Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 2, No. 1, 280-290
2018
DOI: 10.33805/2576-8484.155

One to Many: A Framework for Scaling Risk Mitigation Assurance

Joel Bigley
California Baptist University, 8432 Magnolia Ave, Riverside, California, USA; jbigley@calbabtist.edu (J.B.).

Abstract: The lack of vulnerability control leads to organizational harm in global businesses when the exploitation of a weakness occurs. How can a global supply chain protect itself from vulnerabilities that can damage their brand and their physical property? In this qualitative case study the author shows how a multi-site corporation can use a method to learn what the vulnerabilities are in a single facility and use a framework to methodically scale the controls needed to mitigate vulnerabilities across the supply chain. This framework allows leadership to keep cost in mind so that the highest vulnerabilities are mitigated as a priority. A team of security experts was used to capture data in framework used for analysis. This framework was then used strategically to reduce the overall risk of threat vectors in the global organization.

Keywords: *Cost controls, Vulnerabilities, Risk loss, Global supply chain, Scaling.*

1. Introduction

Recently Barnum and Bailey Circus closed their business after more than 145 years of entertaining many thousands of people [1]. While this is a loss, they were very fortunate. The life-cycle of businesses today is usually much shorter than this. The Boston Consulting Group warns about a tremendous increase in failure among publicly listed companies in the U.S. which now stands at 32 percent (BCG Perspectives, 2015). Furthermore, UNCTAD (2015) reported a 16 percent reduction in Foreign Direct Investment (FDI) flows because of geopolitical concerns, policy uncertainties and governance issues. Operating across borders magnifies the complexity of risk management [2].

How can firms strategically mitigate risk vulnerabilities across global supply chains? This article aims to show a method based on a case study that was successful in risk mitigation. The strategy was structured and expedient leading to brand dominance in a field where high value assets were handled. While many firm's flounder with achieving a high level of vulnerability mitigation, the success of the program was a significant competitor's advantage in this case.

This article is based on a facility-based global supply chain case study that can be considered as informational to other locations. Some limitations on generalizability exist as all locations are not the same, however, the general structure can be applied in a multi-site organization. Even though many facilities are unique, the tools presented are transferrable and with minor modifications could be practically used. While some leaders in facilities are taking significant measures to protect their employees, many others believe that the risks they could incur are tolerable. Some of this risk comes from threat sources, while other sources are risks associated with a lack of compliance with policy. To understand this better, leaders must understand what the threats are, how well they are being mitigated, and have an interest to mitigate the residual risk that exists. The residual risk is the type and magnitude of the threat that has not yet been addressed by the controls that have already been introduced. This risk continues to be carried by the leadership of the facility and should be known to them. It may be referred to as risk appetite.

This article is broken into five main sections after the introduction. First, a literature review explores single site vulnerability, the de-escalation of threat vectors, and an introduction to the risk register. The discussion of threat vectors relates to individual facilities. The de-escalation of these vectors will require tools to be deployed and validated as effective prior to scaling vulnerability mitigation capabilities across many facilities. The impact and likelihood of harm must be understood to drive decision making. The methods for the study are covered and then the findings are discussed. The findings will show that an engaged leader must have mechanisms in place that enable the discovery of threats before vulnerabilities are exploited. The insight gleaned from the tools presented in this article can be used to create transparency in the environment on an ongoing basis. A tool is discussed that ultimately will enable the visualization of the threatscape in its current form and then with the augmented controls enacted. Finally, the conclusion summarizes the study and the implications and limitations of the study follow to conclude the article. Now, some comments on risk to introduce the concept and its applicability to this study.

A few comments on risk management are needed to set the stage for the case. Risk is both visible and invisible. The management of risk is different if it is visible as opposed to being invisible. Risk is seen by the author as the opportunity for harm. In some cases the opportunity is exploited resulting in the harm of a firm's reputation, physical harm, financial harm, brand reputation harm, and any damage to the company that would dissuade any stakeholder from supporting and engaging willfully in the success of the company.

Invisible risk and emerging risks are unknown; however, they need to be discovered before they can be mitigated. Uncertainty is invisible but inevitable; however, discovery is always possible, even more so with a structured approach that is capable. Uncertainty must be governed with effectiveness to mitigate vulnerabilities that continually emerge. This governance is not always perfect and there are false alarms because risk analysts are often proven to be wrong just as there are exploited risks that occur that could not have been mitigated. In fact, risk analysts often fail to predict or mitigate significant disasters. Even so, those who are in harm's way need protection and resilience against any vulnerability that can cause damage. While many companies execute financial audits and have quality assurance programs, many do not have mature risk mitigation assurance efforts. Some firms are required to come under the scrutiny of industry groups and must submit to audits that uncover vulnerability and challenge business continuity.

Even so, there is variability in auditing effectiveness. Auditees learn how to answer questions and may even lie or mislead auditors to skirt possible penalties or additional costs for controls. Audits may be internal or external and may produce different assessment results within the same audit scope.

