Title: Criterion Clarification for Cybersecurity Readiness for the Energy Industry and Alternative Cybersecurity Readiness Models

Course: Dissertation Credits 11 and 12

Year: March 16, 2022

Author(s): Aaron Cavanaugh

Report No.:

ABSTRACT

This paper discusses and clarifies the criterion selected for the authors Hierarchical Decision Model to be verified and validated by experts in the field of Cybersecurity in the Energy Industry. The 29 criterions were vetted through a previous bibliometric research project conducted by the author. This paper also provides a summary of current Cybersecurity Readiness models created for Energy and closely related industries.

TABLE OF CONTENTS

ABSTRACT i
Introduction 1
Criterion Grouping 1
Hierarchical Decision Model (HDM) Criterion Discussions 4
Change Management Is Considered (1) – Technical 4
Computer User's Settings And Permissions Are Known (3) – Organizational 5
Cyber Awareness Of All Staff Is Checked (1) – Professional 5
Cybersecurity Goals Of Energy Organization Are Identified (2) – Leadership 5
Cybersecurity Learning Sources Are Available (3) – Leadership 6
Cybersecurity Readiness Assessments (4) – Organizational 6
Cybersecurity Risk Is Considered Priority By C-Suite (4) – Leadership 7
Data Loss Prevention (DLP) System Is In Place (10) – Technical 7
Documents Are Marked And Protected (1) – Organizational 8
Energy System Outages Are Planned For (1) – Technical 8
External Reporting Is Done (4) – Professional 9
External Vendor/Supply Coordination Is Done (2) – Professional 9
Information Officer Is In Contact With Internet Service Provider (1) – Technical 9
Logging Is Sufficient For Security And Forensics (6) – Technical 9
Machine Limitations Are Recorded (3) – Technical 10
Network And System Admin Procedures Documented (4) – Technical 11
Network Modeling For IoT Is Done (3) – Technical 11
Outages Are Not Required For Security Updates (1) – Technical 11
Planning For Forensic Evidence Collection (3) – Technical 12
Policies Are Updated (2) – Leadership 12
Presence Of Implementation Oversight (4) – Organizational 13
Presence Of Legislative Understanding (2) – Organizational 13
Professionals With Cyber Certifications Are In Operations Roles (1) – Leadership 14
Retention Periods Are In Place And Used For Information And Data (2) – Technical 14
Social Impact Of Breaches Is Talked About In The Company (1) – Organizational 14
Standards Are Understood (1) – Technical 15
Supply Chain Cyber Risk Is Considered During Procurement (1) – Leadership 15
There Is An Organizational Common Vocabulary For Cybersecurity In The Energy Industry (1) – Organizational 15
Threats To Organization Are Modeled (2) – Professional 15
Current Cybersecurity Readiness Models Closely Related To The Energy Industry 16
A Conceptual Model For Digital Forensic Readiness 17
A Generic Digital Forensic Readiness Model For BYOD Using Honeypot Technology 17
A Socio-Technical Analysis Of China's Cybersecurity Policy: Towards Delivering Trusted E-Government Services 18
Adoption Of Cybersecurity Capability Maturity Models In Municipal Governments 18
Evaluating The Cyber Security Readiness Of Organizations And Its Influence On Performance 19
Factors Affecting Perceptions of Cybersecurity Readiness Among Workgroup IT Managers 20
ICS Testbed Tetris: Practical Building Blocks Towards a Cyber Security Resource 21
Internet of Things & Cybersecurity Readiness in Smart-government and Organizations 22
Mobile Cloud Forensic Readiness Process Model for Cloud-Based Mobile Applications 23
Towards a Systemic Framework for Digital Forensic Readiness 24
Towards verifiable evidence generation in forensic-ready systems 24
Conclusion 25

Appendices 26
Appendix A: HDM Model (Version 6) 26
Appendix B: 74 Article Data Points for HDM Model Criterion (Sorted by Competency) 27
Appendix C: 29 Sorted Criterion from 74 Data Points 33
References 36

Introduction

The previous literature search uncovered the 29 criterions. The perspective groupings may be debated; however, the findings are reflective of the literature on Cybersecurity Readiness in the Energy Industry. While there is some duplication/crossover of the criteria, the initial finding is that, technical considerations are the most prevalent in the cybersecurity domain.

Criterion Grouping

Each paper included in the 36 articles that created the Hierarchical Decision Model (HDM) model had themes that are summarized in Table 1 below. Each article was given a unique Identification (ID) in the taxonomy. A few articles were not finalized into the table because they did not meet qualifications [1]. Thus, there are numerical gaps in categorization tables below.

The literature was often teaching others based on what they the authors had learned. This type of article was labeled as Instructive Material. The additional articles were categorized as follows: one paper was a report on interviewing; two papers were literature reviews and summaries; many published articles were model attempts; some models were little more than tables; others had more quantitative approaches; a couple models were created based on a literature review; and another was a survey; one was an artifact was a poster for a roadmap; one author created a prototype for a computer system; two articles were semi-structured interviews; one was a statistical analysis; and the remaining were surveys combined with other previously mentioned approaches (see Table 1). Articles in the category Business or Functional frequently guided readers towards articles relevant to their further interest. The summary column provides a brief elaboration on the keyword row so that a researcher can make an informed decision as to whether to further read the article.

Table 1 - Article Keywords and Methods Sorted by Method

Article #	Article	Business or Functional Category	Method	Summary
15	Cyber Security Basic Defenses and Attack Trends	Threat/Victim	Instructive Material	Covers defense and attacks using the confidentiality, integrity, availability model
17	Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation	Financial	Instructive Material	A comprehensive overview of the financial services cybersecurity landscape
20	Cyber-Terrorism: Nigeria's Payment System Infrastructural Readiness	Financial	Instructive Material	Defining cyber terrorism and how governments can respond
26	Forensic Readiness of Smart Buildings: Preconditions for Cybersecurity Tests	Forensics	Instructive Material	Asks a lot of questions about forensic-ability of the organization

27	Graded security forensics readiness of SCADA systems	Industrial Control Systems	Instructive Material	A light overview of SCADA network security
31	Information Security Standards	Standards	Instructive Material	A good summary of standards around the year 2010.
32	Managing Cyberthreat	Policy/Law	Instructive Material	An overview of breaches in critical infrastructure sectors
38	The Need for Integrated Cybersecurity and Safety Training	Standards	Instructive Material	Cybersecurity training goals and risk rankings are discussed
39	The Current State of Insider Threat Awareness and Readiness in Corporate Cyber Security - An Analysis of Definitions, Preventions, Detection, and Mitigation	Literature Review	Instructive Material	Insider threat histories and motivations are discussed.
34	New tool assesses banks' cybersecurity readiness	Financial	Interview	An interview with bank officials on a financial cybersecurity reporting tool available.
30	Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0	Forensic	Literature Review	A thorough review of handling cloud forensic information
37	Technology Readiness and the Smart Grid	Government, Business, Standards	Literature Review	A review of Technology Readiness Levels developed by NASA and how they could be applied to Smart Grid
6	ICS Testbed Tetris: Practical Building Blocks Towards a Cyber Security Resource	Zones, Testing	Model	A model of smart grid zone testing to stimulate and support discussion
7	Towards verifiable evidence generation in forensic-ready systems	Forensic	Model	Defining cyber structure for proper evidence handling
9	A conceptual model for digital forensic readiness	Forensic	Model	Systematic evidence-based criteria are needed
12	A Generic Digital Forensic Readiness Model for BYOD using Honeypot Technology	Forensic	Model	Creates a theoretical workflow, which includes a BYOD and honeypot, for forensics
21	Towards a Systemic Framework for Digital Forensic Readiness	Forensic	Model	Forensic readiness factors are binned with links to sources
33	Mobile Cloud Forensic Readiness Process Model for Cloud-Based Mobile Applications	Cloud, Forensic	Model	Acceptable evidence documentation procedures concepts are highlighted.
8	A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-Government services	Policy/Law	Model, Literature Review	Trust in technology = Trust in government
25	Factors Affecting Perceptions of Cybersecurity Readiness Among Workgroup IT Managers	Sociology	Model, Statistics	Talks about the human factor of cybersecurity

24	Evaluating the cyber security readiness of organizations and its influence on performance	Hypothesis	Model, Structural Equation Modeling	Proposes hypothesis about cybersecurity and then tests through Structural Equation Modeling
11	Internet of Things & Cybersecurity Readiness in Smart-government and Organizations	Government	Model, Survey	Governments are using more IoT devices
35	Verification of Forensic Readiness in Software Development: A Roadmap	Model	Poster One-Pager	A timeline with definitions that could help lay people understand digital forensics
22	Secure Logging in Operational Instrumentation and Control Systems	Forensic	Prototype	How to log entries and correlate data from different sources
18	Cybersecurity incident response capabilities in the Ecuadorian financial sector	Financial	Semi-structured interviews	Motivation and effectiveness of their organizational cybersecurity responses
23	Cybersecurity Readiness of E-tail Organisations: A Technical Perspective	Business	Semi-structured interviews	Some basic themes from experts are identified
29	Information Security: Cybersecurity Standards Adoption Among Malaysian Public Listed Companies	Standards	Statistics	Do organizations in Malaysia intended to comply with standards
14	Expert's reviews of a could forensic readiness framework for organizations	Cloud, Forensic	Survey	A perspective diagram of forensic readiness was created based on expert feedback
16	Cyber security readiness in the South Australian Government	Government	Survey	Are information security management systems successfully deployed
19	Cybersecurity Readiness as a Business Value	Business	Survey	A Likert based maturity survey based on threats
36	Cybersecurity Readiness: An Empirical Study of Effective Cybersecurity Practices for Industrial Control Systems	Industrial Control Systems, Business	Survey	A survey of businesses on current methods, reporting, and board involvement
10	Adoption of Cybersecurity Capability Maturity Models in Municipal Governments	Government	Survey, Model	Are organizations adopting cyber maturity models?
5	An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses	Business	Survey, Statistics	Are small businesses prepared and do they perceive cyber risk
13	CISTAR Cybersecurity Scorecard	Business	Survey, Statistics	A survey on Natural Gas (NG) cyber capabilities

28	Factors Influencing Cybersecurity Readiness in Deposit Taking Savings and Credit Cooperatives: A Case Study of Nairobi County	Policy/Law	Survey, Statistics	A survey of small financial institutions cybersecurity posture in Kenya
40	Cyber Security Readiness Assessment Model in Kenyas' Higher Learning Institutions: A Case of University of Nairobi	Academia	Survey, Statistics	A survey of university departments IT practices under the scope of one university

Although 36 articles were found in the Literature review, on Cybersecurity Readiness in the Energy industry, some did not include or identify gaps to be included in this HDM Model. The 29 articles finally used from Table 1 in the HDM Model are: 5,6,7,8,9,10,11,12,14,15,16,17,18,20,21,22,23,24,25,26,27,28,29,30,32,33,34,36,39. Each of the 29 articles are assigned to one or more categories in the HDM model (See Appendix A). Several articles had more than one gap thus there were 74 data points for building the HDM model (See Appendix B). 13 for the Leadership perspective, 15 for Organizational, 9 for Professional, and 37 for Technical (which is half of the total).

Hierarchical Decision Model (HDM) Criterion Discussions

The following paragraphs are elements, problems, and commentaries on each criterion selected for Cybersecurity Readiness in the Energy Industry HDM model (see Appendix C for criterion listings). Each criterion below has a numerical number listed representing the count of articles for each criterion. The criterion below is discussed in alphabetical order.

Change Management Is Considered (1) – Technical

Elements: A repeatable and sustainable framework. Naming conventions, version control system, and document and storage retrieval system. Scope assessment against: quality, risk, schedule, cost, resources, and customer satisfaction are realized.

Problem: When change is not logged there is an out-of-control situation, that is no one is aware of the current state of vulnerability.

