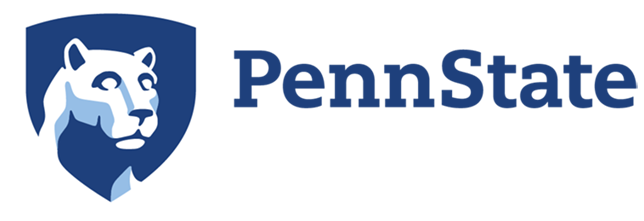
Pritsiolas, John J

JJP46@PSU.EDU



Reducing Cybersecurity Risks for a Gas Industry Company by Creating an Information Security Program

**Abstract**

The energy sector has seen an increase in cyber-attacks over the last decade, with little signs of a trough in the foreseeable future. At a granular level, gas organizations have also bore the burden of some of these attacks within the sector (Bronk & Tikk-Ringas, 2013). In light of the increase in cyber-attacks, gas organizations can do their part in reducing cyber risk and help stem the rise in attacks. In this sense, gas organizations can utilize an information security program and the respective program components to mitigate the cyber risk that confronts their firm. This research endeavor focuses on these components and how some gas organizations have implemented them in their information security program. The primary question of this research study is to determine: What role does an information security program play in reducing the cyber risk that a gas organization faces? Within the confines of this research endeavor, I examine the different components of an information security program and then juxtapose these components against the real world application of these components in a gas organization. As a result of the subsequent examination, I have developed the ISP (Information Security Program) Model. The model itself resembles a honeycomb and demonstrates the interdependency of each component within an information security program.

**Introduction**

The gas industry currently faces a future that is plagued by poor security practices and a lack of resources devoted to cybersecurity efforts. As a result, there is a genuine need for the creation of information security programs within gas organizations to reduce the cyber risk that they face. Additionally, while the energy sector as a whole has been targeted by a number of APTs including Duqu and Night Dragon (Wueest, 2014), the sector as a whole has not seen a demonstrable increase in cyber security spending. Despite repeated cyber-attacks, it has been estimated that organizations in this sector still spend less than 0.02% of their overall revenue on cybersecurity (Malik, 2018).

The lack of comprehensive information security programs and absence of resources has even drawn a warranted level of concern from the Department of Energy, with a recent report being released for public consumption. One notable statistic found that in 2016, ICS-CERT responded 290 cyber incidents in the United States, with 59 incidents belonging to the energy sector. Alarmingly, this equates to roughly 20.3% incidents being addressed specifically in the energy sector. To compound matters further, 26% of the 59 incidents that occurred in the sector could be directly attributed to spear phishing attacks. These types of incidents introduced persistent malware and even disrupted a power grid (“Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”, 2017). Moreover, the report detailed poor cyber security awareness and even the improper assessment of current assets. In order to combat the different cyber risk and threats confronting the sector, the Department of Energy made several recommendations. The DOE recommended that all energy organizations devote more resources to their cyber security departments, continuously conduct cyber risk impact analyses, and seek public-private initiatives to share information (“Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure”, 2017).

Needless to say, high levels of cyber risk could leave gas organizations vulnerable to cyber-attacks that could severely disrupt the economy of the United States. In light of the DOE report, it has previously been found that organizations who create a comprehensive information security program are in a better position to not only to reduce cyber risk, but also to safeguard themselves against cyber threats. In this regard, organizations with an information security program tend to have a stronger security-oriented culture and a positive effect on employee behavior (Chen, Ramamurthy, & Wen, 2015). On that note, the following literature review will provide additional context for the audience regarding this matter

**Literature Review**

## Introduction

The literature review was composed of research papers, journal articles, and magazine articles to best understand how an information security program and its components can reduce the cyber risk that a gas organization faces. The review was dependent on a number of scholarly sources including the IEEE Xplore Digital Library and Google Scholar. Different keywords and phrases were used to find scholarly sources, including: cyber risk management, the influence of information security policies, energy sector information security programs, cyber risk controls, and security awareness metrics. As a result of a rapidly changing threat landscape, the literature review consists of sources published within the last eleven years (2007 to 2018). The purpose of this literature review was to further develop the need for the creation of an information security program and the components that are necessary to reduce cyber risk in a gas organization.

## Information Security Program

Information security programs are instrumental in safeguarding a company as they can severely reduce the amount of cyber risk faced by an organization. An organization’s information security program includes several different foundational components. To start, information security policies play a significant role in the creation of a successful information security program. These policies tend to be concise documents that are internally available to all employees. Generally speaking, companies require employees to follow the information security policies that are published by the organization as punitive action may result for negligent behavior (Donaldson, Siegel, Williams, & Aslam, 2015). Another foundational component of an information security program pertains to cyber risk management. Cyber risk management adheres to the risk appetite of an organization and will establish controls within an organization to protect both critical and non-critical assets. These controls tend to be business oriented and meet the needs of the organization (Ross, 2011). A third component of an information security program is security awareness. Security awareness initiatives are used to train employees on different cybersecurity threats and trends that may be harmful to an organization. Security awareness initiatives also rely on metrics to judge the effectiveness of awareness training and can help determine the effectives of an information security program. Many security awareness initiatives tend to also incorporate industry standards and regulations within their training courses (Tsohou, Karyda, & Kokolakis, 2015).With that being said, there are currently several facets of a gas industry-specific information security program that remain unknown. In order for an information security program to be successful in helping to secure an organization, there needs to be an understanding of the business objectives of an organization. Likewise, the organization must be able to identify and classify critical assets in order to reduce a potentially high level of cyber risk.

Moreover, more research is required to determine how a mature information security program will evolve and adapt to a changing threat landscape in the gas industry. On this subject matter, understanding how gas organizations and even other energy organizations have traditionally handled a changing threat landscape, will be crucial for further study. Historical actions can provide valuable insight about the success and failure of these organizations in this regard.