Reputation protection can be a proactive or reactive activity and may include not failing an audit that would be made known to clients or the industry. In either case, the mitigation strategy is different. In the latter, in a reactive context, the harm has already happened and containment, then recovery, is the objective. In the former, the proactive context, the harm is pending and efforts are expended to keep vulnerabilities from existing or being exploited. Both require resources. Failure to address both scenarios will impact competitiveness, reputation, and the ability to enter markets [3]. A critical question to leadership is, "Are the known vulnerabilities in the corporation's portfolio of concerns?" and "At what level of priority are they?" Ultimately, the worst case scenario is possible where vulnerabilities are linked and a small trigger birth's a catastrophe. Some refer to this as "the alignment of the planets" event. An effective risk management strategy will mitigate vulnerabilities so that they are not exploited.

As illustrated below, the ability to mitigate vulnerabilities comes from internal and external sources. Both should be executed with transparency and be welcomed by auditees. The endogenous cycle of influence comes from external sources that interact with the entity. These sources can be auditors, law enforcement, industry groups, etc. Additionally, vulnerability mitigation influences should come from internal sources. Many entities only rely on external sources and avoid allocating effort to internal sources of influence. These internal influences can include culture, work environment, discovery through assessments, and leadership inquiry. A mature entity from a vulnerability mitigation perspective would be one where leadership, internal and external assessment are all capable of discovering and mitigating vulnerabilities (**Figure 1**).

History: Received: 9 September 2018; Accepted: 4 December 2018; Published: 8 December 2018
* Correspondence: jbigley@calbabtist.edu

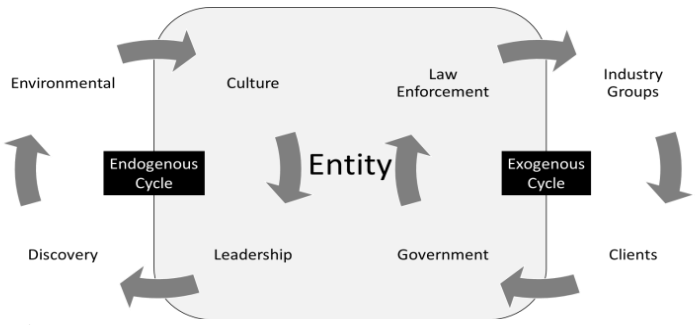

Figure 1.
The endogenous and exogenous cycle of influence on an entity.

The goal of assessment is discovery and vulnerability mitigation that leads to a more mature posture. The entity can be a facility, a department, a cell, or any unit of manageable size. How can the maturity of a single entity influence a global supply chain? The answer is one entity at a time. While every entity in the supply chain is different, similarities exist and the structure may be duplicated. With this in mind, the first location can be strategically chosen and achieve the highest level of maturity. Specifically, the original site (S0) can migrate from maturity level 1 to a higher level over time. This entity can then influence a sequenced list of entities (S1 or site 1 to S6 or site 6) in order of their priority in relation to change capacity (and data classification, if applicable). Each entity may not need to achieve the same level of maturity. This depends on the service lines and products allocated to those facilities. This allocation of work should be known before any transformation begins. In some cases, the vulnerabilities are acceptable and in other cases they don't exist due to physical uniqueness. In the case where maturity levels need to be achieved, the goal would be for the site to migrate towards the goal by leveraging what has already been accomplished at the original site. Specifically, as is illustrated in **Figure 2** below, site 2 (S2) strives to achieve a maturity level 3 as part of the overall plan. Site 4 (S4) does not have this requirement because the data classification or the vulnerability in the workflows does not have the same level of vulnerability as are present in S2. If this information is known each site can plan to mature in parallel based on the requirements. To assure that the appropriate maturity levels are achieved quickly, should a change happen regarding vulnerabilities in a site, the site in question can obtain and implement the controls already present in S0 as illustrated. In an efficient way, then, the controls validates are relevant and effective in one site (S0) are transferred to all sites (S1 to S6) in the supply chain as required by customers' expectations and by internal risk assessment and risk appetite.

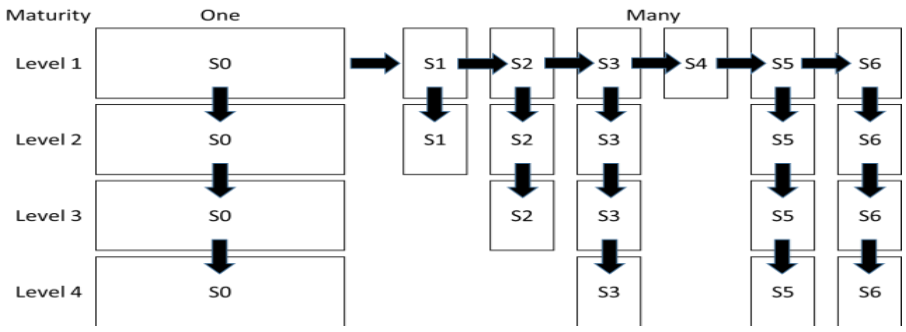

Figure 2.
The scaling of maturity in a global supply chain from Site 0 (S0) to Site 6 (S6).

