger & Mulligan, 2011).

Two constants are noted in all regulatory and contractual compliance requirements. The first is creation and dissemination of security policies that provide instruction and management expectations about how to make good security decisions. The second is communication of security policies through IS awareness, training and education (ISATE) content. The importance of ISATE content for compliant and positive security behavior has been established in literature, but there is no one agreement academically about the design, deployment and effectiveness measurement of content within programs (Bauer, Bernroider & Chudzikowski, 2017).

This research is believed to be the first to identify a standardized content definition for ISATE program activities based on literature review, assessment of existing regulatory, contractual, standard and framework definitions and information obtained from specialized practitioner survey data. It is understood to be the first effort to align and synthesize cross-industry compliance requirements, topics for delivery and organizational relevance within information security awareness program content.

Problem Statement

The problem identified for investigation was lack of standard ISATE program content definitions supporting internal organizational relevance and external compliance mandates. There are real-world business reasons to consider this problem. Security risks and resultant breaches affect personal health or financial information, trade secrets or intellectual property (IP) and are increasing globally (Ponemon, 2016; Sen & Borle, 2015).

In response to security breaches, varied and diverse US information security regulations have been enacted. Public and private organizations are faced with

inconsistent compliance requirements because of these differing regulations (Cunningham, 2016; Kam, Katerattanakul & Gogolin, 2013). US compliance requirements have been generally created or legislated in reaction to a specific crime or breach, resulting in siloed and non-systemic approaches to compliance. As a result, a patchwork of Federal, state, local and third party IS compliance requirements exist. These requirements are non-systemic in approach and methodology (Chaudhry et al., 2013; Duncan & Whittington, 2014; Johnson, Lincke, Imhof & Lim, 2014). In an attempt to manage this patchwork, academic, commercial and practitioner frameworks applicable to regulatory and contractual requirements have been identified (Atoum, Otoom & Ali, 2014; Nicho & Muamaar, 2016).

Within frameworks and regulatory/contractual compliance regulations, there is acknowledgement that an individual's security behavior, combined with technical and physical controls, can help manage security risk and breaches in organizations (Safa, Von Solms & Furnell, 2016). Appropriate security behavior may be accomplished through ISATE program efforts as part of an effective security risk management program that is developed, delivered, tracked and measured (Karjalainen & Siponen, 2011). ISATE programs must be deployed to increase organizational security policy compliance, improve decision-making behaviors, increase efficiency and reduce security risk (Rocha Flores, Antonsen & Ekstedt, 2014).

Policies promote effective IS security behaviors by providing holistic, consistent, clear and relevant instruction to reduce risk. This instruction helps individuals reflect on policy, consider how to respond to a situation and take risk-based, informed and appropriate actions. Inconsistent policy-related content and instructions, generated from

differing sources, may cause inappropriate security behavior that can increase security risk.

Organizations are compelled to provide program content without standard definitions and organizationally-relevant content. Prior studies have not identified standard definitions of ISATE activities - the terms awareness, training and education are used interchangeably. Varied definitions used within compliance requirements add complexity to achieving and maintaining compliance. Appendix B contains a sampling of prevalent – and differing - definitions and requirements. Lack of standardized ISATE definitions may prevent organizational ability to meet compliance requirements – and perhaps more importantly – increase security risk through inappropriate security behaviors.

Addressing this research problem is believed to be practical and useful to security practitioners because it focused on a newly identified issue within organizations (Terrell, 2012). The research problem was identified by the author as observed in a real-world business situation. Literature did not reveal suitable approach to resolving this problem.

Results are believed to be an original contribution to information/cyber security practitioners, with findings of interest to academic researchers, standards/framework bodies, auditing/risk management practitioners and learning/development specialists. The resulting standardized content delivery framework is detailed in design but simple in execution and may be effectively used by virtually any organization to standardize and measure program success.

Goal of the Study

The goal was to develop a standard content definition framework for organizations to use while managing IS risk management and compliance efforts. Two primary activities were conducted:

- A research survey obtained information about current state of organizational programs, content, frameworks, importance of organizational relevance and compliance mandates affecting organizations. This was done through analysis of electronic survey response data as provided by a group of ISATE practitioners responsible for content delivery in their organizations.
- A standard content definition framework was developed to support regulatory and contractual requirements balanced with need for organizational relevance.

Understanding ISATE component definitions, content, organizational relevance and compliance requirements in use at US-based organizations provided insight as to the validity of the research problem. This framework may be used by virtually any organization that wishes to standardize and leverage efforts to meet internal and external compliance requirements to reduce risk.

Research Questions

Research questions evolved as the problem was examined and generated supporting survey questions.

- RQ1: What US-based regulatory and contractual requirements impose internal and external ISATE program delivery?
- RQ2: What are the impacts of external (third party) requirements on current ISATE programs?
- RQ3: What ISATE program definitions are currently used?
- RQ4: Is organizationally-relevant ISATE program content important?
- RQ5: Will organizations accept standard definitions of awareness, training and education?

Research questions were informed through data collection via an electronic survey issued to practitioners responsible for ISATE activities within their organizations.

Barriers and Issues

This research problem was acknowledged as a business issue before formal acceptance as a research problem. Chief or Corporate Information Security Officers (CISOs), practitioners, vendors, analyst groups and industry experts were asked if they could identify impact of inconsistent content definition. An original concern was possible introduction of new US-based compliance and regulatory requirements as a liability; this in fact caused the opposite effect, as while newer requirements were identified, more definition diversity and differences emerged.

An additional concern was that ISATE vendors would recognize the problem and act on it from a commercial perspective, negating research originality. Interestingly, vendors have not approached this idea commercially, but standards bodies have indeed recognized need to address this issue from a governance perspective. An American Society for Industrial Security (ASIS), International Information Systems Security Certification Consortium (ISC²) and Information Systems and Control Association (ISACA) joint working group was established in 2016 to draft and issue a new global Security Awareness Standard (ASIS, 2016).

Finally, there was concern that industry practitioners would decline to share what was perceived as confidential or sensitive organizational information during data collection. This was alleviated when a leading ISATE professional group agreed to support and participate in an electronic data collection survey.

Acronyms

ACM	Association of Computing Machinery
ANSI	American National Standards Institute
ASIS	American Society for Industrial Security
CAEIAE	Center of Academic Excellence, Information Assurance Education

CFPB	Consumer Financial Protection Bureau
CI	Critical infrastructure
CISO	Chief or Corporate Information Security Officer
CISSP	Certified Information Systems Security Professional
CLIA	Cruise Lines Industry Association
COBIT	Control Objectives for Information and Related Technology
CSI	Computer Security Institute
CSV	Comma separated value (CSV) file format
DHS	Department of Homeland Security
EU GDPR	European Union General Data Protection Regulation (2016 on)
FCRA	Fair Credit Reporting Act
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FI	Financial institution
FISMA	Federal Information Security Management Act
FRB	Board of Governors of the Federal Reserve System, commonly known as the Federal Reserve Board
GLBA	Gramm-Leach-Bliley Act (Financial Services Modernization Act of 1999)
GTM	Grounded Theory Method
HR	Human resources
HTTPS	Hypertext Transport Protocol Secure
IA	Internal audit
IDS	Intrusion detection system(s)
IEEE	Institute of Electrical and Electronics Engineers
IoT	Internet of Things
IASAP	International Association of Security Awareness Professionals
IP	Intellectual property
IRB	Nova Southeastern University Institutional Review Board
IS	Information security
ISACA	Information Systems and Control Association
ISATE	Information security education, training and awareness
ISC ²	International Information Systems Security Certification Consortium
IT	Information technology
ISMS	Information Security Management Systems
ISO/IEC	International Organization for Standardization/International Electrotechnical Commission
NAIC	National Association of Insurance Commissioners
NCSL	National Conference of State Legislatures
NERC CIP	North American Electric Reliability Corporation Critical Infrastructure Protection
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NSU	Nova Southeastern University
OCC	Office of the Comptroller of the Currency

PCI DSS	Payment Card Industry Data Security Standard
PCI SSC	Payment Card Industry Security Standards Council
PDF	Portable Document Format (PDF) file format
PII	Personally identifiable information
PMT	Protection Motivation Theory
RCT	Rational Choice Theory
SCDF	Standard Content Definition Framework
SOX	Sarbanes-Oxley Act of 2002
TPB	Theory of Planned Behavior
URL	Uniform Resource Locator (internet term)
US	United States

Definition of Terms

Encryption	A process or algorithm to make information hidden or secret. By transforming or converting data into a random, meaningless and unintelligible form (Mathur, 2012).
Firewall	A component connected at the border of two or more networks that inspects communications to prevent attacks against applications, networks or other computing service (Cropper et al., 2015).
Malware	Short for <i>malicious software</i> , this is used synonymously with <i>virus</i> . It infiltrates, damages or obtains information from a computer system without the owner's consent or knowledge (Mujumdar, Masiwal & Meshram, 2013).
Mobile devices	May include smart phones, tablets, wristwatches, glasses, universal serial bus (USB) or "thumb" drives and other forms of wearable computing (Mayrhofer, 2015).
Organizational relevance	Perception of what is - or is not - important to a company when protecting against security risk. Every organization has different perspectives and definitions of security risk (Banfield, 2016).
Phishing	A targeted attempt to obtain personal information (username, password, credit card details) by posing as a friendly company or person in an email or through a web browser on order to facilitate identity theft (Arachchilage, Love & Beznosov, 2016).
Security culture	Ways individuals behave with administrative, technical and physical security controls that protect information (da Veiga & Martins, 2015).
Security framework	A formal, controls-based, defined approach to protect organizations and individuals from security risks. NIST 800-53 is an example (Guarino, 2015).
Social media	Online platforms (including, but not limited to, Facebook and Twitter) that provide online discussions to promote a personal or corporate product, idea or brand (Dijkmans, Kerkhof & Beukeboom, 2015).
Spam	Unsolicited email containing malicious attachments sent to a large number of email addresses (Matejka, 2016).

Training	Improving secure behavior through courses, workshops, formal presentations, or online content (Safa, Von Solms & Furnell, 2016). Awareness and education definitions are often used interchangeably with training – hence the origination of the research problem.
Value chain	Relationships among businesses, vendors, contractors or local, state and Federal government agencies (Patnayakuni & Patnayakuni, 2014).

Summary

Chapter 1 has presented research problem background, problem statement, research questions and supporting information used during the course of the research project.

Chapter 2 will document literature review of prior research. Chapter 3 focuses on methodology selected to investigate the research problem. Chapter 4 discusses findings and Chapter 5 presents findings and implications for practitioner and academic communities.

Chapter 2

Review of the Literature

Overview

Literature review was conducted to validate or refute if the research problem had been studied in prior academic work. Daily keyword searches were applied to Google Scholar (<https://scholar.google.com/>); on average, 50 journal articles or other publications were identified for review per daily search. Keyword searches evolved over time, but generally focused on topics including “user reaction to security regulations”, “IS compliance requirements”, “awareness policy”, “security culture”, “third party IS risk management”, “security learning”, “security behavior”, “compliance attitude”, “standard IS definitions” or other similar description. Once potential keywords were identified, publication databases including (but not limited to) Association of Computing Machinery (ACM), Science Direct, ProQuest, Elsevier and Institute of Electrical and Electronics Engineers (IEEE) were accessed to obtain documents for review.

Prior literature was observed to examine several policy and behavior-related areas very closely: compliance with policy, ignoring risk due to workload or inconvenience, social/peer influence, resistance to technical controls and perceived incentives/penalties (Bulgurcu, Cavusoglu & Benbasat, 2010). Behavioral theories were examined as pertaining to ISATE programs, including theory of planned behavior (TPB), rational choice theory (RCT) and protection motivation theory (PMT) (Bulgurcu, Cavusoglu & Benbasat, 2010; Safa et al., 2015). These topics provided rich context, but identification of the research problem in literature remained elusive.

Literature search was refined to focus on the following areas to support the problem

statement.

- Security Risk Management
- Contractual and Regulatory Compliance Requirements
- Security Policies Supporting Risk Management
- Communicating Security Culture and Policies
- Nonstandard Frameworks and Inconsistent Definitions
- Organizational Relevance

The order of presentation is intended to illustrate a cascade of information that helped define and inform RQs and subsequent data collection activities.

Security Risk Management

Information loss is a significant risk to organizations of all types and sizes. Public and private organizations must consistently and iteratively identify, assess, and manage risk to information assets through security programs and policies (NIST, 2014). Organizations are increasingly required to implement technical, physical and administrative/behavioral controls intended to effectively delay or deter malicious activities against electronic and physical information (DHS, 2014). Technical risks may be prevented through anti-malware suites, spam/phishing detection and blocking, application and network firewalls, role-based authentication and intrusion detection systems (IDS) (Safa, Von Solms & Furnell, 2016). Physical risks may be managed through facility access restrictions, limiting access to physical/hardcopy information, or identifying hardware-based threats such as counterfeit parts in information technology (IT) systems that may divert information or disrupt system, network or information availability (DiMase et al., 2015).

Administrative, human-based behavioral controls must be implemented by organizations to manage security risk. These controls optimally include requirements to comply with policies and participate in awareness activities. Security risk is understood to decrease when employees and/or third parties make appropriate decisions based on

behavioral guidance and instruction (Safa, Von Solms & Furnell, 2016).

Contractual and Regulatory Compliance Requirements

ISATE programs are mandated by a bewildering array of external compliance requirements. Organizational programs should reflect applicable security regulations organizations take to mitigate internal risk (Herold, 2010).

From a regulatory compliance perspective, ISATE programs are mandated based on services provided by an organization (DHS, 2014). Little research has been done to assess organizational impact of new regulatory requirements. Regulatory rules are imprecise and variable. Regulated organizations are confused about measuring security program compliance (Bamberger & Mulligan, 2011). Imposed regulatory requirements can be costly and ineffective (Miller, 2014). Compliance with laws and regulations mandate standardized security program efforts to avoid potential agency and/or legal consequences (Narain Singh, Gupta & Ojha, 2014). Hu, Hart and Cooke (2007) posed that employees react more positively to ISATE programs based on regulatory requirement than those based on external standards such as ISO 27002.

ISATE programs are mandated and examined through third party contractual requirements as well. For example, the Payment Card Industry Data Security Standard (PCI DSS) mandates annual formal security awareness efforts within organizations that manage, issue, process or access credit card information (PCI DSS, 2014). Contractual agreements with an organization's value chain may contain compliance requirements that may require third parties to comply with external policies, procedures and processes (Killingsworth, 2014). Contractual agreements among organizations and third parties

may include ambiguous or differing mandates for awareness, training or other education requirements (Patnayakuni & Patnayakuni, 2014).

Security Policies Supporting Risk Management

An information security policy is a formal document that executive management uses to communicate guidance and direction to individuals. Policy content may include acceptable use of organizational information and systems, ethical system use, social media use, role-based roles and responsibilities, and risks of policy noncompliance (Ahmad et al., 2016; Ifinedo, 2017).

Implementing security policies is a core recommendation of many guidelines and standards as illustrated in Appendix C. Security practitioners face three challenges when considering policy implementation. The first is interpreting varied and diverse standards, guidelines, organizational requirements and best practices into an organizational policy framework. The second challenge is aligning regulatory and contractual compliance requirements with the established framework (Niemimaa & Niemimaa, 2017). The third challenge is promoting these policies so individuals can reduce risk by being engaged, informed and compliant (Haeussinger & Kranz, 2017).

Information security policies identify standards, boundaries, and responsibilities that individuals must observe in order to prevent risk. Policies influence individual risk awareness and organizational security culture (Cram, D'Arcy & Proudfoot, 2017) as well as provide formal strategic, tactical guidance and instruction (Ahmad, et al., 2016).

Policies articulate and direct an individual's security behavior, compliance decisions and risk management actions. These policies should be aligned with organizational objectives, be easily understood and reasonable to comply with. Policies should be

communicated so that intended informational and instructional content is delivered effectively (Alkhurayyif & Weir, 2017).

The credibility of an organization's security program depends on well drafted security policies (Chaudhry et al., 2013). Organizational security policies are the primary source of compliance-related information and are deployed to provide instruction and guidelines (Cavallari, 2012). Policies document security-related actions and their consequences, both positive and negative. Policies establish a foundation by which public and private organizations ensure individual compliance to regulatory and contractual requirements (Al-Khalifa, Kohun & Skovira, 2015). Since security risk must be managed through technical, administrative, and physical controls, policies informing employees and third parties about these controls must be disseminated (D'Arcy & Herath, 2011). However, when policies are complex, individuals are unable to understand the reason behind the compliance policy, and as a result, non-compliance can occur (Cavallari, 2012). Policies provide uniformity, increase understanding, and improve management of regulatory or contractual requirements (Al-Ahmad & Mohammad, 2012).

Given numerous security contractual and regulatory requirements imposed on organizations, research about compliance with organizational security policy is necessary and highly desirable (Warkentin, Johnston & Shropshire, 2011). Security policies inform individuals why risk management is essential, while security policy communication guides individuals about policy compliance. Therefore, policy communication is as important as the policy itself (Soomro, Shah & Ahmed, 2016).

Policies must be current, easily accessible, relevant, meaningful and written in clear and understandable language. Literature highlights the importance of establishing policies

first, then promoting them as the fundamental and essential basis of an effective organizational awareness, training and education program (Haeussinger & Kranz, 2017).

Communicating Security Culture and Policies

Literature indicates that an individual's compliance with information security policies is highly influenced by organizational culture, which in turn cultivates security culture, or how individuals behave with administrative, technical and physical security controls that protect information (da Veiga & Martins, 2015). Information security policy communication is critical to establishing security culture (da Veiga, 2016). Security culture must be organizationally demonstrated to guide employee and third party behavior to reduce risk (da Veiga & Martins, 2017). Risk may be reduced through a culture that promotes information protection as a daily job function (Santos-Olmo et al., 2016). Security culture is communicated in many forms but is prevalently presented through security policies.

Communication about security policy compliance is generally accomplished through content delivered in organized programs that can take many forms and provide necessary knowledge to comply with security policies (D'Arcy, Hovav & Galletta, 2009). From a regulatory and compliance perspective, policies can help communicate importance of regulatory requirements so individual performance is based on updated security beliefs and practices (Walker, 2014).

Organizational security policies must include cross-cultural considerations; understanding insider threat as well as external influences; developing and maintaining security culture; and obtaining management leadership and support of security program efforts (Crossler et al., 2013).

Prior studies strongly indicate that effective training is the most common policy compliance approach. Relevant behavioral training design would help improve security policy compliance through alignment with adult learning principles, showing relevance to a learner's role or information types used and holding an adult learner's attention (Offor & Tejay, 2014). The importance of researching policy compliance is understood by scholars and practitioners but is underdeveloped from a research perspective. There are limited academic studies to choose from (Karjalainen & Siponen, 2011).

Policies should define consistent and meaningful terminology and provide meaningful and applicable content. Program messaging should be clear and persuasive in order to mobilize recipients about making appropriate security decisions to prevent risk (McDaniel, 2013).

Cram, D'Arcy and Proudfoot (2017) studied security policy literature and identified five frequently examined areas:

- design and implementation of policies;
- influence of security policies on organizational security culture and individuals;
- influence of organizational and individual factors on policy compliance (personality, sanctions, rewards);
- influence of policy compliance on risk management objectives; and
- adjustments to policy design (e.g., policy updating and maintenance) (Cram, D'Arcy & Proudfoot, 2017).

Examination of policy-related literature revealed that while need for clear and actionable policies is evident, policy standardization terms specific to awareness, training and education are not as clearly defined.

Nonstandard Frameworks and Inconsistent Definitions

Nonstandard Frameworks

Organizations do not have standard frameworks and/or standards by which to create or acquire IS training content, delivery or measurement. All organizations, large and small, face a changing landscape of IS standards (Caldwell, 2013). Organizations do not have specific guidance or direction from regulators, frameworks or standards by which to create or acquire ISATE content, delivery or measurement. Many security guidelines are generic and do not take risk, geographic or organizational cultural factors into consideration (Rocha Flores, Antonsen & Ekstedt, 2014).

ISO/IEC (International Organization for Standardization and International Electrotechnical Commission) 27001 is the international standard establishing best practices for Information Security Management Systems (ISMS). It is used to establish foundational security controls to protect information confidentiality, integrity and availability. It illustrates a generic risk management approach applicable to many organizations (Fagade & Tryfonas, 2017). ISO/IEC 27002 is more granular than 27001 and is often used as a program content guideline within diverse organizations (ISO, 2013; Periera & Santos, 2014). The 2013 version of the guideline, Information technology – Security techniques – Code of practice for information security controls establishes 133 generic administrative, physical, and technical controls in the areas of:

- Security Awareness Program
- Organization of Information Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications, Operations and Network Management
- Access Control

- Information Systems Acquisition, Development and Maintenance
- Information Security Incident Management
- Business Continuity (ISO, 2013)

External regulatory and contractual requirements mandate delivery of multiple security training programs to employees and third parties. Contractual and regulatory compliance requirements have baseline similarities (Mohammed, 2015) but no specific context for ISATE training content or delivery exists in US federal and state legislation (Chaudhry et al., 2013).