Commentaries: The concern with Change Management is that it is not considered. That is there is no monitoring for changes to the network [2]. The objective of sustainable, and thus profitable business, is to have a repeatable and sustainable framework. A *Configuration* Management Plan defines: naming conventions, version control system, and document storage and retrieval system. The *Change* Management Plan describes how changes are managed and controlled. Scope changes need to have a constraint/impact assessment against: quality, risk, schedule, cost, resources, and customer satisfaction. When changes are not logged using a configuration management system then the project or program becomes out of control. Thus, there is a security gap as no one is aware of the current state of vulnerability. Changes that can

lead up to vulnerabilities include but are not limited to: Baseline incorrect, Baseline update exceeding 30 days, Missing security controls testing evidence, Monitoring exceeds a 35-day requirement, Pre/Post Implementation results not captured, and Unauthorized changes taking place [3].

Computer User's Settings And Permissions Are Known (3) – Organizational

Elements: What each staff person needs to know is understood.

Problem: Overprivileged setting can lead to more chances for breaches of data. Users setting unknown is a gap in security.

Commentaries: Settings and Permissions are part of a defense in depth strategy which means there must be multiple security protocols in place in order to breach a computer system. If line management does not understand what each staff person needs to know (their profiles) [4] then overprivileged settings may occur which can lead to breaches of data either from insiders or outsiders. It could also be that a user mistakenly delete a file or setting required that disables a system thus leaving it vulnerable. The need for and how to setup cyber user settings must be known and communicated. If user settings are unknown then there is a gap in security. In order to mitigate this threat, the organization and management must develop and review security requirements on a regular basis [5]. User settings and permissions are at the crux of cybersecurity practices, and need to be tested [6]. Having the correct permissions set ensures organizational performance.

Cyber Awareness Of All Staff Is Checked (1) – Professional

Elements: Rogue access points awareness by Wi-Fi users.

Problem: Malicious links create a man in the middle attack possibility. Vulnerable employees will likely lead to vulnerable organizational assets.

Commentaries: Awareness training is usually done with online courses. If staff doesn't thoroughly understand the difference between good and bad cyber behavior there may be rogue access points for Wi-Fi or clicking on malicious links that steal cookies that create a man in the middle browser attack. When awareness of behavior is not trained and checked then the company has no record to go back to for checking security maturity of the organization. Not checking cyber awareness with staff leads to vulnerable employees, which leads to a vulnerable organizations computer systems and data. The question to answer here is: Does your team understand the difference between good and bad cyber behavior? [7] Behavior of users can be somewhat mitigated with information on practice sent and captured to a logging system, which must be retrievable and understandable by design.

Cybersecurity Goals Of Energy Organization Are Identified (2) – Leadership

Elements: Tools make controls and updating control viable. Dashboards keep goals top of mind.

Problem: Executive priorities of the energy business not tied to cybersecurity realities can put other users (including consumers) at risk.

Commentaries: Goals must be updated to ensure that the desirability of the organization strategy is met. If cybersecurity goals are not updated periodically a misalignment is created with business realities. The updated controls in place [8] ensure continued viability using internet and IoT tools and technologies. A dashboard for security status (e.g., people, processes, and technology) [9] is a great way to keep on top of goals of the organization's security. It keeps security top of mind.

Cybersecurity Learning Sources Are Available (3) – Leadership

Elements: Resources on cybersecurity and the energy system specific topic threats. Online training on crime organizations and nations with malicious intent. Those with cybersecurity training and responsibilities should know all policies and practices.

Problem: Smaller organizations don't think they are a target but they are breached in order to get credentials to larger organizations machines, by theft of more credentials or because of implicit trust.

Commentaries: As is often the case in security criterion share the same or similar concerns. One area where cyber training is focused, especially in the defense and energy industries, is terrorism. The Advanced Persistent Threat (APT) of nation state actors and/or organized crime is a concern that users should be aware of so that they understand the risk. Terror is an important risk because often smaller organizations are breached in order to get "keys" to larger organizations. Security resources should be made available to staff [10] for Question and Answer (Q&A). Online training is only one part of learning resources. More internal resources on cybersecurity and Energy Industry threat should be made available in the organization. During and after training security awareness improvements should be documented [9]. When staff doesn't understand policies and practices [11] they will be unprepared to take action when an incident occurs.

The Board must make available strategy resources for the organization to put effort into it. For those with cybersecurity training and responsibility they should know all the organizations policies and practices. Cybersecurity must be considered as a key risk as organizations depend on internet connectivity/systems, and data for transacting business.

Cybersecurity Readiness Assessments (4) – Organizational

Elements: Quantitative self-rating aids in identifying if the organization is missing controls.

Problem: No assessments mean no cybersecurity integration is likely being done with the rest of the operations.

Commentaries: In order to minimize disruption [12] to the organization and increase usefulness [13] of organizational assets: behaviors, practices, processes, controls, trainings, detections, and responses must be assessed [11]. If no quantitative self-rating through assessments is done then

the organization is likely missing controls. No assessments or lack of an assessment such as a survey and checklist [5] for auditing not only means the audit is lacking, but also that there is no integration of cybersecurity with the rest of operations. In the assessment the organization needs to incorporate both assets and data [14]. A simple checklist for sufficiency can ask: have you analyzed if audits are done are effectively [15], and do you rate your cyber assessment methods annually [16]?

Cybersecurity Risk Is Considered Priority By C-Suite (4) – Leadership

Elements: The board, and or C-Suite, is not considering cyber a risk. The organization should be paying the same or more attention on security than on ease of use and time to market. The Chief Information Officer (CIO) should be making strategic decisions as an equal on the Board if exists.

Problem: There is no comprehensive plan and recognition of experts for cybersecurity at the strategic level.

Commentaries: Security is the guarding of your data and assets. If your assets are important then are you paying the same or more attention on security than on ease of use and time to market [17]? This is where having the Chief Information Officer (CIO) on the board will infer that the board has an Information Technology (IT) security awareness [15]. Thus, cybersecurity needs to be a key component of the risk management program [18].

A risk register or list is the first place to start capturing risks. Cybersecurity should be on this list. In the energy industry an organization should ask: is terrorism secured against [19]? The Board sets the priorities and if not considering cyber a risk then it cannot be said that there is a comprehensive plan for terror activities.

Data Loss Prevention (DLP) System Is In Place (10) – Technical

Elements: Data Loss Prevention system is essential for critical information and assets. DLP systems provide: logging, malfunction information, forensics, threat information, retention, reporting, and cloud information. A forensic model is in place for when an event occurs is one aspect of DLP.

Problem: No DLP means there is no large integrated system for threat management.

Commentaries: Although DLP is the most cited criteria by readiness authors in the bibliometric research, DLP systems [11] are inherently complex. DLP is useful if you have critical information such as the energy industry (if not it is burdensome to maintain for small organizations without time and money).

DLP systems are big in scope: logging, malfunctioning, forensics, threats, retention, reporting, and cloud are all included. Evidence retention is important after an event in order to prosecute and attribute for renumeration. Thus, an organization should have a forensic model in place for when an event occurs as one pillar of a DLP plan. A forensic model [20], policy and plan should also cover cloud assets [21]. There are limitations in cloud forensics so contracts must be

carefully reviewed. Note that an Information Security Management System (ISMS) [14] can take the place of a DLP system. Prevention and detection, if included in a DLP means that the organization has a system for threat management [22].

You can ask: do you prevent, detect, and combat attacks [6]? If so they you have a kind of DLP system. Insufficient and Bad Logging are two of the most egregious errors in DLP systems. Logging is the foundation of response and is a key question to ascertain if a cyber data loss prevention system exists. Data loss refers to the unwanted removal of sensitive information either due to an information system error, or theft by cybercriminals. The next step is to make sure the logging is setup correctly. Check that the log time is protected, to correctly attribute and sync of egregious actions, and make sure that the logging storage is functioning correctly.

Post-incident procedures [9] (aka response and recovery) add to a comprehensive list of security considerations [15] specific to organizations use case (such as an energy system or Internet of Things (IoT)) implementation. Procedures for reporting and escalation [15] for incidents should be written down. Also, Cloud information should be able to be isolated [23] if there is an incident based on the provider contract.

Documents Are Marked And Protected (1) – Organizational

Elements: Sensitive attachments should be stored separately on protected systems.

Problem: Haphazard and inconsistent markings that are not standards based (merely organizationally specific) create confusing language for auditors.

Commentaries: Especially in government industries, some of which are energy providers sensitive documents should be marked and protected. Policies aren't normally protected from those without the need to know, and they should be available to all. Attachments that have classified information should be stored separately on differently protected systems [19]. In industry there can be haphazard/inconsistent markings that are merely organizational specific and not using any recognized government vocabulary for marking. This results in organizational documents that are unprotected because language is confused and not universally understood.

Energy System Outages Are Planned For (1) – Technical

Elements: There should be a plan for power loss.

Problem: Unplanned failures may lead to cascading grid failures.

Commentaries: Outages are taken in order to maintain equipment. Sometimes they are planned for on a maintenance cycle, but sometimes something breaks and then a backup needs to be ready to go into production or the work needs to be rerouted. If no contingency plan for loss of power then users will have vulnerabilities of availability (one of the three parts of the Confidentiality, Integrity, Accessibility (CIA) cybersecurity triad). Long term energy outages that are not contingency planned for may lead to catastrophic grid failures.

Do you have a contingency plan for energy system outages if your organization is without power for a prolonged period of time [15]?

External Reporting Is Done (4) – Professional

Elements: Electricity Information Sharing and Analysis Centers and Computer Security Incident Response Teams help keep industry a step ahead of criminals.

Problem: If no security reports are being made the criminals have a knowledge advantage.

Commentaries: External reporting [14, 24] brings awareness through anonymous organizations like Electricity Information Sharing and Analysis Center (E-ISAC), which can then be escalated to organizations through Computer Security Incident Response Teams (CSIRT's). If no external or association security reports is being made then it is likely others will be attacked with the same measures. Sharing information on cybersecurity with your partners [19] is a way to keep a step ahead of criminals who share information with one another. An association to supervise cybersecurity [18] is another approach and is even better than just reporting.

External Vendor/Supply Coordination Is Done (2) – Professional

Elements: Coordination of security information with other organizations in the supply chain.

Problem: If no updates then information sharing (thus security) is immature.

Commentaries: Finding a weak or complicit link in a supply chain vendor is an easy way to get your exploit/payload into a sensitive area such as a power system. Not having coordination of security information with other organizations [8] in your supply/value chain means that cyber security information sharing is immature. Based on your costs and contracting you should be getting cybersecurity information updates [19] from the chains.

Information Officer Is In Contact With Internet Service Provider (1) – Technical

Elements: There is communication between Chief Information Office (or delegate) and the Internet Service Provider.

Problem: The Internet Service Provider is part of the internet network interfaces and can add to complete cyber awareness.

Commentaries: Although an Internet Service Provider (ISP) may not be in your supply/value chain the internet is a part of communication business today. There should be communication about security between Chief Information Officer (CIO)/or delegate and the ISP. If the Information Officer/IT doesn't communicate, talk to, or in contact with Internet Service Provider [4] then the organization can't say that it's completely cyber aware.

Logging Is Sufficient For Security And Forensics (6) – Technical

Elements: Logs must be retrievable and understandable. Log time settings must be protected in order to correctly attribute violations.

Problems: Bad logging is a limiting factor for forensic teams work so an attack may not be remediated correctly.

Commentaries: Sufficiency is a relative term something that is based on a risk assessment and maturity. Insufficient logging is the most limiting factor in cyber investigations [25]. As stated in the criteria Cyber Awareness is Checked by all staff; the logging system (and information that is sent to it), must be retrievable and understandable by design [7]. Knowing that you can't collect everything is helpful. Think about; based on your network size have you scoped out what you will and will not be able to collect [9]?

Insufficient and bad Logging are two of the most egregious errors in security of data systems. Logging is the foundation of response and is a key question to ascertain if a cyber data loss prevention system exists. The next step is to make sure the logging is setup correctly. Check that the log time is protected (that is accurate time being logged in logs [26]), to correctly attribute and sync of egregious actions.

Good questions to ask are: Are timestamps of events able to be recorded with certainty that the timestamp has not been changed [13]. Is the organization sure that the logging storage is functioning correctly? Are storage devices automation completely protected [27]?

Logging can be rolled up into a larger DLP system.

