Journal of Cybersecurity Education, Research and Practice

Volume 2017 | Number 2 Article 4

December 2017

Synergistic Security: A Work System Case Study of the Target Breach

Martha Nanette Harrell
Arkansas Tech University, mharrell3@atu.edu

Synergistic Security: A Work System Case Study of the Target Breach

Abstract
Recent publicized security breaches can be used to evaluate information security programs. The processes and procedures that allowed the event to occur can be examined in a case study and then be used to find methods for future mitigation of risk. The Target security breach is used in this study to examine the organization's information security program using a macro-ergonomic model. This research posits that an information security program should consider the work system design, based in macro-ergonomics, to help mitigate information security risk to the organization and ensure an efficient and effective information security program. Based on a seminal macro-ergonomic model, the Leavitt Diamond Model (1965), an information security model was designed. The Synergistic Security Model can be used to examine relationships between macro-ergonomic information system constructs. The relationships that occur between the structure of the organization (policies, procedures, leadership, etc.), the people, the technology, and the tasks can have an impact on the efficiency and effectiveness of an information security program. For the purpose of examining these relationships, the Synergistic Security Model is divided into triads, consisting of: Triad 1: Information Security Structure- Information Security Technology-People (Information Security Behavior); Triad 2: Information Security Structure-Information Security Tasks-People (Information Security Behavior); Triad 3: Information Security Tasks-Information Security Technology-People (Information Security Behavior); and Triad 4: Information Security Tasks-Information Security Technology-Information Security Structure. This paper will examine the relationships found in the Target data breach, reported in December 2013.

Keywords
information security behavior; information security compliance; work system design; information security program; data breach; case study

SYNERGISTIC SECURITY: A WORK SYSTEM CASE STUDY OF THE TARGET BREACH

1. Introduction

Insider threats to organizational information systems are a significant security concern. Considerable damage to organizational information systems has occurred by insiders with legitimate access to the organization's data and many executives report that organizational users are more likely to cause damage to the system than outsiders. (Carnegie Mellon CERT Program; CSO Magazine; PricewaterhouseCoopers & United States Secret Service, 2013). One means of causing this damage is when organizational employees can unknowingly allow outside hackers to gain access to sensitive information. Information system employees make decisions and organize their activities on a daily basis. Their actions have the potential to affect the entire organization, positively or negatively. Hackers know employees are a potential weakness in the information security fortress. Because of the nature of the design of an organization and the work that must be done to make the business successful, information system users often face decisions between choosing to complete their job tasks efficiently and effectively or to follow information security controls. Previous research indicates that users will often circumvent information security controls when they are attempting to complete their job tasks (Dhillon, 2001; Nash & Greenwood, 2008; Stanton, Stam, Mastrangelo & Jolton, 2005). This circumvention creates a substantial risk to the organization. Recent publicized information security breaches, such as the Target breach of December 2013, can be used to analyze the efficiency and effectiveness of an information security program. Forbes (Sept 8, 2014) indicated that Target experienced a cost of $148 million due to the breach.

Research indicates that users will often choose to complete job tasks over choosing to follow information security controls (Albrechtsen, 2007; Besnard & Arief, 2004; Post & Kagan, 2007). As users complete their work, they will determine their goals and values, which in turn will affect their actions and behaviors (Beautement, Sasse & Wonham, 2008; Dhillon & Torkzadeh, 2006; Hedstrom, Kolkowska, Karlssom & Allen, 2011). This situation is a trade-off where users are making a choice between "right versus right" (Badaracco, 1993).

Organizational goals are focused on productivity and to minimize costs. Information security goals focus on protecting the information systems and often do not examine the effect that the security program has on the user's task completion. At the same time, organizational leaders consider the information security program a cost to the organization and therefore leaders often look for ways to cut those costs. The organization's employees struggle to find the right direction

and the correct choices. This struggle is caused by a disharmony between the different constructs of a macro-ergonomic system. Creating harmony between these constructs can assist organizations with creating an efficient and effective information security program. The macro-ergonomic model, Synergistic Security Model, can be used to assist researchers and practitioners in examining areas of the information system program that have disharmony and therefore cause the program to be inefficient and ineffective. This research will gain insight into factors that contribute to poor information security decisions and assist in shedding some light on possible solutions to the issue.

2. Literature Review

There has been significant research on information security policy and procedure compliance (Albrechtsen, 2007; Besnard & Arief, 2004; Ifinedo, 2012; Kraemer & Carayon, 2007; Post & Kagan, 2007; Siponen, Mahmood & Pahnila, 2009, Siponen, Pahnila & Mahmood, 2014; Stanton et al., 2005). Additionally, previous research has indicated that information security can interfere with user job tasks (Post & Kagan, 2007; Ruighaver, Maynard & Chang, 2007). Information security must be a balance between data access for the authorized users and ensuring the protection of the data. Organizations need to understand the impact of information security programs on employees. Organizations should consider the relationship information security has on all of the basic systems within the organization. Information security leaders can examine this relationship between the constructs of the work system to minimize the pressure on employees to disregard security requirements. When organizations implement information security within an organization, the relationships between the structure, technology, people and tasks will be impacted. Disharmony between these constructs will impact human behavior and can cause them to make poor choices. For example, employees may choose to complete a job task over following information security controls.

Previous research has considered the human behavior aspect to understand user's non-malicious circumvention of information security controls. For example, one study examined how people viewed their security related risks using threat assessments and another study examined user wants or needs, such as convenience (West, 2008; Workman, Bommer & Straub, 2008). Still other studies related to human behavior included habit, protection motivation theory (PMT), knowledge, training, or skills (Leach, 2003; Vance, Siponen and Pahnila, 2012). However, these studies do not consider the all of the components of a work system. They only focus on the user or the people construct of the work system. Using a macro-ergonomic perspective can provide additional information on user behavior that may not be evident from a 'user only' perspective.