2. Literature Review

2.1. Achieving a High level of Maturity at S0

Even though high loss events are infrequent, threats should be known and captured on a Risk Register [4, 5]. The Risk Register must identify which vulnerabilities have been mitigated/minimized, list which vulnerabilities remain, and be periodically updated. The Risk Register contents should be known by leadership who engage in assessment or Environmental Scanning (ES) activities. Leaders may enact mitigations based on priorities and resources. When mitigations are omitted, leaders must also agree to live with the vulnerabilities that have not experienced any mitigating action.

The amount of time between assessment activities should increase when there is environmental uncertainty; however, scanning frequency decreases when uncertainty is overwhelming, when absorptive capacity is exceeded [6, 7], or when useful information is not accessible [8, 9]. If frequency is too high, it just adds to the chaos. Why? Because it does not produce meaningful results. Concurrently, a perception of diminishing returns from scanning efforts in a stable environment may lull an organization into catatonic complacency [8] or entropy [10, 11] while risk threats accumulate unnoticed.

Informal, or ad hoc, scanning by leadership teams is typically short term, infrequent, fragmented, and may be initiated by a crisis [12-15]. Even though leaders typically conduct scanning more frequently [14], strategy making may be linked to subjective interpretations in difficult to comprehend and rapidly changing environments [14, 16, 17]. A proactive stance may be further inhibited when leaders assume that team leaders are performing scanning when in fact they are not [14].

Scanning accuracy is dependent on the threat domains selected and the approach taken [18]. For example, a worker might abide by clear-cut policies, while leaders without clear role definitions or explicit bounds might have a more ambiguous linkage to threat domains [14]. Perception accuracy is a basis for managerial action [19] and scanning is the first step in the development of perceptions [20, 21]. Consequently, vulnerability assessment voids are particularly risky [14] jeopardizing needed control implementation. It is clear that continuous scanning must include structured data collection using optimized frameworks that clarify perceptions, tasks, and reveal actual results from actions taken [22].

Two general measures of scanning strategy are frequency and scope [23, 24]. The range of characteristics of an expected environment helps leaders make decisions today that align them with a desired future, at a suitable pace. In high risk organizations, scanning frequency, scanning intensity, and scanning type [25] matches, or exceeds, the environmental change rate [6] so that desired future states can be realized in time [8]. A lack of predictability, environmental fluidity, and complexity drive scanning strategies [26-30]. Leaders in complex and risk-laden environments are especially challenged to comprehend threats [31-34]. Organizations perceive their environments differently. This perception depends, at least partially, on their strategic approach, and if data collection is involved [35]. Furthermore, organizational intelligence influences strategic decision making. Data completeness and analyzability influences sense-making [36]. Proactively, data structures must assist with processing needed to develop, pursue, and monitor a strategy [17, 37]. Otherwise, facility leaders may decide that an environment is unanalyzable avoiding environmental scanning at their own peril [12, 38]. Ultimately, sense-making from ES activities occurs when leaders construct an assessment strategy by framing experiences and by creating new capabilities [39]. Strategic enactment occurs when activity, often simultaneous, is introduced to accomplish tasks, create new capabilities, and create sense within them. It is clear then that leaders with limited capacity for information processing have to be efficient in their approach [40] to get a predictive picture of what is to come, hence a need for scanning accuracy.

2.2. Threat Vector De-Escalation

Vulnerability may be exploited for purposes of harm to the firm. These threat vectors are specific to each facility; however, similarities exist between facilities allowing for synergies to be leveraged. To illustrate, **Figure 3** describes a threat vector and illustrates the increase in loss potential if the vulnerability is not de-escalated early. In this case the threat vector, one of the

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 2, No. 1: 280-290, 2018
DOI: 10.33805/2576-8484.155

elements on a Risk Register, is shown among other threat vectors all of which contribute to risk loss. As time elapses the armed robber's moves from trespassing to homicide as the risk loss potential increases. With a proactive de-escalation response the vulnerability to loss is decreased.

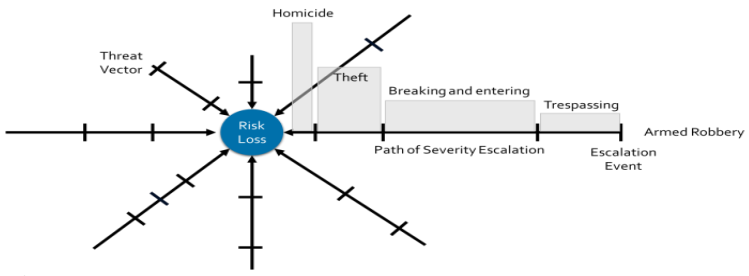

Figure 3.
Threat vector and de-escalation.