Machine Limitations Are Recorded (3) – Technical

Elements: Limitations of systems configurations ability must be known (before installing preferred). What configuration you can or cannot do (e.g., hardening) because of design limitations is making the organization aware. Protocol limitations of machines are known.

Problem: Machines that cannot be configured to work security in networked environments (such as IoT/ICS) or are misconfigured leave critical infrastructure vulnerable.

Commentaries: In order to understand the barriers to a "full implementation" of cybersecurity the limitations of systems must be known. For example, the ICS control systems are often run-on old ladder logic software that is compatible only with older versions of Windows, or variants of Linux which has known unpatched vulnerabilities. Cybersecurity intrusion detection software cannot be used on some of these systems, thus those policies and limitations (network and system admin) on systems (hardware, software, IoT/embedded) must be formally documented [9] and vetted for best possible protection.

The concern with cyber components is that interconnected assets information is shared across networks and systems [17]. Knowing what systems can or cannot do (through hardening or because of design limitations) leads to better awareness of security capabilities.

Subnetting is one way to isolate networked components which make it difficult to do many attacks on machines. When subnets are created then attackers must resort to trying to get credentials in other parts of the system in order to break through to that subnetwork in

order to have access to the next group of machines. Subnetting over zones is complex [28], but critical infrastructure such as energy systems requires the highest security possible.

Protocols used should be captured and known so that sniffers can capture and flag unknown traffic as potentially malicious. A baseline known good snapshot should be taken before putting machines into production. All open source and/or propriety software should be documented with all the security limitations of those [9].

Network And System Admin Procedures Documented (4) – Technical

Elements: Setup policies and procedure settings are known. Administrators are identified.

Problems: Without the policies and procedures thoroughness and clarity are not complete.

Commentaries: Procedures are important to boots on the ground operations. When the technical work has to be done IT persons use procedures to setup cybersecurity intrusion detection machine policy settings. These procedures should be formally documented and vetted for thoroughness and clarity. The settings themselves should be documented. Administrators themselves should be documented in the plan and procedures.

Network interfaces should be hardened [13]/configured for only serving on common ports and normal protocols unless an exceptional circumstance is documented. Any device or interface that is interconnected should be considered above a low risk by default [17]. Cybersecurity controls should be externally vetted and supported to ensure they are accurate. Controls should be verified and validated [11].

Network Modeling For IoT Is Done (3) – Technical

Elements: A security model is done based on protocols and network connections. Cloud assets are modeled.

Problems: Contracts without specifications on network responsibilities and/or without modeling done are likely to cause a dropping the ball situation with security.

Commentaries: IoT networks are often remote, physical systems that may operate on different vulnerable protocols like ZigBee. Non-Transmission Control Protocol/Internet Protocol (TCP/IP) networks will need their own security model [29]. TCP/IP device remote control will need another. Mitigating access control will vary depending on protocol and the embedded devices used. IoT logs should be backed up [9] just as any network connected computer is. Visibility and control of cloud assets [9] is always a question that comes down to contracting and that concern should be modeled in the IoT network.

Outages Are Not Required For Security Updates (1) – Technical

Elements: Spares enable continuous operation.

Problems: Asset work stoppages can lead to access failures.

Commentaries: Security updates should be able to be installed without taking a machine down [17]. If work stoppage outages are needed for security processes to be run then continuous operation is impossible. This leads to an accessibility failure issue (from the CIA triad). If possible, try to procure and install assets where security assessments can be done while systems are up.

Systems can be brought down to test, but there need to be spares to enable continuous operation of the interconnection.

Planning For Forensic Evidence Collection (3) – Technical

Elements: A model for evidence collection enables attribution and/or remuneration by shoring up legal loopholes. There are separate legal considerations for cloud providers.

Problems: Without forensic planning legal loopholes can leave criminals free.

Commentaries: Forensic evidence is needed when attribution or remuneration is required for damages. A model for evidence collection before an event must be created because the requirements for valid evidence are strict and require adherence to legal standards. When evidence collection is not considered then attribution and or renumeration may be impossible because of legal loopholes. Evidence collection must be planned for separately for cloud providers as it may or may not be possible to gather evidence from a provider without cloud providers help [21]? Cloud forensic inability is a concern and needs to be planned for.

Industry guidelines should be used for digital evidence collection [30] and National Institute of Standards and Technology (NIST) has some free guidelines that can be used to start planning your forensic collection methods. A key concept of forensics is the chain of custody which is the procedure and evidence handling which needs to be written down [9] for evidentiary planning and case building.

Policies Are Updated (2) – Leadership

Elements: Organizational policies should match jurisdictional security and privacy requirements. Penalties should be listed. Technical authentication policies should be reviewed and updated regularly.

Problems: Without policy updates disclosure of data is impossible administratively.

Commentaries: Policies are the top-level strategic overview of adherence for cybersecurity. Privacy legislation is one of the key drivers of data confidentiality. In Europe the General Data Protection Regulation (GDPR) legislation limits what information, web servers, can legally spread/share across the internet. For example, looking up people and geolocation information in Europe on Melissa.com is much more limited than in the United States of America (USA) where virtually all data if it is gleaned can be made known. This means that policies need to be in tune at the organizational level to match the jurisdictional security and privacy requirements.

Not being up on legislation can lead to lawsuits. Policies not updated can lead to mitigation actions that need to be taken. For example, data from cyber experts (and really all data) should be anonymized [31] to inhibit full disclosure would be a policy level decision that could be implemented through plans and procedures in further iterations.

Penalties for non-conformance should be listed to encourage implementation. Authentication policies should be addressed [13] because so many attacks rely on privilege escalation tactics. Policies should be updated at regular intervals.

Presence Of Implementation Oversight (4) – Organizational

Elements: Test plans should be verifying baselines. "Need to know" should be incorporated into an oversight plan. User settings should be communicated between employee and manager.

Problems: Standards implementation that is lacking puts the financials of the organization at risk

Commentaries: For verification and validation of process and procedures. For example, mandatory standards with oversight will be followed while voluntary standards are likely to receive little attention by time and money constrained organizations. Oversight and its validation is a key security measure for controls because when not consistently implemented [12] things fall through the cracks. The implementation will be lacking as a result. A consistent implementation of security measures ensures that baseline, in control, may be used to measure against. Test plans should be used to verify the baselines.

Line management should understand staffs "need to know" settings and this is a data point that is incorporated into the implementation oversight plan. Cyber/Internet user settings need to be communicated between employee and line manager.

When new technology complexities arise training [6] and requirements need to be updated in and from the baseline. Questions to ask are: Have polices for firewalls been documented and vetted based on changes [11]? Are proactive practical/operational procedures in place [32] based on high level requirements?

Presence Of Legislative Understanding (2) – Organizational

Elements: Lack of legal understanding can lead to non-compliance and additional forced oversight.

Problems: Legal issues can have a costly monetary penalty.

Commentaries: Legal issues have their own complexities. For example, as mentioned before privacy legislation based on geographic laws must be reviewed. For those companies not up on legislation a misstep can be a costly monetary penalty [31]. If a company is only operational focused (for example on energy systems) or IT focused (on cyber systems) the lack of legislative understanding can lead to non-compliance and additional forced oversight from external

entities. A best practice is to have someone assigned to review the latest privacy and security legislation [17].

Professionals With Cyber Certifications Are In Operations Roles (1) – Leadership

Elements: Those hired should feel that they are aware of the entire landscape from governance to theory.

Problems: Security could be not fully implemented. Costly incidents can happen if a problem spins out of control.

Commentaries: Although not often mentioned industry certifications and formal academic degrees should often be required for security jobs. Hiring "off the street" may lead to a less rigorous implementation of cyber practices. Not hiring certified professionals can be cheaper in the short run but more costly in the long run if problems human or technical develop. Those hired should feel aware of the cybersecurity technologies [11] (both IoT/embedded, industry specific, and IT).

Retention Periods Are In Place And Used For Information And Data (2) – Technical

Elements: Attribution, solving data issues, restoration of data are some reasons why retention is a concern.

Problems: If no offline backups (based on organization retention goals) then data could be lost in an attack or too much data could be exposed in an attack.

Commentaries: If an event occurs then retaining and discovering information will be important. If there is no model for evidence retention then after an event it may be impossible to attribute, solve, or restore data. Evidence retention must be considered and planned for; including, but not limited to a model for cloud assets [20]. A question to ask is: do you have offline backups [9] of information and data?

Social Impact Of Breaches Is Talked About In The Company (1) – Organizational

Elements: Social con artistry, which is one of the easiest ways to get information, is discussed including impacts.

Problems: Breaches are a concern and when unplanned for information/reputation could be lost.

Commentaries: Social engineering, aka con artistry, must be discussed including impacts to self and others. Especially in the energy industry as the sector is vital to all other modern infrastructure sectors. Electricity is the foundation of a modern society. If no discussion of social impact and/or social breach then concerns are likely to be muted and unplanned for when an incident occurs. Social engineering awareness should be covered: including effects on user [4], how it takes place, the risks it poses, and the vectors used.

Standards Are Understood (1) – Technical

Elements: Create a model to follow tailored to your organization.

Problems: When standards are misunderstood there may be violations.

Commentaries: Cybersecurity standards are industry best practices and in some cases mandatory for industry (such as North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)). Standards can be very complicated but need to be thoroughly understood [16]. When standards are misunderstood an auditor will likely find violations when an assessment is done. Standards a good place to start when going through a checklist or trying to create a model tailored for your organization.

Supply Chain Cyber Risk Is Considered During Procurement (1) – Leadership

Elements: Communications and controls (such as contracts) are setup with vendors and suppliers.

Problems: Third parties may have vulnerabilities.

Commentaries: In recent years as events have become publicly known around vendor hardware scams and manipulations supply chain has become a cyber concern. A supply chain plan should cover communications and controls (such as contracts) to and with vendors. If supply chain is not addressed it leaves an attack vector open for malicious actors. Ask your organization: do you control activities of third parties in the supply chain [2]?

There Is An Organizational Common Vocabulary For Cybersecurity In The Energy Industry (1) – Organizational

Elements: A defined technical vocabulary should be defined.

Problems: If users don't understand vocabulary around detection and prevention they cannot discuss or deal with cyberattacks.

Commentaries: Issues may arise because employees in one department don't understand the technical vocabulary being used by IT or security. If users don't understand the cyberattack detection and prevention language, and concerns and detection and protection are not defined, then users will likely not be able to detect and prevent cyberattacks [4].

Threats To Organization Are Modeled (2) – Professional

Elements: A corpus to prioritize and deal with threats.

Problems: If don't have a threat model then awareness of security and attack vectors is not present.

Commentaries: Organizations that are not aware of threats and/or that don't have a threat model that specifically pertains to the organization don't have the awareness of security problems and attack vectors. A threat model should be verified and validated [10] with experts

(such as those with certifications, academic degrees, and/or a lot of work experience). Any news of threats and breaches should be shared often, [32] internally, and with trusted partners.

Current Cybersecurity Readiness Models Closely Related To The Energy Industry

Bibliometric research resulted in 11 articles that have created a model/framework for Cybersecurity Readiness in an industry closely related to Energy. The 11 article summaries are discussed below.