There are no commonly agreed to or understood standard measurements or guidance for organizational ISATE activities (Gundu & Flowerday, 2013). Common guidelines, best practices and standards exist to help organizations establish programs; however, these are largely conceptual, generic and do not include discussion of organizational relevance in content (Alshaikh et al., 2018).

Inconsistent Definitions

ISATE may be thought of as systemic acquisition of knowledge, skills and attitudes that together lead to improved performance in a particular environment (Salas & Lazzara, 2014). Wide differences of opinion on standard definitions of ISATE exist (Tsohou, Kokolakis, Karyda & Kiountouzis, 2008).

Rocha Flores, Antonsen & Ekstedt (2014) suggested that awareness-level activities are primarily simple activities designed to attract attention to a given subject. Target audiences are mostly passive recipients of information and the knowledge gained is short-term, immediate and specific. Another definition indicates IS awareness activities help people recognize threats and inform them of organizational sanctions as defined in IS policies (Cavusoglu et al., 2015). Jaeger (2018) defines awareness outcomes as

cognitive, process-related or behavioral. While this definition is helpful in designing measurable program deliverables, it illustrates outcomes of an awareness effort, not an actual framework for creating program content; this definition does not address awareness, training and education as separate and distinct learning activities.

From a training perspective, the primary goal is to increase organizational knowledge to support decision-making, improve efficiency, reduce training cost, and reduce risks (Rocha Flores, Antonsen & Ekstedt, 2014). Standard training is desirable in order to provide uniformity, ease overall understanding, and improve management of regulatory or contractual requirements (Al-Ahmad & Mohammad, 2012). IS training provides information protection skills (Cavusoglu et al., 2015).

Education efforts primarily focus on providing role-based, specialized analytical skills to help minimize security risk. For example, system and network penetration skills and tools needed by practitioners to identify sophisticated attacks are obtained through specialized education programs such as those conducted at Nova Southeastern University (NSU) through its designation as a National Security Agency (NSA) and Department of Homeland Security (DHS) Center of Academic Excellence in Information Assurance Education (CAEIAE) (Li, 2015; NSU, 2016).

There are no commonly agreed to or understood standard measurements or guidance for organizational ISATE activities (Gundu & Flowerday, 2013). Literature review validated that development of a standard content definition framework would be of academic and practitioner interest.

Organizational Relevance

Every organization has different perspectives and definitions of security risk and

solutions to mitigate risk (Banfield, 2016). Externally-mandated policies (and by inference, awareness and training about these imposed policies) may not engage management or individuals from the organization being urged to participate in external content. The involvement of relevant stakeholders in the content development process is a success factor for effective security policy and subsequent ISATE programs (Ahmad, et al., 2016).

ISATE programs communicate policy-based direction to individuals about personal behavior in preventing organizational security risks. Strong understanding and perception of organizational risk may help reduce noncompliance to IS policies (Ifinedo, 2016). Program content should be communicated in a timely manner with consistent messaging and with organizational relevance (Safa, Von Solms & Furnell, 2016). Literature has examined compliance-related program topics, but little mention is made of considering relevant, business-related content delivered to individuals to support business goals (Faily & Ki-Aries, 2017).

Flexibility and organizational relevance of ISATE content should be allowed to provide most optimal impact to participants (Karjalainen & Siponen, 2011). Program content should be designed to address organizational context, desired behaviors and role-based relevance to influence security behavior (Faily & Ki-Aries, 2017). Specific internal organizational social norms and attitudes must be communicated as part of ISATE programs (Bauer & Bernroider, 2017).

Organizational relevance is briefly mentioned in compliance requirements. PCI SSC states “The key to an effective security awareness program is in targeting the delivery of relevant material to the appropriate audience in a timely and efficient manner” (PCI SSC,

2014). The FFIEC requires that companies “Determine whether management adjusts the information security program for institutional changes and changes in legislation, regulation, regulatory policy, guidance, and industry practices” (FFIEC, 2016, p. 61). As with the problem of inconsistent ISATE terms and definitions, organizational/institutional relevance definition is observed to be inconsistent in reviewed literature. Since there is high emphasis and direction to focus program content on contractual and regulatory compliance topics, organizational relevance within content may potentially be reduced or eliminated.

Summary

Chapter 2 provides literature-based context to refute or validate the research problem. Literature review was conducted to examine lack of standard frameworks and definitions and need for organizational relevance for content. Prior studies have acknowledged need for personal connectivity with security instruction. Chapter 3 will present the methodology selected to investigate the research problem.

Chapter 3

Methodology

Overview

The research problem was based in a real-world business condition felt to be new and not previously studied. Qualitative research defined orderly answers to research questions (RQs) posed in an online survey tool to experienced practitioners. These questions elicited information about current regulatory and contractual requirements, external (third party) impacts, content definitions, organizational relevance, willingness to accept standard content definition framework and program demographics. The qualitative assessment of practitioner responses provided understanding of details and conditions that enabled knowledge development (Corbin & Strauss, 2008).

Survey participants were carefully considered and selected based on ability to provide detailed and expert input to the qualitative inquiry and research design process. By using an online survey tool, data were collected in a way familiar to respondents and in its final delivery presented information in language understood by practitioners (Creswell, 2013).

Granular literature review identified grounded theory methodology (GTM) as the appropriate qualitative research approach because of its treatment of process and context when assessing new organizational issues and research problems (Urquhart & Fernández, 2013). GTM-based analysis of qualitative data provided foundational basis for the standard content definition framework (Corbin & Strauss, 2008). GTM as a research methodology is frequently accepted by information systems/information security researchers (Lawrence & Tar, 2013; Urquhart & Fernández, 2013).

The International Association of Information Security Awareness Professionals (IASAP) participated in the survey during for one month. Results identified the perceived usefulness and applicability of standard ISATE program definitions and content to support internal organizational relevance and external compliance mandates. It is believed that results will be valuable to IASAP members, global practitioners and influence future research into ISATE program success factors.

Research Questions

The following RQs were the basis of survey design and deployment. These questions are believed to be unique; similar questions were not observed in literature.

- RQ1: What US-based regulatory and contractual requirements impose internal and external ISATE program delivery?
- RQ2: What are the impacts of external (third party) requirements on current ISATE programs?
- RQ3: What ISATE program definitions are currently used?
- RQ4: Is organizationally-relevant ISATE program content important?
- RQ5: Will organizations accept standard definitions of awareness, training and education?

Additional information was obtained in Section 5 of the survey about organizational business demographics. Research findings were interpreted and a standard content definition framework to meet multiple compliance requirements was developed in practitioner language.

Research Design

Qualitative research was chosen to obtain reflective insight and perspectives of people familiar with the research questions to be answered. Experience, familiarity and social context were needed to provide detail and context about awareness and training, compliance and organizational relevance (George & Gao, 2014). Qualitative research,

especially when conducted with expert practitioners, is appropriate when insufficient information exists about a problem to perform quantitative analysis (Silic & Back, 2014).

Qualitative research can be appropriate when conducted by an individual with experience, knowledge and history of the topic to be examined. Researcher reflexivity, or position on a topic, was an important consideration when identifying practitioners to participate in data collection activities (Creswell, 2013). Qualitative research was selected to provide detailed information based on expert practitioner perspective and detailed understanding of security program requirements (George & Gao, 2014). Table 1 illustrates rationale for qualitative research selection based on Creswell's qualitative research characteristics.

Table 1

Qualitative Research Characteristic and Research Application

Qualitative Research Characteristic (Creswell, 2013)	Research Application
Research is conducted in a natural setting familiar to research participants.	Research was felt to be accepted by practitioners because of familiarity with online survey tools and subject matter expertise.
The researcher uses complex reasoning to derive findings.	Deep examination and analysis was believed to be required to provide practical and relevant findings.
Provides context for participants (organizational/job role/experience).	Data was elicited based on participant feelings, attitudes and perspectives. Specialized skills, credentials and experience were prerequisite to survey participation.
Research questions reflect on, and interpret, the researcher's experience, background and identity.	Research questions were designed to investigate the real-world business problem from a practitioner perspective to validate or refute the research problem.
The research should present a holistic picture of findings and conclusions.	Investigation of "current state" of program efforts at participating organizations was intended to provide benchmarking value to participants.
The final written report should include participant voices, research interpretation, contribution to literature OR a call to change.	Since the research problem was believed to be original, practitioner responses were felt to generate unique findings and an appropriate standard content definition framework for consideration and further investigation.

A limited amount of quantitative information was expected to be revealed, primarily to validate regulatory and contractual requirements present in respondent practitioner organizations. For example, the number of regulatory requirements mandated within organizations was examined as well as numbers of hours needed for specific program delivery activities. Quantitative information derived was intended to inform benchmarking demographics for participating practitioners.

GTM Approach

Once qualitative information was determined to be primarily obtained, more granular literature review identified GTM as the most appropriate qualitative research approach. Creswell (2013) suggests five approaches to qualitative research: narrative, phenomenological, ethnographic, case study and grounded theory. Of these approaches, GTM was selected because of its treatment of process and context when studying new organizational issues and research problems (Urquhart & Fernández, 2013). GTM as a research methodology is frequently accepted by information systems/information security researchers (Lawrence & Tar, 2013; Urquhart & Fernández, 2013).

GTM was also selected because of its data collection approach and analysis process. Researchers using GTM collect and study data before providing analysis and findings. The goal was to perform field work (the survey tool) first and then interpret results into findings and standard content definition framework. Other research methodologies propose a framework or theory first as basis for research and then confirm findings through field work (Charmaz, 2014; Cho & Lee, 2014; Lawrence & Tar, 2013; Urquhart & Fernández, 2013). The research approach needed to be bottom-up as opposed to top-

down and consider data as it was collected, not at the conclusion of the data gathering collection process (Charmaz, 2014).

Organizational context also supported selection of GTM. The research problem was identified as organizationally challenging and not previously studied in literature. Survey questions were designed to understand respondent organizational compliance requirements and context (Lawrence & Tar, 2013; Urquhart & Fernández, 2013). GTM helped explain relationships of ISATE requirements to people and organizations (Lawrence & Tar, 2013).

Preparation

In order to “test the waters” of research problem validity, several exploratory activities were seen as critical. Commercial ISATE vendors were contacted to identify if commercial offerings or prior research of this particular detail had been conducted. In parallel, discussion was felt to be required with senior and executive practitioners (corporate/chief information security officer (CISO) or organizational equivalent) to evaluate context and practical impact of the research problem. Common US-based ISATE contractual and regulatory regulations were carefully reviewed to provide examples of disparate and differing language. After these activities were completed, more granular selection of the research participant population was conducted.

Research Participant Selection

Information security practitioners, a unique and specific target audience, were initially identified to participate in data collection. GTM had already been selected due to its holistic, creative, and fresh perspectives through a structured research process with knowledgeable participants (Cho & Lee, 2014). GTM, as a bottom up approach, required

flexibility, adaptability and personal interpretation of the conditions being researched (Creswell, 2013; Charmaz, 2014). GTM strives to understand a problem from unique perspective of those people closest to the problem; identifying the best respondents based on personal insights and expertise into the research problem essential (Corley, 2015). Information security practitioners were felt to best provide credible, original, useful and informative basis for research (Hussein, Hirst, Salyers & Osuji, 2014).

However, the population of information security practitioners, as a whole, is quite large and was felt to be an unrealistic target audience. In the US, as of January 1, 2018, there were 79,617 Certified Information Systems Security Professional (CISSP) practitioners as designated by the International Information Systems Security Certification Consortium (ISC²). The CISSP is an objective measure of excellence and is the most globally recognized standard of achievement in the industry (ISC², 2018). CISSPs are certified in a wide domain of information security topics including ISATE.

Specialized and detailed expertise in ISATE content and delivery was felt essential as a respondent characteristic. In order to narrow the respondent selection further, approaching practitioners using social network LinkedIn was considered, as well as reaching out and contacting practitioners individually via email. Both approaches were eliminated since security practitioners are typically hesitant to share sensitive organizational information about security practices or events due to negative publicity, even under anonymous conditions (Crossler et al., 2013). Identifying the most knowledgeable, credible and appropriate respondent group was a critical task.

At this point, the International Association of Information Security Awareness Professionals (IASAP, <http://www.iasapgroup.org/>) was contacted. IASAP is an

independent, non-profit association comprised of corporate organizations who manage ISATE programs in a wide variety of industries. The IASAP originated from the Security Awareness Peer Group under Computer Security Institute (CSI) which evolved into the current-day IASAP organization.

IASAP members are responsible for developing and deploying program content within their organizations (IASAP, 2017). Their detailed knowledge of security-related compliance issues is validated through their corporate membership in IASAP. The selection of this group supported the premise that expert practitioner perspective and detailed understanding of the research problem is core to GTM (George & Gao, 2014). IASAP members were selected as a purposeful sample because of: daily program-related activities; response trustworthiness criteria; credibility of survey findings; transferability of findings to different organizational needs; and dependability of survey responses as supported by confirmability of participant credentials (Flowerday & Tuyikeze, 2016).

Extensive coordination and communication was conducted with IASAP management and leadership to obtain participation commitment. IASAP management was approached in January 2017 about participating in data collection supporting research questions. Several formal presentations to IASAP leadership requested member participation. An additional formal presentation was shared with general membership to generate participation interest and promote high completion rates. Approval was obtained in May 2017 to issue an electronic survey to gather respondent data. The process took longer than planned due to IASAP leadership and management examining the suitability of the research problem and establishing confidence in the project. A YouTube video was requested and produced to introduce the project to general membership

(<https://www.youtube.com/watch?v=YAe-kZ3iO10>) (Curran, 2017). Research as performed by a qualified, peer practitioner with shared identities, experiences, values and norms was highly important to IASAP management and leadership (Greene, 2014). The use of detailed practitioner language and content was acknowledged as effective in communicating the intent of the proposed survey (Hussein, Hirst, Salyers & Osuji, 2014).

Instrumentation

Use of an electronic survey tool was allowed for obtaining information from IASAP members. Respondent results were the only data used to draw conclusions. Results are intended to inform the larger information security practitioner and academic field (Barton, Tejay, Lane & Terrell 2016).

Protection of Respondent Identity and Organizational Information

Given the specialized experience and knowledge of IASAP leaders and members, security of online data collection sessions and storage of survey responses underwent close scrutiny to assure protection of respondent identity and organizational information. Online survey tools provide varying levels of license-based security controls to secure survey responses. Leading web-based survey tools were evaluated for ability to protect respondent information and provide respondent anonymity. SurveyMonkey (<https://www.surveymonkey.com/r/8X8TJG9>, now closed) was licensed monthly to securely manage survey distribution and responses. Survey responses were stored on SurveyMonkey systems maintained in physically secured environments. Online survey sessions were encrypted using Hyper Text Transport Protocol Secure (HTTPS) during survey participation. HTTPS provides privacy and integrity during Web browsing sessions (Felt et al., 2017).

Survey content was carefully reviewed for language and meaning so as not to elicit excessive participant or organizational information. The survey web page was communicated from IASAP management via email to members for added security and validation that the survey was from a legitimate source.

Survey Design

The survey was designed as a cross-sectional data collection activity (one-time) as opposed to a longitudinal activity (conducted over a long period of time) (Creswell, 2014; Crossler et al., 2013; Fink, 2013). Within information security-related research, longitudinal studies increase understanding of behavioral activities or other trends; for this research project, one-time, cross-sectional analysis was conducted (Crossler et al., 2013).

Survey data needed to support or refute each RQ was identified during ideation of the problem statement and RQs. Context and appropriateness of RQs were derived from literature review and practitioner guidance (Baxter & Jack, 2008).

The purpose of the survey was articulated, terms defined, and each RQ evaluated to ensure data would be obtained properly to support or refute the RQ (Creswell, 2014; Fink, 2013). Survey question categories (demographics, compliance requirements, ISATE program components, others) were identified. Data analysis techniques for each survey question were considered (including percentages, averages, comparison and relationships). Survey participation minimal response rate/survey success threshold was determined as 24 (eighty members representing 40 organizations, 30% participation rate) with a view of regulatory and contractual compliance requirements. IASAP membership

does not include auditors and vendors, so a very targeted responder population of experienced practitioners was identified.

Survey Question Design

Survey questions were intended to elicit candid, current and detailed responses providing illuminating insights and fresh perspective through repeated examination of survey responses (Hussein, Hirst, Salyers & Osuji, 2014). Survey questions were configured to provide a reasonable range of responses based on detailed knowledge of the survey topics (Fink, 2013).

The survey was designed as a cross-sectional data collection activity (one-time) as opposed to a longitudinal activity (conducted over a long period of time) (Fink, 2013). Within information security-related research, longitudinal studies are needed to increase understanding of behavioral activities or other trends; for this research project, one-time, cross-sectional analysis will be conducted (Crossler et al., 2013).

In its final form, the survey contained 33 questions organized into five sections. The questions were intended to elicit information to support or refute research questions and identify if the research problem was valid.

Section 1 examined the contractual and regulatory compliance requirements imposed on participating organizations. Section 2 identified if external, third party content delivery had been mandated and the impact of this requirement on participating organizations. This section also examined current internal programs being delivered. Section 3 focused on current definitions of program content (awareness, training and education) and if there was organizational interest in accepting a standard definition of each term. Section 4 addressed need for organizational relevance within program content

and identified current topics felt to be important for program inclusion. Finally, Section 5 requested organizational benchmarking data about program organization, guidelines and standards observed and roles supporting program activities.

Data Collection, Storage and Analysis

Data collection steps were identified to provide credibility and usefulness of survey responses (Fink, 2013). Survey questions were quality checked for clarity and completeness and a cross-reference of RQs to survey questions was mapped.

- RQ1: Section 1, questions 1.1 and 1.2
- RQ2: Section 2, questions 2.1-2.7
- RQ3: Section 3, questions 3.1-3.5
- RQ4: Section 4, questions 4.1 and 4.2
- RQ5: Section 4, questions 4.3-4.5

IASAP management disseminated the survey to its membership and monitored participation. Two weeks were originally proposed for survey completion, but after detailed discussion with IASAP leadership, the survey remained open for one month. It was believed that leaving the survey open for longer participation would yield strong completion percentages, strengthen member support and establish a working relationship with IASAP.

Participants were allowed to start and save the survey for convenience. Survey responses were stored in physically secure environments and encrypted in transit. Survey data was maintained in spreadsheets stored locally on a local laptop, an attached hard drive, Carbonite cloud storage (<https://www.carbonite.com/data-protection/endpoint-protection/>) and Google Cloud (<https://cloud.google.com/security/>) backups. Survey responses were stored in Excel spreadsheet, Adobe Portable Document Format (PDF) and comma separated value (CSV) formats for manual and semi-automated analysis and

review. Careful review of themes, concepts, ideas, suggestions or other comments provided by survey respondents provided inferences and conclusions (Fink, 2013).

Data analysis was performed manually. The “bottom to top” data analytics process presented by Creswell (2014) was adapted to assess and rationalize survey responses.

- Obtain final survey results and manually export data for analysis;
- Organize and prepare data for analysis;
- Critically read (and re-read) responses with an eye toward themes and concepts to assess responses;
- Organize responses and identifying trends and concepts to explore (Corbin & Strauss, 2008);
- Interpret the meaning and relevance of responses and demographic data; and
- Validate information accuracy (Creswell, 2014).

Licensing a qualitative data analysis software tool was considered based on cost, ease of use and applicability to a small amount of responses. NVivo (<http://www.qsrinternational.com/nvivo-product>), Quirkos (<https://www.quirkos.com/index.html>) and Dedoose (<http://www.dedoose.com/>) were investigated, with Quirkos acquired based on anticipated ease of use and graphical presentation. However, after evaluation and testing, the use of Quirkos as a data analysis tool was discontinued. This was a considerable change in the analysis plan.

The detail and candid input and responses from IASAP membership was felt to be sufficient to derive qualitative findings without the use of a data analysis tool. The investigation and learning curve associated with these tools caused delay in the research process and overly complicated data analysis. This was a key “lesson learned” in planning and subsequent execution processes.