Previous research also considered organizational factors that could impact a user's choice to circumvent information security controls. For example, one study indicated that the organizations should focus on attempting to influence the user behaviors and normative beliefs (Dhillon, 2001). General Deterrence Theory was also examined as an organizational method for modifying user information security behavior (D'Arcy, Hovav & Galletta, 2009). Research was conducted that considered the use of shaming within the organization to influence user information security behavior (Harris & Furnell, 2012). Yet another example of organizational influences on information security behavior is the establishment of an information security culture (Alfawaz, Nelson, Mohannak, 2010; De Veiga & Eloff, 2009; Vroom & von Solms, 2004). While these studies considered the organizational perspective, they do not include all of the constructs of a work system design. For example, the Dhillon (2001) study aimed at user behavior and normative beliefs, but did not consider the impact of poorly designed policies or old and unreliable technology on employee security behavior.

Usability of information security controls has been analyzed as an influence on user information security behavior. Often system developers do not focus on the usability of information security controls, but rather on the implementation of security requirements and the technical systems (Pfleeger & Caputo, 2012). For example, users are sometimes required to remember dozens of passwords, work under a policy that prevents the passwords from being written down, and are not provided a technical solution to assist users with storing all of their passwords (Adams & Sasse, 1999). Of course, their job tasks require they must log into all of these systems. This situation provides the perfect setup for user circumvention of information security controls (circumvention of the policy that says they cannot write down passwords). Usability examines the relationship between the technology and the people, but does not consider the structure or task constructs that may also play a role in the behavior of the users. Perhaps the policy against writing down the passwords could be adjusted to say users can store the passwords in a secure manner, but cannot store them in an easily accessible location. Or perhaps the organization can purchase a password management system or use a single sign-on application.

Little research considers the organizational view using socio-technical examination of user information security behavior. The multiple password example could benefit from the socio-technical view, analyzing the impact of the security requirements using four constructs, human behavior, the tasks required, the structure of the organization (policies, processes and leadership) and the technology available. One seminal macro-ergonomic model that can assist with this analysis is the Leavitt Diamond Model (Leavitt, 1965). The Leavitt Diamond Model contains the four constructs listed above: People, Tasks, Structure, and

Technology. The Leavitt Diamond Model (1965), a work system design, will assist in the understanding of user information security behaviors. The socio-technical structure of work system designs can have a significant impact on user information security behavior. A work system that is not in harmony impacts employee behavior and causes them to circumvent information security requirements in the process of completing job tasks.

3. Theoretical Model

Previous information security studies have applied the macro-ergonomic perspective to information security (Kraemer & Carayon, 2007; Kraemer, Carayon & Clem, 2009). Factors in computer and information security vulnerabilities were studies conducted by Kraemer et al. (2009). Kleiner (2006) indicates that macro-ergonomics is centered on making the organizational system work in a harmonious way. When the organizational system is working harmoniously, the organization will experience fewer problems, such as errors or violations because everything is working smoothly together. Macro-ergonomics is a mixture of two schools of thought. The first is the Classic school of thought with studies on supervision, hierarchy, reward systems, and span of control. The second school of thought is on Human Relations, which includes things like teams, motivation, and machine automation. The balance between these two schools of thought is where the macro-ergonomic perspective fits (Smith and Sainfort, 1989). This research posits that a harmonious work system for information security will result in fewer problems, such as errors and violations.

The Leavitt Diamond model is a seminal theory within the macro-ergonomic school of thought (Leavitt, 1975). There are four components within the model: Structure, Technology, Task, and People. See Figure 1 for an illustration of the Leavitt Diamond research model. Each component cannot be changed without an impact on the other three. For example, if a new technology were introduced into the organization, the other three constructs will adjust to the change. In some cases, the adjustment could have a negative impact on the organization and other times the change could be positive. When introducing a change, the organization needs to make sure the constructs of the work system are in harmony to ensure the work system is efficient and effective. Disharmony between the constructs will prevent the work system design from being as efficient or effective as it should be. By examining the areas of disharmony between each of the constructs and making necessary changes to create harmony, the work system will then begin to adjust to a more efficient and effective state.

The Leavitt Diamond model can be a basis to create a framework for examining the information security socio-technical work system. This research posits that the Leavitt Diamond model can be used to develop a macro-ergonomic model for

Information Security. This information security model is called The Synergistic Security Model, Figure 2.

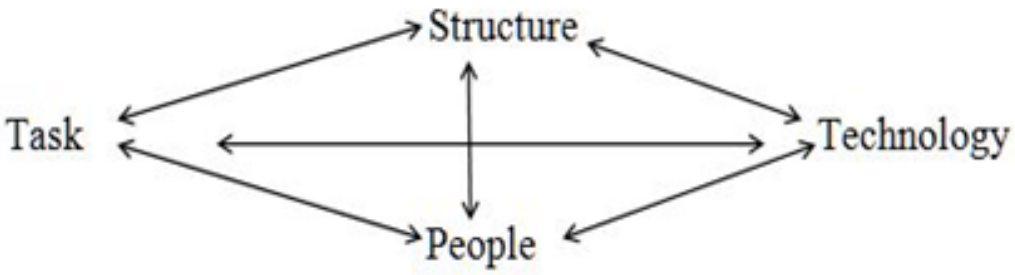

Figure 1: Leavitt Diamond Model (1965)

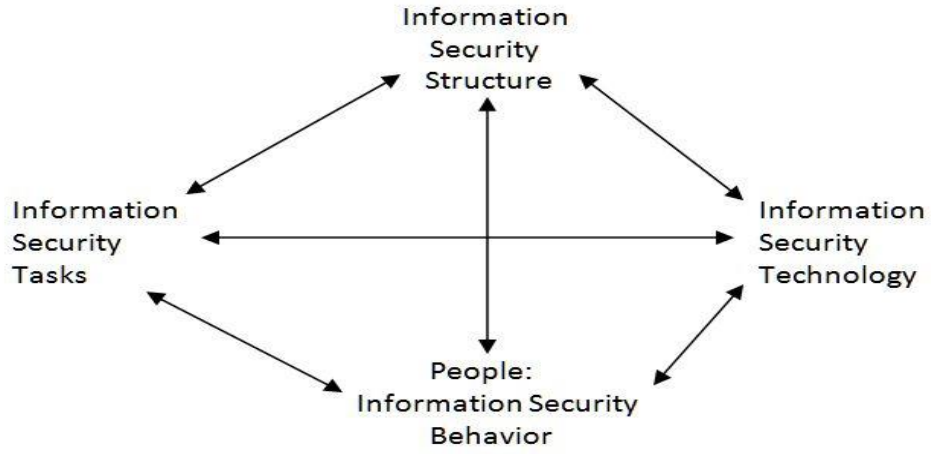

Figure 2: The Synergistic Security Model

The structure component of the model includes policies and procedures, as well as organizational relationships, workflow systems, or the systems of authority. The technology component of the model would represent any problem solving inventions. The technology component could include anything from a pencil, to a word processor to an entire information system. The people component includes the attitudes of the people, their abilities, or their skills and understanding. The last component is the task component, which includes all of the things that must be completed to produce goods and services.