Figure 1 - Cybersecurity Readiness Methods Found

Article #	Article	Business or Functional Category	Method	Summary
9	A conceptual model for digital forensic readiness	Forensic	Model	Systematic evidence-based criteria are needed
12	A Generic Digital Forensic Readiness Model for BYOD using Honeypot Technology	Forensic	Model	Creates a theoretical workflow, which includes a BYOD and honeypot, for forensics
8	A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-Government services	Policy/Law	Model, Literature Review	Trust in technology = Trust in government
10	Adoption of Cybersecurity Capability Maturity Models in Municipal Governments	Government	Survey, Model	Are organizations adopting cyber maturity models?
24	Evaluating the cyber security readiness of organizations and its influence on performance	Hypothesis	Model, Structural Equation Modeling	Proposes hypothesis about cybersecurity and then tests through Structural Equation Modeling
25	Factors Affecting Perceptions of Cybersecurity Readiness Among Workgroup IT Managers	Sociology	Model, Statistics	Talks about the human factor of cybersecurity. Psychological theories using Cronbach's Alpha.
6	ICS Testbed Tetris: Practical Building Blocks Towards a Cyber Security Resource	Zones, Testing	Model	A model of smart grid zone testing to stimulate and support discussion
11	Internet of Things & Cybersecurity Readiness in Smart-government and Organizations	Government	Model, Survey	Governments are using more IoT devices
33	Mobile Cloud Forensic Readiness Process Model for Cloud-Based Mobile Applications	Cloud, Forensic	Model	Acceptable evidence documentation procedures concepts are highlighted.
21	Towards a Systemic Framework for Digital Forensic Readiness	Forensic	Model	Forensic readiness factors are binned with links to sources
7	Towards verifiable evidence generation in forensic-ready systems	Forensic	Model	Defining cyber structure for proper evidence handling
Total		**11**		

A Conceptual Model For Digital Forensic Readiness

In this University of South Africa (SA) conference paper, a literature review was conducted to create a forensic readiness model though identifying gaps [27]. The paper studied the impact of fraud/white collar crime on organizations. As forensics are across networks this paper tries to bring previous forensic research into one conceptual model. The authors created data tables to present the information found from seven university databases from articles written after 2002 when the SA cybersecurity law was put into place.

The authors used interrater reliability (Cohens Kappa) which counts a record when two or more people independently observe the same behavior. Creating a dump/bitstream of an image (which is hashed) is one method used. Live/fast forensics are time based in the first few hours of when an investigation begins (usually on-site). Dead analysis is used with only the software that was originally on the machine when the event occurred. A boot disk can be used but will make changes to the running system (memory and disk). A running system snapshot is called blurry because it is making changes while the image is being created (so is less permissible in court).

The model is a quad chart which puts: people, process, policy, and technology into quadrants as the overarching perspectives with proactive and reactive activities assigned to each quadrant. In addition, the paper lists steps that are appropriate for incidents. For example, an Incident Response Plan (IRP), an Incident Response Team, a forensic methodology, policy plans, appropriate technology (such as Intrusion Detection Systems), appropriate resources/standards for awareness and hardening.

A Generic Digital Forensic Readiness Model For BYOD Using Honeypot Technology

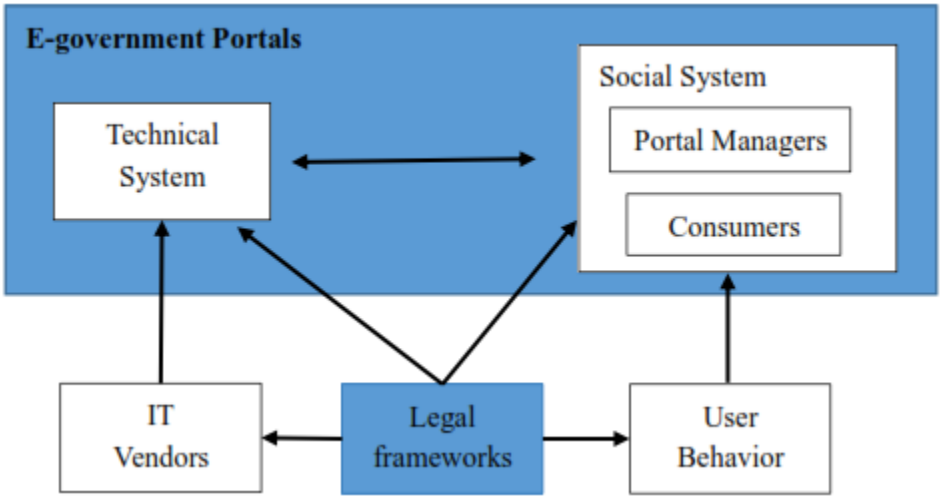
This Africa conference paper proposes honeypots to attract, harvest, and encrypt evidence for legal proceedings of a security incident. Bring Your Own Device (BYOD) decreases end user computing distributed costs. The increased interconnectivity has made organizations accept BYOD as an alternative to providing work machines.

International Organization for Standardization (ISO) 27043 “classes of evidence” are referenced. Protecting and investigating data are discussed. A honeypot is a decoy machine that if hit will send an alert, and/or collect information, to be sent to the computer administrator. The model creates an Object-Oriented generic proactive approach/model to manage users in the environment. Pre-incident planning is discussed to reduce cost. Internet Protocol (IP) packet logging for preservation is proposed. A sequence of execution of deploying, gathering, and hashing is proposed to enhance investigations, and environments using BYOD.

A Socio-Technical Analysis Of China's Cybersecurity Policy: Towards Delivering Trusted E-Government Services

A paper presented at the Research Conference on Communications, Information, and Policy (TPRC) discusses, and outlines the provisions, China's 2016 Cybersecurity Law (CSL) [31]. The paper investigates e-government (considered critical information infrastructure (CII) by the authors based on the Cyberspace Administration of China (CAC) definition) services usage and impact on users based on a social technical systems (STS) theory. Legal, technical, managerial, and human elements are analyzed with a focus on comparing social vis-à-vis technical and show that legal concern is most important factor to both in e-government China. Expert (10+ years in government) semi-structured interviews were done to identify these impacts and make the model.

Figure 2 - China e-government conceptual model



Note: Take from H. Zhang, Z. Tang, and K. Jayakar, "A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-Government services," in TPRC, 2017.

The Technology Acceptance Model (TAM) is referenced as a source to gauge whether users will actually use the product. Overall, expectations of users were reviewed from prior literature. The literature review findings were categorized into a table with each domain: technical, perception of government, trust, and safety further broken down into further dimensions associated with each such as risk, usefulness, etc. Although the law is in place there is no money for actual oversight in local jurisdictions in China.

Adoption Of Cybersecurity Capability Maturity Models In Municipal Governments

This Master's thesis was written for a Canadian university [8]. Data about Cybersecurity practices from Canadian municipalities (including but not limited to energy) was gathered from surveys. The surveys were validated with expert advice. Capability Maturity Models (CMM) were reviewed but were noted as not pertaining to municipalities critical infrastructure. Rogers

Diffusion of Innovation, and its references to consequences, good and bad, on parties involved; was used as a baseline format to build a Cybersecurity Capability Maturity Model (CCMM), based on International Organization for Standardization (ISO) 27000 domains. The hope of the paper is to increase diffusion of the CCMM into local governments.

CMM is measuring progress, usually through self-assessments, towards a target state. Resiliency and Security CMM's that currently exist are listed. International Organization for Standardization (ISO's) provide prescriptive standards whereas a CMM would not. CMM can be used to implement/mitigate controls. CMM's however lack specificity needed for action. After the surveys were conducted Analysis of Variance (ANOVA) and chi-squared cluster (good fit - that is, a valid variable for any data statistic) analysis tables were calculated to show improvement possibilities by using a CMM. The author also tested if CMM's are deemed beneficial and the answer was yes.

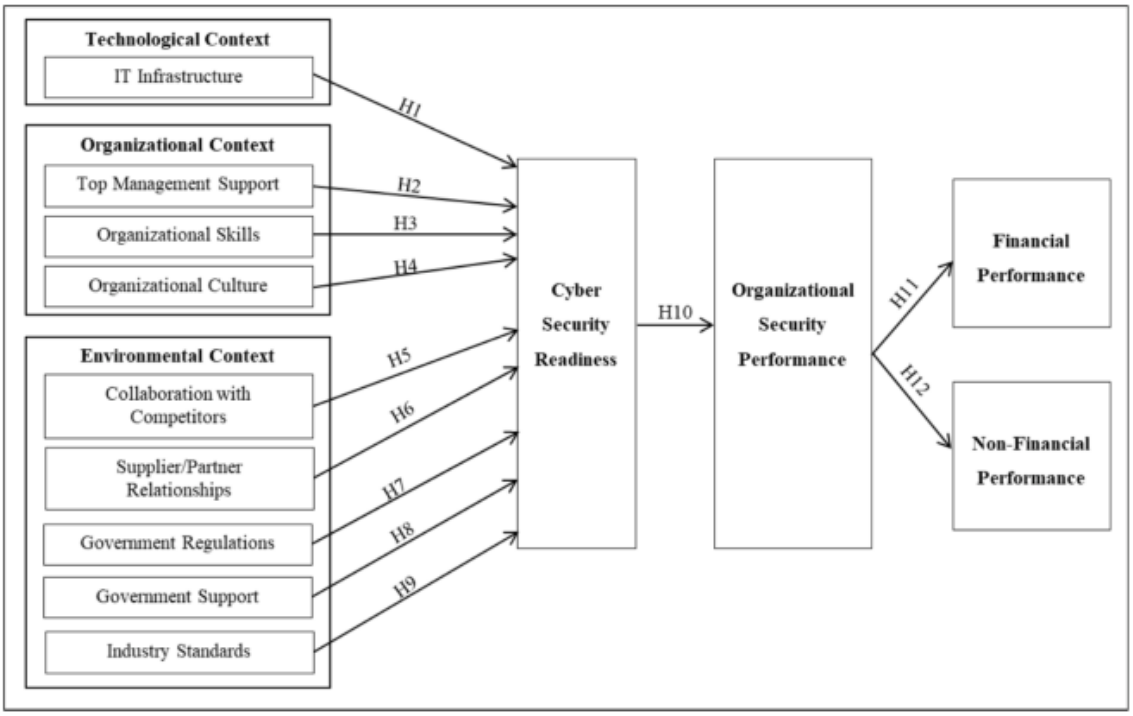
Evaluating The Cyber Security Readiness Of Organizations And Its Influence On Performance

This article in the Journal of Information Security and Applications is an Australian and Malaysian authored paper [6]. This article uses a Technology and Organization and Environment (TOE) framework. People, Processes, and Technology are considered the core elements of Cybersecurity by the authors based on their research. Takeaways comes from a literature review factor and theory categorization table. The authors note that Cybersecurity's impact on performance (decreasing breaches, reputation concerns, processes, capabilities, and capacities) has not been empirically tested. A holistic theory of Cybersecurity on organizations has not been realized.

16 papers theories were identified as the most critical to the TOE framework: Institutional Theory; Game Theory; Deterrence Theory (GDT) – abuse, passive and active restrictions and punishment; and other lesser known - more minor, little discussed in the paper, theories (including Balanced Scorecard). Based on the 16 theories nine factors were identified and incorporated into the aforementioned TOE inspired categorization table. Next a visual model was created based on, if greater than or if the existence of, a control then the overall model/hypothesis calculation for readiness is higher.

A discussion for each hypothesis is included. A Kingdom of Bahrain survey validated the model by experts, and a statistical analysis reviewed the arrowed relationships. The study found that management, standards, and partner relationships are the most important factors to readiness in Cybersecurity.

Figure 3 - Hasan et al, Cybersecurity Readiness Model Based on Hypothesis



Note: Taken from S. Hasan, M. Ali, S. Kurnia, and R. Thurasamy, "Evaluating the cyber security readiness of organizations and its influence on performance," Journal of Information Security and Applications, vol. 58, p. 102726, Feb. 4 2021.