Resources

Nova Southeastern University's Institutional Review Board (IRB) reviewed and approved survey content and participants (see Appendix D). IASAP management and leadership agreed, after long discussion and socialization, to allow its members to participate in an electronic Web-based survey tool. A letter following IRB guidance was issued to IASAP management and leadership to formally announce the survey (see Appendix E). Eighty members were invited to participate in the research survey by IASAP board leaders on October 17, 2017. IASAP leadership and management promoted lengthy availability for survey participation and provided frequent response/participation reminders. SurveyMonkey (<https://www.surveymonkey.com/r/8X8TJG9>, closed) was licensed on a monthly basis to manage survey distribution and responses. Standard Microsoft Office Home and Student 2016 for Mac software was used to manage Word, PDF, Excel and PowerPoint files. The survey was closed on November 17, 2017, with content, results and analysis presented in Appendix F.

Summary

Qualitative research as articulated through GTM was selected as project methodology. An online survey tool with appropriate security controls was acquired and deployed to IASAP, a professional organization with extensive expertise with ISATE programs. The use of a one-time electronic survey tool was determined most appropriate for data collection and was designed to elicit data to support or refute research questions. During a one-month period, 55 of 80 individuals responded (68.75% participation rate) to one or more sections of the survey. Chapter 4 will discuss results derived from survey activities.

Chapter 4

Results

Overview

Marshall and Rossman (2014) opined “The process of bringing order, structure and interpretation to a mass of collected data is messy, ambiguous, time-consuming, creative, and fascinating” (p. 207). This observation proved true during analysis of final survey responses. Survey responses were qualitatively assessed to build GTM about the research problem through careful thought and analysis (Marshall & Rossman, 2014). In Chapter 4, research results are provided as prelude to Chapter 5 conclusions, implications and recommendations.

The original research problem statement evolved over time. In its final form, research sought to investigate lack of standard information security awareness, training and education (ISATE) program definitions and content impacting internal organizational relevance and external compliance mandates. When interpreting survey results and formulating findings, it was frequently important to refine the original research problem to maintain scope, perspective and objectivity.

Research questions also evolved as literature review and guidance from practitioners helped simplify and clarify core elements of the research problem. Researchers including Creswell (2014) indicate that research questions can – and should – evolve over time due to continual review and reformulation, particularly in a GTM context.

Data Collection and Analysis

International Association of Information Security Awareness Professionals (IASAP) respondents accessed the SurveyMonkey online portal during a one-month period. Survey responses (data) were securely managed, maintained on the web portal, stored locally on a laptop and in cloud-based services.

Data analysis was performed manually. A “bottom to top” data analytics process as identified in literature review was used to understand and interpret survey responses (Charmaz, 2014; Creswell, 2013). Data were organized based on RQ and cross-referenced to survey question (see Appendix F). Qualitative and quantitative evaluation was applied to validate or refute RQs. Demographic information was assessed to examine “current state” of respondent programs and to establish a benchmark of specific activities supporting ISATE program delivery.

Survey Response Analysis

Fifty five of 80 members responded (68.75% participation rate) to one or more sections of the survey, significantly exceeding the 30% participation rate established with IASAP. Participation varied within each section of the survey. Fifty one of 55 IASAP participants (92%) responded to Section 1. The number of Section 2 responses varied depending on whether they were impacted by third party compliance requirements, but in general averaged 7 responses (12.72%) for each question in the section. In section 3, forty responses were on average recorded for each question (72.72%), and in Section 4, forty responses (72.72%) were the norm. Section 5 was primarily concerned with program information and consistently had forty responses (70.90%) to each question.

Section 1, Questions 1.1 and 1.2: Regulatory and Contractual Requirements

These questions sought to identify the current state of compliance requirements at respondent US-based organizations. Understanding ISATE compliance at member organizations would validate that varied and inconsistent ISATE terms exist in compliance requirements. Fifty one of 55 participants (92%) responded.

In response to question 1.1, the most common regulatory requirements identified by survey respondents were Sarbanes-Oxley Act of 2002 (SOX), Health Insurance Portability and Accountability Act/Health Information Technology for Economic and Clinical Health Act (HIPAA/HITECH), National Institute of Standards and Technology (NIST) 800-53, Gramm-Leach-Bliley Act (GLBA), state security laws, and North American Electric Reliability Corporation Critical Infrastructure Protection Plan (NERC CIP) Standards. These requirements are intended to secure assets required for operating North America's bulk electric system (Ingram, Martin & Pena, 2017). Federal Reserve Board (FRB) as influenced by the Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook, FFIEC Cybersecurity Awareness guidance (FFIEC, 2017) and Office of the Comptroller of the Currency (OCC) requirements were also listed. These responses validate that varied regulatory compliance requirements are posed to organizations. Research validates that many of these requirements have differing ISATE definitions and requirements.

Eight respondents indicated contractual requirements to provide content from third parties in addition to PCI DSS and HIPAA/HITECH in response to question 1.2. This number was lower than expected, but the number of responses is felt sufficient to validate

that external third party requirements in fact exist. This is a good benchmark for future work with IASAP to see if this number increases over time.

Section 2, Questions 2.1–2.7: Impacts of Third Party Compliance Requirements

These questions intended to identify the current state of third party compliance requirements at respondent US-based organizations. This is a detailed reflection on current state of external compliance requirements that prepares to inform the standard content definition framework. The number of Section 2 responses varied depending on whether they were impacted by third party compliance requirements, but in general averaged 7 responses (12.72%) for each question in the section.

In response to question 2.1, 6 respondents indicated that external, third party content was required to be provided. This differs from the 8 indicated in question 1.2 but could be due to question formatting. Of particular note, 10 respondents were not sure or did not know the status of this requirement. A “call for action” may be to determine actual status and see if the same respondents identified additional requirements. This follow-up research could indicate shift to a ‘Yes’ response. These responses can be re-examined over time with IASAP to see if there is gradual increase in this requirement. Responses validate that third party program content and delivery is mandated in organizations. If third party content was not indicated as required, the survey branched to question 2.6. If third party compliance was indicated as a requirement, questions 2.2–2.5 applied.

Respondents to question 2.2 were almost evenly divided about whether they integrated external content into existing programs (3) or delivering content separately (2). One respondent is in the process of assessing this process, and one indicated that their organization will not deliver external content at all.

Question 2.3 generated 7 responses about perceived impact of external requirements as illustrated in Table 2.

Table 2
Perceived Impact of Third Party Requirements

Impact (positive/negative)	No/Low Impact	Medium Impact	High Impact
Increased program management complexity (negative impact)	3	4	0
Increased compliance tracking (negative impact)	2	4	1
Increased confusion about policy direction (negative impact)	5	2	0
Increased participation/attendance time (negative impact)	3	4	0
Increased budget requirements (negative impact)	4	3	0
Increased content management responsibilities (negative impact)	1	6	0
Increased understanding of external policies and procedures (positive impact)	2	4	1
Increased communications (positive impact)	5	1	1
Improved compliance ratings/scores/assessment results (positive impact)	2	5	0

The inference is that the most significant negative impacts to respondents are in the areas of increased compliance tracking and increased content management responsibilities. Positive impact is primarily observed in the areas of increased understanding of external policies and procedures and improved compliance assessment results. This is believed to be the first time an evaluation of actual or perceived impacts (positive or negative) of third party program requirements has been conducted.

Question 2.4 inquired about specific time allocations and frequencies for annual externally-mandated program activities during a 12 month period. For awareness activities, the majority of respondent attendees participated in less than one hour's time annually. Six indicated no time or less than one hour for training activities, and a close match is observed for education, which accounted for no time or less than one hour. Since this is the first known assessment of external content provisioning, these numbers may serve as indicative of what other organizations might experience in the future. The key may be in the question: "entirely new, external program content".

External content delivery frequency was examined in Question 2.5. Awareness activities are seen as conducted quarterly and annually, with four respondents reporting no awareness activity conducted at all. Training requirements were indicated as strongly none (or annual – no middle ground was noted in this frequency). Very little was provided for educational content in new, externally mandated program content. The inference is that more focus is applied to internal program content frequency of delivery than external content frequency of delivery.

Starting with question 2.6, parallel internal program time allocations and frequencies were examined. In a twelve month period, respondents estimated that a time allocation

perspective, the wide majority of respondents indicated annual awareness time allocations as 1-5 hours. Training and education times were lower, with the majority reporting less than one hour to 2 hours. Question 2.7 inquired about frequency of program activities during a 12 month period. Surprisingly, a wide majority indicated that no awareness activities were conducted at all; this suggests that awareness activities are viewed as optional or discretionary. Awareness activities were reported as primarily conducted monthly, quarterly or annually. Training was conducted primarily annually; education was primarily none or annually. Since this is the first assessment of internal content delivery, these numbers may serve a baseline or metric indicator of what other organizations might be required to provide on an annual basis.

Section 3, Questions 3.1 – 3.5: Definitions Used and Program Documentation

These questions were designed to identify current definitions for awareness, training and education at respondent organizations. Obtaining different perspectives on definitions would inform the standard content definition framework. In section 3, forty responses were on average recorded for each question (72.72%).

Question 3.1 asked respondents to describe the title of their overall US-based program used to communicate ISATE. Seventeen of 42 respondents called their efforts “awareness training program”; this may be due to use of this term in common regulatory and contractual requirements. The remaining 25 responses indicated a wide range of different titles used, including awareness education, awareness, security education, training/education and formal awareness training. Six comments provided different program definitions than originally provided in the survey.

- Awareness (we push info out via articles, etc.) and training (CBTs, etc.);
- Security Awareness and Education (training falls under education);
- Information Security Awareness and Training;
- Security Training and Awareness Program;
- Education and Awareness; and
- Cyber Security Awareness and Education.

These responses validated that many differing program titles are in use within US-based organizations.

Question 3.2 posed a sample definition of awareness activities to determine if formal definitions exist, and if so, was the sample definition close to what was currently in use. The sample awareness definition was synthesized from common contractual and regulatory compliance language as “dialogue, collaboration and response to posters, presentations, emails; using personal interaction, visual cues and prior experience to make decisions about IS-related behaviors. (An example of awareness content would be “We have seen an increase in phishing attempts. Here is how you can recognize them”.)”

Thirty-two respondents indicated “this is close to our definition of awareness”, while 6 did not have a formal definition and 3 respondents used different definitions. This question helped build the foundation for the standard content definition framework.

In question 3.3, a similar definition was provided for *training* as “one-way instruction tested (T/F), measured (pass rates and attendance) and tracked. Training may be administered through annual or onboarding processes as mandated by contractual and regulatory requirements. (An example of training content would be (“You can only share social security numbers with others based on policy and your job role”).

Twenty-nine respondents indicated “this is close to our definition of training”, while 9 did not have a formal definition and 3 respondents used different definitions. This question also helped build the foundation for the standard content definition framework.

Question 3.4 indicated a wider difference of education definition based on the definition as “mix of passive and/or active instruction to enhance skills for a specific job role. Education may be required by contractual and regulatory requirements or through role competency requirements. (An example of educational content would be “You must develop secure website applications by learning detailed and complex coding techniques to prevent database and website application breaches”).

A wider difference of opinion was observed in responses. Twenty-one responded that this was a close approximation of their current definition, while 16 did not have a formal definition for education and 3 used different definitions. This question also helped build the foundation for the standard content definition framework.

Closing this section, question 3.5 inquired where ISATE programs is defined and/or explained. This was designed to understand how and where ISATE activities are communicated and where standard definitions might be presented. Sixteen respondents defined their current program in a security or other company policy. Remaining responses included defining program information in both company policies and program content and others define their program in content only. Program charters were also used, while some have not formally defined their program in any documentation.

Section 4, Questions 4.1–4.5: Organizational Relevance and Definition Acceptance

The questions in this section were intended to identify need for organizational relevance in ISATE content as well as appetite to adopt standard program definitions.

Within Section 4, forty responses (72.72%) were the norm.

Question 4.1 asked respondents to identify the importance of organizational relevance within their organizations. By a wide margin, organizational relevance was considered highly or somewhat important in awareness (38 of 40 respondents), training (36 of 40 respondents) and education (36 of 40 respondents). This supports literature indicating that ISATE content should be communicated in a timely manner with consistent messaging and with organizational relevance (Safa, Von Solms & Furnell, 2016). Flexibility and organizational relevance of ISATE content should be allowed to provide most optimal impact to participants (Karjalainen & Siponen, 2011).

In a more granular approach, question 4.2 asked respondents about program topics considered important to their organizations. Many responses can be considered “traditional” such as escalation instructions, clear explanation of policies and explaining penalties for non-compliance. Of interest were suggestions for more contemporary inclusion such as sharing recently identified risks/likely attack vectors, personal security topics (keeping children safe online, identity theft, home routers, etc.) and threat avoidance. Further in the survey, question 5.9 identified phishing campaigns and simulations as potential metrics and are considered in the analysis of this question as well.

Question 4.3 posed this definition of awareness: “Content mostly customized to organizational culture, relevance and current threats/risks; informal; focused on current events, threats, trends and risks affecting the organization” and asked about

organizational willingness to accept this definition. Twenty three respondents would accept this definition of awareness. Thirteen were not sure or did not know; this is linked to questions 5.7 about organizational responsibility for content and 5.8 about use of an oversight/ or governance committee that influences program content. Only three respondents indicated they would not accept this definition.

A definition for training was posed in question 4.4: “Internal and external content synthesized into one program focused on formal learning process; limited treatment of organizational culture, relevance and current threats/risks”.

Responses to this definition were almost equally split in favor of (17) or not sure of (16) accepting the definition. Six responded they would not accept this definition. Two comments primarily focused on needing organizational content in the training definition. “Organizational culture would be part of main focus”; and “Organizational culture is important in our environment” were mentioned. Compared to awareness definition acceptance, this definition had less acceptance from respondents.

Question 4.5 asked about this definition of education: “Role-based, specialized learning customized for risk management (secure code training, for example); very little treatment of organizational culture”. A slightly higher number of respondents would accept this definition (19), while 6 responded “no” and 13 were not sure.

Responses to this question were similar to 4.4. The responses to this definition were not as definitive as those for awareness. Nineteen respondents indicated the definition posed would be acceptable, but 13 responded “Don’t know/unsure”. As with the definition for training, 6 respondents stated they would not accept this definition.

To summarize the acceptance of standard definitions in respondent organizations, respondents were generally equally divided between acceptance or not knowing if definitions would be accepted. The number of “no” responses were low. Based on additional comments provided and low – or unknown – acceptance rates, the definitions were refined and are presented in Chapter 5.

Section 5, Questions 5.1–5.12: Demographic and Security Program Questions

Section 5 of the survey requested high-level organizational information and granular information about program format, ownership and delivery. Section 5 was primarily concerned with program information and consistently had 39 responses to each question.

Questions 5.1 and 5.2 inquired about organizational type and size. IASAP responders work in energy, financial services/banking, healthcare/public health manufacturing, consumer goods, insurance, technology, public utility, retail, hospitality, consulting and telecommunications industries. Most IASAP organizations (25) had 10,000+ employees and contractors. This provided context about the varied landscape of US-based regulatory and compliance requirements as well as program content.

Question 5.3 asked for information about security guidelines, standards or other frameworks used in respondent programs. NIST standards, specifically NIST 800-39, Managing Information Security Risk (20 respondents); NIST 800-30, Guide for Conducting Risk Assessments (16); NIST 800-61, Computer Security Incident Handling Guide (16); and NIST 800-53, Security and Privacy Controls for Federal Systems and Organizations (16) were the most frequently used security guidelines, standards or other frameworks used in respondent programs. They ranked consistently higher than ISO27001 (12) or 27002 (10), presumably an indicator of risk management focus in

participating organizations as well as governmental requirements for US Federal organizations. The SysAdmin, Audit, Network and Security Institute (SANS, <https://www.sans.org/>) (13) ranked highly as did Information Technology Infrastructure Library (ITIL, <https://www.axelos.com/>) (12).

In question 5.4, respondents were asked to identify what organizational groups were responsible for program content and administration. Dedicated information security departments were identified as responsible for managing and administering security programs within 33 responding organizations. Risk Management was listed by eight respondents and departments mentioned in additional comments included Corporate Security (three responses) and Corporate Compliance.

Buy or build content? Question 5.5 sought to learn if respondents developed their own content or purchased it externally (hybrid approach), or a combination of both approaches. Eighteen respondents build awareness content in-house, while 19 use a hybrid (build and buy) approach. Training and education content is largely obtained through a hybrid “build and buy” approach.

A project management office (PMO) role is not used frequently to assist with security program functions as articulated in question 5.6. Twenty six of 39 respondents answered “no”, while eight do use PMO for some program activities. Respondent comments indicate PMO support is more frequently used for specialized programs or campaigns.

Question 5.7 asked what organizational roles develop program content. Identifying program content was observed to be a collaborative effort among the CISO, privacy, physical security, legal, risk management, internal audit (IA) and other roles. Given the

high number of organizations required to comply with Sarbanes-Oxley Act (SOX), finance and treasury roles do not appear to have much content input.

Most organizations responding to question 5.8 (26 of 39 respondents) have an information security oversight/governance committee that influences program content. This is positive from a “tone at the top” and organizational relevance perspective.

In question 5.9, respondents were asked to identify prevalent metrics used to measure program activity. Thirty identified learning management system (LMS) reports as important, followed by other “traditional” measurements such as testing results, annual policy attestation, online surveys, and other measurements.

Prevalent content delivery mechanisms were identified based on responses to question 5.10. In awareness delivery, posters/signage, open houses/special events, videos, physical handouts and guest speakers (presumably at special events) were widely used. Training and education delivery was conducted primarily via web-based platforms (both live and recorded), videos and classroom sessions. Delivery mechanisms that were typically not used included mobile device training (live or recorded), popup reminders, banner messages and social media.

And finally, questions 5.11 and 5.12 identified that privacy and physical security content is combined with information security content in the wide majority of responding organizations. For detailed RQ/survey question cross reference, actual survey responses and additional analysis, refer to Appendix F.

Summary of Results

Survey responses informed the research problem and provided data that after analysis answered research questions. Information obtained provided basis for a standard content

definition framework for promotion to academic and practitioner audiences. Some survey responses were unexpected and helped inform and develop an improved standard content definition framework. Chapter 5 will present the standard content definition framework and research findings.

Chapter 5

Conclusions, Implications, Recommendations and Summary

Research questions are answered in this chapter. A standard content definition framework (SCDF) is presented that may benefit and inform information security awareness, training and education (ISATE) programs large and small. ISATE program benchmarking considerations, deployment implications and future research recommendations are provided that may benefit academic and practitioner communities. Strengths, weaknesses and limitations of the research are acknowledged. Finally, a short summary provides closure to the project.

Research Problem Answered

The problem identified for investigation was lack of standard ISATE program definitions and content impacting internal organizational relevance and external compliance mandates.

Research Questions Answered

RQ1: What US-based regulatory and contractual requirements impose internal and external ISATE program delivery? Varied compliance requirements add complexity to information security programs. Laws and regulations mandate information security program efforts to avoid potential agency and/or legal consequences (Narain Singh, Gupta & Ojha, 2014). Little research has been done to assess organizational impact of new, imprecise and variable security compliance requirements. (Bamberger & Mulligan, 2011).

Findings from this RQ validate that 1) compliance requirements are mandated on US-based organizations and 2) varied and inconsistent ISATE definitions exist within

regulatory and contractual compliance requirements. Results provide a view of US-based regulatory and contractual compliance requirements experienced at respondent organizations. The most common requirements were identified, and inconsistency among content definitions, delivery and measurement validated. While the response to this question may seem intuitive, validating that varied compliance mandates currently exist in respondent organizations was essential and foundational to the remainder of the study. This validation helped set the foundation for examining inconsistent and multiple compliance language.

Review of compliance requirements imposed on respondent organizations revealed and built the case for later standard content definition framework that varied and inconsistent ISATE terms exist in compliance requirements. The most common regulatory requirements identified by survey respondents were SOX, HIPAA/HITECH, NIST 800-53, state security laws, NERC and GLBA. Contractual requirements to provide content from third parties in addition to PCI DSS and HIPAA/HITECH were examined. While the number of actual third party requirements imposed on member IASAP organizations was low, responses provided were felt sufficient for analysis.

RQ2: What are the impacts of external (third party) requirements on current ISATE programs? To date, the impact of third party compliance requirements on organizations has not been fully evaluated. Contractual agreements now contain compliance requirements that may require third parties to comply with external policies, procedures and processes (Killingsworth, 2014). Literature review failed to reveal new academic publications since 2014 in this area. Findings from this RQ validate that third party

compliance requirements affect participating organizations and identified perceived negative and/or positive impact of these requirements.

A lower number of organizations are impacted by third party program requirements than was originally expected. However, the existence of internal and external compliance requirements was verified. Negative and positive impacts of third party compliance requirements were identified. Respondents indicated negative impacts in the areas of increased compliance tracking and increased content management responsibilities. Positive impact was primarily observed in the areas of increased understanding of external policies and procedures and improved compliance assessment results.