4. A Case Study

A case study method is often used to examine "how" and "why" questions and provides the opportunity to analyze processes and procedures used in the course of completing a job task (Yin, 2012). The case study can also help to understand a phenomenon or to understand a particular situation or to understand interactions between information technology and other innovations (Darke, Shanks & Broadbent, 1998; Lee, 1989; Stake, 1995). Additionally, this research tested a theory for use in the implementation and management of information systems security. The Target data breach of December 2013 was used as a case to examine the relationships between the constructs of the Synergistic Security Model. Target is the second largest United States discount retail chain (Trustmark National Bank and Green Bank, N.A. v Target Corporation and Trustwave Holdings, Inc., 2014). Target experienced a major data breach that was reported to the general public in December 2013. The loss of data occurred from November 27, 2013 through December 15, 2013 (Trustmark National Bank and Green Bank, N.A. v Target Corporation and Trustwave Holdings, Inc., 2014). The data collected on this data breach was used to create the case study for this research. Extensive publications were created about the Target data breach. These publications have detailed information that is readily available for review. Most recent data breaches did not have the extensive amount of detail available that the Target breach had. Therefore, the Target case could be examined through the lens of this research model.

Each section of the model was divided into triads to allow a more narrow focus on the relationships. The researcher used online resources that included news reports, law suite records, the PCI Security Standards, and government reports regarding the December 2013 Target data breach. The research data was uploaded into qualitative data analysis software, Atlas.ti, where it could be coded, categorized, stored and analyzed. This allowed the researcher to look for patterns and to record relationships that developed between the data.

Using Atlas.ti, the researcher coded the research documents as either "Structure", "Technology", "Task", or "People". Statements and quotes were coded according to where they fit within each of these categories and four families of codes were established based on the four constructs. A total of 92 codes were created. The researcher used the query tool to form groups of coded material, based on each of the Synergistic Security model triads. This allowed the researcher to analyze the data through each triad's perspective. Additionally, the researcher used the search feature to find key words, such as "PCI-DSS" when reviewing the impact of specific constructs in relation to a triad.

4.1 The Case: A Summary Of The Target Data Breach

While most of the collected data breach research indicated that Target was not PCI-DSS compliant, Trustwise, Inc. had completed a security audit just weeks prior to the data security breach. This audit indicated Target was PCI-DSS compliant. The results of the Senate review on how the breach occurred indicated that an HVAC vendor was a victim of a phishing attack, causing a compromise to one of the logins used to access Target's billing and invoice system (A "Kill Chain" Analysis of the 2013 Target Data Breach, 2013). Moving from the billing system, the attackers were then able to install malicious malware on the point of sale (POS) systems, where the credit card data was collected during sales and before data encryption occurred. Over time, the attackers were able to compromise a Target internal server and create a location to store the stolen POS data. Periodically, the internally stored stolen data was then transported to an external FTP server using another Target server. From there, the data was collected using a Russian-based server and a few other external data drop locations.

5. Discussion Of Model Relationships

Many of the construct relationships found in the data can fit into more than one triad. The constructs are very interrelated and different triad perspectives of the model can be used to examine the same situations. The triad allows the researcher to view the data from the various perspectives of the research model. For example, three of the triads discussed in this research include the impacts on behavior.

Figure 3 indicates how the structure, task, and technology constructs can impact compliance behavior. Organizational leaders and the status of the work system design have the ability to place pressures on the employees.

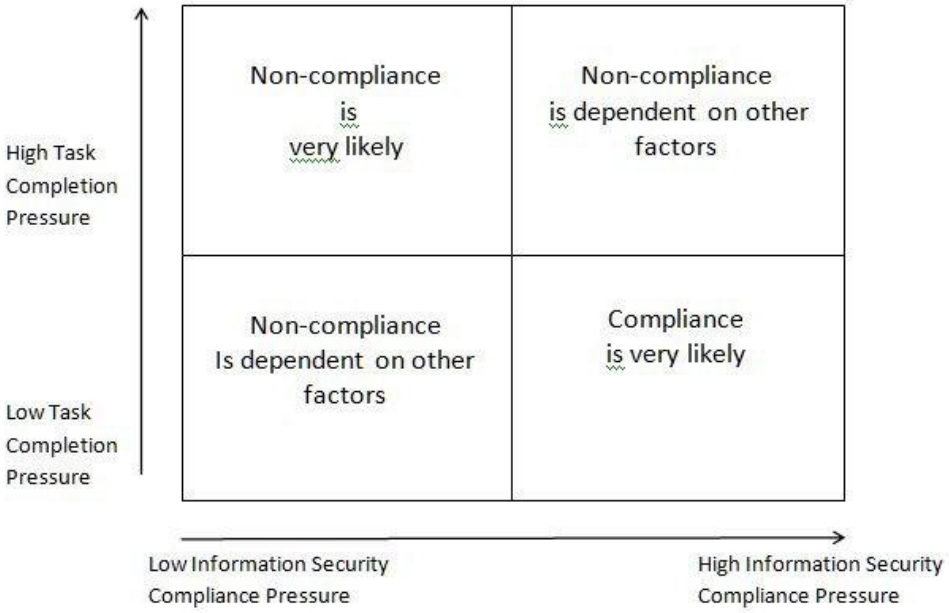

Figure 3: Organizational and management influences and pressure outcome matrix

Employees will react to these pressures in ways that leadership is often unaware. Kluge, Badura, Urbas and Burkolter (2010) examined how framing affects production within an organization. Subjects of the study could be "seduced to violate rules in a production setting when explicitly asked". The study indicated that leaders must frame newly introduced safety rules as a gain for the company and for the employees to minimize vulnerability to violations (Kluge et al., 2010). Rules to safeguard information systems will be subject to the same vulnerabilities as rules that safeguard the physical welfare of employees. Management framing is an element of the structure construct in the Synergistic Security Model.