Factors Affecting Perceptions of Cybersecurity Readiness Among Workgroup IT Managers

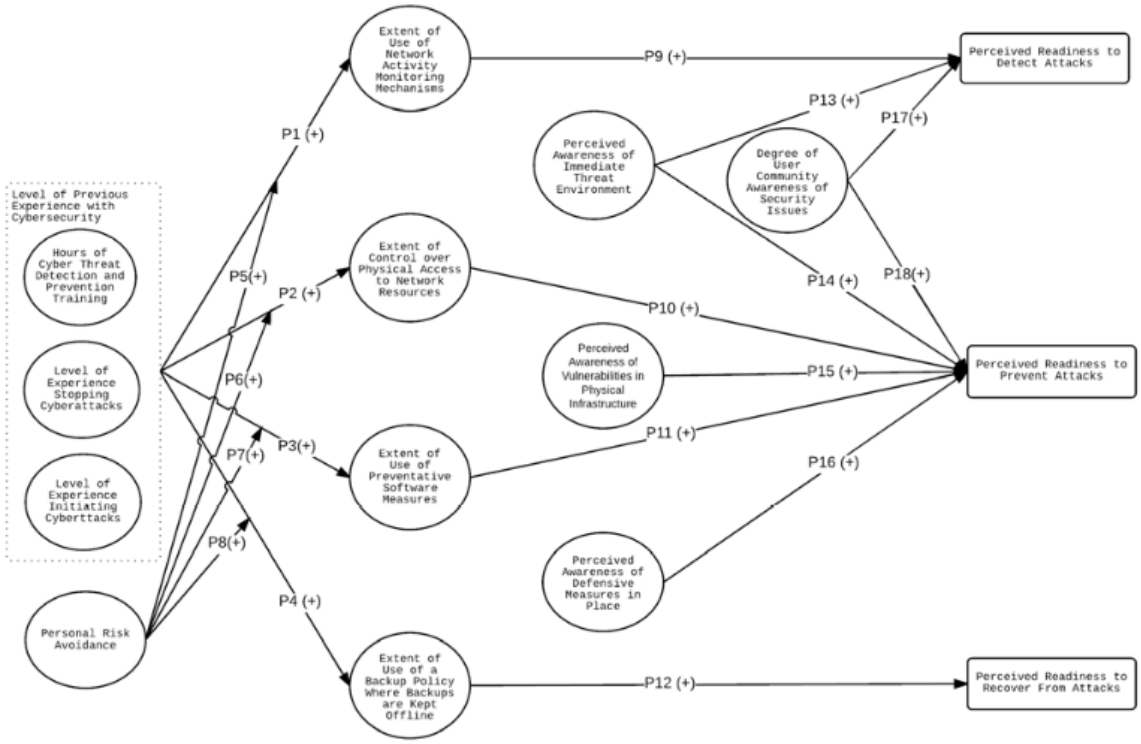
This PhD Dissertation, at the University of Mississippi in the USA, studied managers factors of: experience, best practice, network infrastructure, and education of their user community (which was added as an additional factor to the model during implementation based on manager concerns of lack of control) [4]. The author notes that research on universities vis-à-vis their own cybersecurity internal practices is limited. A survey was conducted to these managers at universities and statistical analysis was done to validate the authors Practice and Awareness Cybersecurity Readiness Model (PACRM). The reliability of the sample was verified with Cronbach's Alpha (which is a .70, aka 70%, threshold for raters for the measure reliability and is thus considered a good/valid question model). This model drew on previous Information Systems models such as Goodhue's and Straub's research on centralized/top management managerial concerns.

PACRM is a statistics model. Theory of Planned Behavior (TPB) about types of beliefs (such as belief in compliance or not) is implemented into the author's model, and references Self-Efficacy Theory (SET). Viruses and Defense-in-Depth are discussed as concerns for IT

managers. The PACRM is correlated to the Center for Internet Security (CIS) controls. Metrics/Measurements for each factor in the model are provided by Chapman. This was an exploratory study with limited observations (135 IT Managers), so it is not a full structural equation model. Path analysis was used instead, averaging out paths, but only a handful of the paths shown (regression) in the model were supported. Meanwhile 11 of the 21 hypotheses were supported (some not shown in the model paths) according to the author.

Overall, the survey asked managers if they were experts, which is a self-efficacy theory idea, and then tried to correlate findings with hypothesis. PACRM was processed in Statistical Package for the Social Sciences (SPSS). R-squared and chi-squared through Confirmatory Factor Analysis (CFA), for model validity, didn't show a great chi-squared fit for the model, but still was considered acceptable by the author.

Figure 4 – Chapmans PACRM Detect, Prevent, Recover Model and each Proposition/Hypothesis Link/Path



Note: Taken from T. A. Chapman, "Factors Affecting Perceptions of Cybersecurity Readiness Among Workgroup IT Managers," Doctor of Philosophy in Business Administration, Management Information Systems, University of Mississippi, 2018.

ICS Testbed Tetris: Practical Building Blocks Towards a Cyber Security Resource

This paper proposes a high-level model/reference architecture for Industrial Controls Systems (ICS) testing environment [28]. The testing environment could be virtual or physical.

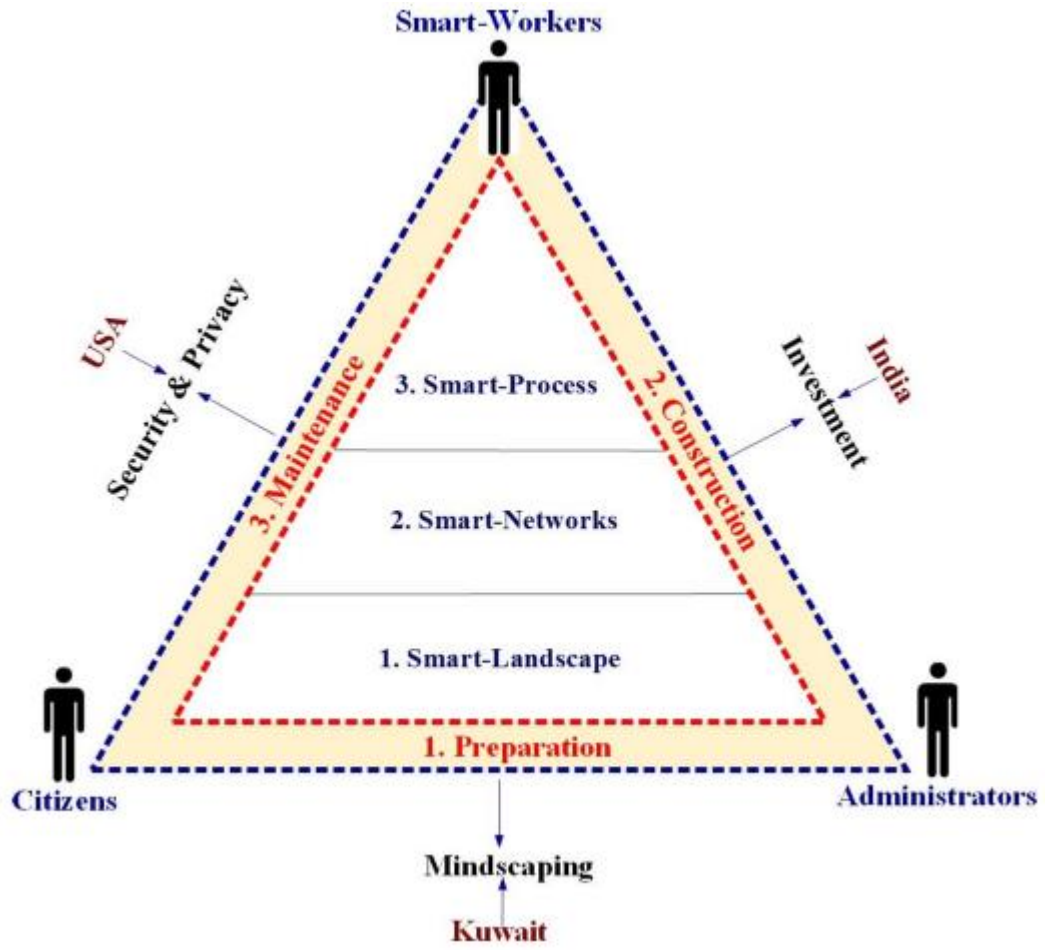
Testing is more that simulations alone and is more practical. A survey was conducted to provide and create the reference model. ICS models at the device level are prescriptive and not generalizable thus this model only creates oversight layers (for engaging a testing strategy). A discussion of devices categories and concerns is provided.

The Purdue model is used as a comparative model to the ICS Testbed model. Like the Purdue model not every level is needed in every environment. A testbed is protected from unauthorized disruption. Layers (e.g., environment, experimental, user) and bridges are the terms used for this model. Safety and security are considered in all parts of the model. In a testbed a single tunnel or access point is recommended for each internet connectivity level.

Internet of Things & Cybersecurity Readiness in Smart-government and Organizations

This Kuwait Master's thesis discusses IoT in cities [5]. Measurement is done through a survey, in India, USA, and Kuwait, on IoT usage and performance. The author states that Closed Circuit Television (CCTV) is a staple for any city to be smart. Economy, mobility, and governance are common categories for smart city measurements. The smart government philosophy is related to open sharing of information and e-data processing.

This paper's model recognizes phases: preparation, construction, and maintenance. The challenge, the author states, is infrastructure investment in these phases. Embedded systems/IoT are terms created by Massachusetts Institute of Technology (MIT) and Cisco Systems over the years of computer history. IoT is still considered a new technology.



Note: Taken from A. AlEnezi, "Internet of Things & Cybersecurity Readiness in Smart-government and Organizations," Master's Degree in Information Technology, Information Technology, Kuwait University, 2020.

Additionally, statistical analysis, that is social science (a small sample dataset structural equation model) was conducted. Conducted from the survey in order to look at relationships between the answers based on Likert scale readiness answers (looking for statistical significance). Investment, Compliance, and Risk were found correlated to Cybersecurity Readiness.

Mobile Cloud Forensic Readiness Process Model for Cloud-Based Mobile Applications

This article from India discusses the peculiarities for mobile and cloud [23]. Cloud severs and systems allows global mobile demands to scale easily. The forensic process takes place after an incident has taken place. Digital, Smartphone, Mobile, and Cloud models, and conceptual

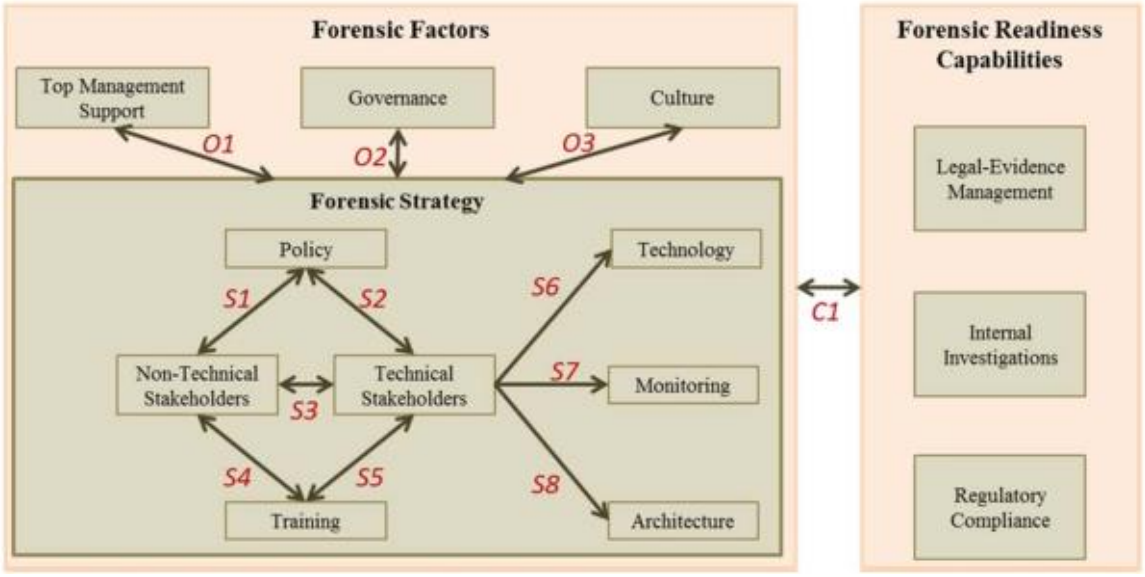
frameworks already have existed. Because forensics it is a costly and time-consuming process readiness work is justified.

The author's model/framework is based on business goals and objectives which is a little different than , but relies heavily on, the legal only goals of other model and frameworks. Integrity, Reliability, Completeness, and Admissibility are important concerns of forensics readiness. The device and the cloud system/database (i.e., the Cloud Service Provider (CSP)) have to be correlated (often a keeping the correct time/date stamp concern) to provide the complete infrastructure-based evidence if needed for the investigation. The contract/Service Level Agreement (SLA) is important to obtaining the CSP concurrence. The CSP also has to be willing to work with the investigator. The author's output was a sequence diagram (aka a workflow) for the investigation process.

Towards a Systemic Framework for Digital Forensic Readiness

This journal article by University of Melbourne Australia authors write about organizational forensic readiness [30]. The framework is based on Literature Review. Forensics are often carried out internally before or even if a jurisdictional proceeding ever occurs. Each factor (including those in strategy) is explained in detail.