The output of an ES activity is a document that enables dialogue about and lists the vulnerabilities and threats in an organization. It is called a Risk Register [4, 5]. Action can be taken from the transparency created by the tool. The quantification of risk across the organization allows leadership to apply their appetite for risk in a more accurate and informed way. Minimally, the risk team and leadership should be made aware of its contents periodically. At risk is organizational continuity, loss of property, loss of life, loss of employee attendance, loss of ongoing revenue, and brand damage. Each section of the Risk Register for this case will be discussed in detail in the Findings section.

2.3. Risk Register: An assessment of Vulnerability

The Risk Register is essential for threat management as it records identified risks, their severity, and the action steps to be taken to reduce threats [4, 5]. It can be a simple document, spreadsheet, or a database system, but an effective format is simply a table. A table presents a significant amount of information in a small area. Security leaders should use the Risk Register as a risk management tool [4, 5]. It should be reviewed and updated continuously so that it can identify, assess, and manage risks to acceptable levels. For leaders to decide what mitigation steps are acceptable, they need to know the risks that are present and have a clear understanding of their risk appetite. Not all risks are known, and some emerge over time, however, existing threats can be determined based on insight from security team members, past events, and from news accounts both local and national. Even with this information in hand, allowances should be made for surprises. The register provides a framework in which known elements that threaten the activities at the facility are captured. Setting up the Risk Register is important for clarity and understanding of the threatscape [4, 5]. Leaders comprehend scanning results when they understand interaction between identified threats and their influence on the local risk taxonomy [12, 13, 15, 41]. Attributes of variables in environmental scanning could include environmental complexity, rate of change, organization size, impact and frequency of risk events, as well as information source reliability [25, 42-44]. The need for these variables, their variety, an acceptable variation range within each one, and their weighting validate the need to customize a scanning framework to a specific location. The literature categorizes variables as controllable (ex. location, employee base, task assignment, organizational structure, and capacity) and uncontrollable (ex. employee behavior, collaboration between functional areas, technology changes, economic conditions, attendance drivers, and regulatory restrictions) [45]. Controllable variables can be influenced while uncontrollable variables typically require forced adaptation [45]. An example of forced adaptation could be the establishment and enforcement of a policy. A vulnerability measuring system needs to accommodate these attributes and accurately represent the threats and associated variables chosen. Of course, data collection planning and analysis methods assure that the data collected is complete, relevant, and timely [6]. The methods for collecting the data for this study are now discussed.

3. Methods

According to Isaac and Michael [46], case and field research studies the background, current status, and environmental interactions of a community. In this case the community was a group of people that occupied a facility. This in depth investigation into risk threat management was facilitated by a group of interested co-researchers that were a part of the organizational security team. Each person contributed input following a list of questions that were posed in phases. This single unit was examined using a number of variables and conditions. A limitation, then, is generalizability to other populations as the data from this case may not be transferable to other cases. Even so, the data exposed in this case brings to light experiences that may be common to other settings thereby providing the opportunity for hypotheses that can be used for further study. The research information was obtained by asking specific questions to eight members of a team at a facility. Subjective bias was controlled by listing all the information that was obtained and then prioritizing it. Furthermore, Likert scales were used that could then be averaged. Each participant understood the objectives of the study; to understand the threats and mitigating controls in existence at the case sight. The Risk Register framework presented in **Figure 4** scaffolded the solicitation of information. In the beginning of the study, survey questions related to the descriptions of historical events that each member of the security team was aware of their either had happened or could happen based on local events documented in media. Members of the security team were well informed of crime in the area as they were also members of the law enforcement community. They had access to video footage stored on site that described historical events. These descriptions were then categorized by the type of crime and an identification number was assigned. The security team members were then asked to provide a probability number and severity number for each description. These were assigned to each item based on a Likert scale shown in **Figure 7**. From the resultant values a high, medium and low designation was assigned. The quantification of the risk loss threat description was then complete and average values could be obtained. Finally, the risk loss type was assigned.

The security team was then asked what the mitigating controls were that were deployed to mitigate these risk loss events. They provided the controls as well as the value of the controls in terms of providing awareness that an event was occurring and also a value of the controls ability to mitigate the event. These were recorded for each item and the average was shown at the bottom of each table for mitigation and awareness. The multiplication of the mitigation and awareness values is the risk priority number. The total of each multiplication resulting in an overall RPN of 617.

The team brainstormed control enhancements. With these in mind projected mitigation and awareness values with these controls in place were determined for each threat vector. If a control did not have a significant impact on the as-is mitigation or awareness variables, then it was dropped. The projected values for mitigation and awareness when multiplied became the projected RPN; 449. This value could be compared against the as-is RPN to see the impact of the enhancements.

Finally, the security team was asked the impact of the loss event would be, what likelihood of the event occurring would be, and how fast the event could happen, for each description. These values were captured using similar Likert scales and documented in the Risk Register. These values were then used for the heat map.