5.1 Triad Relationship: Structure – Technology – People

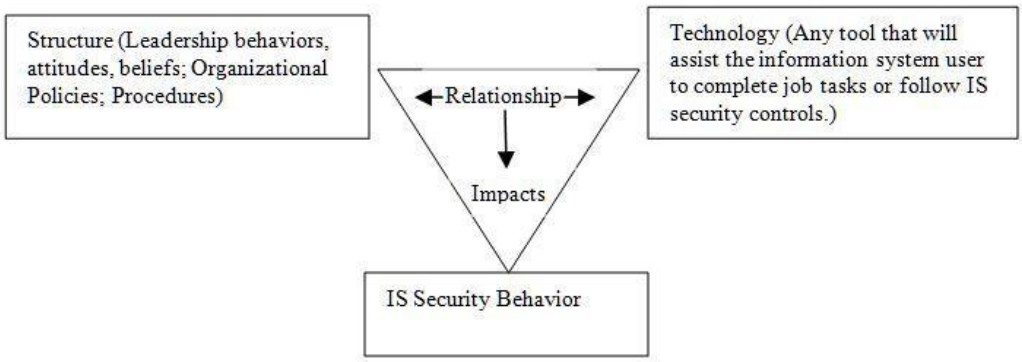

Figure 4: The Information Security Structure – Information Security Technology – People (Information Security Behavior)

The structure construct of the model is represented in the research data by examining the Payment Card Industry Data Security Standard (PCI–DSS)(PCI-DSS, 2013). Additionally, the structure construct includes the Target leadership goals and priorities. A review of the research data would indicate a possible lack of understanding for Target's leadership for both the design of Target's information system and the PCI-DSS standard. Target's leadership trusted a third party vendor, Trustwise, Inc., to determine their compliance and Target appeared to rely on the results of the Trustwise audit as an indication that all was well with the information system (A "Kill Chain" Analysis of the 2013 Target Data Breach, 2013). The disharmony between the structure component and the technology component can be examined by considering each of the PCI-DSS standards.

One PCI-DSS standard states: install and maintain a firewall configuration to protect cardholder data. This standard addresses the requirement for Target to control unauthorized access. The unauthorized access took place in U.S. Target stores from November 27th through December 15th, 2013. Target had firewalls, but the firewalls were configured in such a way to allow the attackers to move freely through the network, both in and out, transporting protected cardholder data. Target's external firewall configuration and architecture can be called into question. Additionally, internal firewalls could have assisted in the prevention of this attack by providing more effective segregation between the billing/invoice application, which the HVAC vendor employee used, and the POS systems that were infected with malware. The technology and structure (policy) constructs are not in harmony; therefore employee behavior can be impacted. The IT staff was not following the required policies of PCI. Structure, in the form of leadership, did not ensure there were a sufficient number of skilled security professionals, who were trained and knowledgeable about protecting the network (Oltsik, 2014). With the lack of proper

firewall management, users have the ability to access unauthorized areas of the network or accidently introduce malware to the Target network. In this case, a user from an outside vendor was able to introduce malware into the Target network (Olstik, 2014). Target's attackers gained access to the POS systems through a billing/invoice application.

There was some network segregation to prevent the attackers from moving from the billing system to the POS systems, but the movement of the hacker was cloaked under a name used by the data center, thereby allowing the traffic to pass through the network undetected (Oltsik, 2014; Riley, Elgin, Lawrence & Matlack, 2014). A well designed network segregation would have limited the type of traffic that could move from the billing system to the POS systems. The lack of a well-designed network segregation that could prevent malicious traffic from moving from one system, the billing/invoice system, to the POS systems is a disharmony between the structure (policy) of the organization and the technology. Target leadership failed to ensure there was harmony between the structure of the organization (policies) and the configuration of firewalls (technology) of the organization. The lack of leadership's concern over the harmony between the policies and the technology impacted the IT team's behavior, which meant the correction of the issue was not addressed. This problem created a significant information security risk to Target and their information system. Examination of this triad relationship could have saved Target significant expense and public embarrassment.

A PCI-DSS policy states to protect all systems against malware and regularly update anti-virus software or programs. Vulnerability scanning and patch management are needed to ensure the security of the information system remains at a maximum level. However, vulnerability scans and patch management can require that the system be unavailable for a period of time. If the leadership of Target did not consider the downtime for these activities of high enough priority, then these activities might not have been completed on a regular basis (Schwartz, 2014). Additionally, Target employees failed to install and update anti-malware on the POS systems. These systems were Microsoft desktop systems and should have been protected using anti-virus and anti-malware. Role based access to the POS systems and the implementation of local firewalls combined, could have stopped the loss of the data. Because Target IT employees did not ensure these security controls were in place, the Target information system was very vulnerable to malware and was infected by the hackers. This was an indication that the structure (policies and leadership's priorities) constructs were not in harmony with the technology (no anti-malware or role based access on the POS system and lack of downtime for scans and patching), which in turn affected the Target IT team's behavior because they did not find it important to ensure all systems were kept up-to-date and protected with these security controls.

PCI-DSS policy states organizations should develop and maintain secure systems and applications. Target data included stored PIN data, which is in violation of the PCI-DSS standard and indicates disharmony between the structure and technology constructs. By storing this data, Target provided a method by which attackers could make the possession of the stolen cardholder data useful. Once again, this situation provides an insight into the relationship between the structure and the technology components of the model. The policy does not allow the storage of this data. The Trustmark suit of Target and Trustwave (2014), indicate the Target leadership did not consider information security a priority, but rather the goals and objectives of the organization took priority, which would include the sale of merchandise to make a profit (Trustmark National Bank and Green Bank, N.A. v Target Corporation and Trustwave Holdings, Inc., 2014).