Figure 5 - Organizational Forensic Readiness Model for Digital Evidence



Note: Taken from M. Elyas, S. B. Maynard, A. Ahmad, and A. Lonie, "Towards a Systemic Framework for Digital Forensic Readiness," Journal of Computer Information Systems, vol. 54, pp. 97-105, January 2014.

Towards verifiable evidence generation in forensic-ready systems

This IEEE conference paper proposes a workflow process, based on a roadmap, for digital evidence from software systems [25]. Syntax, Semantic (knowledge if A affects or

answers B), quality (timestamps, chain of custody, etc.) being followed, and handling data so it's "not dirty." This model can be used for attacks and/or failures of systems and software. Trusted evidence like an airplanes black box is the goal of this papers output.

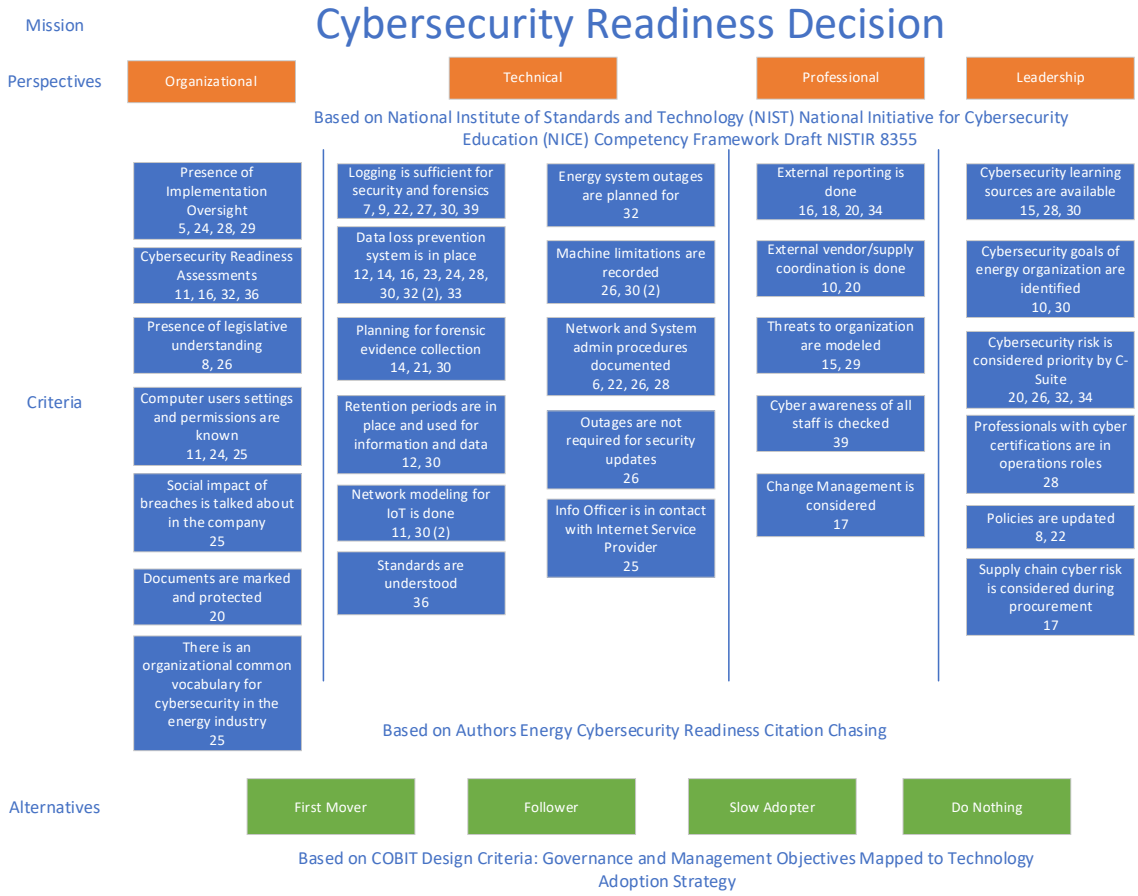
Conclusion

In the research leading up to this Criterion Clarification paper an in-depth literature was review performed on the topic of Cybersecurity Readiness in the Energy Industry. This paper is a follow-on that elaborates and clarifies the criterion gaps found in that research in order to provide details into the categorization of articles, the overall takeaways, and the open and remaining questions are to be answered through further research and expert judgement.

While there has been some Cybersecurity readiness modeling, i.e., Cybersecurity Readiness in Energy and closely related Industries, most models are statistical in nature rather than decision model based. Yet, some research is process models, some is merely theoretical, and some are categorizations/checklists that can help in practical assessments. However, no Multicriteria Decision Model for Cybersecurity Readiness in the Energy Industry (only partial models) has yet been published.

Appendices

Appendix A: HDM Model (Version 6)



Note: Current Portland State University (PSU) web based HDM software tool allows only up to 11 criterions in any Perspective grouping.

Appendix B: 74 Article Data Points for HDM Model Criterion (Sorted by Competency)

Article #	NIST NICE Competencies	Article Name	Criterion
15	Leadership	A. A. Cardenas, T. Roosta, G. Taban, and S. Sastry, "Cyber Security Basic Defenses and Attack Trends," in Homeland Security, ed, 2008, pp. 73-102.	Cybersecurity learning sources are available
30	Leadership	K. A. Z. Ariffin and F. H. Ahmad, "Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0," Computer & Security, vol. 105, Feb. 15 2021.	Cybersecurity learning sources are available
10	Leadership	W. Miron, "Adoption of Cybersecurity Capability Maturity Models in Municipal Governments," Master of Applied Science, Technology Innovation Management, Carleton University, Ottawa, Canada, 2015.	Cybersecurity goals of energy organization are identified
30	Leadership	K. A. Z. Ariffin and F. H. Ahmad, "Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0," Computer & Security, vol. 105, Feb. 15 2021.	Cybersecurity goals of energy organization are identified
34	Leadership	E. Gott and K. Greenfield, "New tool assesses banks' cybersecurity readiness," The Risk Management Association Journal, vol. 98, 2015.	Cybersecurity risk is considered priority by C-Suite
32	Leadership	L. J. Trautman, "Managing Cyberthreat," Santa Clara High Technology Law Journal, vol. 33, pp. 230-287, Jan. 2 2017.	Cybersecurity risk is considered priority by C-Suite
28	Leadership	N. Muraguri, T. Mwalili, and T. Mose, "Factors influencing cybersecurity readiness in deposit taking savings and credit cooperatives: A case study of Nairobi County," International Academic Journal of Information Systems and Technology, vol. 2, pp. 157182, 2019.	Cybersecurity learning sources are available
28	Leadership	N. Muraguri, T. Mwalili, and T. Mose, "Factors influencing cybersecurity readiness in deposit taking savings and credit cooperatives: A case study of Nairobi County," International Academic Journal of Information Systems and Technology, vol. 2, pp. 157182, 2019.	Professionals with cyber certifications are in operations roles
26	Leadership	E. Bajramovic, K. Waedt, A. Ciriello, and D. Gupta, "Forensic Readiness of Smart Buildings: Preconditions for Cybersecurity Tests," IEEE, 2016.	Cybersecurity risk is considered priority by C-Suite
22	Leadership	E. Bajramovic, "Secure Logging in Operational Instrumentation and Control Systems," Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), 2019.	Policies are updated
20	Leadership	D. G. Datong, "Cyber-Terrorism: Nigeria's Payment System Infrastructural Readiness," Master of Conflict Security and Development (MCSD), Department of History and War Studies, Nigerian Defence Academy (NDA), 2018.	Cybersecurity risk is considered priority by C-Suite
17	Leadership	A. L. Johnson, "Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation," UNC School of Law: North Carolina Banking Institute, vol. 20, March 1 2016.	Supply chain cyber risk is considered during procurement

8	Leadership	H. Zhang, Z. Tang, and K. Jayakar, "A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-Government services," in TPRC, 2017.	Policies are updated
5	Organizational	D. Eilts, "An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses," Doctor of Philosophy in Information Systems, College of Computing and Engineering, Nova Southeastern University, Florida, 2020.	Presence of Implementation Oversight
29	Organizational	M. Abdalla and Y. Arshad, "Information Security: Cybersecurity Standards Adoption Among Malaysian Public Listed Companies," International Journal of Engineering Research & Technology (IJERT), vol. 9, pp. 929-933, August 2020.	Presence of Implementation Oversight
11	Organizational	A. AlEnezi, "Internet of Things & Cybersecurity Readiness in Smart-government and Organizations," Master's Degree in Information Technology, Information Technology, Kuwait University, 2020.	Cybersecurity Readiness Assessments
32	Organizational	L. J. Trautman, "Managing Cyberthreat," Santa Clara High Technology Law Journal, vol. 33, pp. 230-287, Jan. 2 2017.	Cybersecurity Readiness Assessments
36	Organizational	A. D. Pereira da Silva and Y. Bobbert, "Cybersecurity Readiness: An Empirical Study of Effective Cybersecurity Practices for Industrial Control Systems," Scientific Journal of Research and Reviews, Dec. 18 2019.	Cybersecurity Readiness Assessments
28	Organizational	N. Muraguri, T. Mwalili, and T. Mose, "Factors influencing cybersecurity readiness in deposit taking savings and credit cooperatives: A case study of Nairobi County," International Academic Journal of Information Systems and Technology, vol. 2, pp. 157182, 2019.	Presence of Implementation Oversight
26	Organizational	E. Bajramovic, K. Waedt, A. Ciriello, and D. Gupta, "Forensic Readiness of Smart Buildings: Preconditions for Cybersecurity Tests," IEEE, 2016.	Presence of legislative understanding
25	Organizational	T. A. Chapman, "Factors Affecting Perceptions of Cybersecurity Readiness Among Workgroup IT Managers," Doctor of Philosophy in Business Administration, Management Information Systems, University of Mississippi, 2018.	Computer user's settings and permissions are known
25	Organizational	T. A. Chapman, "Factors Affecting Perceptions of Cybersecurity Readiness Among Workgroup IT Managers," Doctor of Philosophy in Business Administration, Management Information Systems, University of Mississippi, 2018.	Social impact of breaches is talked about in the company
24	Organizational	S. Hasan, M. Ali, S. Kurnia, and R. Thurasamy, "Evaluating the cyber security readiness of organizations and its influence on performance," Journal of Information Security and Applications, vol. 58, p. 102726, Feb. 4 2021.	Computer user's settings and permissions are known
24	Organizational	S. Hasan, M. Ali, S. Kurnia, and R. Thurasamy, "Evaluating the cyber security readiness of organizations and its influence on performance," Journal of Information Security and Applications, vol. 58, p. 102726, Feb. 4 2021.	Presence of Implementation Oversight
20	Organizational	D. G. Datong, "Cyber-Terrorism: Nigeria's Payment System Infrastructural Readiness," Master of Conflict Security and Development (MCSD), Department of History and War Studies, Nigerian Defence Academy (NDA), 2018.	Documents are marked and protected