Case studies are made of materials collected while working with a group of individuals in a community. The intent of this case was to present a problem through awareness and then determining ways to reduce the potential impact or frequency of occurrence of the aspects within the problem. The author carefully considered the balance between providing important information and keeping confidential material protected. It is not possible to ensure that all of the materials collected are in fact accurate and complete. However, to a significant extent the facts as stated can be verified by other researchers, even in other communities that have similar threats.

4. Findings

4.1. Risk Register

The Risk Register must be current and transparent to leadership, so they can see which risks or vulnerabilities they are tolerating, and which ones are being addressed [4, 5]. Leaders may flag risks that haven't been registered so that they are

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 2, No. 1: 280-290, 2018
DOI: 10.33805/2576-8484.155

included in the vulnerability measurement and so that leadership can provide options for risk mitigation. There are several key sections to the register. An overview of the figure below, an actual facility Risk Register is discussed.

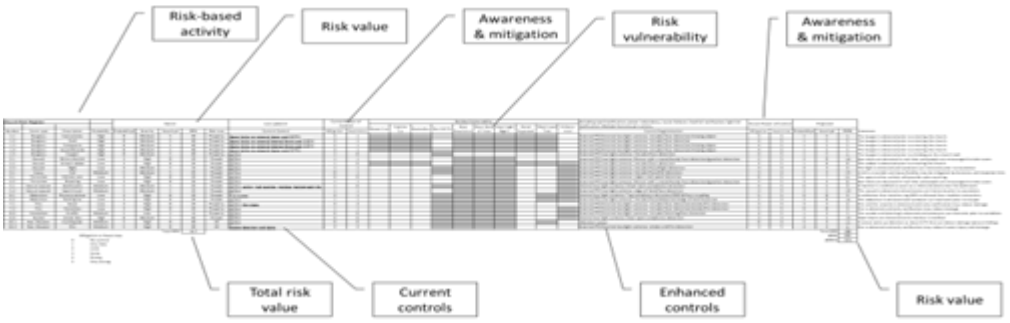

Figure 4.
Risk Register sections. The content is intentionally unreadable to focus attention on the sections.

The Risk Register has an owner that is listed at the top on the left next to the facility that the Risk Register is for. This person should be on the security team and be responsible for adding threats as they are discovered, and as they emerge. The source of this information can be external due to trends or internal from any stakeholder. The landscape is constantly changing, and the Risk Register needs to be kept up to date so that leadership is aware of the vulnerabilities and actions taken to mitigate them. Each threat was assessed on several levels. First, the threat, once registered, was given an item number for reference. The first digit was related to the type of threat (ex. Burglary) with the decimal number being the action from the threat source (ex. stealing instruments). This allows for a breakdown of a threat into risk loss categories, and is illustrated in **Figure 5** below.

Risk Register		
Number	Event type	Description
1.1	Burglary	Instruments
1.2	Burglary	Cash
1.3	Burglary	Computers
1.4	Burglary	Sound Boards
1.5	Burglary	Copper
2.1	Assault	Active shooter
2.2	Assault	Armed robber
2.3	Assault	Fight
3.1	Injury	Fall
4.1	Terrorism	Vehicle ram
4.2	Terrorism	Shooting
5.1	Sexual assault	Bathrooms
5.2	Sexual assault	Sport Court
6.1	Abduction	Nursery pickup
6.2	Abduction	Parking lot
7.1	Fire	Arson
7.2	Fire	Homeless
8.1	Vandalism	Graffiti
9.1	Animal	Animal bite
10.1	Nat. Disaster	Earthquake
10.2	Nat. Disaster	Fire

Figure 5.
Risk register threats.

Each threat action was described in terms of the probability and severity of the occurrence. The probability and the severity are simply defined as High, Medium, or Low. No one knows this better than the security team as they know the history and the impact of losses. The probability and severity numbers are an 8 for high, a 5 for medium and a 3 for low. These two numbers (probability and severity) multiplied by each other produce the Risk Priority Number (RPN). The spreadsheet can be sorted on this column from highest to lowest to produce a prioritized list of threats. This may help with consensus on what to work on first. By reducing the highest priority threats first, the RPN is reduced faster. The average probability and severity will be reduced with increased mitigation influence on the risk. In the meantime, these three numbers can be used as a baseline for the current threatscape along with the existing mitigating controls. Typically, when the risk-loss type is human the severity number will be higher. These elements are shown in **Figure 6**.

In a column to the right of the risk loss type the existing controls can be listed as shown below. It is good to know how strong the controls for mitigating the risk are. Where the controls are not strong, they could be enhanced to reduce the RPN. The influence of the controls is represented by two values based on a Likert scale in **Figure 7**.

In the Current Power of Control section, the mitigation column is the extent to which the current control reduces a threat. The second column, awareness, is the extent to which the control makes those who can take action to mitigate a loss aware of the threat so that they can respond [47]. Again, the average of the mitigation and awareness variables at the bottom of the columns can be seen as a baseline to be improved. These values characterize the current state **Figure 8**.