Figure 1 presents some of the common components that are found in an organization’s information security program.

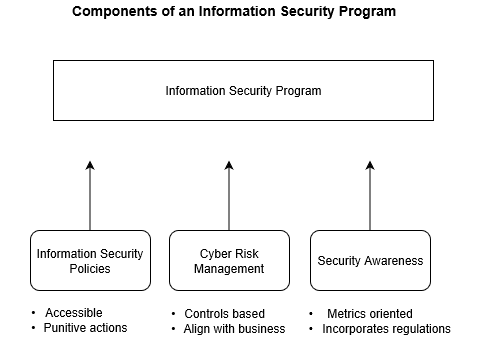


Figure 1. Information Security Program Components

## Information Security Policies

Information security policies will help employees adhere to an organization’s information security program. In this sense, employees are required by the terms of employment to abide by the information security policies created by the respective organization. Information policies should also be readily available to provide employees with a concise understanding of the different areas of cybersecurity that they are responsible for. These areas of responsibility can include basic security principles, such as acceptable computer use within the organization. More complex principles, such as the proper use of encryption, can also be found in these documents (Donaldson, Siegel, Williams, & Aslam, 2015). It has also been found that the presence of information security policies minimizes the chance for security incidents within an organization. This is in direct relation to the organization enforcement of punitive actions for an employee’s failure to act in accordance with the laid-out policies. Some consequences may negatively impact an employee’s performance report or even result in the employee being terminated from the organization (Donaldson, Siegel, Williams, & Aslam, 2015).

With that being said, additional information is required about information security policies that are exclusive to the gas industry. Similarly, there is also a need to understand employee responsibilities in both the gas industry and energy sector. These responsibilities have a bearing on the amount of cyber risk that is inherent within an organization and can have a direct impact on the formation of information security policies for a gas organization. A better understanding of these responsibilities is also necessary to determine the effects of punitive actions against negligent employees in this industry.

## Cyber Risk Management

Cyber Risk Management is another important aspect of an information security program because this component is responsible for the security controls that mitigate risk. Security controls are often implemented due to vulnerabilities or gaps found within an asset. However, the use of these controls is dependent upon the risk appetite of the organization. The risk appetite is the level of risk that an organization will accept before taking measures to lower risk that they deem unacceptable (Ross, 2011). The type of controls that are implemented after a vulnerability has been discovered are known as corrective controls. From this perspective, corrective controls can be implemented to reduce in the risk in an ad-hoc fashion (Chen, Desmet, & Huygens, 2014). In this context, ad-hoc refers to controls that are added to an asset that has already been developed or is currently in use. If a viable control cannot be found, a compensating control is introduced to reduce the level of cyber risk. A compensating control is added to another asset of the organization that is directly linked to the vulnerable asset. Ultimately, this serves to reinforce other assets to compensate for the weaknesses within the vulnerable asset. On another note, an indirect benefit can also be attributed to cyber risk management, as the use of controls has a positive effect on employee behavior. In this regard, employees are forced to practice safer cybersecurity practices as they work the controls that have been put in place (Brown, 2017).

Furthermore, a number of different frameworks could apply to organizations in the energy sector. These types of frameworks that are used within the sector can help gain an understanding for the types of controls that could be transposed to the gas industry. An example of this would be the ISO 27002 family of standards, which details the introduction, implementation, and perpetuation of security controls for information systems within the energy sector (Da Veiga & Eloff, 2010). Additionally, NIST 800-53 can be utilized as a federal framework to determine and apply general IT security controls that are not sector-specific (Cardenas et al., 2009). Other frameworks, such as ISA-99 can be explored for potential use, but these controls may be tied to specific industrial control systems outside of gas organizations (Cardenas et al., 2009).

With that being said, the implementation of security controls must be weighed against the objectives of the business to ensure that they do not interfere with employee workflow. Similarly, these implemented controls can also be costly and difficult to sustain over a period of time, as additional costs become associated with the use of that asset (Tisdale, 2015). Furthermore, controls may also be failed to be enforced uniformly across an organization, creating unforeseen discrepancies (Wueest, 2014).

From a cyber risk management standpoint, the impact of energy specific controls has yet to be understood. Specifically, this lack of understanding pertains to controls that may not function well in different sectors (such as transitioning a control from the finance sector to the energy sector). In addition, further examination of established frameworks is necessary to utilize controls that could help enforce the different components of an information security program in the gas industry.

## Security Awareness

Security awareness is also an integral part of an information security program. Security awareness heavily contributes to a security-oriented security culture within an organization as employees are trained on the appropriate use of corporate assets. Different metrics are used to determine the success of the program, such as phishing susceptibility, cyber incident reporting, and the completion of security training (Bada & Sasse, 2014). Furthermore, security awareness training helps ensure compliance with the information security program through the use of security presentations (Siponen, Pahnila, & Mahmood, 2010). As a result of the security awareness training in organizations, it has been found that this training reduces the chances of cyber threats impacting an organization (Safa, Von Solms, & Furnell, 2016).

With that being said, information sharing is also part and parcel of security awareness. On this subject, the federal government has been instrumental in fostering a private-public partnership between the public sector and private entities (Rodin, 2014). In the same manner, LOGIIC was created with the encouragement of Homeland Security to increase collaboration between both the oil and gas industries (Giroux & Melkunaite, 2013). On a general level, information sharing has also been used to share information about cyber risks across different sectors, through mediums like US-CERT (Safa et al., 2016).