16	Organizational	B. Borgman, S. Mubarak, and K.-K. R. Choo, "Cyber security readiness in the South Australian Government," vol. 37, pp. 1-8, 2015.	Cybersecurity Readiness Assessments
11	Organizational	A. AlEnezi, "Internet of Things & Cybersecurity Readiness in Smart-government and Organizations," Master's Degree in Information Technology, Information Technology, Kuwait University, 2020.	Computer user's settings and permissions are known
8	Organizational	H. Zhang, Z. Tang, and K. Jayakar, "A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-Government services," in TPRC, 2017.	Presence of legislative understanding
16	Professional	B. Borgman, S. Mubarak, and K.-K. R. Choo, "Cyber security readiness in the South Australian Government," vol. 37, pp. 1-8, 2015.	External reporting is done
18	Professional	F. E. Catota, G. M. Morgan, and D. C. Sicker, "Cybersecurity incident response capabilities in the Ecuadorian financial sector," Journal of Cybersecurity, vol. 0, pp. 1-20, 2018.	External reporting is done
20	Professional	D. G. Datong, "Cyber-Terrorism: Nigeria's Payment System Infrastructural Readiness," Master of Conflict Security and Development (MCSD), Department of History and War Studies, Nigerian Defence Academy (NDA), 2018.	External reporting is done
34	Professional	E. Gott and K. Greenfield, "New tool assesses banks' cybersecurity readiness," The Risk Management Association Journal, vol. 98, 2015.	External reporting is done
15	Professional	A. A. Cardenas, T. Roosta, G. Taban, and S. Sastry, "Cyber Security Basic Defenses and Attack Trends," in Homeland Security, ed, 2008, pp. 73-102.	Threats to organization are modeled
29	Professional	M. Abdalla and Y. Arshad, "Information Security: Cybersecurity Standards Adoption Among Malaysian Public Listed Companies," International Journal of Engineering Research & Technology (IJERT), vol. 9, pp. 929-933, August 2020.	Threats to organization are modeled
10	Professional	W. Miron, "Adoption of Cybersecurity Capability Maturity Models in Municipal Governments," Master of Applied Science, Technology Innovation Management, Carleton University, Ottawa, Canada, 2015.	External vendor/supply coordination is done
20	Professional	D. G. Datong, "Cyber-Terrorism: Nigeria's Payment System Infrastructural Readiness," Master of Conflict Security and Development (MCSD), Department of History and War Studies, Nigerian Defence Academy (NDA), 2018.	External vendor/supply coordination is done
39	Professional	R. R. Mills, "The Current State of Insider Threat Awareness and Readiness in Corporate Cyber Security - An Analysis of Definitions, Preventions, Detection, and Mitigation," Master of Science in Cybersecurity, Utica College, 2018.	Cyber awareness of all staff is checked
7	Technical	L. Daubner, M. Macak, B. Buhnova, and T. Pitner, "Towards verifiable evidence generation in forensic-ready systems," in 2020 IEEE International Conference on Big Data (Big Data), 2020, pp. 2264-2269.	Logging is sufficient for security and forensics
30	Technical	K. A. Z. Ariffin and F. H. Ahmad, "Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0," Computer & Security, vol. 105, Feb. 15 2021.	Logging is sufficient for security and forensics
39	Technical	R. R. Mills, "The Current State of Insider Threat Awareness and Readiness in Corporate Cyber Security - An Analysis of	Logging is sufficient for security and forensics

		Definitions, Preventions, Detection, and Mitigation," Master of Science in Cybersecurity, Utica College, 2018.	
28	Technical	N. Muraguri, T. Mwalili, and T. Mose, "Factors influencing cybersecurity readiness in deposit taking savings and credit cooperatives: A case study of Nairobi County," International Academic Journal of Information Systems and Technology, vol. 2, pp. 157182, 2019.	Data loss prevention system is in place
30	Technical	K. A. Z. Ariffin and F. H. Ahmad, "Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0," Computer & Security, vol. 105, Feb. 15 2021.	Data loss prevention system is in place
23	Technical	M. H. Shah, R. Muhammad, and N. Ameen, "Cybersecurity Readiness of E-tail Organisations: A Technical Perspective," presented at the I3E 2020 – 19th IFIP Conference on e-Business, e-Services and e-Society, Skukuza, Kruger National Park, South Africa, 2020.	Data loss prevention system is in place
24	Technical	S. Hasan, M. Ali, S. Kurnia, and R. Thurasamy, "Evaluating the cyber security readiness of organizations and its influence on performance," Journal of Information Security and Applications, vol. 58, p. 102726, Feb. 4 2021.	Data loss prevention system is in place
32	Technical	L. J. Trautman, "Managing Cyberthreat," Santa Clara High Technology Law Journal, vol. 33, pp. 230-287, Jan. 2 2017.	Data loss prevention system is in place
22	Technical	E. Bajramovic, "Secure Logging in Operational Instrumentation and Control Systems," Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), 2019.	Logging is sufficient for security and forensics
27	Technical	J. Li, E. Bajramovic, Y. Gao, and M. Parekh, "Graded security forensics readiness of SCADA systems," Informatik 2016, 2016.	Logging is sufficient for security and forensics
21	Technical	M. Elyas, S. B. Maynard, A. Ahmad, and A. Lonie, "Towards a Systemic Framework for Digital Forensic Readiness," Journal of Computer Information Systems, vol. 54, pp. 97105, January 2014.	Planning for forensic evidence collection
30	Technical	K. A. Z. Ariffin and F. H. Ahmad, "Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0," Computer & Security, vol. 105, Feb. 15 2021.	Planning for forensic evidence collection
16	Technical	B. Borgman, S. Mubarak, and K.-K. R. Choo, "Cyber security readiness in the South Australian Government," vol. 37, pp. 1-8, 2015.	Data loss prevention system is in place
32	Technical	L. J. Trautman, "Managing Cyberthreat," Santa Clara High Technology Law Journal, vol. 33, pp. 230-287, Jan. 2 2017.	Data loss prevention system is in place
14	Technical	A. Alenezi, H. F. Atlam, and G. B. Wills, "Experts reviews of a could forensic readiness framework for organizations," Journal of Cloud Computing: Advances, Systems and Applications, vol. 8, 2019.	Planning for forensic evidence collection
30	Technical	K. A. Z. Ariffin and F. H. Ahmad, "Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0," Computer & Security, vol. 105, Feb. 15 2021.	Retention periods are in place and used for information and data
12	Technical	V. R. Kebande, N. M. Karie, and H. S. Venter, "A Generic Digital Forensic Readiness Model for BYOD using Honeypot Technology," in IST-Africa 2016, 2016.	Retention periods are in place and used for

			information and data
30	Technical	K. A. Z. Ariffin and F. H. Ahmad, "Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0," Computer & Security, vol. 105, Feb. 15 2021.	Network modeling for IoT is done
12	Technical	V. R. Kebande, N. M. Karie, and H. S. Venter, "A Generic Digital Forensic Readiness Model for BYOD using Honeypot Technology," in IST-Africa 2016, 2016.	Data loss prevention system is in place
14	Technical	A. Alenezi, H. F. Atlam, and G. B. Wills, "Experts reviews of a could forensic readiness framework for organizations," Journal of Cloud Computing: Advances, Systems and Applications, vol. 8, 2019.	Data loss prevention system is in place
30	Technical	K. A. Z. Ariffin and F. H. Ahmad, "Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0," Computer & Security, vol. 105, Feb. 15 2021.	Machine limitations are recorded
33	Technical	P. Sharma, D. Arora, and T. Sakthivel, "Mobile Cloud Forensic Readiness Process Model for Cloud-Based Mobile Applications," Internal Journal of Digital Crime and Forensics, vol. 12, pp. 58-76, September 2020.	Data loss prevention system is in place
11	Technical	A. AlEnezi, "Internet of Things & Cybersecurity Readiness in Smart-government and Organizations," Master's Degree in Information Technology, Information Technology, Kuwait University, 2020.	Network modeling for IoT is done
30	Technical	K. A. Z. Ariffin and F. H. Ahmad, "Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0," Computer & Security, vol. 105, Feb. 15 2021.	Network modeling for IoT is done
36	Technical	A. D. Pereira da Silva and Y. Bobbert, "Cybersecurity Readiness: An Empirical Study of Effective Cybersecurity Practices for Industrial Control Systems," Scientific Journal of Research and Reviews, Dec. 18 2019.	Standards are understood
32	Technical	L. J. Trautman, "Managing Cyberthreat," Santa Clara High Technology Law Journal, vol. 33, pp. 230-287, Jan. 2 2017.	Energy system outages are planned for
30	Technical	K. A. Z. Ariffin and F. H. Ahmad, "Indicators for maturity and readiness for digital forensic investigation in era of industrial revolution 4.0," Computer & Security, vol. 105, Feb. 15 2021.	Machine limitations are recorded
28	Technical	N. Muraguri, T. Mwalili, and T. Mose, "Factors influencing cybersecurity readiness in deposit taking savings and credit cooperatives: A case study of Nairobi County," International Academic Journal of Information Systems and Technology, vol. 2, pp. 157182, 2019.	Network and System admin procedures documented
26	Technical	E. Bajramovic, K. Waedt, A. Ciriello, and D. Gupta, "Forensic Readiness of Smart Buildings: Preconditions for Cybersecurity Tests," IEEE, 2016.	Network and System admin procedures documented
26	Technical	E. Bajramovic, K. Waedt, A. Ciriello, and D. Gupta, "Forensic Readiness of Smart Buildings: Preconditions for Cybersecurity Tests," IEEE, 2016.	Machine limitations are recorded

26	Technical	E. Bajramovic, K. Waedt, A. Ciriello, and D. Gupta, "Forensic Readiness of Smart Buildings: Preconditions for Cybersecurity Tests," IEEE, 2016.	Outages are not required for security updates
25	Technical	T. A. Chapman, "Factors Affecting Perceptions of Cybersecurity Readiness Among Workgroup IT Managers," Doctor of Philosophy in Business Administration, Management Information Systems, University of Mississippi, 2018.	Info Officer is in contact with Internet Service Provider
25	Organizational	T. A. Chapman, "Factors Affecting Perceptions of Cybersecurity Readiness Among Workgroup IT Managers," Doctor of Philosophy in Business Administration, Management Information Systems, University of Mississippi, 2018.	There is an organizational common vocabulary for cybersecurity in the energy industry
22	Technical	E. Bajramovic, "Secure Logging in Operational Instrumentation and Control Systems," Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), 2019.	Network and System admin procedures documented
17	Technical	A. L. Johnson, "Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation," UNC School of Law: North Carolina Banking Institute, vol. 20, March 1 2016.	Change Management is considered
9	Technical	A. Pooe and L. Labuschagne, "A conceptual model for digital forensic readiness," 2012.	Logging is sufficient for security and forensics
6	Technical	B. Green, R. Derbyshire, W. Knowles, J. Boorman, P. Ciholas, D. Prince, et al., "ICS Testbed Tetris: Practical Building Blocks Towards a Cyber Security Resource," School of Computing and Communications, Lancaster University, United Kingdom, 2020.	Network and System admin procedures documented
Total	**74**		

Appendix C: 29 Sorted Criterion from 74 Data Points

Article #	NIST NICE Competencies	Criterion	Raw concerns of the article
17	Technical	**Change Management is considered**	Do you monitor changes to your network
11	Organizational	**Computer user's settings and permissions are known**	Have you developed security requirements lately
24	Organizational	**Computer user's settings and permissions are known**	Have you tested cybersecurity practices against organizational performance?
25	Organizational	**Computer user's settings and permissions are known**	Do line managers understand cybersecurity profiles for staff
39	Professional	**Cyber awareness of all staff is checked**	Does your team understand the difference between good and bad cyber behavior?
10	Leadership	**Cybersecurity goals of energy organization are identified**	Controls in place for progressive cyber goals
30	Leadership	**Cybersecurity goals of energy organization are identified**	Do you have a dashboard for security status (e.g., people, processes, and technology)?
15	Leadership	**Cybersecurity learning sources are available**	Do you have security resources for people on your staff
28	Leadership	**Cybersecurity learning sources are available**	For those with cybersecurity responsibility do they know all the organizations policies and practices?
30	Leadership	**Cybersecurity learning sources are available**	Are continuous security improvement processes documented?
11	Organizational	**Cybersecurity Readiness Assessments**	Have surveys and checklists for auditing
16	Organizational	**Cybersecurity Readiness Assessments**	Does assessment incorporate both assets and data
32	Organizational	**Cybersecurity Readiness Assessments**	Have you analyzed if audits done are effective?
36	Organizational	**Cybersecurity Readiness Assessments**	Do you rate your cyber assessment methods annually?
20	Leadership	**Cybersecurity risk is considered priority by C-Suite**	Is terrorism secured against?
26	Leadership	**Cybersecurity risk is considered priority by C-Suite**	Are you paying same or more attention on security than on ease of use and time to market?
32	Leadership	**Cybersecurity risk is considered priority by C-Suite**	Does the board have IT security minds?;
34	Leadership	**Cybersecurity risk is considered priority by C-Suite**	Is cybersecurity a key component of the risk management program?
12	Technical	**Data loss prevention system is in place**	A forensic model in place for when an event occurs
14	Technical	**Data loss prevention system is in place**	A forensic model for cloud assets
16	Technical	**Data loss prevention system is in place**	Do you have an infosec mgmt. System in place
23	Technical	**Data loss prevention system is in place**	Do you have a system for threat management?
24	Technical	**Data loss prevention system is in place**	Do you prevent, detect, and combat attacks?
28	Technical	**Data loss prevention system is in place**	Is there a cyber data loss prevention system?