Risk Register			Risk Analysis					
Number	Event type	Description	Probability	Probability#	Severity	Severity#	RPN	Risk Loss
1.1	Burglary	Instruments	High	8	Medium	5	40	Property
1.2	Burglary	Cash	High	8	Medium	5	40	Property
1.3	Burglary	Computers	High	8	Medium	5	40	Property
1.4	Burglary	Sound Boards	High	8	Medium	5	40	Property
1.5	Burglary	Copper	High	8	Medium	5	40	Property
2.1	Assault	Active shooter	Low	3	High	8	24	People
2.2	Assault	Armed robber	Low	3	High	8	24	People
2.3	Assault	Fight	Low	3	Medium	5	15	People
3.1	Injury	Fall	Medium	5	Medium	5	25	People
4.1	Terrorism	Vehicle ram	Low	3	High	8	24	People
4.2	Terrorism	Shooting	Low	3	High	8	24	People
5.1	Sexual assault	Bathrooms	Medium	5	Medium	5	25	People
5.2	Sexual assault	Sport Court	Medium	5	Medium	5	25	People
6.1	Abduction	Nursery pickup	Low	3	High	8	24	People
6.2	Abduction	Parking lot	Low	3	High	8	24	People
7.1	Fire	Arson	Low	3	High	8	24	Property
7.2	Fire	Homeless	Low	3	High	8	24	Property
8.1	Vandalism	Graffiti	Medium	5	Low	3	15	Property
9.1	Animal	Animal bite	High	8	Medium	5	40	People
10.1	Nat. Disaster	Earthquake	Medium	5	High	8	40	All
10.2	Nat. Disaster	Fire	Medium	5	High	8	40	All
			Average	5.00	Average	6.33	617	Total RPN

Figure 6.
Risk analysis.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 2, No. 1: 280-290, 2018
DOI: 10.33805/2576-8484.155

Mitigation or Awareness	
0	No control
2	Very little
4	Little
6	Some
8	Strong
10	Very strong

Figure 7.
Likert scale for mitigation and awareness values.

Risk Register			Risk Mitigation	Current Power of Control	
Number	Event type	Description	Current Control	Mitigation	Awareness
1.1	Burglary	Instruments	Alarm/locks on external doors and CCTV	2	1
1.2	Burglary	Cash	Alarm/locks on external/internal doors and CCTV	2	1
1.3	Burglary	Computers	Alarm/locks on external/internal doors and CCTV	2	1
1.4	Burglary	Sound Boards	Alarm/locks on external doors and CCTV	2	1
1.5	Burglary	Copper	CCTV	1	0
2.1	Assault	Active shooter	CCTV	1	1
2.2	Assault	Armed robber	CCTV	1	0
2.3	Assault	Fight	CCTV	1	1
3.1	Injury	Fall	CCTV	0	1
4.1	Terrorism	Vehicle ram	CCTV	0	0
4.2	Terrorism	Shooting	CCTV	1	1
5.1	Sexual assault	Bathrooms	CCTV, policy, hall monitor, training, background chk.	1	0
5.2	Sexual assault	Sport Court	CCTV	1	1
6.1	Abduction	Nursery pickup	Tag system	2	1
6.2	Abduction	Parking lot	CCTV	1	1
7.1	Fire	Arson	CCTV, fire alarm	4	3
7.2	Fire	Homeless	CCTV	1	1
8.1	Vandalism	Graffiti	CCTV	0	0
9.1	Animal	Animal bite	CCTV	0	0
10.1	Nat. Disaster	Earthquake	CCTV	0	0
10.2	Nat. Disaster	Fire	Smoke detectors and alarm	4	4
			Average	1.29	0.90

Figure 8.
Existing controls and their impact.

The current threatscape is now documented. The known threats are registered along with their potential impact. The existing mitigating controls and their influence are documented with measures. With this information the solutions part of the Risk Register can be exploited to reduce the baseline values. Leadership will need to decide if physical and/or procedural controls will be used. If procedural controls are used, a discussion about enforcing the procedures will be relevant to their impact. Additionally, the reaction time to threats must be minimized and methods for the enforcement of policies will need to be considered. The choices made have an effect on the existing vulnerabilities and reduce the risk threat values. The mitigations taken are unique to each site and so are not listed; however, their impact is in **Figure 9** below.

The table indicates that each control was augmented to a varying degree based on a like-for-like assessment in relation to the based control. The net impact in this case study is a 73% reduction in the RPN. This reduction is reflected by the difference between the current and the future RPN, or the Projected Risk Priority Number (PRPN), is shown as the percent reduction between these two numbers. The control augmentations and enhancements (intentionally not listed as it is proprietary) will need to be assessed for their influence on the threats resulting in an improvement in awareness of threats, an improvement in mitigation power, a reduction in probability of occurrence, and a reduction in severity if the vulnerability is exploited. While the percent reduction in risk is not exact, it represents a method that was applied to a case to measure risk threats. And, it shows considerable impact from the actions that were taken. If the percent reduction were ten percent, then leadership would need to require more analysis so that stronger solutions are brought forward.