PCI-DSS states that organizations must maintain a policy that addresses information security for all personnel. The contractual agreement between Target and the HVAC vendor can come into question here. There should be requirements for Target's outside users when accessing the Target systems. Perhaps this indicates that organizations should ensure their vendors are implementing proper information security controls before a contract is signed. Vendor collaboration on information security could have assisted Target in the protection of the credit card information (A "Kill Chain" Analysis of the 2013 Target Data Breach, 2013). Target leadership and security personnel were either not aware of or did not consider the importance of meeting this PCI-DSS standard. The leadership would be responsible for ensuring all contracts with vendors meet the organization's information security requirements. The lack of concern from Target leadership with the management of the vendor employee's access and ensuring their technology was meeting PCI-DSS requirement impacted the security team's ability to protect the Target network.

It appears that Target's leadership relied on a Trustwise Inc. vendor to ensure the protection of the information system. Research of the data indicates that Target's leadership lacked an emphasis to their employees about the criticality of information security controls. Leadership falls under the structure component of the research model. The Target leadership indicated they were PCI-DSS compliant and they had the Trustwise, Inc audit to validate their beliefs, and yet the very design of the network would call that into question. This is a disharmony between the structure component and the technical component of the research model. Target deferred their information security responsibilities to a third party and then appeared to consider that sufficient to protect the information system. The disharmony would then affect the behaviors of the Target system users. The Target employees would have assumed the system was well protected, just as it appears their leadership had done. The Target employees would have assumed that no changes or additional work was required to ensure the information system's

security. An additional consideration is that Target system users do not just include Target employees. The HVAC employee who initially compromised the system could be considered a Target system user, as well. The need for harmony between the structure component and the technology component with the HVAC vendor is evident in that the initial infiltration into Target's network environment began at this point. Some practitioners believe that the PCI-DSS standard is not sufficient for protecting sensitive information (Litan, 2014). While aiming to meet this specific standard through the use of a third party vendor, Target's leadership failed to ensure that every aspect of the information system was as secure as possible while remaining usable for those who need to access the data.

The review and improvement of the PCI-DSS standard (structure construct) and the requirements for updated credit cards with chips (technology construct) could have assisted in the mitigation of risk to the Target customers. Using the Synergistic Security Model could assist organizations in finding areas of the model that have room for improvement. Improvements to the banking standard, such as requiring companies to encrypt the card data while in transit, whether on the company's internal network or on its way to a processor, would be an example of changing the structure of the model. A review would then be needed to determine the impact on the other constructs. Changing the technology used (chip cards instead of magnetic strips) could have had a significant impact on the results of the Target breach, saving the company their reputation, as well as their financial losses (Kitten, 2013; Liten, 2014). Updating this technology would have required a change to the structure construct in that a policy would need to require companies' use of the new technology. Then, the tasks impacted and the behavior of the people would need to be examined to determine how the structure and technology construct changes affected these two constructs.

5.2 Triad Relationship: Structure – Task – People

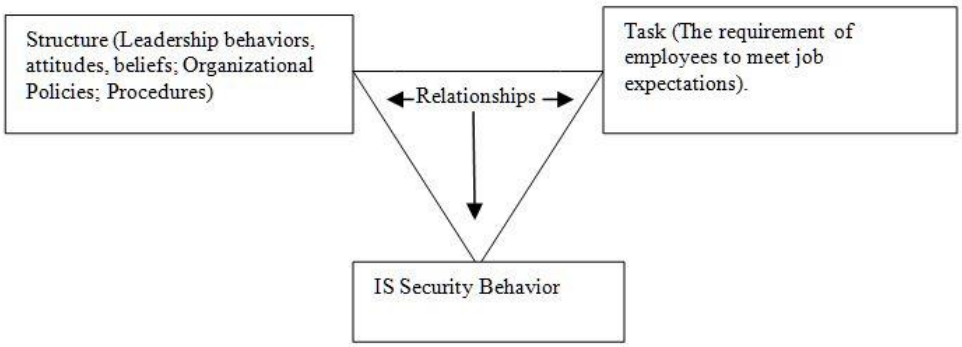

Figure 5: The Information Security Structure- Information Security Task-People (Information Security Behavior) relationship

One of the very obvious situations in the Target data breach that provides an indication of the relationship between the structure, task, and people components of the model was the lack of the Target security team in providing sufficient monitoring for the information system. This is evident in that the new monitoring tool installed at Target just six months before the incident was providing multiple, high level alerts to the IT team. However, there was no response from Target's employees (Riley, Elgin, Lawrence & Matlack, 2014). The PCI-DSS standard requires the logs and firewalls to be monitored every day (PCI-DSS, 2013). A detailed monitoring of the alerts received by Target's monitoring system would have provided sufficient details for the attack to be circumvented. However, the attack continued for 18 days (Acohido, 2013). To analyze the Structure – Task – Behavior relationship, several situations could be considered. If the new monitoring system was providing a significant number of false positive alarms, the team would have eventually ignored the alerts. This disharmony would cause the Target security team to fail to analyze the situation. If viewing the incident with a perspective that the Target security team did notice the alarms, then the team may have been unsure of the proper response to the alert. The lack of Target's response to the alerts could be attributed to a disharmony between the structure (policies and procedures) and task components of the model. This lack of response indicates the information security team was not provided proper tasks, or processes, when placed in a situation they had not experienced before. The team would fail to behave in a required manner. Additionally, the lack of response could also indicate the Target team did not have sufficient training or skills to understand how the monitoring tools work or how the team was to analyze the alerts and logs when they saw a system alert. Since the monitoring system was fairly new, then the lack of response could indicate the Target security team was not sufficiently familiar with the tool to understand what the alert was indicating. The leadership should assist the team with processes and procedures that ensure the security team will monitor the information system as required and respond to alerts in a specific, organized manner. This disharmony was a significant factor in the success of the data breach attack.

PCI-DSS requires the organization to regularly test security systems and processes. The impact of the Target data breach indicates the testing of the security systems and processes was very weak and the testing scenarios failed to consider all information security risks and vulnerabilities. Testing a system for vulnerabilities can affect system performance and, if not controlled well, can cause a system to go down. Additionally, testing systems and processes requires time and effort, an activity that Target may not have considered important enough to interrupt normal business. As suggested in the Trustmark lawsuit of Target and Trustwave, the Target leadership may have considered the operations of Target to have more priority than conducting information security tests (Trustmark National

Bank and Green Bank, N.A. v Target Corporation and Trustwave Holdings, Inc., 2014). If the accusations Trustmark made in the lawsuit are accurate, it indicates disharmony between the structure and task constructs and it impacts the people (behavior) component of the research model. The leadership priorities (structure construct) and the relationship with the tasks required, impacted the IT employees behavior.