A number of respondents were not sure of, or did not know, the answer to this question; respondent organizations may desire to determine if any contractual requirements exist they are unaware of. Alternatively, respondents may decide to discuss this topic with information security oversight/governance committee members identified as established at most respondent organizations.

External content delivery approach is found to be evenly divided. Respondents either integrate external content into existing programs or deliver content separately. Shorter amounts of attendance time and less frequency were allocated to external content delivery than amounts of attendance time and frequency of internal content delivery. The inference is that more focus is applied to internal program content frequency of delivery than external content frequency of delivery as required in respondent organizations.

RQ3: What ISATE program definitions are currently used? ISATE definitions and approaches are varied as identified in contractual and regulatory requirements. There are wide differences of opinion on standard definitions of ISATE (Tsohou, Kokolakis,

Karyda & Kiountouzis, 2008). Haeussinger and Kranz (2013) state that information security awareness is a significant element of IS policy compliance, but the definition of awareness is universally lacking in prior research. Findings from this RQ identified definitions for awareness, training and education programs and delivery components used within respondent organizations. These definitions were used to inform the standard content definition framework.

Many respondents were aligned on the term “awareness training program” for overall program title. This may be due to use of this term in common regulatory and contractual requirements. The majority of responses indicate a wide range of different titles used, including awareness education, awareness, security education, training/education and formal awareness training. Only one respondent includes use of “cyber security” in their program title. The term is discussed later in this chapter. These responses validate that many differing program titles are in use within US-based organizations.

More granular questions examined respondent organizational definitions for awareness, training and education. Example definitions for each term were presented to determine if definitions existed in respondent organizations, if they were formally accepted, and to look for wide variances in definition terms. Example definitions were synthesized from common contractual and regulatory compliance language. These questions helped establish foundation for the standard content definition framework.

The example definition for awareness was prevalently accepted by respondents, while the definition for training was less accepted, and in the example of education, even fewer respondents agreed with the example definition. A standard content definition framework

may help organizations measure program activities and provide relevant instruction for program participants.

The last finding applied to this RQ provides understanding of how and where ISATE activities are communicated and where standard definitions might be presented. Most respondents define their current program in a security or other company policy. Others define program information in both policies and program content, while others define their program in delivered content only. Some programs are not defined at all within respondent organizations, and even less frequently within program charters.

RQ4: Is organizationally-relevant ISATE program content important? Literature indicates strong support for organizational relevance in ISATE content. Regulations now mandate the delivery of relevant material (PCI SSC, 2014). ISATE content must be understood by attendees, be organizationally applicable and relevant from the viewpoint of their work (Siponen & Vance, 2014). By a wide margin, organizational relevance was considered highly or somewhat important in awareness, training and education activities. “Traditional” program topics considered important to respondent organizations included escalation instructions, clear explanation of policies and explaining penalties for non-compliance. These topics are documented extensively in literature and in practice. Suggestions for more contemporary inclusion such as sharing recently identified risks/likely attack vectors, personal security topics (keeping children safe online, identity theft, home routers, etc.) and threat avoidance were provided. Phishing campaigns and simulations were noted as used within respondent programs.

RQ5: Will organizations accept standard definitions of awareness, training and education? Organizations do not have standard and specific guidance or direction from

frameworks and standards by which to create or acquire ISATE content, delivery or measurement (Caldwell, 2013). A proposed definition of awareness was accepted by the majority of respondents, but with many respondents not sure of, or not knowing if their organization would accept the definition as presented. The proposed definition of training was less enthusiastically supported, with fewer respondents indicating acceptance and many also not sure of, or not knowing if their organization would accept the definition. Training definition responses highlighted importance of organizational relevance and resulted in rewording of the standard content definition framework. The proposed definition of education had slightly higher acceptance by respondents and a high number of respondents unsure about acceptance. These findings are similar to those observed in RQ3. Respondent organizations may desire to discuss the topic of definition acceptance with information security oversight/governance committee members identified as established at most respondent organizations.

To summarize the acceptance of standard definitions in respondent organizations, respondents were generally equally divided between acceptance or not knowing if definitions would be accepted. The number of “no” responses were low.

Benchmarking Results

A series of questions inquired about organizational demographics and program governance. IASAP membership represents energy, financial services/banking, healthcare/public health manufacturing, consumer goods, insurance, technology, public utility, retail, hospitality, consulting and telecommunications industries. Most IASAP members have 10,000+ employees and contractors. This provided context about the

varied landscape of US-based regulatory and compliance requirements as well as program content.

Within respondent programs, NIST standards were the most frequently used security guidelines, standards or other frameworks cited. ISO27001 and 27002 are also commonly used to inform programs as well as SANS guidance and ITIL methodology.

Dedicated information security departments were identified as responsible for managing and administering security programs within the majority of responding organizations. Risk Management, Corporate Security and Corporate Compliance also maintained programs. A project management office (PMO) role is used for specialized programs or campaigns, but not for general program delivery activities.

Content input is obtained from CISO, privacy, physical security, legal, risk management, internal audit (IA) and other roles. Given the high number of organizations required to comply with SOX, finance and treasury roles do not appear to provide much content input. Content is obtained through a combination of in-house development (build) and a hybrid (build and buy) approach. Privacy and physical security content is combined with information security content in the wide majority of responding organizations.

Most respondent organizations have an information security oversight/governance committee that influences program content. This is positive from a “tone at the top” and organizational relevance perspective.

Learning management system (LMS) reports are important measurement metrics cited by respondents, followed by other “traditional” measurements such as testing results, annual policy attestation, online surveys, and other measurements.

Prevalent awareness content delivery mechanisms were noted as posters/signage, open houses/special events, videos, physical handouts and guest speakers (presumably at special events) were widely used. Training and education delivery was conducted primarily via web-based platforms (both live and recorded), videos and classroom sessions. Delivery mechanisms that were typically not used included mobile device training (live or recorded), popup reminders, banner messages and social media.

Standard Content Definition Framework (SCDF) Recommendations

The SCDF is simple in design but carefully constructed. The number of differing contractual and regulatory compliance requirements affecting ISETA program content can be large. Organizational relevance in ISETA content needs to be maintained. The SCDF proposed in this section is derived from literature review, examination of common US-based regulatory and contractual compliance requirements, review of standards, frameworks and guidance, practitioner input and survey responses.

The SCDF may be of benefit to information security practitioners as they plan, create, deploy, manage and measure their ISATE programs. The SCDF may reduce training time and costs, provide clear direction to program participants, identify more accurate budget, resource and timing requirements, demonstrate regulatory and contractual compliance, reduce content subjectivity issues, result in fewer ISATE-related audit findings, and provide effective measurements and metrics to illustrate program success. Third party contract language may be standardized such that organizations issuing or receiving third party compliance mandates have a consistent approach to value chain compliance. The following provides notional guidance for practitioners to consider.

Pre-Planning for SCDF Deployment

SCDF can be used to codify and standardize program content and definitions in existing programs or can be considered foundational for new programs. SCDF may also be used to inform success/improvement metrics and may be considered a program maturation goal. Properly deployed SCDF will help clarify roles, responsibilities, resource requirements and compliance capabilities. The following are suggested steps to consider when pre-planning SCDF either for existing or new programs.

1. **Identify Current Regulatory and Contractual Requirements.** This will help assess the most appropriate program title and supporting content definitions to be used. Collaboration with legal, procurement, financial and risk management roles may be required for current compliance requirements. Internal and external requirements must be examined. The process of contract issuance and approval may need to be examined for inclusion of standard language as discussed in this guidance.
2. **Socialize Standardization.** If an information security oversight/governance committee does not exist, it might be considered at this point in SCDF planning, as well as collaboration with the CISO, privacy, physical security, legal, risk management, internal audit (IA) and other management roles. The approach of establishing a steering committee or trusted network in organizations builds consensus on organizational security risk helps establish security culture (Auffret et al., 2017).
3. **Identify organizationally-relevant program content.** Determine if there are current risks that need to be communicated, or if business requirements

necessitate a shift in current content. Technical as well as human-based risks must be freshly identified to provide organizational relevance. Literature supports engaging individuals to provide input to program content and delivery to improve participant awareness and policy compliance behavior. Participation increases individual awareness of existing security risks and helps provide organizational relevance through alignment with business objectives (Haeussinger & Kranz, 2017).

4. Revisit/revalidate approach to security guidelines, standards or other frameworks that are core to the program. Organizational appetite may exist to adapt new frameworks or begin analysis of updated guidance.
5. Validate where SCDF will be defined and/or explained. This will identify how SCDF is communicated and where program definitions are presented. SCDF may be defined in a security or other company policy. Formal definition and communication of the SCDF is felt essential in order to measure its effectiveness successfully.
6. Select the best program title. Organizations may choose to use “awareness, training and education program” within the title, as this term is commonly found in US-based regulatory and contractual requirements, common practice and academic literature.
7. Select the best program content definitions. Organizational relevance cannot be overlooked when considering content definitions. References to delivery mode (formal or informal), cadence (scheduled or ad-hoc), level of organizational relevance, participant role/responsibilities and management

support are recommended. Suggested definitions as modified from original survey questions include:

Awareness: content delivered formally or informally to all individuals on a scheduled or emergency basis; includes organizational relevance and delivers basic information about current/emerging events, threats, trends or risks.

Examples: annual security policy review and attestation; mobile device security techniques; protecting the full range of online activities individuals conduct (being secure at home, at work and while traveling); secure browsing practices; selecting appropriate passwords and other online credentials; emergency alerts or advisories; specific instruction on how to help contain a malware or phishing emergency; and how to report a physical or electronic security issue or concern.

Training: content delivered formally on a scheduled basis to specific individuals based on job role; includes organizational relevance and delivers a formal learning process emphasizing risk management and compliance with regulatory/contractual requirements.

Examples: PCI DSS mandated training for individuals in credit card payment processing roles (PCI SSC, 2014); NIST 800-53 SA-16 secure coding practices for application developers to reduce vulnerable code (NIST, 2013); and FACTA Red Flags Identity Theft Protection Program (FTC, 2017).

Education: content delivered formally on a scheduled basis to specific individuals based on job role; includes organizational relevance

emphasizing specialized certifications, credentials or targeted risk management techniques or technologies.

Examples: CISSP and Certified Secure Software Lifecycle Professional (CSSLP) certifications (ISC², 2018); Certified Fraud Examiner (CFE) (ACFE, 2018); and Global Information Assurance Certification in Penetration Testing (GIAC GPEN) (GIAC, 2018).

8. Select the best program delivery mechanisms based on definition. Not all delivery methods are appropriate for every content type. As learned from survey respondents, awareness delivery generally consists of posters/signage, open houses/special events, videos, physical handouts and guest speakers. Training and education delivery was identified as conducted primarily via web-based platforms (both live and recorded), videos and classroom sessions. Delivery mechanisms that were typically not used included mobile device training (live or recorded), popup reminders, banner messages and social media.
9. Select meaningful measurement metrics. Improved compliance tracking, increased understanding of internal/external policies or improved compliance assessment results. LMS reports may be felt important, followed by other “traditional” measurements such as testing results, annual policy attestation, online surveys, and other measurements. Referring to terms used in the sample definitions, metrics can be derived quantifying scheduled/emergency communications and events, timing or frequency variances and other measurements.

In all cases, emphasis should be to promote, leverage and continually improve the SCDF based on organizational relevance and current or perceived risk.

Future Research Considerations

A large focus of this research was dedicated to understanding standardization and normalization of practitioner terms awareness, training and education. During literature review, additional disparate terms and definitions were observed but felt to be out of scope.

First, the lack of a common definition (and even spelling) of the term cybersecurity (or cyber security) is noted in literature and practitioner documents. Programs deployed to support information security awareness, training and education were evaluated, not cyber security programs. The use of the term cyber security in a program title is understood to be limited as seen in survey results from question 3.1. Only one comment from a respondent used the term in their program titled “Cyber Security Awareness and Education”. Poor definition of the term, in either spelling or representation, is seen as a considerable issue that has been acknowledged in literature (Bashroush, Schatz & Wall, 2017). One possible definition is that information security is primarily dedicated to protecting information in an organizational context, with cyber security extending past an organization’s defenses (Gcaza et al., 2017) and into value chain relationships conducted among businesses, vendors, contractors or local, state and Federal government agencies (Patnayakuni & Patnayakuni, 2014) as discussed in Chapter 1.

Literature acknowledges confusion in the research community about the use of the term cyber security interchangeably with information security. Some argue that there are glaring differences in these concepts even though they closely relate (Gcaza et al., 2017).

When considering approaches to managing risk and protecting information, it may make sense to ensure that a standard catalogue of terms is defined to identify, communicate and manage cyber/information security risk.

Inconsistent terminologies, definitions and content concerning security policies were also identified. Policy inconsistency may complicate ISATE program content development and delivery. There may be confusion among security practitioners responsible for defining policies and then communicating policy content (Alshaikh et al., 2016).

Similarly, lack of standardized definitions of information security culture was identified. Mahfuth et al. (2017) performed qualitative study and determined that 18 separate security culture frameworks exist in literature and identified at least 12 differing definitions of security culture. Identifying additional, higher-order information security definitions and content framework seems sensible and beneficial but was not in scope for this project.

Secondly, this research problem was addressed from a US-based perspective only. US-based practitioner respondents provided data and feedback. Global perspective can and should be evaluated in a separate research effort. Of particular interest, EU GDPR is mandated in May 2018 as a singular, comprehensive and detailed directive that protects global processing and movement of information (EU GDPR, 2015). The EU GDPR is being emulated by many other countries so a level of standardization is being accomplished globally and gradually (Cunningham, 2016). Evaluating GDPR in the context of global SCDF is a logical next step to be considered.

Strengths and Weaknesses

Expert practitioner input from IASAP and support from IASAP management and leadership were key strengths of the data collection/survey process. There is reluctance among security practitioners to participate in information security research, which leads to typical low response rates to security research, unless there is an established relationship with the participating organization (Betz, 2016). Collaboration with IASAP was essential to collecting data, developing findings and drawing conclusions. Continued work with IASAP is hoped to result in value to their membership.

The wording of survey questions, in retrospect, caused weakness in the number of respondents. Wording should have been more carefully constructed and more options provided for feedback. While this observation is not felt to have adversely impacted findings validity, improved and more thoughtful questions may have yielded even more valuable data for analysis.

Author bias toward the number of respondents having external third party compliance requirements was identified. The number of IASAP respondents impacted by third party program requirements was much lower than originally expected. However, the existence of internal and external compliance requirements was verified and reflects a real-world view of the research problem.

Finally, within the survey instrument, two NIST publications were omitted that may have provided additional data for analysis but were felt to be superseded by later Federal guidance and standards. NIST Special Publication (SP) 800-50, Building an Information Technology Security Awareness and Training Program, provides guidance for building an effective security program and supports requirements specified in FISMA. It covers

awareness and training program design, awareness and training material development, program implementation and post-implementation (NIST, 2003). A companion publication is NIST SP 800-16, Information Technology Security Training Requirements: A Role- and Performance-Based Model (NIST, 1998). SP 800-50 works at a strategic level, and SP 800-16 describes approaches to role-based security training. These were not included as options for selection within the survey. Interestingly, these were not added within respondent comments, but the omission must be noted.

Limitations

The following limitations are noted as potential opportunities for future research.

1. IASAP Participation: Survey participation was limited to IASAP members. A larger sampling of information security practitioners may have added additional validation of SCDF program and content definitions. Caution was exercised in limiting the respondent group to IASAP membership due to need for specialized experience and expertise in responding to the research survey. IASAP respondents only focused on US-based programs but may have global program responsibility or authority.
2. Outward-Facing Compliance Requirements: Sixty two percent of respondents to a 2017 Ponemon Institute survey indicated their organizations require third parties to ensure compliance with their security and privacy practices (Ponemon, 2017). The Ponemon Institute conducts research to identify trends in practices, perceptions and potential threats affecting personal and organizational privacy and security. Survey questions did not ask if there are external requirements imposed in internal program content on third parties in

their value chain. Identifying this requirement in future Ponemon studies may provide data to continue validation of the problem statement and may be respectfully suggested to the Institute.

Conclusions

The purpose of the research was to investigate lack of standard ISATE program definitions and content impacting internal organizational relevance and external compliance mandates. The results are seen as practical and useful to security practitioners because they focus on a recently identified issue within organizations (Terrell, 2012). It is believed to be the first effort to understand current perspectives on this topic as identified by industry practitioners. A standard content delivery framework (SCDF) is believed to assist organizations balance organizational relevance external regulatory and contractual compliance requirements within their ISATE programs.

A Web-based survey was issued to a professional organization of security professionals (IASAP) that was selected for participation based on subject matter expertise, familiarity, credibility and experience. Overall IASAP participation was high due to the encouragement and support of IASAP leadership. Fifty-five of 80 members responded (68.75% participation rate) to one or more sections of the survey. Survey response rates dropped in certain questions, a limitation discussed further in this chapter. Responses were solicited only for US-based program activities. Survey responses provided insight and clarity to the research problem and associated research questions. Conclusions include:

- Multiple and varied regulatory and contractual compliance requirements are verified as imposed on organizations. While this finding may seem intuitive, the actual number of compliance mandates currently in existence in respondent organizations was needed to set foundation for examining inconsistent and multiple compliance requirement language.
- A lower number of organizations are impacted by third party program requirements than was originally expected. However, the existence of internal and external compliance requirements is verified. Detailed findings provide benchmarking of issues encountered when addressing third party requirements.
- Negative and positive impacts of third party compliance requirements are identified. Respondents indicating third party compliance requirements experienced negative impacts in the areas of increased compliance tracking and increased content management responsibilities. Positive impact was primarily observed in the areas of increased understanding of external policies and procedures and improved compliance assessment results.
- Where applicable, time and frequency dedicated to external content appears to be much less than internal content. Respondents indicated increased time and frequency for internal awareness, training and education program activities.
- The title of ISATE program efforts in organizations is very diverse. The majority of respondents had different titles for their programs, with “awareness training program” less commonly used to describe ISATE efforts.
- Definitions of awareness, training and education vary in respondent organizations. Awareness definitions are more commonly established, followed by training and

to a far lesser extent the definition of education is established.

- ISATE programs are documented in a variety of organizational methods. The program is mostly articulated in security or other company policy and less frequently in a program charter or within ISATE content itself. Programs are also informally defined but not documented.
- Respondents may consider accepting standard definitions for awareness, training and education. Responses were virtually mixed on accepting new definitions or being unsure of acceptance. However, the number of “no” responses was low.
- Organizationally-relevant program content is highly important. Respondents desired a balance between external content requirements and organizational relevance.
- Program topics supporting organizational relevance reflect traditional and contemporary content. “Traditional” topics such as escalation instructions, clear explanation of policies and explaining penalties for non-compliance were noted. However, suggestions for more contemporary inclusion such as recently identified risks/likely attack vectors, personal security topics (keeping children safe online, identity theft, home routers, etc.), phishing and threat avoidance were provided.
- A picture of current ISATE programs was defined.
 - At participating organizations, dedicated information security departments are primarily responsible for managing and administering security programs.

- ISATE content is both bought externally and built internally and influenced heavily by NIST standards.
- The project management office (PMO) role is not used frequently to assist with security program functions but rather for specialized programs or campaigns.
- Identifying program content is observed to be a collaborative effort among the CISO, privacy, physical security, legal, risk management, internal audit and other roles. Many of these roles may participate in the information security oversight/governance committee established at most respondent organizations.
- Prevalent metrics used to measure program activity include learning management system (LMS) and other “traditional” measurements such as testing results, annual policy attestation, online surveys, and other measurements.
- Popular awareness delivery mechanisms include posters/signage, open houses/special events, videos, physical handouts and guest speakers. Training and education delivery is conducted primarily via web-based platforms (both live and recorded), videos and classroom sessions.
- Delivery mechanisms typically not used include mobile device training (live or recorded), popup reminders, banner messages and social media.
- Privacy and physical security content is combined with information security content in the wide majority of responding organizations.

Detailed survey results are discussed in Appendix F.

Implications

This research is believed to be of interest to industry practitioners and academia and accepted in both domains. Industry practitioner acceptance of the SCDF and research findings may be positive due to credibility of IASAP subject matter expertise, familiarity with the research problem and knowledge of RQ conditions. IASAP responses reflected specialized and credible feelings, attitudes and perspectives. The specialized skills and experience of IASAP membership were essential to the research and deeply appreciated.

These findings and the framework are believed to be original, practical and relevant to researchers as well. Research questions investigated the original problem statement from a practitioner perspective and as derived from literature review. Existence of varied and inconsistent ISATE definitions and content from a research perspective was validated. Analysis of prevalent regulatory and contractual compliance requirements substantiated the diverse definitions and requirements imposed on US-based organizations.