Risk Register			Future Power of Control		Projected		
Number	Event type	Description	Mitigation	Awareness	Probability#	Severity#	PRPN
1.1	Burglary	Instruments	4	5	1	5	5
1.2	Burglary	Cash	4	5	1	5	5
1.3	Burglary	Computers	4	5	1	5	5
1.4	Burglary	Sound Boards	4	5	1	5	5
1.5	Burglary	Copper	4	5	1	5	5
2.1	Assault	Active shooter	2	5	2	8	16
2.2	Assault	Armed robber	4	5	1	8	8
2.3	Assault	Fight	3	4	2	3	6
3.1	Injury	Fall	3	4	5	3	15
4.1	Terrorism	Vehicle ram	0	5	3	7	21
4.2	Terrorism	Shooting	2	5	2	4	8
5.1	Sexual assault	Bathrooms	4	5	0	5	0
5.2	Sexual assault	Sport Court	3	4	2	5	10
6.1	Abduction	Nursery pickup	5	5	0	8	0
6.2	Abduction	Parking lot	2	3	2	8	16
7.1	Fire	Arson	3	4	3	3	9
7.2	Fire	Homeless	5	5	0	8	0
8.1	Vandalism	Graffiti	4	5	1	3	3
9.1	Animal	Animal bite	3	3	2	5	10
10.1	Nat. Disaster	Earthquake	0	4	5	3	15
10.2	Nat. Disaster	Fire	3	5	2	3	6
			3.14	4.57	1.76	5.19	168
			-59%	405%	-65%	-18%	449
							73%

Figure 9.
Threatscape with augmented controls.

4.2. Threat Scape Management

The contents of the register will indicate if the facility is a hard or soft target [4, 5]. This posture will be clear to lone-wolfs and burglars alike, leading to either an invitation or deterrence. The register includes the value assigned to the risk, the crime type, the description of the crime, the probability of occurrence of the action happening, the severity if it did happen (high, medium, low), the type of risk (people, property, reputation, etc.), the mitigation decided upon and if the mitigation control is effective or not.

A domain is weighted relative to the influence of other domains in the framework. A dominant outcome driver, or dominant domain, should not be ignored or treated as an equal. Domain weights can be assigned using a Likert scale, or be linked to variable significance. Domain specific tasks and their weights inform the overall strategic plan. An understanding of

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 2, No. 1: 280-290, 2018
DOI: 10.33805/2576-8484.155

the dynamic nature of internal and external metrics [48], a prospect of future expectations [49], and an awareness of the weighted performance drivers on the critical path are essential to the strategic plan.

The security team and the leadership representation on the security team decided what the mitigation to deploy should be based on a cost benefit analysis. The team must also assure that the augmented control is deployed and meets expected performance levels. And, they must have a means to know if the control has fallen out of place such that it is not mitigating the threat anymore. For example, a new sign could have been placed in the field of view of a camera making it ineffective. While the threat risk may be reduced, it may not disappear. When it is still present, it should stay on the register. It may be described differently if needed. The outcome of the process was that the frequency of occurrence of a loss was reduced when the mitigations where deployed.

4.3. The Illusion of Vulnerability Mitigation Assurance

Many leaders embrace an illusion of security. For example, a facility may have 140 surveillance cameras in place. Some of these cameras may be off line, broken, dirty, not focused, with insufficient resolution, have an inability to handle luminance changes, have a poor field of view, have a blocked field of view, or be pointed in the wrong direction. When the leader is asked if they have adequate security management, the response is that there are 140 cameras covering the campus. While providing some deterrent value, having a large number of cameras does not provide the mitigating control to reduce threats as obfuscation techniques are well known. While insurance companies value camera systems, they typically do not check to see if they are effective or even capable to produce evidence for forensic analysis in the event that harm occurs. The intention is that cameras are a forensic tool to find out what happened after the crime was committed assuming the needed footage is available. In the event that the criminals do not remove the video storage device, other issues with the system may keep forensic footage from being available to law enforcement. Cameras may not handle light well, not have an appropriate field of view, go black in the dark, be out of service, flare when pointed towards sunlight, be obstructed, or be blinded by a nearby light source. The perception of security is not the same as good security. Understanding threats is the start of a mitigating design. Having a system that is able to de-escalate a threat scenario will reduce recovery losses as they may mitigate a harmful act before it happens. Consequently, a threat-based approach is not only more effective, it is also cheaper. For example, purchasing surveillance equipment to cover areas where the threat is low, or non-existent, is a waste of resources as these resources should be collecting data where the risk is higher. An example of poor light management is shown in **Figure 10** below. In this case a light was placed in the field of view of a camera.

Figure 10.
Capability challenges of video collection.