Nonetheless, more exploration is required for security awareness and training in the gas industry. Further research would entail a better understanding of the awareness metrics that are specific to both the gas industry and energy sector. On that note, research will also be conducted on how industry standards and federal regulations are incorporated into security awareness training for employees. Table 1 below explains the different security metrics that could help gauge the effectiveness of an information security program.

## Table 1

## *Security Awareness Metrics Table*

| Metrics | Description | Sources |
| --- | --- | --- |
| Phishing Susceptibility | Used to gauge the organization’s vulnerability to phishing attacks; utilizes data from real attacks or simulated exercises sent out by the organization. | Jaeger, 2018; Kirlappos, & Sasse, 2012 |
| Reporting of Cyber Incidents | Grasps how employees respond to cyber incidents. Higher reporter rates indicate a large volume of attacks or a vigilant workforce. Lower reporter rate indicate poor security practices or a lack of communication within an organization. | Jaeger, 2018; Talib, Clarke, & Furnell, 2010 |
| Security Training Completion Rate | This measure helps gauge employee participation in the security culture of an organization. A low participation rate could indicate a lack of emphasis on security. | Jaeger, 2018; Kirlappos, & Sasse, 2012 |

# Conclusion

The overall goal of this literature review was to determine how an information security program could effectively reduce the cyber risk that a gas organization faces. In this respect, the literature review identified the different components of an information security that play an essential role in reducing cyber risk. Outside of the overarching information security program, the reduction in cyber risk ultimately boils down to the effectiveness of the information security policies, cyber risk management, and security awareness aspects of the program itself.

The literature review emphasized several research gaps where there was a lack of pertinent information for this industry. However, a major gap found in the literature review centers around the absence of information security programs in the gas industry. As a result of the gap in previous research, the objective of this study could explore how gas organizations utilize information security programs and how they ensure that these programs remain effective.

Gas organizations may consider utilizing information security programs and their established components to reduce the cyber risk that they are confronted by. Therein, gas organizations should also determine how to ensure that their information security program remains effective with the passage of time. Gas organizations should also create relevant information security policies that reflect the business needs and assets used within the organization. To this end, gas organizations can look towards different industries to determine how other organizations have devised industry-specific policies. Similarly, cyber risk management needs to be developed in a way that not only reflects the best practices with the use of reputable control frameworks, but in a manner that is also reflective of business-oriented controls. Gas organizations also need to utilize industry centric security awareness metrics that capture alarming trends such as data misuse or risk laden cyber behaviors.

**Research Question**

What role does an information security program play in reducing the cyber risk that a gas organization faces?

**Sub-questions:**

1. What are the critical components of information security program?
2. What factors impact the sustainable effectiveness of an information security program.

# **Research Design and Methods**

## **Research Design Justification**

The literature review has underscored the importance of an information security program in reducing cyber risk in an organization. The prior research has also identified the different foundational components that help reinforce the information security program. To this end, it has been found that organizations with an information security program have a security-oriented culture and an overall beneficial effect on employee behavior (Chen, Ramamurthy, & Wen, 2015). However, this was necessary to determine how a gas industry-specific information security program can reduce cyber risk. Likewise, it was also necessary to understand how an information security program in a gas organization could remain effective with the passage of time. In this respect, a grounded theory approach was used to capitalize on the information gathered from security professionals in the field. The information gathered using the grounded theory approach was used to develop the ISP (Information Security Program) Model.

In this regard, the gathered data was necessary to better understand how an information security program has been implemented in gas organizations. This has assisted the current research efforts by determining the role that different components play in an information security program. Similarly, having a grasp of the different components in an information security program will provided a better understanding of how a gas organization could specifically reduce the amount of cyber risk present in their organization. Consequently, a semi-structured interview was an ideal option for the purposes of this study. The interview method helped in capturing and identifying the role that the components of an information security program play in reducing cyber risk. These components included aspects such as information security policies, security awareness, and cyber risk assessments. This method also assisted research efforts in determining how these components can be gas industry specific and even provide insight into how a gas organization’s information security program can remain effective over time. The semi-structured interviews utilized the knowledge of professionals in this field to understand the role that an industry specific information security program plays in mitigating cyber risk. Furthermore, the research efforts addressed the different aspects of the research question. The research identified the manner in which an information security program reduced cyber risk within a gas organization. Secondly, the research determined how an information security program could remain effective over a period of time.

## **Sampling and Recruitment of Study Participants**

Numerous email invitations were sent out to cyber security professionals that currently work within a gas organization. The respective email contained details about the semi-structured interview as well as context surrounding the data collection process. A number of requirements needed to be satisfied in order for the interviewee to sit for the semi-structured interview. These criteria included higher-education requirements as well as security certification requirements. Other areas, such as the level of expertise in IT governance, risk, and security analysis played a crucial part during the selection of candidates.

The email contained information about how the interviews were conducted and discussed what information will be collected during the interview. The interviewee candidate was made aware of the research problem and how the interview process sought to better understand what role an information security program may play in reducing cyber risk.

## **Data Collection Method**

The data for the semi-structured interviews was collected in the following manner. Five professionals from gas organizations were interviewed about their background, credentials, and experience with the information security program within their organization. Access to these individuals was attained through in-person interviews. The five semi-structured interviews were recorded and extensive notes were taken to capture each interviewee response.

## **Data Analysis Method**

During the course of my research endeavors, I identified different codes that were prevalent throughout my interviews. For example, codes were assembled in alphabetical order, and went up to the letter U. As interviews took place, previous codes that were identified were also utilized in the analysis of the new interviews. Likewise, the initial interviews were also analyzed for new codes that surfaced in the subsequent interviews. Table 2 lists the various codes that were identified throughout the data collection process.