A policy (Structure) from PCI-DSS states: Do not use vendor-supplied defaults for system password and other security parameters. The Target attackers were able to exploit a default BMC Software account name and password, meaning that the BMC Software system defaults were not renamed, which allowed the hackers to gain entry (Oltsik, 2014). Target indicated they met the PCI-DSS standards, but the technology was not configured in such a way to meet those standards. This is a disharmony between the structure and the technology components of the model. Structure (Policy) says they must rename the default password of the BMC software. However, in reality, the behavior of the IT team was to leave the default password as it was. The resulting behavior was that the Target employees did not follow the policy. Target employees followed leaderships premise that the Trustwise, Inc. PCI-DSS audit was an indication the information system was secure and there were not problems to investigate (A "Kill Chain" Analysis of the 2013 Target Data Breach, 2013).

5.3 Triad Relationship: Task – Technology – People

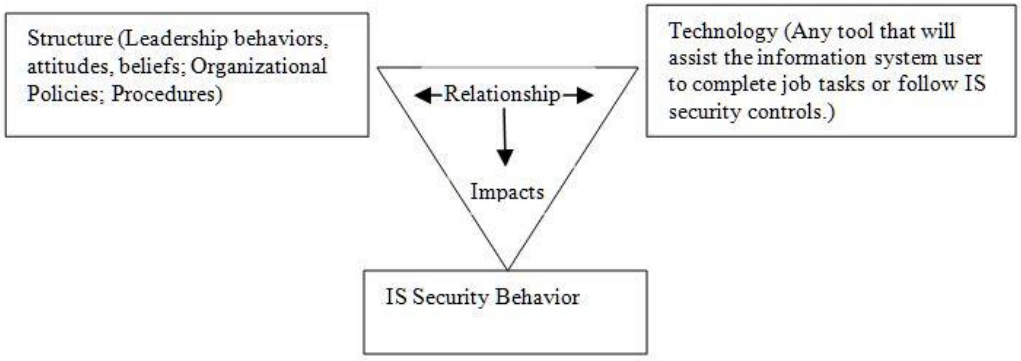

Figure 6: The Information Security Task- Information Security Technology- People (Information Security Behavior) relationship

Segregation of the network was required according to the PCI-DSS standards (PCI-DSS, 2013). These standards fall under the structure component of the research model. The technology component was to implement and configure firewalls and V-LANs and other network segregation practices to ensure the network would be secure. The Task component of the network would include the assigned job tasks

that the Target security team should have been completing in order to ensure the network segregation was meeting sufficient levels. Because of the successful nature of the Target data breach, it is very obvious that the relationship between these three components was inharmonious. Organizations should review their systems and ensure there is harmony between each area of the research model to ensure that the information security of the organization is being addressed and managed efficiently and effectively. Another data element to analyze for this research model triad is the warning the Target security team received from the Symantec Endpoint Protection (an antivirus system) that identified suspicious behavior on the server that was also identified by the monitoring system (A "Kill Chain" Analysis of the 2013 Target Data Breach, 2013; Riley, Elgin, Lawrence & Matlack, 2014). The PCI-DSS standard applies in this situation. The technology is Semantic software that was sending out warnings to the Target security team, yet the security team's behavior was not sufficient to prevent the attack from continuing. The disharmony between the structure, which provided the policies and standards, the technology, which provided alerts, and the behavior of the technical team caused a serious situation to go un-noticed for a significant number of days. Target leadership relied on the Trustwise, Inc audit to ensure security controls were at a sufficient level.

The POS data was stolen at the actual point of sale because of malware that was introduced by a user (Oltsik, 2014; Vijan, 2014). The user most likely fell for a phishing attempt or some other social-engineering event. Once the user logged onto the Target system while completing a job task, the hacker was then able to glean login and password information for access to the Target system. This fits the relationship between the task (where the user was completing a job task) and technology (where the user was using technology). It also appears that anti-malware may not have been active or up to date (technology). This can be coupled with the people construct where a lack of understanding or awareness of social engineering risks is evident. There was a disharmony in the information security model that allowed the malware to provide access to the Target hackers.

5.4 Triad Relationship: Task – Technology – Structure

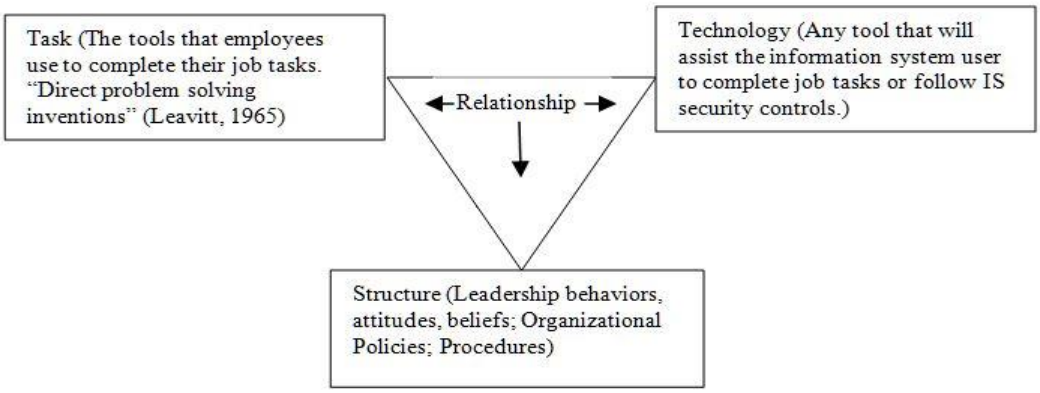

Figure 7: Information Security Task – Information Security Technology – Information Security Structure