Investigation of “current state” program efforts at respondent organizations are believed to provide benchmarking value to IASAP membership and inform potential, additional investigation. The SCDF framework, while consisting of a short program title and brief working content definitions, is felt to be foundational and appropriate for organizational and academic consideration.

Recommendations

In parallel with this research, the author is participating in an ASIS, ISC² and ISACA joint working group to draft and approve a new Security Awareness Standard that will be issued globally (ASIS, 2016). The SCDF has been integrated into working versions of the draft and submitted for consideration by global approval committees. The SCDF

addresses regulatory and contractual requirements, standardized definitions and organizational relevance in program content that may be of benefit within the new global standard. Additional findings will be integrated where appropriate in sections of the draft.

Summary

Background

Information security (IS) risks affect global organizations on a daily basis as a result of insecure global, interactive electronic connectivity among public and private organizations (Biener, Eling & Wirfs, 2015). Risks are introduced through technical or human-based activities and have increased significantly due to availability and exploitation of web-based applications, mobile devices, cloud-based computing, social media and Internet of Things (IoT)-connected devices (Safa et al., 2015).

In response to these risks and threats, layers of regulatory and contractual compliance mandates have emerged. Governments have imposed new regulations and business partners increasingly include specific contract language requiring responsible security practices (Haeussinger & Kranz, 2017).

Security-related compliance requirements vary in length, detail, scope, direction, guidance, consistency and language (Yimam & Fernandez, 2016). New, updated or differing regulations and requirements enlarge effort of achieving and maintaining regulatory and contractual compliance (Thalman et. al., 2012). Little research has been done to assess organizational impact of new, imprecise and variable security compliance requirements. Regulated organizations are confused about measuring compliance (Bamberger & Mulligan, 2011).

The importance of ISATE content to promote compliant and positive security

behavior has been clearly established in literature, but there is no one agreement academically about the design, deployment and effectiveness measurement of content within programs (Bauer, Bernroider & Chudzikowski, 2017). Compliance with organizationally-relevant policies and instruction is understood to be foundational and critical to prevent security risk.

Problem Statement and Research Questions

Based on observation of conditions discussed in this section, the problem identified for investigation was lack of standard ISATE program definitions and content impacting internal organizational relevance and external compliance mandates. Research questions evolved as literature review and survey design activities were conducted. In final state, they sought to understand:

RQ1: What US-based regulatory and contractual requirements impose internal and external ISATE program delivery? Findings from this RQ would be used to validate or refute that varied and inconsistent ISATE terms exist in compliance requirements.

RQ2: What are the impacts of external (third party) requirements on current ISATE programs? Findings from this RQ would be used to validate or refute that organizations face increased external requirements to participate in ISATE programs from third parties.

RQ3: What ISATE program definitions are currently used? Findings from this RQ would validate or refute that varied or inconsistent ISATE definitions are used in respondent programs.

RQ4: Is organizationally-relevant ISATE program content important? Findings from this RQ would validate or refute that organizations desire a balance between external content requirements and internal organizational relevance.

RQ5: Will organizations accept standard definitions of awareness, training and education? Findings from this RQ would validate or refute that organizations would accept and standardize on definitions as provided in survey content.

Review of the Literature

Literature review centered on several key topics:

- **Security Risk Management:** Administrative, human-based behavioral controls must be implemented by organizations to manage security risk and may include elements of policy compliance and participation in learning activities. Security risk is understood to decrease when employees, contractors and/or third parties make good decisions based on behavioral guidance and instruction (Safa, Von Solms & Furnell, 2016). Risk may also be reduced through an organizational culture that promotes information protection as a daily job function (Santos-Olmo et al., 2016).
- **Security Policies:** Information security policies identify standards, boundaries, and responsibilities that individuals must observe in order to prevent risk. Policies influence individual risk awareness and organizational security culture (Cram, D'Arcy & Proudfoot, 2017) as well as provide formal strategic, tactical guidance and instruction (Ahmad et al., 2016). Policies articulate and direct an individual's security behavior, compliance decisions and risk management actions. These policies should be aligned with organizational objectives, be easily understood and reasonable to comply with. Policies should be communicated so that intended informational and instructional content is delivered effectively (Alkhourayyif & Weir, 2017).

- **Communicating Security Policies:** Literature highlights the importance of establishing policies first, then promoting them as the fundamental and essential basis of an effective organizational awareness, training and education program (Haeussinger & Kranz, 2017). Organizations do not have specific guidance or direction from regulators, audit frameworks or standards by which to create or acquire content, delivery or measurement. Many security guidelines are generic and do not take risk, geographic or organizational cultural factors into consideration (Rocha Flores, Antonsen & Ekstedt, 2014). There are no commonly agreed to or understood standard measurements or guidance for organizational ISATE activities (Gundu & Flowerday, 2013).
- **Lack of Standard Frameworks and Definitions:** Although there are many reference models and guidance, no unified framework exists to define ISATE content as required by contractual and regulatory requirements. Vendors offer templates and/or services that can be purchased, but they may be too general to meet compliance requirements and/or lack organizational relevance.
- **Organizational Relevance:** Every organization has different perspectives and definitions of security risk and solutions to mitigate risk (Banfield, 2016). Common guidelines, best practices and standards exist to help organizations establish programs; however, these are largely conceptual, generic and do not include discussion of organizational relevance in content (Alshaikh et al., 2018). Strong understanding and perception of organizational risk may help reduce noncompliance to IS policies (Ifinedo, 2016). ISATE content should be communicated with organizational relevance (Safa, Von Solms & Furnell,

2016). Literature acknowledges need to include specific internal organizational social norms and attitudes as part of ISATE programs (Bauer & Bernroider, 2017).

- Contractual and Regulatory Compliance Requirements: Organizational programs should reflect applicable security regulations organizations take to mitigate internal risk (Herold, 2010). Little research has been done to assess organizational impact of new regulatory requirements. Regulatory rules are imprecise and variable. Regulated organizations are confused about measuring security program compliance (Bamberger & Mulligan, 2011). Imposed regulatory requirements can be costly and ineffective (Miller, 2014). Compliance with laws and regulations mandate standardized security program efforts to avoid potential agency and/or legal consequences (Narain Singh, Gupta & Ojha, 2014).

Methodology

Qualitative research derived from input by experienced practitioners was selected as research methodology. The qualitative assessment of practitioner responses provided understanding of details and conditions that enabled knowledge development (Corbin & Strauss, 2008). Further literature review identified grounded theory methodology (GTM) as the most appropriate qualitative research approach because of its treatment of process and context when studying new organizational issues and research problems (Urquhart & Fernández, 2013). GTM was also selected to understand respondent organizational compliance requirements and context (Lawrence & Tar, 2013; Urquhart & Fernández, 2013) and explain relationships of ISATE requirements to people and organizations (Lawrence & Tar, 2013).

Research Participant Selection

Information security practitioners, a unique and specific target audience, were selected to participate in data collection activities in order to provide credible, original, useful and informative basis for researching content and delivery efforts (Hussein, Hirst, Salyers & Osuji, 2014). The IASAP, an independent, non-profit association comprised of corporate organizations who manage ISATE programs in a wide variety of industries, agreed to participate.

Data Collection, Storage and Analysis

To collect data for analysis, a cross-sectional (one-time) electronic survey was selected as opposed to a longitudinal (multiple) (Creswell, 2014; Crossler et al., 2013; Fink, 2013). In its final form, the survey contained 33 questions organized into 5 sections to validate or refute research questions and may be seen in Appendix F.

Survey participation minimal response rate/survey success threshold was determined as a minimum to contain 24 responses as returned from IASAP members (80 members representing 40 organizations, 30% participation rate). Fifty-five of 80 members responded (68.75% participation rate) to one or more sections of the survey, significantly exceeding the 30% participation rate established with IASAP. Participation varied within each section of the survey. Data collection steps were identified to provide credibility and usefulness of survey responses (Fink, 2013). Survey results were quality checked for clarity and completeness; a cross-reference of RQs to survey questions was mapped.

The survey remained open for one month to yield a strong completion percentage and establish a lasting working relationship with the organization. Survey data were maintained locally, in cloud-based storage, and within the Web-based survey portal. Data

analysis was performed manually. The detail and candid input and responses from IASAP membership was felt to be sufficient to derive qualitative findings without the use of a data analysis tool.

Research Conclusions

- Multiple and varied regulatory and contractual compliance requirements are verified as imposed on organizations.
- A lower number of organizations are impacted by third party program requirements than was originally expected.
- Negative and positive impacts of third party compliance requirements are identified.
- Where applicable, time and frequency dedicated to external content appears to be much less than internal content.
- The title of ISATE program efforts in organizations is very diverse.
- Definitions of awareness, training and education vary in respondent organizations.
- ISATE programs are documented in a variety of organizational methods.
- Respondents may consider accepting standard definitions for awareness, training and education.
- Organizationally-relevant program content is highly important.
- Program topics supporting organizational relevance reflect traditional and contemporary content were identified.

Based on these conclusions, a proposed Standard Content Definition Framework (SCDF) was recommended. This framework, detailed in design but simple in execution, may be effectively used by virtually any organization to standardize and measure

program success. The framework presents recommendations for program titles and then recommends synthesized and consistent definitions for awareness, training and education.

Awareness: content delivered formally or informally to all individuals on a scheduled or emergency basis; includes organizational relevance and delivers basic information about current/emerging events, threats, trends or risks.

Training: content delivered formally on a scheduled basis to specific individuals based on job role; includes organizational relevance and delivers a formal learning process emphasizing risk management and compliance with regulatory/contractual requirements.

Education: content delivered formally on a scheduled basis to specific individuals based on job role; includes organizational relevance emphasizing specialized certifications, credentials or targeted risk management techniques or technologies.

Recommendations for organizational relevance in content and meaningful metrics are further presented in the framework. The framework, while simple in design, is believed to be an original contribution to information/cyber security practitioners, with findings of interest to academic researchers, standards/framework bodies, auditing/risk management practitioners and learning/development specialists.

Appendix A

Regulatory and Contractual ISATE Requirement Examples

C-TPAT (Customs-Trade Partnership Against Terrorism)
COPPA (Children's Online Privacy Protection Act)
ECPA (Electronic Communications Privacy Act)
EFTA (Electronic Fund Transfer Act, Regulation E)
FACTA and FCRA (Fair and Accurate Credit Transaction Act (FACTA), including Red
Flags Rule; Federal Rules of Civil Procedure (FRCP)
FAST (Free and Secure Trade Program)
FFIEC (Federal Financial Institutions Examination Council)
FISMA (Federal Information Security Management Act)
FCPA (Foreign Corrupt Practices Act)
GLBA (Gramm-Leach-Bliley Act)
HIPAA/HITECH (Health Insurance Portability and Accountability Act/Health
Information Technology for Economic and Clinical Health Act)
IRS 1075 (Internal Revenue Service Publication 1075, Tax Information Security
Guidelines for Federal, State and Local Agencies)
NERC (North American Electric Reliability Corporation)
NIST 800-53 (National Institute of Standards and Technology Special Publication
Security and Privacy Controls for Federal Information Systems and Organizations)
PCI DSS (Payment Card Industry Data Security Standard)
SOX (Sarbanes-Oxley Act)
SSNPA (Social Security Number Protection Act)
State laws as applicable within the United States

Appendix B

Regulatory and Contractual Language Examples

Requirement	Language/Description
Sarbanes-Oxley Act of 2002 (SOX)	<p>This act applies to accounting firms and any organization that manages financial records. Failure to comply may result in financial penalties. The Public Company Accounting Oversight Board (PCAOB) is charged with overseeing, regulating and disciplining (Dunlap, Cummings & Janicki, 2017).</p> <p>Title III Section 302 (a)(4): (A) Establishing and maintaining internal controls; (B) Designed internal controls to ensure material information is made known to officers. The SEC derives compliance from Section 404 of COBIT in section DS 7.2, Appoint trainers and organize training sessions on a timely basis. Registration attendance and performance evaluations should be recorded (Herold, 2010).</p>
Health Insurance Portability and Accountability Act of 1996 (HIPAA)/ Health Information Technology for Economic and Clinical Health (HITECH) Act	<p>HIPAA applies to any and all offices which handle patient healthcare data while protecting a patient’s personal health information. Health and Human Service’s Office of Civil Rights is charged with enforcing these regulations (Dunlap, Cummings & Janicki, 2017). Protections apply to covered entities (CEs), including healthcare providers, health plans, healthcare clearinghouses and business associates.</p> <p>HIPAA consists of five sections, one of which addresses information privacy and security and contains the Privacy Rule and Security Rule. The Privacy Rule focuses on policies and procedures that give individuals greater rights and privacy protections for health information and applies to all formats of PHI: electronic, paper, and oral. The Security Rule protects electronic health information specifically and applies to entities that create, maintain, or transmit PHI. The Security Rule requires that entities ensure the confidentiality, integrity, and availability of electronic PHI, protect PHI against reasonably anticipated threats and inappropriate use or disclosure, and ensure employee compliance with the regulation requirements (Herold, 2010).</p> <p>HITECH was passed in 2009 to better safeguard patient PHI and enforce the Security Rule. It expanded the definition of CE’s which must adhere to HIPAA and increased noncompliance penalties. It also expanded patients’ rights related to access and use of PHI and breach notification (Herold, 2010; Martin, Imboden & Green, 2015).</p>

NIST 800-53	The organization provides basic security awareness training (NIST, 2013). The derivative US Cybersecurity Framework of 2014, section Protect/Awareness and Training (PR.AT) requirements state “The organization’s personnel/partners are provided cybersecurity awareness education and are adequately trained to perform duties and responsibilities consistent with related policies, procedures and agreements” (The White House, 2014).
State laws	<p>NCSL indicates that over 170 new cybersecurity laws have been introduced across 37 states in 2015-2016. This shows the ever-evolving landscape of legislation that organizations must address (Dunlap, Cummings & Janicki, 2017).</p> <p>As example, Massachusetts Data Security Law (201 CMR 17.03(2)) requires a comprehensive security program containing administrative, physical and technical safeguards and ongoing employee (including temporary and contract employee) training to identifying and assess reasonably foreseeable internal and external risks; Massachusetts Data Security Law (201 CMR 17.04 (8)) requires education and training of employees on the proper use of the computer security system and the importance of personal information security (Radke & Waters, 2015). New York State 23 NYCRR 500 says Section 500.10, “Cybersecurity Personnel and Intelligence,” requires each Covered Entity to utilize qualified cybersecurity personnel of the Covered Entity, an Affiliate, or a Third Party Service Provider; provide such personnel with cybersecurity updates and training; and verify that key cybersecurity personnel take steps to maintain current knowledge of changing cybersecurity threats and countermeasures. Section 500.14, “Training and Monitoring,” requires each Covered Entity to implement risk-based policies to monitor the activity of Authorized Users and detect unauthorized access or use of Nonpublic Information, and to provide regular cybersecurity awareness training for all personnel (NYDFS, 2017).</p>
PCI DSS Version 3.1, § 12.6 (PCI DSS, 2014)	Implement a formal security awareness program to make all personnel aware of importance of cardholder data security. A full description is found at <i>Information Supplement: Best Practices for Implementing Security Awareness Program</i> (PCI SSC, 2014).

Appendix C

IS Standards, Guidelines and Frameworks

COBIT (Control Objectives for Information and Related Technology)
Cybersecurity Framework Act of 2014
ISO/IEC 27001:2005 (Information Security Management System - Requirements)
ISO/IEC 27002:2005 (Code of Practice for Information Security Management)
ITIL (Information Technology Infrastructure Library)
NIST 800-30 (Guide for Conducting Risk Assessments)
NIST 800-39 (Managing Information Security Risk)
NIST 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations)
NIST 800-61 (Computer Security Incident Handling Guide)
SANS (SysAdmin, Audit, Network and Security) Institute

Appendix D

IRB Approval 2017-308: Proceed with Study



MEMORANDUM

To: Theresa M Curran
College of Engineering and Computing

From: Ling Wang, Ph.D.,
Center Representative, Institutional Review Board

Date: May 3, 2017

Re: IRB #: 2017-308; Title, "Standardizing instructional definition and content supporting information security compliance requirements"

I have reviewed the above-referenced research protocol at the center level. Based on the information provided, I have determined that this study is exempt from further IRB review under **45 CFR 46.101(b) (Exempt Category 2)**. You may proceed with your study as described to the IRB. As principal investigator, you must adhere to the following requirements:

- 1) **CONSENT:** If recruitment procedures include consent forms, they must be obtained in such a manner that they are clearly understood by the subjects and the process affords subjects the opportunity to ask questions, obtain detailed answers from those directly involved in the research, and have sufficient time to consider their participation after they have been provided this information. The subjects must be given a copy of the signed consent document, and a copy must be placed in a secure file separate from de-identified participant information. Record of informed consent must be retained for a minimum of three years from the conclusion of the study.
- 2) **ADVERSE EVENTS/UNANTICIPATED PROBLEMS:** The principal investigator is required to notify the IRB chair and me (954-262-5369 and Ling Wang, Ph.D., respectively) of any adverse reactions or unanticipated events that may develop as a result of this study. Reactions or events may include, but are not limited to, injury, depression as a result of participation in the study, life-threatening situation, death, or loss of confidentiality/anonymity of subject. Approval may be withdrawn if the problem is serious.
- 3) **AMENDMENTS:** Any changes in the study (e.g., procedures, number or types of subjects, consent forms, investigators, etc.) must be approved by the IRB prior to implementation. Please be advised that changes in a study may require further review depending on the nature of the change. Please contact me with any questions regarding amendments or changes to your study.

The NSU IRB is in compliance with the requirements for the protection of human subjects prescribed in Part 46 of Title 45 of the Code of Federal Regulations (45 CFR 46) revised June 18, 1991.

Cc: Gertrude Abramson, Ed.D.
Ling Wang, Ph.D.

Appendix E

IRB Letter to IASAP



Standardizing Instructional Definition and Content Supporting Information Security Compliance Requirements

Principal investigator: Terri (Theresa) Curran Doctoral Candidate Nova Southeastern University College of Engineering and Computing (CEC) 3301 College Avenue Fort Lauderdale FL 33314 617-686-6398	Co-investigator: Dr. Gertrude Abramson Professor Emeritus, Information Systems Nova Southeastern University College of Engineering and Computing (CEC) 3301 College Avenue Fort Lauderdale FL 33314 954-262-2070
---	--

Institutional Review Board (IRB)
Nova Southeastern University
3301 College Avenue Fort Lauderdale, FL 33314
IRB@nsu.nova.edu

Description of Study: Terri Curran is a doctoral candidate at Nova Southeastern University engaged in research for the purpose of satisfying a requirement for the Doctor of Philosophy (Ph.D.) in Information Systems/Information Security (IS) degree. As principal investigator, she is ready to issue a web-based research survey that will provide data to inform her final research.

- The research survey will obtain information about the current state of IS programs, content, frameworks, importance of organizational relevance and compliance mandates affecting organizations.
- Based on survey results, a prototype framework and content definitions will be proposed that could support global security compliance program efforts based on prevalent regulatory and contractual regulations.

How You Can Help: International Association of Information Security Awareness Practitioners (IASAP) leadership and executive board members have agreed to support this research by participating in an online survey via a Zoho web portal (<https://www.zoho.com/survey/>). IASAP participation and support is sincerely appreciated.

Survey Specifics: The survey will take approximately thirty minutes to complete. The survey URL will be provided by IASAP leadership to provide anonymity and reiterate management/board support for the research. The target participation rate is 30% (80 members representing 40 organizations). A three-week turnaround time for responses will be provided. Participants will be allowed to start and save the survey for convenience.

Participation Benefits: There will be two benefits provided to participants: a short-term finding report to illustrate “current state” of IS program efforts and in the longer-term, a copy of the proposed framework developed as a result of research and survey data results. There is no cost for participation in this study. Participation is completely voluntary and no payment will be provided other than the two reports.

Confidentiality: Information obtained from the survey tool is confidential. Survey responses (data) are stored in secured Zoho facilities, and data is encrypted in transit. Responses will be maintained on Zoho for the duration of the research project. Once the project is deemed complete, survey data will be maintained for 36 additional months as per Nova Southeastern University IRB requirements. Responses will be stored in spreadsheets stored locally on a laptop, an attached hard drive and on Google Cloud backups. Survey questions have been developed to preserve confidentiality and reduce risk of information loss.

Institutional Approval: The Nova Southeastern University IRB has approved this survey (IRB # 2017-308).