#### Table 2

*Identified Codes*

|  |  |
| --- | --- |
| Code | Description |
| A | Mitigate Cyber Risk |
| B | User Education on Information Security Program |
| C | Reinforce Behavior |
| D | Application Security Control |
| E | Device Security Control |
| F | Security Control Risk Impact |
| G | Security Control Awareness |
| H | Business Alignment with Controls |
| I | Security Control Issues |
| J | Enhancing Security Control Experience |
| K | Security Awareness Approach |
| L | Security Awareness Metrics |
| M | Security Awareness Improvements |
| N | Penetration Testing |
| O | Risk Assessments |
| P | Frameworks and Regulation |
| Q | Threat Landscape |
| R | SCADA Use |
| S | Updating the Information Security Program |
| T | Information Sharing and Collaboration |
| U | Corporate Espionage |

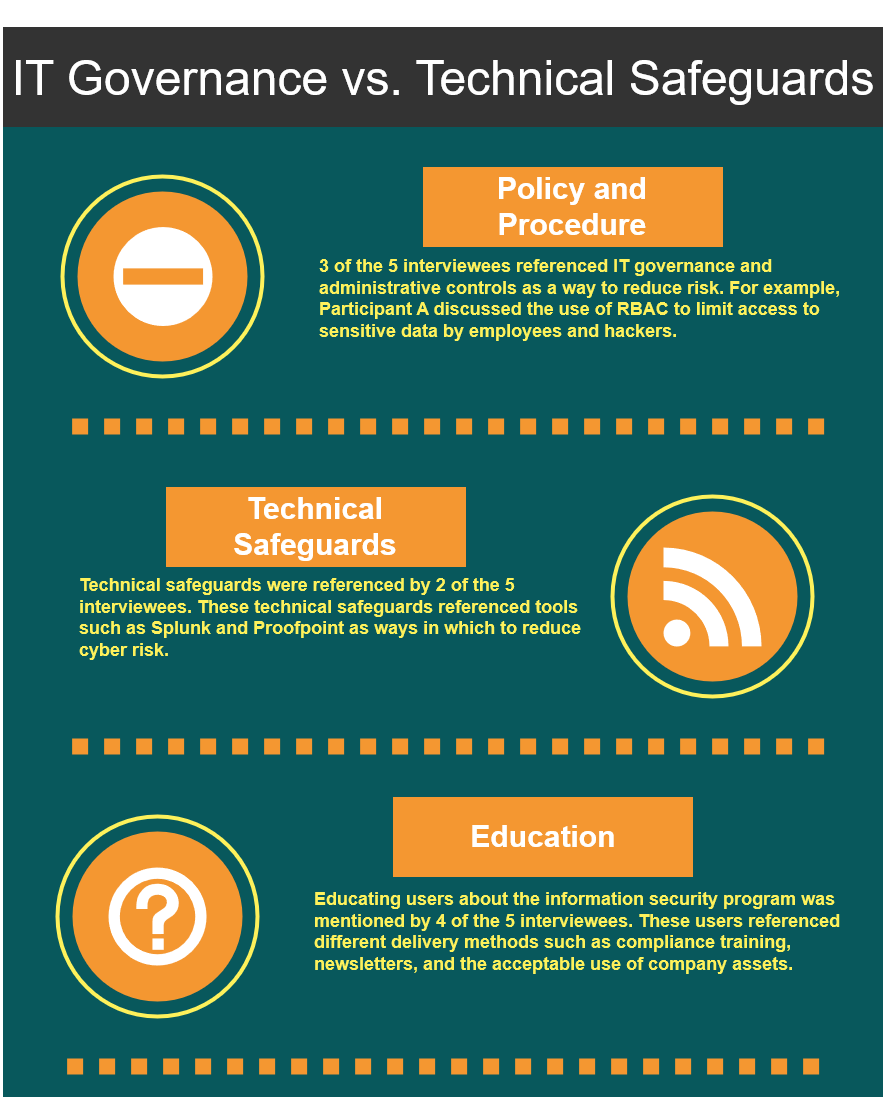
As codes were classified and identified throughout each interview, codes were routinely compared for similarities and prevalence in other interviews. This process helped identify categories where each respective code could be placed. This process was also utilized to reframe questions and seek additional information from later interviews. Ultimately, this process helped paved the way for the further analysis of themes and categories, which was pivotal in the grounded theory approach.

# **Results**

Throughout the interview process, interviewees discussed the importance of an information security program and how the different components helped reduce cyber risk within a gas organization. Five interviewees were also questioned on how these components could be improved and how information sharing within the industry could help mitigate cyber risk. The differing interviewee profiles led to a variety of perspectives being included in the research results.