When considering the relationship between the triad components of task, technology and structure for Target's data breach, the disharmony becomes very obvious. The structure construct of the research model does not only address PCI-DSS, but it also includes internal policies, procedures and processes that are expected from the employees. This construct will also include the leadership's attitudes and values, organizational structures and any other organizational design that can influence the actions of the employees. As discussed earlier, the structure construct of the research model was not in harmony with the technology construct. While the required technology tools appears to have been purchased by Target, the implementation and configuration of these tools appears to have been lacking, creating exceptional risk for the Target information system. The relationship between the structure and task constructs was discussed earlier, as well. There was disharmony between these constructs because the required actions of the Target employees and the required processes, procedures and leadership appear to have been lacking. Last, the relationship between the tasks and technology was in disharmony as it appears that the Target employees were unsure of how to use or react with the security monitoring system when the alerts were provided. If the employees were properly trained, it is also a possible issue that the configuration of the monitoring tools could have needed to be adjusted to ensure alerts were not creating too many false positives. As mentioned earlier regarding the compromised server that stored the stolen data, the structure construct required the default login and password be changed, the technology existed that would easily allow this task to be completed, yet the task was never completed. The harmony between each of these areas was not there. If the employees had too little time, too little skills, or lack of knowledge, it was an issue that should have been recognized and addressed. The structure construct in the form of leadership should ensure the employees have

all of the knowledge, tools, and time needed to implement the security of the information system. Using the Synergistic Security Model to analyze the harmony of the security program could have assisted with the correction of some, if not all, of these issues.

This triad examines the relationships between the information security tasks, the information security technology and the behavior of the employees. The Target security team was not very familiar or comfortable with the new system and may not have developed a trust of that system, which would be a change that was introduced to the Synergistic Security Model. The Target security team may have experienced usability issues with the new monitoring tool. The relationship between the required tasks for Target's security team and the new technology may not have been in harmony. While earlier analysis indicated that the PCI-DSS standard required consistent and reliable log and firewall monitoring, the task did not occur effectively. The new monitoring system was installed six months earlier, but the multiple alerts went completely unnoticed and were not responded to (Riley, Elgin, Lawrence & Matlack, 2014). This is not the only example of disharmony between the task, technology and structure constructs of the research model.

A task that the Target leadership could have done to ensure the harmony between PCI-DSS compliance and the technology was to ensure all systems, including the POS systems, were protected with anti-virus software. The leadership should have ensured the tasks necessary for information security were completed by the employees, which most likely meant a requirement for training and planning for incidents to occur. Additionally, the POS systems could have been configured to disallow new applications (i.e. malware) to be installed without specific requirements. These data elements indicate a disharmony between task-technology-structure. Had the Leadership ensured all of the components of the research model were in harmony, the data breach may not have happened, or at least may not have been nearly as severe.

6. Limitations

Due to the fact that this research investigates sensitive data that has the potential to expose weaknesses and vulnerabilities of not only organizations, but also individuals involved, it is very difficult to obtain deeper information into the "why" and "how" the incident occurred. Some speculation based on actions of individuals and statements made by those involved and those conducting the investigations have to be employed.

Obtaining the documents on the Target Data breach assisted with the analysis, but to have had access to those involved and obtain direct quotes would have been

of great benefit. The current research was limited to information that was publically available.

Last, this was a single case study, which indicates that added case studies would shed additional light onto the impact of the Synergistic Security Model and would provide further evidence of the impact of harmony between the constructs. Further work needs to be conducted to investigate the impact of the Synergistic Security Model on the efficacy of an information security program.

7. Conclusions

The Synergistic Security Model is based on the seminal macro-ergonomic model, The Leavitt Diamond Model (1965). The analysis of the data from public sources indicated that poorly designed security work systems can impact the efficiency and effectiveness of an information security program. A well designed information security program should include constructs that work in harmony. Each of these constructs impact the other constructs. Therefore, when a change is made to any one of the constructs, an analysis of the impact of that change should be conducted. A thorough analysis could prevent information security incidents and assist the organization with establishing a well-designed information security program.

Triads of the model were used to assist with the analysis. However, since a change of one construct can impact all other constructs, many of the discussed events fit into several different triads. For example, the fact that the security personnel at Target did not monitor the alerts from the FireEye Company and India could be the result of the leadership placing more emphasis on sales and less on security (Oltsik, 2014). However, this could also be the result of the employees not receiving sufficient training or it could be the result of the lack of sufficient staff (Oltsik, 2014). All situations can exist and each situation can fit into the information Synergistic Security Model, indicating an impact on the other constructs.

The Synergistic Security Model can be used as a work system framework to ensure that all constructs of an information security program are in harmony. The harmony of these constructs creates a work system environment that helps researchers and practitioners understand the impact these constructs can have on the information system users. This research only looked at the impact of non-malicious behavior caused by disharmony within the research model. This research did not consider malicious behavior.

This research did consider the pressures on employee behavior caused by out of balanced constructs in the Synergistic Security Model. Organizational leaders must work toward creating the balance between the pressure to complete job tasks and the pressure to ensure information security compliance.

It is important that researchers and practitioners continue to examine methods for ensuring users follow information security controls consistently, thereby ensuring a more secure information system.

References

Acohido, B. (2013). Q&A: PCI rules could help stymie Target data thieves. USA Today. Retrieved September 15, 2014 from http://www.usatoday.com/story/cybertruth/2013/12/23/qa-pci-rulescould-help-stymie-target-%20data-thieves/4179941/

Adams, A. & Sasse, M. (1999). Users are not the enemy. *Communications of the ACM*, *42*, 41-46.

A "Kill Chain" Analysis of the 2013 Target Data Breach. (2013). Majority Staff Report for Chairman Rockefeller. Retrieved September 15, 2014 from http://www.commerce.senate.gov/public/?a=Files.Serve&File_id=24d3c229-4f2f-405d-b8db-a3a67f183883

Albrechtsen, E. (2007). A qualitative study of users' view on information security. *Computer & Security*, *26*, 276-289.

Alfawaz, S., Nelson, K. & Mohannak, K. (2010). Information security culture: A Behavior compliance conceptual framework. *Eighth Australasian Information Security Conference*, Brisbane, Australia.

Badaracco, J. (1993). Whats the matter with business ethics? *Harvard Business Review*, 38-48.

Beautement, A., Sasse, M. & Wonham, M. (2008). The compliance budget: Managing security behavior in organizations. *Proceedings of the 2008 workshop on New Security Paradigms*, Lake Tahoe, California, 47-58.

Besnard, D. & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security*, *23*, 253-264.