If you have any questions regarding the survey or this research project in general, please contact Terri Curran or her advisor, Dr. Gertrude Abramson. If you have any questions concerning IASAP membership rights as research participants, please contact the IRB of Nova Southeastern University at:

Human Subjects Protection/Institutional Review Board
Nova Southeastern University
3301 College Avenue
Fort Lauderdale, FL 33314
(954) 262-5369/Toll Free: 866-499-0790
irb@nova.edu

Sincerely,



Terri (Theresa) Curran
Doctoral Candidate
CIPP, CISM, CISSP, CPP, CRISC
Email (NSU): TC722@mynsu.nova.edu
Mobile: 617-686-6398

Appendix F

Survey Questions, Detailed Responses and Analysis

Survey Introduction

October 2017

Dear IASAP colleague,

Thank you for participating in this survey! The responses you provide will inform my doctoral dissertation project. I appreciate the support IASAP has extended to me during my study and research.

This survey will ask about your organizational approach to information security awareness, training and education programs (called "programs" in the survey), with specific focus on:

- external (third party), US-based program requirements;
- perceived and/or actual impacts of external (third party) compliance requirements on your program;
- if your organization would accept a set of standard program definitions to meet internal/external compliance requirements;
- how important organizational relevance is within your program activities;
- and demographic information to be used for benchmarking purposes and context.

This survey should take less than 30 minutes to complete. Please respond within three (3) weeks of receipt of the survey. Your name/organization name will not be requested or used in any form. If you are part of a global organization, please respond ONLY for US-based program activities and compliance requirements. Future research may evaluate this problem in a global context.

There will be two benefits provided to you: a short-term finding report to illustrate "current state" of programs and in the longer-term, a copy of the proposed framework developed as a result of my research and this survey.

Let's start the survey! Thanks again for your help and support.

Terri Curran
Doctoral Candidate, Nova Southeastern University
tc722@mynsu.nova.edu

Before we start...

Does your organization conduct information security awareness, training and/or education efforts?

NOTE: if your answer is "No" or "Don't know/unsure", the survey will conclude.

- Yes
- No
- Don't know/unsure
- Other (please specify)

(If "No" or "Don't Know/Unsure", the survey branched to "thank you, goodbye" page.)

Section 1

This section examines external (third party), US-based regulatory and contractual information security requirements that are currently required at your organization. Regulatory compliance requirements might include state or Federal laws or standards (examples: GLBA or NIST). Contractual compliance requirements might include mandates for specific business activities (example: PCI DSS).

1.1 Please indicate **US regulatory compliance requirements** mandating you to provide programs. This means that you **MUST** provide awareness, training and/or education within your organization specific to these requirements. Please check all that apply for your US-based organization.

ANSWER CHOICES	RESPONSES
▼ Sarbanes-Oxley Act (SOX)	41.18% 21
▼ HIPAA/HITECH (Health Insurance Portability and Accountability Act/Health Information Technology for Economic and Clinical Health Act)	35.29% 18
▼ NIST 800-53 (National Institute of Standards and Technology Special Publication Security and Privacy Controls for Federal Information Systems and Organizations)	33.33% 17
▼ Don't know	21.57% 11
▼ State laws as applicable within the United States	21.57% 11
▼ Other (please specify) Responses	17.65% 9
▼ NERC (North American Electric Reliability Corporation)	17.65% 9
▼ GLBA (Gramm-Leach-Bliley Act)	13.73% 7
▼ FFIEC (Federal Financial Institutions Examination Council)	7.84% 4
▼ FACTA and FCRA (Fair and Accurate Credit Transaction Act (FACTA), including Red Flags Rule; Federal Rules of Civil Procedure (FRCP)	5.88% 3
▼ IRS 1075 (Internal Revenue Service Publication 1075, Tax Information Security Guidelines for Federal, State and Local Agencies)	5.88% 3
▼ FISMA (Federal Information Security Management Act)	3.92% 2
▼ Not applicable	3.92% 2
▼ None	3.92% 2
▼ EFTA (Electronic Fund Transfer Act, Regulation E) (4)	3.92% 2
▼ C-TPAT (Customs-Trade Partnership Against Terrorism)	3.92% 2
▼ SSNPA (Social Security Number Protection Act)	1.96% 1
▼ COPPA (Children's Online Privacy Protection Act)	1.96% 1
▼ ECPA (Electronic Communications Privacy Act)	1.96% 1
▼ FCPA (Foreign Corrupt Practices Act)	0.00% 0
▼ FAST (Free and Secure Trade Program)	0.00% 0
Total Respondents: 51	

Responses to this question informed RQ1: What US-based regulatory and contractual requirements impose internal and external ISATE program delivery?

Responses validate that varied regulatory compliance requirements are mandated in respondent organizations.

The most common regulatory requirements identified by survey respondents were SOX, HIPAA/HITECH, NIST 800-53, state security laws, GLBA and NERC CIP Standards.

Responses to “Other” included European Union (EU) General Data Protection Regulation (GDPR) Payment Card Industry Data Security Standard (PCI DSS), and state gaming regulations. The Federal Reserve Board (FRB) as influenced by the Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook, FFIEC Cybersecurity Awareness guidance (FFIEC, 2017) and Office of the Comptroller of the

Currency (OCC) requirements were also mentioned. It was felt these GDPR and PCI did not affect overall responses to this question, since GDPR was not considered part of the survey and PCI DSS is a contractual mandate as covered in question 1.2.

Eleven respondents indicated ‘Don’t know’ to this question, which could indicate confusion in the wording of the question or other condition. A “call for action” within their organizations may be sought to determine actual status. These responses could change results in subsequent surveys but validation is expected to remain the same.

1.2 Please indicate US **contractual compliance** requirements mandating you to provide programs. This means that you **MUST** provide awareness, training and/or education within your organization specific to these requirements. Please check all that apply for your US-based organization.

ANSWER CHOICES	RESPONSES
▼ PCI DSS (Payment Card Industry Data Security Standard)	58.82% 30
▼ HIPAA/HITECH (Health Insurance Portability and Accountability Act/Health Information Technology for Economic and Clinical Health Act)	37.25% 19
▼ Don't know	21.57% 11
▼ Third party (partner, provider, etc.)	15.69% 8
▼ Other (please specify) Responses	11.76% 6
▼ None	5.88% 3
▼ Not applicable	5.88% 3
Total Respondents: 51	

Responses to this question informed RQ1: What US-based regulatory and contractual requirements impose internal and external ISATE program delivery?

Responses validate that varied contractual compliance requirements are mandated in respondent organizations.

PCI DSS and HIPAA/HITECH were the most common regulatory requirements identified by survey respondents.

Eight respondents had contractual requirements to provide content to third parties in addition to PCI DSS and HIPAA/HITECH. This was a lower number than expected but felt sufficient for this research.

Responses to “Other” included mention of state gaming regulations, NERC, client contracts and New York state law. NERC requirements are covered in question 1.1. Additional responses were illustrative and did not affect overall responses to this question.

Eleven respondents indicated ‘Don’t know’ to this question, which could indicate confusion in the wording of the question or other condition. A “call for action” within their organizations may be sought to determine actual status. These responses could change results in subsequent surveys but validation is expected to remain the same.

Section 2

This section will ask questions intended to understand your internal program and perceived and/or actual impacts of external (third party) regulatory or contractual compliance requirements on your programs.

We'll start by focusing on *externally-mandated* program activities. A "No" or "Don't know/unsure" response here will bring you to the section of the survey dealing with internal program activities.

2.1 Please indicate if your organization has been required to provide **external** program content in the last 12 months. This means you had existing internal program content; you now need to provide new, separate and different instructions, concepts or language to participants.

ANSWER CHOICES	RESPONSES	
▼ No	65.96%	31
▼ Don't know/unsure	21.28%	10
▼ Yes	12.77%	6
TOTAL		47

[Comments \(2\)](#)

Responses to this question informed RQ2: What are the impacts of external (third party) requirements on current ISATE programs?

Responses validate that third party program content and delivery is mandated in respondent organizations.

Six responses indicated that external, third party content was required to be provided. This was a lower number than expected but felt sufficient for this research. An author bias was revealed here as the number of organizations impacted by third party requirements was anticipated to be much higher. Thirty-one respondents indicated that they were not impacted by external requirements.

Ten respondents indicated ‘Don’t know’ to this question, which could indicate confusion in the wording of the question or other condition. A “call for action” within their organizations may be sought to determine actual status. These responses could change results in subsequent surveys but validation is expected to remain the same.

Two comments indicated “We were not "required" to provide external program content, but as a community service, we have a version of our annual training on our website” and “(We were) required to include malicious insider training”.

2.2 If you were required to provide external program content, how did you incorporate it into your program?

ANSWER CHOICES	RESPONSES
▼ We added externally mandated regulatory and contractual content into our existing, internal program content, providing one content set.	42.86% 3
▼ We provided external content through separate program activities (for example, attending internal programs plus attending external PCI DSS or Red Flags).	28.57% 2
▼ We are in the process of figuring out how to deliver both types of programs.	14.29% 1
▼ We decided not to deliver external content.	14.29% 1
Total Respondents: 7	

Comments (1)

Responses to this question informed RQ2: What are the impacts of external (third party) requirements on current ISATE programs?

Responses validate that there is organizational impact in respondent organizations and explain how they provide external program content.

Responses were virtually equal among those integrating external content into existing programs or delivering content separately. Other respondents are in process or won't deliver external content at all.

One comment indicated "not applicable", but since 7 responses are accounted for, the comment did not affect overall responses to this question.

2.3 If you were required to provide external program content, please indicate actual or perceived impacts (positive or negative) of having new, separate and different instructions, concepts or language imposed on your organization.

	NO IMPACT (1)	LOW IMPACT (2)	MEDIUM IMPACT (3)	HIGH IMPACT (4)	TOTAL
Increased complexity of program management (negative impact)	14.29% 1	28.57% 2	57.14% 4	0.00% 0	7
Increased compliance tracking (negative impact)	14.29% 1	14.29% 1	57.14% 4	14.29% 1	7
Increased confusion about policy direction because of multiple policies to follow (negative impact)	28.57% 2	42.86% 3	28.57% 2	0.00% 0	7
Increased participation/attendance time (negative impact)	28.57% 2	14.29% 1	57.14% 4	0.00% 0	7
Increased budget requirements (negative impact)	28.57% 2	28.57% 2	42.86% 3	0.00% 0	7
Increased content management responsibilities (negative impact)	14.29% 1	0.00% 0	85.71% 6	0.00% 0	7
Increased understanding of external policies and procedures (positive impact)	14.29% 1	14.29% 1	57.14% 4	14.29% 1	7
Increased communications with third party (positive impact)	28.57% 2	42.86% 3	14.29% 1	14.29% 1	7
Improved compliance ratings/scores/assessment results (positive impact)	28.57% 2	0.00% 0	71.43% 5	0.00% 0	7

Comments (1)

Responses to this question informed RQ2: What are the impacts of external (third party) requirements on current ISATE programs?

Responses validate that there is organizational impact in respondent organizations and explain actual or perceived impacts (positive or negative).

No responses (either positive or negative) were felt to be of significant (high) organizational impact. Negative external content impacts fell primarily into the “medium impact” category and included:

- increased program management complexity;
- increased compliance tracking;
- increased confusion about policy direction;
- increased participation/attendance time
- increased budget requirements; and
- increased content management responsibilities.

Positive external content impacts fell primarily into the “medium impact” category and included:

- increased understanding of third party security requirements;
- increased communication with third parties; and
- improved compliance scores/ratings.

One respondent commented on the lack of a “not applicable” option.

2.4 If you were required to provide entirely new, external program content in the last 12 months, approximately how much time did each employee or contractor spend reviewing this program content?

	NONE	LESS THAN ONE HOUR	1-2 HOURS	3-5 HOURS	5-7 HOURS	7+ HOURS	TOTAL
Awareness	28.57% 2	57.14% 4	0.00% 0	14.29% 1	0.00% 0	0.00% 0	7
Training	42.86% 3	42.86% 3	0.00% 0	14.29% 1	0.00% 0	0.00% 0	7
Education	42.86% 3	42.86% 3	14.29% 1	0.00% 0	0.00% 0	0.00% 0	7

[Comments \(2\)](#)

Responses to this question informed RQ2: What are the impacts of external (third party) requirements on current ISATE programs?

Responses validate that third party program content and delivery exist in organizations and explain the duration of delivery time participation. It is an assumption that these times are an incremental increase to existing internal program efforts.

For awareness activities, the majority participated in less than one hour’s time. Two did not provide awareness and one provided 3-5 hours of awareness content. Six indicated no time or less than one hour for training activities; one participant indicated 3-5 hours. A close match is observed for education, with accounted for no time or less than one hour for educational activities; one participant indicated 1-2 hours. One respondent indicated “this will occur in the coming 12 months” and another indicated “not applicable”.

Since this is the first assessment of external content provisioning and impact, these numbers may serve as indicative of what other organizations might expect to provide in the future. The key is in the question: “entirely new, external program content”.

2.5 If you were required to provide entirely new, external program content in the last 12 months, how frequently was each employee or contractor required to attend these activities?

	NONE (1)	WEEKLY (2)	MONTHLY (3)	QUARTERLY (4)	ANNUALLY (5)	SEMI-ANNUALLY (6)	TOTAL
▼ Awareness	57.14% 4	0.00% 0	0.00% 0	14.29% 1	28.57% 2	0.00% 0	7
▼ Training	42.86% 3	0.00% 0	0.00% 0	0.00% 0	57.14% 4	0.00% 0	7
▼ Education	57.14% 4	0.00% 0	14.29% 1	0.00% 0	28.57% 2	0.00% 0	7

Comments (2)

Responses to this question informed RQ2: What are the impacts of external (third party) requirements on current ISATE programs?

Responses validate that third party program content and delivery exist in organizations and explain the frequency of delivery time participation.

The question asks about *annual* requirements. For awareness activities, a surprising majority did not indicate participation. Training activities are also surprising with only 4 organizations reporting annual participation. Education was not provided to over ½ of responding organizations; one provided training monthly and two participated annually. As with question 2.4, one respondent indicated “this will occur in the coming 12 months” and another indicated “not applicable”. Followup is needed to understand why the requirement to provide new program content exists but is not seen as being delivered within a regular cadence.

Since this is the first assessment of external content provisioning and impact, these numbers may serve as indicative of what other organizations might expect to provide on a recurring basis. The “None” category would be expected to change over time.

We'll now focus on your *internal* program activities.

2.6 In the last 12 months, approximately how much time did each employee or contractor spend on existing internal program activities?

	NONE (1)	LESS THAN ONE HOUR (2)	1-2 HOURS (3)	3-5 HOURS (4)	5-7 HOURS (5)	TOTAL	
▼ Awareness	2.27% 1		31.82% 14	45.45% 20	15.91% 7	4.55% 2	44
▼ Training	4.55% 2		40.91% 18	43.18% 19	9.09% 4	2.27% 1	44
▼ Education	5.00% 2		37.50% 15	50.00% 20	7.50% 3	0.00% 0	40

Comments (3)

Responses to this question informed RQ2: What are the impacts of external (third party) requirements on current ISATE programs?

Responses validate that internal program content and delivery requirements exist in organizations and explain duration of delivery time participation.

More clearly defined program resource and timing requirements emerge than were identified with external content delivery. For awareness, the wide majority of the 44 respondents indicated participation as less than one hour to 5 hours. Training requirements followed suit with a slightly higher percentage of respondents indicating less training provided. Only 40 responded to education requirements with high concentration in less than one hour to 3-5 hours.

The question asks about *annual* requirements. Two respondents commented that “Our program is not mandatory for all, so employees devote different amounts of time to it, and not all participate”; “(This is) estimated but difficult to assess since it’s a mixture of direct, indirect and varies across XXX locations” (number of locations sanitized to provide anonymity). One additional respondent indicated this question was not applicable.

Since this is the first assessment of internal content provisioning and impact, these numbers may serve a baseline or metric indicator of what other organizations provide on an annual basis. The “None” category would be expected to change over time.

2.7 In the last 12 months, how frequently was each employee or contractor required to attend existing internal program activities?

	NONE (1)	WEEKLY (2)	MONTHLY (3)	QUARTERLY (4)	SEMI-ANNUALLY (5)	ANNUALLY (6)	TOTAL RESPONDENTS
Awareness	42.86% 18	2.38% 1	14.29% 6	16.67% 7	4.76% 2	19.05% 8	42
Training	26.19% 11	0.00% 0	0.00% 0	7.14% 3	7.14% 3	61.90% 26	42
Education	45.24% 19	0.00% 0	4.76% 2	7.14% 3	4.76% 2	40.48% 17	42

Comments (3)

Responses to this question informed RQ2: What are the impacts of external (third party) requirements on current ISATE programs?

Responses validate that internal program content and delivery exist in organizations and explain the cadence of delivery time participation.

More clearly defined program resource and timing requirements emerge than were identified with external content delivery. The question asks about *annual* requirements. Forty-two respondents indicated a wide range of annual requirements. Awareness responses were spread across an annual measurement, with the wide majority indicating that no awareness activities were conducted. Training responses were primarily “annually”. Education was primarily none or annually.

Comments included “It varies with each employee”; “(These) answers reflect a projection, as only training is required - awareness and education are support activities; and “NERC CIP impacted employees require annual awareness and training, quarterly education”.

Section 3

This section proposes standard definitions of awareness, training and education based on many of the contractual and regulatory requirements discussed earlier in this survey.

3.1 What words most closely describe your overall US-based program?

ANSWER CHOICES	RESPONSES	
▼ Awareness training program	40.48%	17
▼ Awareness education	16.67%	7
▼ Other (please specify)	14.29%	6
▼ Awareness	9.52%	4
▼ Security education	9.52%	4
▼ Training and education	7.14%	3
▼ Formal awareness training	2.38%	1
TOTAL		42

Responses to this question informed RQ3: What ISATE program definitions are currently used?

Responses validate that responses validate that differing program titles are in use within US-based organizations.

Forty-two responses substantiate that differences exist in definitions of awareness, training and education. Most call their efforts “awareness training program”; this may be due to use of this term in common regulatory and contractual requirements. Six comments help shed light on the diversity of the program definition within organizations:

- Awareness (we push info out via articles, etc.) and training (CBTs, etc.);
- Security Awareness and Education (training falls under education);
- Information Security Awareness and Training;
- Security Training and Awareness Program;
- Education and Awareness; and
- Cyber Security Awareness and Education.

Use of term “cyber” is discussed in Chapter 5.

3.2 Is this a close definition of **awareness** activities in your organization? If not, do you have a definition?

Awareness: dialogue, collaboration and response to posters, presentations, emails; using personal interaction, visual cues and prior experience to make decisions about IS-related behaviors. (An example of awareness content would be “We have seen an increase in phishing attempts. Here is how you can recognize them”.)

ANSWER CHOICES	RESPONSES	
▼ Yes, this is close to what we call "awareness"	78.05%	32
▼ We don't have a formal definition	14.63%	6
▼ Other (please specify) Responses	4.88%	2
▼ No, we use something totally different	2.44%	1
TOTAL		41

Responses to this question informed RQ3: What ISATE program definitions are currently used?

Responses validate that the proposed definition would have wide acceptance within respondent program content and/or frameworks.

Additional respondent feedback included “Security Awareness is not limited to just IS-related issues; it's physical, technical and national security based” and “The given definition but also specifically includes computer based training and annual campaigns”.

3.3 Is this a close definition of **training** activities in your organization? If not, do you have a definition?

Training: one-way instruction tested (T/F), measured (pass rates and attendance) and tracked. Training may be administered through annual or onboarding processes as mandated by contractual and regulatory requirements. (An example of training content would be “You can only share social security numbers with others based on policy and your job role”.)

ANSWER CHOICES	RESPONSES	
▼ Yes, this is close to what we call "training"	70.73%	29
▼ We don't have a formal definition	21.95%	9
▼ Other (please specify) Responses	4.88%	2
▼ No, we use something totally different	2.44%	1
TOTAL		41

Responses to this question informed RQ3: What ISATE program definitions are currently used?

To a lesser degree than in 3.2, responses validate that the proposed definition would have wide acceptance within respondent program content and/or frameworks. A slightly larger number of respondents do not have a training definition.

Two responses indicated “Our training is part of the annual employee required modules (interactive videos and vignettes) in ten key areas and includes affirming compliance statements” and “We don't have a formal definition, but for this survey I am considering training to be our phishing drills”.

3.4 Is this close to your current definition of **education** in your organization? If not, do you have a definition?

Education: mix of passive and/or active instruction to enhance skills for a specific job role. Education may be required by contractual and regulatory requirements or through role competency requirements. (An example of educational content would be “You must develop secure website applications by learning detailed and complex coding techniques to prevent database and website application breaches.”)