## **Information Security Program Policies and Procedures**

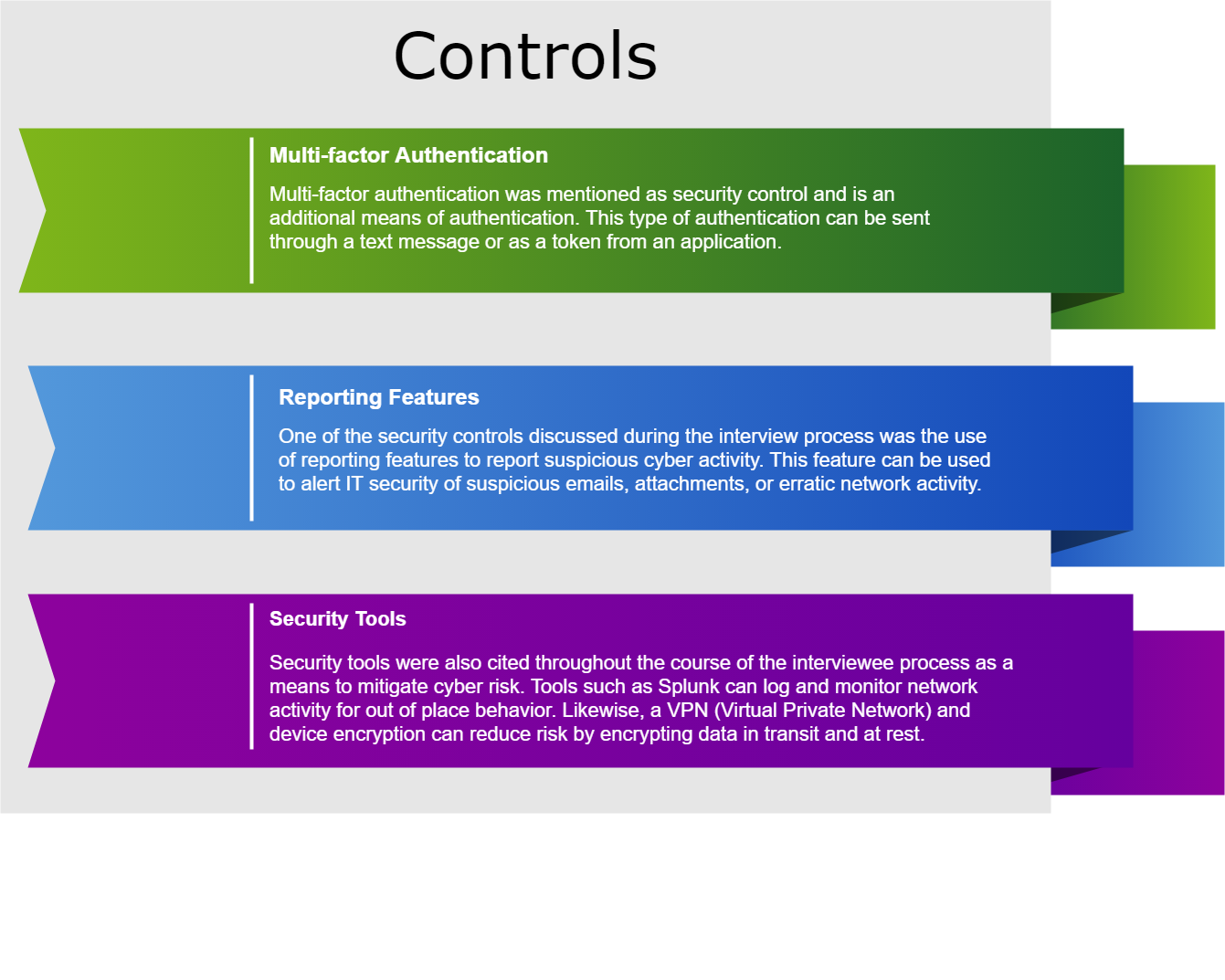
One role of an information security program in an organization reduces cyber risk through the enforcement of security policies and policies in an organization. Every interviewee attested to the notion that these policies and procedures curtailed cyber risk within an organization. In this regard, interviewees also attributed this to the education of users surrounding the program, which helped accentuate the effectiveness of each organization’s program. Further analysis disseminates the information and reveals that there was a split between IT governance and technical safeguards. To this effect, one interviewee mentioned the importance of using Role Based Access Controls (RBAC) to limit access to data. This administrative control relies heavily on the defined security policies and procedures within an organization. Other users discussed the importance of security tools, incident response, and the need to remediate vulnerabilities. For example, one interviewee stated that “… risk can be mitigated through policies and procedures that revolve around incident response, operational security, pen testing, and classifying assets” (J. Johnson, personal interview, March 12, 2019). However, a nearly unanimous consensus was reached on the importance of educating employees about the organization’s information security program. The infographic below illustrates the preferences for the five individuals that were interviewed.



#### Figure 2. Comparing IT Governance and Safeguards

## **Understanding the Impact of Security Controls**

As evidenced by the interview process, security controls also play an important role in an information security program. With that being said, the interviewees stated that these controls reduced cyber risk through various means. Different forms of security controls were evident in user authentication, user reporting features, idle activity locks, and the use of security tools. The graphic below displays some of the different types of controls discussed by the interviewees.



#### Figure 3. Different types of security controls

With that being said, a number of issues were also observed with the use of security controls throughout gas organizations. One interviewee reported being prevented from accessing an area that they already had access to because of strict access controls, while another user complained about the inconvenience of multi-factor authentication. This sentiment tended to coincide with the consensus that security controls required time and resources to implement. While issues were observed with the implementation of security controls within gas organizations, these organizations have also strived to make these controls convenient for employees. Some of these features included reporting buttons in Outlook that automatically flagged suspicious emails and the use of RSA tokens for authentication. Awareness about user conscious controls was evident with some organizations looking for a common ground between security and usability.

## **Applying Security Awareness in an Organization**

Security awareness was found to be widespread throughout interviews from varying gas organizations. While security awareness was ubiquitous in these utility companies, the intentions and application varied. One organization relied on security awareness techniques for informational purposes, sending out newsletters and providing training, while other firms took a different approach. In particular, one firm took a punitive approach to security awareness, where they had “… a 5-strike system in place where the employee is fired after five opened emails” (J. Doe, Personal Interview, March 5, 2019). However, other firms tended to rely on an educational approach, reinforcing positive user behaviors with training videos and games.



#### Figure 4. Security Awareness Approaches

## **Assessing Risk**

Assessing risk was a common element that was found during the course of each interview. Interviewees discussed the importance of determining risk within their organization. However, while the course of action was conducive to assessing cyber risk, organizations differed in their approach. For example, when it came to penetration testing, one firm utilized red team vs blue team exercises, while another firm relied on social engineering audits. In other cases, risk assessments were used to determine if an application was configured securely, while others used these assessments to isolate vulnerable industrial control systems.