Carnegie Mellon CERT Program, CSO Magazine; PricewaterhouseCoopers & United States Secret Service. (2013). Retrieve July 19, 2014 from http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/us-state-of-cybercrime.pdf

D'Arcy, J., Hovav, A. & Gallette, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. *Information Systems Research*, 20(1), 79-98.

Darke, P. Shanks, G. & Broadbent, M. (1998). Successfully completing case study research; combining rigour, relevance and pragmatism. *Information Systems Journal*, *8*, 273-289.

Da Veiga, A. & Eloff, J. (2009). A framework and assessment instrument for information security culture. *Computers & Security*, *2009*, 1-12.

Dhillon, G. (2001). Violation of safeguards by trusted personnel and understanding related information security concerns. *Computers & Security*, *20(2)*, 165-172.

Dhillon, G. & Torkzadeh, G. (2006). Value-focused assessment of information system security in organizations. *Information systems Journal, 16*, 293-314.

Harris, M. & Furnell, S. (2012). Routes to security compliance: be good or be shamed? *Computer Fraud & Security, December*, 12-20.

Hedstrom, K., Kolkowska, E., Karlsson, F. & Allen, J. (2011). Value conflicts for information security management. *Journal of Strategic Information Systems (2011)*, 1-12.

Huang, D., Rau, P., Salvendy, G. Gao, F. & Zhou, J. (2011). Factors affecting perception of information security and their impacts on IT adoption and security practices. *International Journal Human-Computer Studies, 69*, 870-883.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*, 83-95.

Kitten, T. (2013). Target Breach: What Happened? Expert Insight on Breach Scenarios, How Banks Must Respond. Retrieved Feb 7, 2015 from: http://www.bankinfosecurity.com/target-breach-what-happened-a-6312/op-1

Kleiner, B. (2006). Macroergonomics: Analysis and design of work systems. *Applied ergonomics, 37*, 81-89.

Kluge, A., Badura, B., Urbas, L. & Burkolter, D. (2010). Violations-inducing framing effects of production goals: Conditions under which goal setting leads to neglecting safety-relevant rules. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 54*, 1895-1899.

Kraemer, S. & Carayon, P. (2007). Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists. *Applied Ergonomics, 38(2007)*, 143-154.

Kraemer, S., Carayon, P. & Clem, J. (2009). Human and organizational factors in computer and information security: Pathways to vulnerabilities. *Computers & Security, 28*, 509-520.

Leach, J. (2003). Improving user security behavior. *Computers & Security, 22*, 685-692.

Leavitt, H. (1965). Appling *organizational change in industry: Structural, technical, and humanistic approaches.* Handbook of organizations, Rand McNally, Chicago, IL.

Lee, A. (1989). A scientific methodology for MIS case studies. MIS Quarterly, 13(1), 33-50.

Litan, A. (2014). How PCI failed Target and U.S. Consumer. Gartner blog. Retrieved September 15, 2014 from http://blogs.gartner.com/avivah-litan/2014/01/20/how-pci-failed-target-and-u-s-consumers/?fnl=search

Nash, K. & Greenwood, D. (2008). The global state of information security. *CIO Magazine, October 15*, Price Waterhouse.

Oltsik, J. (2014). Lessons Learned from the Target Breach: Congressional report points to people, process, and technology. Networkworld. Retrieved September 15, 2014 from http://www.networkworld.com/article/2226629/cisco-subnet/lessons-learned-from-the-target-breach.html

Payment Card Industry (PCI) Data Security Standard. (2013). PCI Security Standards Council, LLC. Retrieved September 15, 2014 from https://www.pcisecuritystandards.org/documents/PCI_DSS_v3.pdf.

Pfleeger, S. & Caputo, D. (2012). Leveraging behavioral science to mitigate cyber security. *Computers & Security, 31*, 597-611.

Post, G. & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security, 26*, 229-237.

Riley, M., Elgin, B, Lawrence, D. & Matlack, C. (2014). Missed alarms and 40 million stolen credit card numbers: How Target blew it. Bloomberg Business Week – Technology. Retrieved September 15, 2014 from http://www.businessweek.com/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data#p1

Ruighaver, A., Maynard, S. & Chang, S. (2007). Organizational security culture: Extending the end-user perspective. *Computers & Security*, 56-62.

Schwartz, M. (2014). Target, PCI Auditor Trustwave Sued By Banks: Trustwave apparently certified the retailer as PCI compliant –but can PCI assessors be held liable for data breaches? Darkreading. Retrieved September 15, 2014 from http://www.darkreading.com/risk/compliance/target-pci-auditor-trustwave-sued-by-banks/d/d-id/1127936

Siponen, M., Mahmood, A. & Pahnila, S. (2009). Are employees putting your company at risk by not following information security policies? *Communications of the ACM, 52(12),* 145-147.

Siponen, M., Pahnila, S. & Mahmood, A. (2014). Employees' adherence to information security policies; an exploratory field study. *Information & Management, 51(2),* 217-224.

Smith, M. & Sainfort, P. (1989). A balance theory of job design for stress reduction. *International Journal of Industrial Ergonomics, 4*, 67-79.

Stake, R. (1995). *The art of case study research*. Sage, Thousand Oaks, CA.

Stanton, J., Stam, K., Mastrangelo, P. & Jolton, J. (2005). Analysis of end user security behaviors. *Computers & Security, 24(2),* 124-133.

Trustmark National Bank and Green Bank, N.A. v Target Corporation and Trustwave Holdings, Inc, (2014). Case: 1:14-cv-02069 (Illinois, 2014).

Vance, A., Siponen, M. & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protections motivation theory. *Information & Management, 49,* 190-198.

Vijayan, J. (2014). Target attack shows danger of remotely accessible HVAC systems. Computerworld, Feb 7 2014. Retrieved February 2015 from http://www.computerworld.com/article/2487452/cybercrime-hacking/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html

Vroom, C. & von Solms, R. (2004). Towards information security behavioral compliance. *Computers & Security, 23,* 191-198.

West, R. (2008). The psychology of security: Why do good users make bad decisions? *Communications of the ACM, 51(4),* 34-41.

Workman, M., Bommer, W. & Straub, D. (2008). Security lapses and the omission of information security measures: A threat control model and empirical test. *Computers in Human Behavior, 24*, 2799-2816.

Yin, R. (2012). *Applications of case study research*. Sage Publications, London