ANSWER CHOICES	RESPONSES	
Yes, this is close to what we call "education"	52.50%	21
We don't have a formal definition	40.00%	16
Other (please specify)	Responses 5.00%	2
No, we use something totally different	2.50%	1
TOTAL		40

Responses to this question informed RQ3: What ISATE program definitions are currently used?

To a far lesser degree than in 3.1 and 3.2, responses validate that the proposed definition would have moderate acceptance within respondent program content and/or frameworks. A much larger number of respondents do not have an education definition.

Two comments included ‘ours is not specific to a job role’ and “We don't have a formal definition, but for this survey I am considering education to be online courses in our LMS”.

3.5 Where is your program defined and/or explained in your organization?

ANSWER CHOICES	RESPONSES	
We define our current program in a security or other company policy	40.00%	16
We define our current program in both company policies and awareness/training/educational content	35.00%	14
We define our current program in a program charter or other document	22.50%	9
We define our current program in awareness/training/educational content	20.00%	8
We have defined our current program informally but it is not documented anywhere	20.00%	8
Other (please specify)	Responses 2.50%	1
Total Respondents: 40		

Responses to this question informed RQ3: What ISATE program definitions are currently used?

This question was developed to understand where the ISATE program is defined and/or mandated. The purpose was to identify if in fact the program was documented. One comment stated that “NERC CIP is defined in policy”.

Section 4

This section has two purposes. First, it identifies the need for organizational relevance about information security topics in your organization. This means information is provided about internal trends, risks, threats or changes, not externally-mandated content. (Example: your organization includes information about real and actual phishing or malware issues that have been experienced.) Secondly, this section examines if your organization would adopt standard program definitions.

4.1 How important is organizational relevance in your current program content and activities?

	HIGHLY IMPORTANT; WE MUST INCLUDE ORGANIZATIONAL INFORMATION	SOMEWHAT IMPORTANT; WE INCLUDE ORGANIZATIONAL INFORMATION IF CONVENIENT	NOT AT ALL IMPORTANT; WE PURCHASE CONTENT AND DELIVER "AS IS" WITHOUT ORGANIZATIONAL INFORMATION	WE HAVE NOT CONSIDERED INCLUDING SPECIFIC ORGANIZATIONAL INFORMATION	WE DON'T PROVIDE THIS CONTENT CURRENTLY	TOTAL
Awareness	45.00% 18	50.00% 20	0.00% 0	5.00% 2	0.00% 0	40
Training	45.00% 18	45.00% 18	2.50% 1	5.00% 2	2.50% 1	40
Education	30.00% 12	60.00% 24	0.00% 0	5.00% 2	5.00% 2	40

Comments (0)

Responses to this question informed RQ4: Is organizationally-relevant ISATE program content important?

Responses validate that that organizations require organizational relevance in their program content.

“Highly important” and “somewhat important” support is indicated for inclusion of organizational relevance in program content. A wide majority consider organizational relevance as highly or somewhat important in awareness activities; a slightly lesser number of respondents felt organizational relevance as highly or somewhat important in their training activities; and a decrease is seen in the number of respondents indicating organizational relevance as highly important in their education activities.

4.2 What current program topics are important to your organization? Please check all that apply for your US- based organization.

ANSWER CHOICES	RESPONSES	
▼ "Who to call" instructions and procedures	87.50%	35
▼ Providing clear explanation of internal policies	72.50%	29
▼ Sharing recent internal risks that have been identified	67.50%	27
▼ Sharing "WIFM: what's in it for me?" concepts	57.50%	23
▼ Describing personal roles and responsibilities	55.00%	22
▼ Explaining reasons for internal policies	35.00%	14
▼ Balancing internal and external compliance requirements	30.00%	12
▼ Explaining penalties for violating internal policies	25.00%	10
▼ Describing internal management support	15.00%	6
▼ Other (please specify)	Responses 12.50%	5
▼ Explaining differences in security-related laws and regulations	5.00%	2
Total Respondents: 40		

Responses to this question informed RQ4: Is organizationally-relevant ISATE program content important?

Responses validate that that organizations require organizational relevance in their program content.

The survey did not ask where these topics were provided or treated (awareness, training or education); this should have been included but now could be considered for further research and/or analysis. If following the definitions suggested in this paper, one could assume these topics would be considered in awareness: "Who to call" instructions and procedures" and "Sharing recent internal risks that have been identified". The remainder could be considered for inclusion in training or education. "Other" responses were interesting and illustrative. "personal security topics (keep kids safe online, identity theft, home routers, etc.)"; "not policy based at the moment"; "Our topics of focus are pretty flexible to what is a likely attack vector we want to defend against"; "Security best practices"; and "Educating on avoidance of threats".

4.3 Would your organization adopt this definition of **awareness**?

Awareness: content mostly customized to organizational culture, relevance and current threats/risks; informal; focused on current events, threats, trends and risks affecting the organization.

ANSWER CHOICES	RESPONSES	
▼ Yes	57.50%	23
▼ Don't know/unsure	32.50%	13
▼ No	7.50%	3
▼ Other (please specify)	Responses 2.50%	1
TOTAL		40

Responses to this question informed RQ5: Will organizations accept standard definitions of awareness, training and education?

Responses validate that that organizations would accept the proposed definition of awareness as part of their program efforts.

Twenty-three respondents would accept this definition of awareness. One responder felt “Use of “mostly” is problematic and unnecessary”; this wording was duly noted and adjusted. For those responding “Don’t know/unsure”, additional research could identify possible reasons this is the case. Only 3 responded “No”, indicating a higher level of acceptance than training and education responses (6 responses for each definition).

4.4 Would your organization adopt this definition of **training**?

Training: Internal and external content synthesized into one program focused on formal learning process; limited treatment of organizational culture, relevance and current threats/risks”.

ANSWER CHOICES	RESPONSES	
▼ Yes	43.59%	17
▼ Don't know/unsure	41.03%	16
▼ No	15.38%	6
TOTAL		39

Responses to this question informed RQ5: Will organizations accept standard definitions of awareness, training and education?

Responses validate that that organizations would accept the proposed definition of training as part of their program efforts. However, responses to this definition were not as definitive as those for awareness.

Seventeen respondents indicated the definition would be acceptable, but 16 responded “Don’t know/unsure”. The number of “No” responses doubled to 6. Additional research could identify possible reasons this is the case. Comments included “Yes, mostly; however, we are so large, the idea of “one program” doesn't quite fit”; “Organizational culture would be part of main focus”; and “Organizational culture is important in our environment”. One respondent noted “limited treatment ...” is not acceptable language. This was duly noted but left as-is.

4.5 Would your organization adopt this definition of **education**?

Education: role-based, specialized learning customized for risk management (secure code training, for example); very little treatment of organizational culture.

ANSWER CHOICES	RESPONSES
▼ Yes	48.72% 19
▼ Don't know/unsure	33.33% 13
▼ No	15.38% 6
▼ Other (please specify)	Responses 2.56% 1
TOTAL	39

Responses to this question informed RQ5: Will organizations accept standard definitions of awareness, training and education?

Responses validate that that organizations would accept the proposed definition of training as part of their program efforts. However, responses to this definition were not as positive as those for awareness.

Responses to this question were similar to 4.4. The responses to this definition were not as definitive as those for awareness. Nineteen indicated the definition posed would be acceptable, but thirteen responded “Don’t know/unsure”. As with the definition for training, six respondents stated they would not accept this definition. One responder indicated “organization culture statement would be removed in our version”. This was duly noted but left as-is.

You're almost done with the survey!

Section 5

This section will ask questions about your US-based organization for demographic purposes and context ONLY.

5.1 What is your organization's primary business function?

ANSWER CHOICES	RESPONSES	
▼ Energy	15.38%	6
▼ Financial Services/Banking (including Loyalty Services)	15.38%	6
▼ Healthcare and Public Health	12.82%	5
▼ Manufacturing	12.82%	5
▼ Consumer Goods	7.69%	3
▼ Insurance	7.69%	3
▼ Technology	7.69%	3
▼ Public Utility	5.13%	2
▼ Retail	5.13%	2
▼ Hospitality	2.56%	1
▼ Consulting	2.56%	1
▼ Other (please specify) Responses	2.56%	1
▼ Telecommunications	2.56%	1
▼ Food and Agriculture	0.00%	0
▼ Commercial	0.00%	0
▼ Dams	0.00%	0
▼ Defense	0.00%	0
▼ Education	0.00%	0
▼ Emergency Services	0.00%	0
▼ Nuclear (Reactors, Materials and Waste)	0.00%	0
▼ Outsourcing Services	0.00%	0
▼ Chemicals	0.00%	0
▼ Engineering/Construction Management	0.00%	0
▼ Entertainment/Media	0.00%	0
▼ Communications	0.00%	0
▼ Transportation	0.00%	0
▼ Water & Wastewater	0.00%	0
▼ Government Facilities	0.00%	0
TOTAL		39

Questions in Section 5 were designed to gather demographic information for practitioners to use while baselining their organizational programs. One respondent should not have participated in this question (“We are NOT a US based organization”).

5.2 How many employees and contractors participate in your programs (US-based only, please)?

ANSWER CHOICES	RESPONSES	
▼ 10,000+	64.10%	25
▼ 5,000 - 9,999	15.38%	6
▼ 50 - 999	10.26%	4
▼ 1000 - 4,999	10.26%	4
▼ 1 - 49	0.00%	0
▼ Don't know	0.00%	0
TOTAL		39

Questions in Section 5 were designed to gather demographic information for practitioners to use while baselining their organizational programs.

5.3 Please indicate information security guidelines, standards or other frameworks used in your overall program. Please check all that apply for your US-based organization.

ANSWER CHOICES	RESPONSES
▼ NIST 800-39 (Managing Information Security Risk)	51.28% 20
▼ NIST 800-30 (Guide for Conducting Risk Assessments)	41.03% 16
▼ NIST 800-61 (Computer Security Incident Handling Guide)	41.03% 16
▼ NIST 800-53 (Security and Privacy Controls for Federal Information Systems and Organizations)	41.03% 16
▼ SANS (SysAdmin, Audit, Network and Security) Institute	33.33% 13
▼ ISO/IEC 27001:2005 (Information Security Management System - Requirements)	30.77% 12
▼ ITIL (Information Technology Infrastructure Library)	30.77% 12
▼ NIST 800-37 (Guide for Applying the Risk Management Framework to Federal Information Systems)	28.21% 11
▼ ISO/IEC 27002:2005 (Code of Practice for Information Security Management)	25.64% 10
▼ OWASP (Open Web Application Security Project)	23.08% 9
▼ COBIT (Control Objectives for Information and Related Technology)	23.08% 9
▼ Cybersecurity Framework Act of 2014	15.38% 6
▼ Other (please specify) Responses	12.82% 5
▼ SIG (Shared Assessments Group - Standardized Information Gathering)	12.82% 5
▼ HITRUST (Health Information Trust Alliance)	10.26% 4
▼ ISF (Information Security Forum)	2.56% 1
▼ AUP (Shared Assessments Group - Agreed Upon Procedures)	2.56% 1
Total Respondents: 39	

Questions in Section 5 were designed to gather demographic information for practitioners to use while baselining their organizational programs. One respondent indicated “EU GDPR (General Data Protection Regulation) is underway”; two indicated NERC CIP Reliability Standards/NERC CIP V6; and one stated “FFIEC IT Booklets (Information Security)”.

5.4 What organizational units are responsible for managing and administering your program? Please check all that apply for your US-based organization.

ANSWER CHOICES	RESPONSES
Information Security	84.62% 33
Risk Management	20.51% 8
Information Technology	15.38% 6
Human Resources	12.82% 5
Legal	12.82% 5
Other (please specify) Responses	12.82% 5
Physical Security	10.26% 4
Internal Audit	7.69% 3
Finance/CFO	2.56% 1
CEO	2.56% 1
COO	0.00% 0
Total Respondents: 39	

Questions in Section 5 were designed to gather demographic information for practitioners to use while baselining their organizational programs.

5.5 Do you develop program content in-house or do you purchase/source it externally?

	FULLY DEVELOPED IN-HOUSE (BUILD)	COMPLETELY ACQUIRED FROM A THIRD PARTY (BUY)	MIXED (HYBRID) APPROACH (BUILD AND BUY)	WE DON'T PROVIDE THIS CONTENT CURRENTLY	DON'T KNOW/UNSURE	TOTAL
Awareness	46.15% 18	5.13% 2	48.72% 19	0.00% 0	0.00% 0	39
Training	18.92% 7	13.51% 5	64.86% 24	2.70% 1	0.00% 0	37
Education	23.68% 9	13.16% 5	55.26% 21	2.63% 1	5.26% 2	38

Comments (0)

Questions in Section 5 were designed to gather demographic information for practitioners to use while baselining their organizational programs.

Buy or build? This question sought to learn if respondents developed their own content or purchased it externally (hybrid approach), or a combination of both approaches. Eighteen respondents build awareness content in-house, while 19 use a hybrid (build and buy) approach. An interesting research follow-up would be to understand if the reason for building in-house awareness content is due to need for organizational relevance. Training and education content is largely obtained through a hybrid “build and buy” approach.

5.6 Do you utilize a project management office (PMO) role to manage program functions?

ANSWER CHOICES	RESPONSES	
Yes	20.51%	8
No	66.67%	26
Plan to in the future	0.00%	0
Don't know/unsure	7.69%	3
Other (please specify)	Responses 10.26%	4
Total Respondents: 39		

Questions in Section 5 were designed to gather demographic information for practitioners to use while baselining their organizational programs. Responses included “Considered a PMO lite. No direct office, but loosely organized”; “Only projects to bring in new tools, training, etc.”; “We use PMO for some programs - but NOT for security awareness program” and “HR manages the program functions”.

5.7 What organizational units or roles develop program content within your organization? Please check all that apply for your US-based organization.

ANSWER CHOICES	RESPONSES	
CISO (Corporate/chief information security officer)	66.67%	26
Privacy	53.85%	21
Physical Security	51.28%	20
Legal	43.59%	17
Risk Management	38.46%	15
Internal Audit	33.33%	13
Security Management Committee	30.77%	12
Human Resources	28.21%	11
CIO/CTO (Corporate/chief information or technology officer)	25.64%	10
Corporate Training/Learning	23.08%	9
Collaborative effort among departments	15.38%	6
Other (please specify)	Responses 10.26%	4
Finance/Treasury	5.13%	2
Don't know/unsure	5.13%	2
None	5.13%	2
Total Respondents: 39		

Questions in Section 5 were designed to gather demographic information for practitioners to use while baselining their organizational programs. Responses included “IT”, “retail divisions”, “Data Security and Cybersecurity” and “Functional areas within the electric utility”.

5.8 Do you have an information security oversight/governance committee that influences program content?

ANSWER CHOICES	RESPONSES	
▼ Yes, we have an oversight/governance committee	66.67%	26
▼ No, we do not have an oversight/governance committee	28.21%	11
▼ We are planning to establish an oversight committee	2.56%	1
▼ Other (please specify) Responses	2.56%	1
▼ We don't have plans for an oversight committee	0.00%	0
Total Respondents: 39		

Questions in Section 5 were designed to gather demographic information for practitioners to use while baselining their organizational programs. One respondent indicated “Yes we have both a governance function and an oversight committee, but they don't influence program content”.

5.9 What metrics are used to measure program activity? Please check all that apply for your US-based organization.

ANSWER CHOICES	RESPONSES	
▼ Learning management system (LMS) reports	76.92%	30
▼ Testing results	46.15%	18
▼ Annual policy attestation	43.59%	17
▼ Online survey	33.33%	13
▼ Completion certificates issued	28.21%	11
▼ URL tracking/statistics	28.21%	11
▼ Quarterly report to management	28.21%	11
▼ Classroom attendance sheets	25.64%	10
▼ Annual report to management	12.82%	5
▼ Other (please specify) Responses	10.26%	4
▼ We don't have program metrics	5.13%	2
▼ Performance appraisals	0.00%	0
Total Respondents: 39		

Questions in Section 5 were designed to gather demographic information for practitioners to use while baselining their organizational programs. Responses included “simulated phishing campaign results”; “Phishing system reporting”; and “phishing simulations”). One indicated “training compliance reports through our LMS system”.

5.10 What delivery mechanisms are used to provide program content?

	AWARENESS	TRAINING	EDUCATION	WE DON'T USE THIS DELIVERY MECHANISM	TOTAL RESPONDENTS
Web-based training (recorded)	48.72% 19	76.92% 30	46.15% 18	5.13% 2	39
Mobile-based training (recorded)	12.82% 5	17.95% 7	12.82% 5	69.23% 27	39
Guest speakers	71.79% 28	12.82% 5	23.08% 9	15.38% 6	39
Web-based training (live participation)	25.64% 10	23.08% 9	23.08% 9	48.72% 19	39
Mobile-based training (live participation)	5.13% 2	7.69% 3	5.13% 2	92.31% 36	39
Classroom sessions	23.08% 9	30.77% 12	46.15% 18	33.33% 13	39
Posters, other signage	92.31% 36	15.38% 6	23.08% 9	7.69% 3	39
Social media (YouTube, other)	48.72% 19	10.26% 4	15.38% 6	48.72% 19	39
Physical handouts ("desk drops")	74.36% 29	7.69% 3	28.21% 11	20.51% 8	39
Popup reminders ("tip of the day")	28.21% 11	5.13% 2	10.26% 4	71.79% 28	39
Banner messages (logon or real-time)	35.90% 14	5.13% 2	12.82% 5	64.10% 25	39
Open houses/special events	79.49% 31	10.26% 4	30.77% 12	17.95% 7	39
Videos	74.36% 29	35.90% 14	33.33% 13	17.95% 7	39

[Comments \(3\)](#)

Questions in Section 5 were designed to gather demographic information for practitioners to use while baselining their organizational programs. Responses included “CBTs were used”; “Buzz Sessions (team meetings) - primarily used for front line employees that don't have access to the company network”; and “Awareness and education emails (quarterly)”.

5.11 Please indicate if your US-based program includes privacy content.

	INFORMATION SECURITY TOPICS ONLY ARE INCLUDED	A COMBINATION OF INFORMATION SECURITY AND PRIVACY TOPICS ARE INCLUDED	PRIVACY TOPICS ARE COVERED IN A SEPARATE PROGRAM	WE DON'T DELIVER ANY PRIVACY CONTENT	TOTAL
▼ Awareness	7.69% 3	74.36% 29	7.69% 3	10.26% 4	39
▼ Training	2.56% 1	58.97% 23	20.51% 8	17.95% 7	39
▼ Education	2.56% 1	58.97% 23	25.64% 10	12.82% 5	39

Questions in Section 5 were designed to gather demographic information for practitioners to use while baselining their organizational programs. One respondent indicated that N/A should have been included as an option.

5.12 Please indicate if your US-based program includes physical security content.

	INFORMATION SECURITY TOPICS ONLY ARE INCLUDED	A COMBINATION OF INFORMATION AND PHYSICAL SECURITY TOPICS ARE INCLUDED	PHYSICAL SECURITY TOPICS ARE COVERED IN A SEPARATE PROGRAM	WE DON'T DELIVER ANY PHYSICAL SECURITY CONTENT	TOTAL
▼ Awareness	5.13% 2	71.79% 28	15.38% 6	7.69% 3	39
▼ Training	5.26% 2	60.53% 23	23.68% 9	10.53% 4	38
▼ Education	7.69% 3	51.28% 20	30.77% 12	10.26% 4	39

Questions in Section 5 were designed to gather demographic information for practitioners to use while baselining their organizational programs. Two comments stated “n/a” and one “NERC CIP requires a physical security role based training”.

Conclusion

Thank you for participating in this survey. After data collection and analysis, a short-term finding report to illustrate “current state” of programs will be provided, followed by a copy of the proposed framework. Your support is sincerely appreciated.

Terri

Please enter any questions, feedback or other comments below. Thanks!