## **Information Sharing**

Information sharing within the gas industry were also noted throughout the interview process. Almost every interviewee emphasized the fact that their firm shared information with other companies within their industry. Interestingly enough, information was also shared with government agencies such as ICS-CERT and US-CERT. The interviewees also highlighted the fact that information sharing was important in addressing risks that threatened the industry. One interviewee demonstrated the importance of a public-private partnership in the industry, with information being shared freely throughout. The interviewee stated that they “... have used Verizon’s VERIS database and US-CERT to rely on shared information about threats.” (J. Doe, Personal Interview, March 5, 2019). However, interviewees were also quick to disclose that their companies took steps to safeguard sensitive data that should not be shared with competitors.

# **Discussion**

The research has shown that gas organizations that adhere to an information security program with certain key components have elaborate pillars of security in place. These pillars include examples such as fully developed security awareness initiatives and complex controls. However, there were negative effects as a result of information security program implementation. Organizations that adhere to an information security program also ran into issues associated with the program, such as problematic access rights or addressing the inconvenience of multi-factor authentication. The problems identified during this research endeavor were not unique to one organization but were prevalent in different forms. Some organizations struggled with restrictive role-based access controls that locked out authorized employees, while another company attempted to make intricate controls more user friendly. A common theme that was discovered shined a light on the resource strain and the overall cost of ownership associated with each control. While each control added a layer of security, there was a noted impact from a financial implementation standpoint.

Assessing risk was a component that was found at different maturity levels at the organizations in question. Some organizations conducted risk assessments to determine the security vulnerabilities found in devices or applications, while other companies used social engineering in their assessment of risk. The varied approach could be attributed to the level of expertise within the security department and even management’s vision. Organization’s with less resources may opt for a more traditional and audit-based approach to security risk assessments. These types of assessments could see security professionals gauging the risk of an application when they are viewed from the lens of the organization’s policies, standards, and procedures. Notably, some organizations also discussed how they relied on industry certifications or government frameworks as a guide for their risk assessments. In an organization with limited resources, relying on established frameworks for risk assessments can be an effective solution for organizations looking to mitigate cyber risk.

Organizations that have the financial flexibility or expertise to mitigate cyber risk, may choose a more arduous approach. In this sense, an organization may pay consultants to conduct social engineering schemes, such as dropping USB drives and monitoring their subsequent use. Other risk assessments could be composed of a tool-based approach, where vulnerability scanners or code analysis could be used.

Irrespective of financial resources and security expertise, information sharing inter-industry can also help triage prevalent risks that affect the gas industry. Government agencies or organizations such as US-CERT or FBI Infragard may also be willing to work with gas companies to address certain risks that are impacting the industry.

From a security awareness perspective, there were many similarities across organizations. Every organization provided a medium for education for their employees. Examples of education include the use of newsletters and even training videos. Variations in security awareness initiatives were evident in the disciplinary action taken against delinquent employees. Some organizations did not punish their employees for falling susceptible to phishing exercises, while other organizations utilized a strike system. The punitive approach would ultimately end up with employees who were in constant violation of the strike system being terminated by the organization.

When it came to ensuring that the information security program was relevant and up-to-date, some companies utilized various guidelines and frameworks. However, the majority of companies took a more reactive approach and revised the program based on the ubiquity of major risks, threats, or vulnerabilities. While this may be effective in larger organizations, a distinction must be made between information security and other areas of the business. While accounting and financial rules may remain static for prolonged periods of time, cyber risks change regularly.

From the lens of a security-based approach, there are a number of ways in which an organization can implement an information security program or ensure that an already mature program remains relevant in the face of change. The Information Security Program Model or ISP Model provides a succinct manner in which organizations can tackle this issue.

# **Mitigating Cyber Risk in a Gas Organization – ISP Model**

The research endeavor that was conducted alludes to the fact that an information security program should be viewed as a whole, rather than the sum of its parts. As evidenced in the components of a program being employed in conjunction with each other, these facets of a program significantly reduce risk when used together. To this effect, the ISP (Information Security Program) Model has been developed to demonstrate how an information security program and the respective tenets can be used to mitigate cyber risk within a gas organization.



#### Figure 5. ISP Model

The ISP Model epitomizes how the whole is greater than the sum of its parts when the information security program is held at a macro level. Without any given component of an information security program, the program could cease to function properly. This notion is also evident in the honeycomb design of the model, where each component is equally important in maintaining the structure and integrity of an information security program. Moreover, a poorly developed program could actually increase cyber risk, rather than assist in mitigating risk. Additionally, each component of the model complements each other. For example, policies and procedures dictate what security controls should be developed, while findings from risk assessments could help provide instruction for future security awareness exercises. Likewise, the previously recognized components in the model would steer the direction of the overall information security program in the form of updates and additions. However, the failure to create or develop a component would ultimately devolve into a process gap, leaving an information security program that is ultimately vulnerable to cyber risk. A breakdown of the importance of each component is provided below:

## **Policies and Procedures**

Policies and procedures are highly influential in ensuring the success of an information security program. In this regard, this component directly influences the creation and application of security controls. Policies and procedures can dictate user settings such as user authentication or even delineate on the type of encryption that is required by the gas organization. If policies and procedures do not exist within an organization, cyber risk will only be exacerbated as security matters are addressed in an ad-hoc fashion.