30	Technical	**Data loss prevention system is in place**	Do you have post-incident procedures?
32	Technical	**Data loss prevention system is in place**	Do you have a comprehensive list of security considerations specific to your use case (e.g., info tech, industrial control system, etc.)?
32	Technical	**Data loss prevention system is in place**	Do you have a reporting and escalation written procedure for incidents?
33	Technical	**Data loss prevention system is in place**	Can cloud information be successfully isolated (without losing the data) if there is an incident?
20	Organizational	**Documents are marked and protected**	Are policies considered classified information?
32	Technical	**Energy system outages are planned for**	Do you have a contingency plan if your organization is without power for a prolonged period of time?
16	Professional	**External reporting is done**	Do you report to an entity on security?
18	Professional	**External reporting is done**	Do you report to an entity on security?
20	Professional	**External reporting is done**	Do you share information on cybersecurity with your partners?
34	Professional	**External reporting is done**	Does your industry have an association to supervise cybersecurity and are you a part of it?
10	Professional	**External vendor/supply coordination is done**	Do you coordinate with other organizations on cyber security sharing
20	Professional	**External vendor/supply coordination is done**	Do you get cybersecurity information updates?
25	Technical	**Info Officer is in contact with Internet Service Provider**	Does the internet service provider and IT manager talk?
7	Technical	**Logging is sufficient for security and forensics**	Insufficient logging was most limiting factor in cyber investigations
9	Technical	**Logging is sufficient for security and forensics**	Are storage devices automation completely controlled
22	Technical	**Logging is sufficient for security and forensics**	Are timestamps of events able to be recorded with certainty that the timestamp as not been changed
27	Technical	**Logging is sufficient for security and forensics**	Is accurate time being logged in logs
30	Technical	**Logging is sufficient for security and forensics**	Based on your network size have you scoped out what you will and will not be able to collect?
39	Technical	**Logging is sufficient for security and forensics**	Is information sent to a log system that is retrievable and understandable?
26	Technical	**Machine limitations are recorded**	Are interconnected assets information known?
30	Technical	**Machine limitations are recorded**	Have you documented your iot device limitations for control?
30	Technical	**Machine limitations are recorded**	If you have open source and/or propriety software have you documented all the security limitations?
6	Technical	**Network and System admin procedures documented**	Subnetting over between zones is complex
22	Technical	**Network and System admin procedures documented**	Are your interfaces hardened for only serving on common ports and normal protocol setups?
26	Technical	**Network and System admin procedures documented**	Are interconnected devices considered above low risk?
28	Technical	**Network and System admin procedures documented**	Do you know if your cybersecurity controls are accurate, if so are they verified and validated?
11	Technical	**Network modeling for IoT is done**	Need model for mitigating cyber iot access control

30	Technical	**Network modeling for IoT is done**	Do you have a backup logging for iot device logs
30	Technical	**Network modeling for IoT is done**	Do you have visibility and control of your cloud assets?
26	Technical	**Outages are not required for security updates**	Can security assessments be done while systems are up or if not can some systems be brought down to test?
14	Technical	**Planning for forensic evidence collection**	Possible to gather evidence from cloud without cloud providers help?
21	Technical	**Planning for forensic evidence collection**	Are industry guidelines used for digital evidence collection?
30	Technical	**Planning for forensic evidence collection**	Do you have forensic collection methods? Do you have a chain of custody written down for evidence if needed?
8	Leadership	**Policies are updated**	Is data from cyber experts anonymized to inhibit full disclosure
22	Leadership	**Policies are updated**	Is authentication security address in policy?
5	Organizational	**Presence of Implementation Oversight**	Consistent implementation of security measures
24	Organizational	**Presence of Implementation Oversight**	Periodic training on new complexities
28	Organizational	**Presence of Implementation Oversight**	Have polices for firewalls been documented and vetted?
29	Organizational	**Presence of Implementation Oversight**	Are proactive practical procedures in place?
8	Organizational	**Presence of legislative understanding**	Are there penalties for non-compliance
26	Organizational	**Presence of legislative understanding**	Is someone assigned to review the latest privacy legislation?
28	Leadership	**Professionals with cyber certifications are in operations roles**	Do you feel aware of the cybersecurity technologies, if so are do you have people with certifications or recent academic degrees?
12	Technical	**Retention periods are in place and used for information and data**	A forensic model for cloud assets
30	Technical	**Retention periods are in place and used for information and data**	Do you have offline backups of everything?
25	Organizational	**Social impact of breaches is talked about in the company**	Is social engineering awareness covered (including effects on user)
36	Technical	**Standards are understood**	Do you have someone on staff who can interpret cybersecurity standards?
17	Leadership	**Supply chain cyber risk is considered during procurement**	Do you control activities of third parties in supply chain?
25	Organizational	**There is an organizational common vocabulary for cybersecurity in the energy industry**	Are users able to detect and prevent cyberattacks?
15	Professional	**Threats to organization are modeled**	Do you have a verified and validated threat model?
29	Professional	**Threats to organization are modeled**	Is news of threats and breaches shared often?
Total	**74**		

References

[1] A. Cavanaugh, "Towards a Cybersecurity Readiness Gap Analysis in the Energy Industry using Citation Chasing and Web of Science Bibliometric Analysis," Portland State Univeristy, Portland, ORJune 11 2021.

[2] A. L. Johnson, "Cybersecurity for Financial Institutions: The Integral Role of Information Sharing in Cyber Attack Mitigation," *UNC School of Law: North Carolina Banking Institute,* vol. 20, March 1 2016.

[3] A. Cavanaugh, "Change and Configuration Management Plan (Proposal)," MESA Oregon, Portland, ORDec. 11 2020.

[4] T. A. Chapman, "Factors Affecting Perceptions of Cybersecurity Readiness Among Workgroup IT Managers," Doctor of Philosophy in Business Administration, Management Information Systems, University of Mississippi, 2018.

[5] A. AlEnezi, "Internet of Things & Cybersecurity Readiness in Smart-government and Organizations," Master's Degree in Information Technology, Information Technology, Kuwait University, 2020.

[6] S. Hasan, M. Ali, S. Kurnia, and R. Thurasamy, "Evaluating the cyber security readiness of organizations and its influence on performance," *Journal of Information Security and Applications,* vol. 58, p. 102726, Feb. 4 2021.

[7] R. R. Mills, "The Current State of Insider Threat Awareness and Readiness in Corporate Cyber Security - An Analysis of Definitions, Preventions, Detection, and Mitigation," Master of Science in Cybersecurity, Utica College, 2018.

[8] W. Miron, "Adoption of Cybersecurity Capability Maturity Models in Municipal Governments," Master of Applied Science, Technology Innovation Management, Carleton University, Ottawa, Canada, 2015.

[9] K. A. Z. Ariffin and F. H. Ahmad, "Indicators for maturity and readiness for digital forensic invesitgation in era of industrial revolution 4.0," *Computer & Security,* vol. 105, Feb. 15 2021.

[10] A. A. Cardenas, T. Roosta, G. Taban, and S. Sastry, "Cyber Security Basic Defenses and Attack Trends," in *Homeland Security*, ed, 2008, pp. 73-102.

[11] N. Muraguri, T. Mwalili, and T. Mose, "Factors influencing cybersecurity readiness in deposit taking savings and credit cooperatives: A case study of Nairobi County," *International Academic Journal of Information Systems and Technology,* vol. 2, pp. 157-182, 2019.

[12] D. Eilts, "An Empirical Assessment of Cybersecurity Readiness and Resilience in Small Businesses," Doctor of Philosophy in Information Systems, College of Computing and Engineering, Nova Southeastern University, Florida, 2020.
[13] E. Bajramovic, "Secure Logging in Operational Instrumentation and Control Systems," Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU), 2019.
[14] B. Borgman, S. Mubarak, and K.-K. R. Choo, "Cyber security readiness in the South Australian Government," vol. 37, pp. 1-8, 2015.
[15] L. J. Trautman, "Managing Cyberthreat," *Santa Clara High Technology Law Journal,* vol. 33, pp. 230-287, Jan. 2 2017.
[16] A. D. Pereira da Silva and Y. Bobbert, "Cybersecurity Readiness: An Empirical Study of Effective Cybersecurity Practices for Industrial Control Systems," *Scientific Journal of Research and Reviews,* Dec. 18 2019.
[17] E. Bajramovic, K. Waedt, A. Ciriello, and D. Gupta, "Forensic Readiness of Smart Buildings: Preconditions for Cybersecurity Tests," *IEEE,* 2016.
[18] E. Gott and K. Greenfield, "New tool assesses banks' cybersecurity readiness," *The Risk Managment Association Journal,* vol. 98, 2015.
[19] D. G. Datong, "Cyber-Terrorism: Nigeria's Payment System Infrastructural Readiness," Master of Conflict Security and Development (MCSD), Department of History and War Studies, Nigerian Defence Academy (NDA), 2018.
[20] V. R. Kebande, N. M. Karie, and H. S. Venter, "A Generic Digital Forensic Readiness Model for BYOD using Honeypot Technology," in *IST-Africa 2016*, 2016.
[21] A. Alenezi, H. F. Atlam, and G. B. Wills, "Experts reviews of a could forensic readiness framework for organizations," *Journal of Cloud Computing: Advances, Systems and Applications,* vol. 8, 2019.
[22] M. H. Shah, R. Muhammad, and N. Ameen, "Cybersecurity Readiness of E-tail Organisations: A Technical Perspective," presented at the I3E 2020 – 19th IFIP Conference on e-Business, e-Services and e-Society, Skukuza, Kruger National Park, South Africa, 2020.
[23] P. Sharma, D. Arora, and T. Sakthivel, "Mobile Cloud Forensic Readiness Process Model for Cloud-Based Mobile Applications," *Internal Journal of Digital Crime and Forensics,* vol. 12, pp. 58-76, September 2020.
[24] F. E. Catota, G. M. Morgan, and D. C. Sicker, "Cybersecurity incident response capabilities in the Ecuadorian financial sector," *Journal of Cybersecurity,* vol. 0, pp. 1-20, 2018.

[25] L. Daubner, M. Macak, B. Buhnova, and T. Pitner, "Towards verifiable evidence generation in forensic-ready systems," in *2020 IEEE International Conference on Big Data (Big Data)*, 2020, pp. 2264-2269.
[26] J. Li, E. Bajramovic, Y. Gao, and M. Parekh, "Graded security forensics readiness of SCADA systems," *Informatik 2016,* 2016.
[27] A. Pooe and L. Labuschagne, "A conceptual model for digital forensic readiness," 2012.
[28] B. Green, R. Derbyshire, W. Knowles, J. Boorman, P. Ciholas, D. Prince*, et al.*, "ICS Testbed Tetris: Practical Building Blocks Towards a Cyber Security Resource," School of Computing and Communications, Lancaster University, United Kingdom, 2020.
[29] A. AlEnezi, "Internet of Things & Cybersecurity Readiness in Smart-government and Organizations," 2019.
[30] M. Elyas, S. B. Maynard, A. Ahmad, and A. Lonie, "Towards a Systemic Framework for Digital Forensic Readiness," *Journal of Computer Information Systems,* vol. 54, pp. 97-105, January 2014.
[31] H. Zhang, Z. Tang, and K. Jayakar, "A socio-technical analysis of China's cybersecurity policy: Towards delivering trusted e-Government services," in *TPRC*, 2017.
[32] M. Abdalla and Y. Arshad, "Information Security: Cybersecurity Standards Adoption Among Malaysian Public Listed Companies," *International Journal of Engineering Research & Technology (IJERT),* vol. 9, pp. 929-933, August 2020.