References

- Al-Ahmad, W. & Mohammad, B. (2012). Can a single security framework address information security risks adequately? *International Journal of Digital Information and Wireless Communications (IJDIWC)*, 2(3), 222-230.
- Al-Khalifa, F., Kohun, F. & Skovira, R. (2015). A discussion about culture and information security policy compliance: a subculturally bound determinant – redefining the Hofstede hypothesis. *Issues in Information Systems*, 16(4).
- Alkhurayyif, Y. & Weir, G. (2017). Readability as a basis for information security policy assessment. In *Emerging Security Technologies (EST), 2017 Seventh International Conference* (114-121). IEEE.
- Ahmad, A., Alshaikh, M., Chang, S. & Maynard, S. B. (2016). Information security policy: a management practice perspective. In *Proceedings of the Australasian Conference on Information Systems (ACIS) 2015, Adelaide, South Australia*.
- Alshaikh, M., Maynard, S. B., Ahmad, A. & Chang, S. (2018). An exploratory study of current information security training and awareness practices in organizations. In *Proceedings of the 51st Hawaii International Conference on System Sciences*.
- Arachchilage, N., Love, S. & Beznosov, K. (2016). Phishing threat avoidance behaviour: an empirical investigation. *Computers in Human Behavior*, 60, 185-197.
- ASIS International (ASIS). *ASIS, ISC² and ISACA to Collaborate on Security Awareness Standard*. Retrieved from [https://www.asisonline.org/News/Press-Room/Press-Releases/2016/Pages/ASIS-International-\(ASIS\),-\(ISC\)-%C2%B2-and-ISACA-to-Collaborate-on--Security-Awareness-Standard.aspx](https://www.asisonline.org/News/Press-Room/Press-Releases/2016/Pages/ASIS-International-(ASIS),-(ISC)-%C2%B2-and-ISACA-to-Collaborate-on--Security-Awareness-Standard.aspx)
- Atoum, I., Otoom, A. & Abu Ali, A. (2014). A holistic cyber security implementation framework. *Information Management & Computer Security*, 22(3), 251-264.
- Auffret, J. P., Snowdon, J. L., Stavrou, A., Katz, J. S., Kelley, D., Rahman, R. S., ... & Warweg, P. (2017). Cybersecurity leadership: Competencies, Governance, and Technologies for Industrial Control Systems. *Journal of Interconnection Networks*, 17(01).
- Bamberger, K. & Mulligan, D. (2011). New governance, chief privacy officers, and the corporate management of information privacy in the United States: an initial inquiry. *Law & Policy*, 33(4), 477-508.
- Banfield, J. M. (2016). *A Study of Information Security Awareness Program Effectiveness in Predicting End-User Security Behavior* (Doctoral dissertation, Eastern Michigan University).

- Barton, K., Tejay, G., Lane, M. & Terrell, S. (2016). Information system security commitment: a study of external influences on senior management. *Computers & Security, 59*, 9-25.
- Bashroush, R., Schatz, D. & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *Journal of Digital Forensics, Security and Law, 12*(2), 8.
- Baxter, P. & Jack, S. (2008). Qualitative case study methodology: study design and implementation for novice researchers. *The qualitative report, 13*(4), 544-559.
- Bauer, S. & Bernroider, E. W. (2017). From information security awareness to reasoned compliant action: analyzing information security policy compliance in a large banking organization. *ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 48*(3), 44-68.
- Bauer, S., Bernroider, E. W., & Chudzikowski, K. (2017). Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. *Computers & Security, 68*, 145-159.
- Benbasat, I., Bulgurcu, B. & Cavusoglu, H. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.
- Bulgurcu, B., Cavusoglu, H. & Benbasat, I. (2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.
- Biener, C., Eling, M. & Wirfs, J. H. (2015). Insurability of cyber risk: an empirical analysis. *The Geneva Papers on Risk and Insurance Issues and Practice, 40*(1), 131-158.
- Caldwell, T. (2013). Setting the gold standard. *Computer Fraud & Security, 12*, 15-19.
- Cavallari, M. (2012). A conceptual analysis about the organizational impact of compliance on information security policy. In *International Conference on Exploring Services Science* (pp. 101-114). Springer Berlin Heidelberg.
- Cavusoglu, H., Cavusoglu, H., Son, J. Y., & Benbasat, I. (2015). Institutional pressures in security management: direct and indirect influences on organizational investment in information security control resources. *Information & Management, 52*(4), 385-400.
- Charmaz, K. (2014). *Constructing grounded theory*. Sage Publications. Kindle Edition.

- Chaudhry, P., Chaudhry, S., Clark, K. & Jones, D. (2013). Enterprise information systems security: a case study in the banking sector. In *Enterprise Information Systems of the Future* (206-214). Springer Berlin Heidelberg.
- Cho, J. Y. & Lee, E. H. (2014). Reducing confusion about grounded theory and qualitative content analysis: similarities and differences. *The Qualitative Report*, 19(32), 1.
- Collinson, M., Massacci, F., Ruprai, R., & Williams, J. (2016). Economic impacts of rules-versus risk-based cybersecurity regulations for critical infrastructure providers. *IEEE Security & Privacy*, 14(3), 52-60.
- Corbin, J. & Strauss, A. (2008). *Basics of qualitative research: Techniques and procedures for developing grounded theory*. Sage Publications.
- Corley, K. G. (2015). A commentary on “What Grounded Theory Is...” Engaging a phenomenon from the perspective of those living it. *Organizational Research Methods*, 18(4), 600-605.
- Cram, W., D’Arcy, J. & Proudfoot, J. (2017). Organizational information security policies: a review and research framework. *European Journal of Information Systems*, 1-37.
- Creswell, J. W. (2013). *Qualitative inquiry and research design: choosing among five approaches*. Sage Publications.
- Creswell, J. W. (2014). *Research design: Qualitative, quantitative, and mixed methods approaches*. Sage Publications.
- Cropper, J., Ullrich, J., Frühwirt, P. & Weippl, E. (2015). *The role and security of firewalls in internet as a service (IaaS) cloud computing*. In *Availability, Reliability and Security (ARES) Proceedings, 10th International Conference*, 70-79. IEEE.
- Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M. & Baskerville, R. (2013). Future directions for behavioral information security research. *Computers & Security*, 32, 90-101.
- Cruise Lines Industry Association (CLIA). (2016). Guidelines on cyber security onboard ships.
- Cunningham, M. (2016). Complying with international data protection law. *University of Cincinnati Law Review*, 2(84).

- Curran, T. [idlewellbay]. (2017, October 13). *Research project introduction and survey request to IASAP*. Retrieved from <https://www.youtube.com/watch?v=YAekZ3iO10>
- D'Arcy, J. & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. *European Journal of Information Systems*, 20(6), 643-658.
- D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, 20(1), 79-98.
- da Veiga, A. (2016). Comparing the information security culture of employees who had read the information security policy and those who had not. *Information & Computer Security*, 24 (2), 139-151.
- da Veiga, A. & Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Computers & Security*, 49, 162-176.
- da Veiga, A. & Martins, N. (2017). Defining and identifying dominant information security cultures and subcultures. *Computers & Security*, 70, 72-94.
- Department of Homeland Security (DHS) Financial Services Sector. (2014). *DHS Financial Services Sector*. Retrieved from <http://www.dhs.gov/financial-services-sector>.
- Dijkmans, C., Kerkhof, P. & Beukeboom, C. J. (2015). A stage to engage: social media use and corporate reputation. *Tourism Management*, 47, 58-67.
- DiMase, D., Collier, Z., Heffner, K. & Linkov, I. (2015). Systems engineering framework for cyber physical security and resilience. *Environment Systems and Decisions*, 35(2), 291-300.
- Duncan, B. & Whittington, M. (2014). Compliance with standards, assurance and audit: does this equal security? In *Proceedings of the 7th International Conference on Security of Information and Networks* (p. 77). ACM.
- Dunlap, L., Cummings, J. & Janicki, T. (2017). Information security and privacy legislation: current state and future direction. *Proceedings of the Conference on Information Systems Applied Research*, Austin Texas (Vol. 2167).
- Edwards, B., Hofmeyr, S., & Forrest, S. (2015). Hype and heavy tails: a closer look at data breaches. In *Workshop on the Economics of Information Security (WEIS) Proceedings*.

- European Union (EU). (2015). *General Data Protection Regulation (GDPR): Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. Brussels: Council of the European Union.
- Faily, S. & Ki-Aries, D. (2017). Persona-centred information security awareness. *Computers & Security*, 70, 663-674.
- Fagade, T. & Tryfonas, T. (2017). Hacking a bridge: an exploratory study of compliance-based information security management in banking organization. *Systemics, Cybernetics and Informatics*, 15(5), 74-80.
- Federal Financial Institutions Examination Council (FFIEC). (2014). *About the FFIEC*. Retrieved from <https://www.ffiec.gov/>
- Federal Financial Institutions Examination Council (FFIEC). (2016). *Information technology examination handbook: information security*. Retrieved from <https://ithandbook.ffiec.gov/it-booklets/information-security.aspx>
- Federal Financial Institutions Examination Council (FFIEC). (2017). *Cybersecurity awareness*. Retrieved from <https://www.ffiec.gov/cybersecurity.htm>
- Felt, A. P., Barnes, R., King, A., Palmer, C., Bentzel, C., & Tabriz, P. (2017). Measuring HTTPS adoption on the web. In *26th USENIX Security Symposium* (pp. 1323-1338).
- Fink, A. (2013). *How to Conduct Surveys: A Step-by-Step Guide: A Step-by-Step Guide*. Sage Publications.
- Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: the what, how and who. *Computers & Security*, 61, 169-183.
- Gcaza, N., von Solms, R., Grobler, M. & van Vuuren, J. (2017). A general morphological analysis: delineating a cyber-security culture. *Information & Computer Security*, 25(3), 259-278.
- George, E. & Gao, J. (2014). A qualitative study of information challenges in the cloud. Australasian Conference on Information Systems (ACIS). 25th Australasian Conference on Information Systems 8th -10th Dec 2014, Auckland, New Zealand.
- Greene, M. J. (2014). On the inside looking in: methodological insights and challenges in conducting qualitative insider research. *The Qualitative Report*, 19(29), 1-13.
- Guarino, A. (2015). Information security standards in critical infrastructure protection. IEEE, Securing Electronic Business Processes, 263-269. Springer Fachmedien Wiesbaden.

- Gundu, T. & Flowerday, S. V. (2013). Ignorance to awareness: towards an information security awareness process. *South African Institute of Electrical Engineers (SAIEE) Africa Research Journal*, 104, 69-79.
- Haeussinger, F. & Kranz, J. (2013). Information security awareness: Its antecedents and mediating effects on security compliant behavior. In *Proceedings of 2013 International Conference on Information Systems (ICIS), Italy, San Milan*.
- Haeussinger, F. & Kranz, J. (2017). Antecedents of employees' information security awareness – review, synthesis, and directions for future research. In *Proceedings of 2017 International Conference on Information Systems (ICIS), Seoul, South Korea*.
- Herold, R. (2010). *Managing an information security and privacy awareness and training program*. CRC Press.
- Hu, Q., Hart, P., & Cooke, D. (2007). The role of external and internal influences on information systems security—a neo-institutional perspective. *The Journal of Strategic Information Systems*, 16(2), 153-172.
- Hussein, M. E., Hirst, S., Salyers, V., & Osuji, J. (2014). Using grounded theory as a method of inquiry: advantages and disadvantages. *The Qualitative Report*, 19(27), 1-15.
- International Association of Information Security Professionals (IASAP) (2017). *About IASAP*. Retrieved from <http://iasapgroup.org/>.
- Ifinedo, P. (2016). Critical times for organizations: what should be done to curb workers' noncompliance with IS security policy guidelines? *Information Systems Management*, 33(1), 30-41.
- Ifinedo, P. (2017). Effects of organization insiders' self-control and relevant knowledge on participation in information systems security deviant behavior [Best Paper Nominee]. In *Proceedings of the 2017 ACM SIGMIS Conference on Computers and People Research* (pp. 79-86). ACM.
- Information Security Forum (ISF). *Standard of Good Practice for Information Security*. (2014). London: Information Security Forum (ISF). Retrieved from <https://www.securityforum.org/>.
- Ingram, M., Martin, M. & Pena, I. (2017). *States of Cybersecurity: Electricity Distribution System Discussions* (No. NREL/TP-5C00-67198). NREL (National Renewable Energy Laboratory (NREL), Golden, CO (United States)).

- International Information Systems Security Certification Consortium (ISC²). *About ISC²*. Retrieved from <https://www.isc2.org/about>.
- ISO/IEC (International Organization for Standardization (ISO) and International Electrotechnical Commission) 27002:2013. (2013). *Information technology – Security techniques – Code of practice for information security management*.
- Jaeger, L. (2018). Information security awareness: literature review and integrative framework. In *51st Hawaii International Conference on System Sciences Proceedings*.
- Johnson, J., Lincke, S. J., Imhof, R., & Lim, C. (2014). A comparison of international information security regulations. *Interdisciplinary Journal of Information, Knowledge, and Management*, 9.
- Kam, H. J., Katerattanakul, P., & Gogolin, G. (2013). A cross industry study: differences in information security policy compliance between the banking industry and higher education. In *34th International Conference on Information Systems (ICIS) Proceedings*.
- Karjalainen, M. & Siponen, M. (2011). Toward a new meta-theory for designing information systems (IS) security training approaches. *Journal of the Association for Information Systems*, 12(8), 518-555.
- Killingsworth, S. (2014). The Privatization of Compliance. In RAND Center for Corporate Ethics and Governance Symposium White Paper Series, Symposium on “Transforming Compliance: Emerging Paradigms for Boards, Management, Compliance Officers, and Government”.
- Lawrence, J., & Tar, U. (2013). The use of grounded theory technique as a practical tool for qualitative data collection and analysis. *The Electronic Journal of Business Research Methods*, 11(1), 29-40.
- Li, C. (2015). Penetration testing curriculum development in practice. *Journal of Information Technology Education: Innovations in Practice*, 14, 85-99.
- Mahfuth, A., Yussof, S., Abu Baker, A. & Ali, N. (2017). A systematic literature review: information security culture. In *Research and Innovation in Information Systems (ICRIIS), 2017 International Conference*, (1-6).
- Marshall, C. & Rossman, G. B. (2014). *Designing qualitative research, 5th edition*. Sage Publications.
- Martin, N. L., Imboden, T., & Green, D. (2015). HIPAA security rule compliance in small healthcare facilities; a theoretical framework. *Issues in Information Systems*, 16(1).

- Matejka, J. (2016). Anti-spam legislation in consideration of personal data protection and other legal instruments. *The Lawyer Quarterly*, 6(2).
- Mathur, A. (2012). A research paper: an ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms. *International Journal on Computer Science and Engineering*, 4(9), 1650.
- Mayrhofer, R. (2015). An architecture for secure mobile devices. *Security and Communication Networks*, 8(10), 1958-1970.
- McDaniel, E. (2013). Securing the information and communications technology global supply chain from exploitation: developing a strategy for education, training, and awareness. In *Informing Science and Information Technology Education Conference Proceedings* (313-324).
- Miller, G. P. (2014). The compliance function: an overview. *NYU Law and Economics Research Paper*, 14-36.
- Mohammed, D. (2015). Cybersecurity compliance in the financial sector. *Journal of Internet Banking and Commerce*, 20(1).
- Mujumdar, A., Masiwal, G. & Meshram, D. B. (2013). Analysis of signature-based and behavior-based anti-malware approaches. *International Journal of Advanced Research in Computer Engineering and Technology (IJARCET)*, 2(6).
- Narain Singh, A., Gupta, M. P., & Ojha, A. (2014). Identifying factors of organizational information security management. *Journal of Enterprise Information Management*, 27(5), 644-667.
- National Association of Insurance Commissioners (NAIC). (2015). Principles for effective cybersecurity: insurance regulatory guidance.
- National Conference of State Legislatures (NCSL). (2018). Data security laws/state government. Retrieved from <http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws-state-government.aspx>.
- National Institute of Standards and Technology (NIST). (1998). Special Publication (SP) 800-16, information technology security training requirements: a role- and performance-based model. Retrieved from <https://csrc.nist.gov/publications/detail/sp/800-16/final>
- National Institute of Standards and Technology (NIST). (2003). Special Publication (SP) 800-50, building an information technology security awareness and training program. Retrieved from <https://csrc.nist.gov/publications/detail/sp/800-50/final>

- National Institute of Standards and Technology (NIST). (2014). Special Publication (SP) 800-53, security and privacy controls for federal information systems and organizations. Retrieved from <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-53r4.pdf>.
- New York State Department of Financial Services (DFS) Title 23, Codes, Rules and Regulations of the State of New York (NYCRR). (2017). Cybersecurity requirements for financial services companies. Retrieved from <https://www.dfs.ny.gov/legal/regulations/adoptions/dsrf500txt.pdf>.
- Nicho, M. & Muumaar, S. (2016). Towards a taxonomy of challenges in an integrated IT governance framework implementation. *Journal of International Technology and Information Management*, 25(2).
- Niemimaa, E. & Niemimaa, M. (2017). Information systems security policy implementation in practice: from best practices to situated practices. *European Journal of Information Systems*, 26(1), 1-20.
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Reliability Standard CIP-004-3: Cyber Security — Personnel and Training. Retrieved from https://cdn2.hubspot.net/hubfs/241394/Knowbe4-May2015-PDF/pa_Stand_Reliability.pdf?t=1521987427393.
- Nova Southeastern University (NSU) (2016). *Center for information protection education and research*. Retrieved from <http://infosec.nova.edu/academic-excellence/>.
- Offor, P. & Tejay, G. (2014). Information systems security training in organizations: andragogical perspective. In *Twentieth Americas Conference on Information Systems Proceedings* (3061-3069). Savannah, GA.
- Patnayakuni, R. & Patnayakuni, N. (2014). Information security in value chains: a governance perspective. In *Twentieth Americas Conference on Information Systems Proceedings* (1920-1929). Savannah, GA.
- Payment Card Industry Data Security Standards (PCI DSS). (2014). *Payment Card Industry Data Security Standard (PCI DSS)*, 3.1.
- Payment Card Industry Security Standards Council (PCI SSC). (2014). *Information Supplement: Best Practices for Implementing Security Awareness Programs*. Retrieved from https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf.

- Periera, T. & Santos, H. (2014). Challenges in information security protection. *Proceedings of the 13th European Conference on Cyber Warfare and Security: ECCWS 2014*. University of Piraeus, Greece.
- Ponemon Institute. (2016). *2016 cost of a data breach survey: global analysis*. Retrieved from <http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03094WWEN>.
- Ponemon Institute. (2017). The internet of things: a new era of third-party risk. Retrieved from <https://www.prevalent.net/resources/the-internet-of-things-iot-a-new-era-of-third-party-risk>.
- Radke, B., & Waters, M. (2015). Selected state laws governing the safeguarding and disposing of personal information. *John Marshall Journal of Information Technology & Privacy Law*, 31(4).
- Rocha Flores, W., Antonsen, E. & Ekstedt, M. (2014). Information security knowledge sharing in organizations: investigating the effect of behavioral information security governance and national culture. *Computers & Security*, 43, 90-110.
- Romanosky, S. (2016). Examining the costs and causes of cyber incidents. *Journal of Cybersecurity*, 0, 1-15.
- Safa, N., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, 53, 65-78.
- Safa, N. S., Von Solms, R. & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 70-82.
- Salas, E. & Lazzara, E. H. (2014). Training and Learning Development for Homeland Security. *Wiley Handbook of Science and Technology for Homeland Security*.
- Santos-Olmo, A., Sánchez, L. E., Caballero, I., Camacho, S. & Fernandez-Medina, E. (2016). The importance of the security culture in SMEs as regards the correct management of the security of their assets. *Future Internet*, 8(3), 30.
- Sen, R. & Borle, S. (2015). Estimating the contextual risk of data breach: an empirical approach. *Journal of Management Information Systems*, 32(2), 314-341.
- Silic, M. & Back, A. (2014). Shadow IT – a view from behind the curtain. *Computers & Security*, 45, 274-283.
- Siponen, M. & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: the case of information security policy violations. *European Journal of Information Systems*, 23(3), 289-305.

- Soomro, Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. *International Journal of Information Management*, 36(2), 215-225.
- Terrell, S. R. (2012). *Statistics translated: A step-by-step guide to analyzing and interpreting data*. Guilford Press.
- Thalmann, S., Bachlechner, D., Demetz, L. & Maier, R. (2012). Challenges in cross-organizational security management. In *System Science (HICSS), 2012 45th Hawaii International Conference on* (pp. 5480-5489). IEEE.
- Tsohou, A., Kokolakis, S., Karyda, M. & Kiountouzis, E. (2008). Investigating information security awareness: research and practice gaps. *Information Security Journal: A Global Perspective*, 17(5-6), 207-227.
- Urquhart, C. & Fernández, W. (2013). Using grounded theory method in information systems: the researcher as blank slate and other myths. *Journal of Information Technology*, 28(3), 224-236.
- Walker, C. (2014). Organizational learning: the role of third party auditors in building compliance and enforcement capability. *International Journal of Auditing*, 18(3), 213-222.
- Warkentin, M., Johnston, A. C. & Shropshire, J. (2011). The influence of the informal social learning environment on information privacy policy compliance efficacy and intention. *European Journal of Information Systems*, 20(3), 267-284.
- The White House (The White House). (2014). Framework for improving critical infrastructure (CI) cybersecurity - executive order, derived from NIST 800-53.
- Yimam, D. & Fernandez, E. B. (2016). A survey of compliance issues in cloud computing. *Journal of Internet Services and Applications*, 7(1), 1-12.