## **Security Controls**

Security controls also have a large impact on an information security program. This aspect of a program ensures that a program has clout and enforcement. From a practical perspective, this is where normative statements in information security can be enforced and subsequently become a reality for an organization. In essence, the governing rules found in a policy, procedure, or standard are enforced through the implementation of security controls. Security controls can take the form of multi-factor authentication, firewalls, or even physical means such as mantraps. If this component is missing or inchoate in nature, then the entire gas organization will remain vulnerable to every perceivable cyber risk. While security controls and other safeguards are inconvenient, the additional layers of protection are necessary in reducing cyber risk. This coincides with the practice of organizations who follow the defense in depth strategy.

## **Risk Assessments**

Risk assessments play an important role in assessing the risk posed by a gas organization’s risk culture and how they tolerate risk. Depending on the risk appetite of a gas organization, some companies may tolerate a higher risk level. Generally, risk culture tends to emanate from the business objectives of the organization. Some organizations may feel the need to pursue ventures that contribute to a higher risk level as a result of costs or the latest innovations. Other firms may be more conservative in their approach depending on maturity or being averse to accepting more cyber risk. In this respect, risk assessments can help assess the inherent and residual risk found in software, device, or industrial control systems. Findings discovered as a result of these assessments can help identify vulnerabilities and cascading risk from concurrent use in a network environment. These findings can also help outline the threat environment for an organization and help them to better understand where their greatest weaknesses may lie.

## **Security Awareness**

Security awareness is a critical component of an information security program. Security awareness is used by gas organizations to help employees identify the latest threats and utilize best practices when it comes to information security. Training can occur through a variety of mediums, including training exercises, such as faux phishing attacks, or through published reading materials. Metrics about employee behavior can also be deduced from security awareness through training results and employee surveys. From a policy and procedure standpoint, security awareness results can also be used to reproach or terminate employees that violate acceptable use policies. A strike system or other paradigm can be used to reprimand employees who are in violation of policies and procedures as a result of training exercises.

## **Information Sharing**

Information sharing is an important tenet of a gas organization’s information security program. Information shared with other utility companies can be paramount in understanding the threat environment that confronts the industry. Furthermore, information can be shared or disseminated from industry groups or government agencies such as US-CERT. These agencies can work hand-in-hand with firms in the gas industry to address widespread threats impacting the gas industry. Without information sharing, an organization’s information security program would not be cognizant of the risk patterns found in other organizations.

## **Updating the Information Security Program**

Keeping the information security program current and updated is vital to the success of the program. An organization that is cognizant of the latest threats, vulnerabilities, and security awareness metrics can use this data to ensure that the program remains relevant. A relevant information security program will help to mitigate cyber risk by ensuring that the appropriate security controls are in place, that the security awareness program remains germane given the current threat environment, and that risk is assessed in the appropriate manner. On that note, an information security program that is not updated will become increasingly susceptible to risk as the components of the program fail to address threats that confront the organization. In this regard, organizations can glean useful information from the latest industry certifications, frameworks, and information that has been shared.

# **Conclusion**

This research endeavor is important because it allowed the capture of data about how gas organizations rely on their information security programs to mitigate cyber risk. The data from the interview was utilized to create the ISP model that illustrates the different components that mitigate cyber risk in a gas organization. The ISP model was created using the security acumen of professionals within various gas organizations. Likewise, the honeycomb structure helps visualize the importance of each component. The experiences of security professionals paved the way for a comprehensive model to be developed in a manner that uniquely addresses cyber risk within a gas organization.

With that being said, this research was not without its challenges. The study was limited to a narrow time window and the resulting study was based off of the input of only five participants. To this effect, I found that while the interviews provided a wealth of data surrounding gas organizations, the scope of the study was constrained by interviewee profiles and time limitations. While the interviewee profiles suited the needs of the current research endeavor, I believe that expanding the scope and including “SecDevOps” (Security, Development, and Operatons) in the study would have been beneficial. Interviewing these types of employees would have provided for a better appreciation of the costs and developmental challenges associated with the implementation of an information security program. Although it was not feasible given the course length, additional time would have provided for a more in-depth research endeavor that allowed for the analysis of an organization’s information security program over a protracted time period. This extended analysis could have allowed for the study of how an information security program evolves in light of changing cyber risks or different approaches within a security department. In this vein, quantitative methods could also be used to measure the variance in risk from a statistical point of view.

I believe that in the future researchers should conduct additional studies on the security controls and risk assessment components of an information security program. While the information security field is in its nascence, cyber risk assessments will only continue to grow in size and scope for gas organizations. In many ways, cyber risk assessments could develop similarly to financial audits, where regulation and industry practices result in increasingly complex risk approaches. Although it is self-evident, security controls enforce the policies of an organization and are essentially the main line of cyber defense in an organization. With time, it is almost certain that increasing scrutiny from regulatory and industry groups will coerce gas organizations into developing intricate controls. Therefore, researchers should focus their efforts on the effects of security controls and risk assessments, within the context of gas organizations. From this perspective, researchers could determine the different strategies that can be employed to implement these security controls as well as predicting the cost of ownership for these controls. Future research could utilize machine learning and specifically linear regression to help predict the cost of security controls over a certain period of time. Ultimately, this would paint a whole picture of an information security program, not only measuring the importance of the program, but also understanding the cost of program implementation.

Finally, the significance of the study comes to fruition with the development of the ISP Model. The ISP Model would be a very useful tool for gas organizations to ensure that new or previously developed information security program can mitigate cyber risk. An easy to remember model name also underscores the foundational elements of the model itself. This user-friendly model offers itself as a medium that be conveyed to every level of employees in a gas organization. Gas organizations can also use this model as a visual aid to assure C-suite executives that security professionals are working to keep cyber risk at an acceptable level. In light of this, firms that are looking to reduce cyber risk should design their information security program around the ISP model to ensure that their program matures and remains pertinent in the face of the latest cyber threats.

**References**

Apostolou, B., Apostolou, N., & Schaupp, L. C. (2018). Assessing and Responding to Cyber Risk: The Energy Industry as Example. *Journal of Forensic & Investigative Accounting,* 10(1), 73-86.

Bada, M., & Sasse, A. (2014). Cyber security awareness campaigns: Why do they fail to change behaviour? Retrieved from <http://discovery.ucl.ac.uk/id/eprint/1468954>

Brown, D. A. (2017). Examining the Behavioral Intention of Individuals' Compliance with Information Security Policies. Retrieved from [https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=4853&context=dissertations](https://scholarworks.waldenu.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com/&httpsredir=1&article=4853&context=dissertations%20)

Bronk, C., & Tikk-Ringas, E. (2013). The cyber attack on Saudi Aramco. *Survival*, 55(2), 81-96.

Cardenas, A., Amin, S., Sinopoli, B., Giani, A., Perrig, A., & Sastry, S. (2009, July). Challenges for securing cyber physical systems. In *Workshop on future directions in cyber-physical systems security* (Vol. 5). Retrieved from <https://pdfs.semanticscholar.org/d514/97e5827cc00d9d00c26e27a769d42284cfba.pdf>

Chen, P., Desmet, L., & Huygens, C. (2014). A study on advanced persistent threats. In IFIP International Conference on Communications and Multimedia Security (pp. 63-72). Berlin, Heidelberg: Springer.

Chen, Y. A. N., Ramamurthy, K. R. A. M., & Wen, K. W. (2015). Impacts of comprehensive information security programs on information security culture. Journal of Computer Information Systems, 55(3), 11-19

Da Veiga, A., & Eloff, J. H. (2010). A framework and assessment instrument for information security culture. Computers & Security, 29(2), 196-207.

Donaldson, S. E., Siegel, S. G., Williams, C. K., & Aslam, A. (2015). Enterprise Cybersecurity Capabilities. In *Enterprise Cybersecurity* (pp. 311-334). Berkeley, CA: Apress,

Giroux, J., & Melkunaite, L. (2013). Information Sharing for Critical Energy Infrastructure Protection: Finding value & overcoming challenges. In Energy Security Forum (No. 8, pp. 20-22). NATO Energy Security Centre of Excellence.

Jaeger, L. (2018). Information Security Awareness: Literature Review and Integrative Framework. Retrieved from <https://scholarspace.manoa.hawaii.edu/bitstream/10125/50482/1/paper0595.pdf>

Johnson, M. E., & Goetz, E. (2007). Embedding information security into the organization. IEEE Security & Privacy, 5(3), 16-24. DOI: 10.1109/MSP.2007.59

Kirlappos, I., & Sasse, M. A. (2012). Security education against phishing: A modest proposal for a major rethink. *IEEE Security & Privacy*, 10(2), 24-32.

Malik, N. S. (2018, April 27). Energy Companies Aren't Doing Much to Defend Against Soaring Cyber Attacks. Retrieved from [https://www.bloomberg.com/news/articles/2018-04-27/-cyber-blindspot-threatens-energy-companies-spending-too-little](https://www.bloomberg.com/news/articles/2018-04-27/-cyber-blindspot-threatens-energy-companies-spending-too-little%20%20%20)

Rodin, D. N. (2015). The cybersecurity partnership: A proposal for cyberthreat information sharing between contractors and the federal government. *Public Contract Law Journal*, *44*(3), 505-528.

Ross, R. S. (2011, March 1). Managing Information Security Risk: Organization, Mission, and Information System View (Special Publication, NIST SP 800-39). Retrieved from https://www.nist.gov/publications/managing-information-security-risk-organization-mission-and-information-system-view

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., & Herawan, T. (2015). Information security conscious care behaviour formation in organizations. *Computers & Security*, 53, 65-78.

Safa, N. S., Von Solms, R., & Furnell, S. (2016). Information security policy compliance model in organizations. *Computers & Security*, 56, 70-82.

Siponen, M., Pahnila, S, & Mahmood, M.A. (2010). Compliance with Information Security Policies: An Empirical Investigation. *Computer*, 43(2), 64-71. DOI: 10.1109/MC.2010.35

Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure. (2017). Retrieved September 13, 2018, from [https://www.energy.gov/sites/prod/files/2018/05/f51/EO13800%20electricity%20subsector%20report.pdf](https://www.energy.gov/sites/prod/files/2018/05/f51/EO13800%20electricity%20subsector%20report.pdf%20%20%20)

Talib, S., Clarke, N. L., & Furnell, S. M. (2010, February). An analysis of information security awareness within home and work environments. In *Availability, Reliability, and Security, 2010*. ARES'10 International Conference on (pp. 196-203). IEEE.

Tsohou, A., Karyda, M., & Kokolakis, S. (2015). Analyzing the role of cognitive and cultural biases in the internalization of information security policies: recommendations for information security awareness programs. *Computers & security*, *52*, 128-141.

Tisdale, S. M. (2015). Cybersecurity: Challenges from a Systems, Complexity, Knowledge Management and Business Intelligence Perspective. *Issues in Information Systems*, 16(3), 91-198.

Virvilis, N., & Gritzalis, D. (2013). The big four-what we did wrong in advanced persistent threat detection? In Availability, Reliability and Security (ARES), 2013 Eighth International Conference on (pp. 248-254). IEEE.

Wolden, M., Valverde, R., & Talla, M. (2015). The effectiveness of COBIT 5 information security framework for reducing cyber attacks on supply chain management system. *IFAC-PapersOnLine*, 48(3), 1846-1852.

Wueest, C. (2014, January 13). Targeted attacks against the energy sector. Retrieved from <http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/targeted_attacks_against_the_energy_sector.pdf>

# \*\*The tables and diagrams used throughout this document are products of my own creation.