It is worth noting that often the assumption is that the building alarm system will take care of the security needs of the facility. Many bad actors have adopted shared 'best practices' (seen on YouTube, for example) that have made them successful in causing harm to facilities. For example, it is possible to cut the power in the power panel (or even at the meter) and cut the telephone or internet lines to the building eliminating communication. It is also possible to disable alarm boxes. Even if communication is not cut, thieves know the response times to get in and get out before the police arrive ('smash and dash') and jammers can be used to block wireless systems. While bad actors may only take items that will return $1000 they may cause $5000 worth of damage to achieve this. Thieves gain entry by damaging doors, however, 'bumpkeys' can be used to gain access to almost any lock without damage. Burglars may also take DVR/NVR video storage with them, removing forensic evidence from the scene. With these scenarios logged in the Risk Register, leaders become aware and may believe that their existing security controls are keeping them secure, when in fact it is not the case.

4.4. A Predictive Approach

This paper is not about the Risk Register, but rather the use of it to improve the security posture of a facility. An analysis produces no value until it is acted upon. Consequently, the scope of the discussion needs to include leadership's status quo posture and a posture that reduces the opportunity for risk-based losses and liabilities. The evolving discussion then includes the author's position on the topic, that there are four types of leaders with regard to risk management. The first is the 'head in the sand' leader. This leader does not think that anything could happen and if it does, then it was supposed to be that way. When an issue occurs, this facility will likely close down. Some workers will be afraid to come to work, and the leaders end up losing their position. The damage is done and the leader did not serve the interests of their employees. A defense that it was supposed to be adequate may be only abdication of responsibility.

The second kind of leader is the reactive leader. The emphasis here is on recovery after a loss. Typically the full value of the loss is not recovered, and so harm to the organization occurs. Even if assets lost are recovered, an amount of loss will be incurred and find its way onto the financial statements of the facility. An insurance claim is filed and the rest of the cost including the deductible is taken from the budget. This money will be used to restore the property to the extent possible over a period of time during which the brand is vulnerable. The third type of leader is a proactive leader. This leader will take action to prevent risk loss from happening. Generally, this posture works except when a threat emerges that was not considered in the risk mitigation plan. In all of these cases, human loss is tragic. The proactive leader must try to minimize losses through preparedness and enhanced controls.

The last and fourth type of leader is the predictive leader who approaches the threatscape anticipating that changes in the threatscape will happen. The best case is that this leader prepares mitigations before threats emerge. Minimally, as threats emerge or occur elsewhere, this leader thinks about mitigations immediately. The predictive leader doesn't need to recover because mitigations are anticipated and in place prior to the threat visiting the facility. The predictive leader will keep property, brand, and human loss from happening.

While all threats cannot be mitigated, leadership demands an approach that prevents losses. Threats should be known and mitigated before they have the opportunity to cause damage. The organization should anticipate the discovery of threats and be able to assume a posture quickly to thwart the threat or discourage it. In some cases, controls may also help keep risk threats from escalating as mitigating action can be executed before the severity of the threat increases. When leaders are ready to deter malicious acts, bad actors stand down.

4.5. Loss Likelihood and Impact

The ability to minimize loss by prioritizing preventive actions can be further understood through a risk threat matrix as shown in **Figure 11** below. In this case, leadership can decide on the actions to take first by looking at the likelihood of a loss and the impact of it. When the existing controls are augmented and deployed, the RPN is reduced.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 2, No. 1: 280-290, 2018
DOI: 10.33805/2576-8484.155

The risk threat matrix can be exploited by using each item on the risk register and giving it a location on a heat map and a relative area. A heat map is a visual representation of data using colors with associated values. The threatscape is essentially a heat map that shows which threats are critical and which ones are relatively insignificant. A severe impact along with an almost certain likelihood is the largest risk-loss threat. In this case, it is armed robbery. Robberies are common, and when armed, bad actors can injure or kill people who are in the facility during the robbery. Other events are also severe, such as a terroristic shooting, however, this act is not as common an occurrence as an armed robbery. The relative values of the threat type can be validated through a quantitative survey or through local crime statistics.

Risk Register			Initial Values		
Number	Event type	Description	Impact	Likelihood	Speed of Onset
1.1	Burglary	Instruments	4	9	7
1.2	Burglary	Cash	4	9	7
1.3	Burglary	Computers	4	9	8
1.4	Burglary	Sound Boards	4	8	7
1.5	Burglary	Copper	6	8	8
2.1	Assault	Active shooter	10	1	10
2.2	Assault	Armed robber	10	9	10
2.3	Assault	Fight	4	3	7
3.1	Injury	Fall	4	6	10
4.1	Terrorism	Vehicle ram	10	1	10
4.2	Terrorism	Shooting	10	3	10
5.1	Sexual assault	Bathrooms	9	7	6
5.2	Sexual assault	Sport Court	9	5	5
6.1	Abduction	Nursery pickup	10	6	8
6.2	Abduction	Parking lot	10	7	9
7.1	Fire	Arson	6	7	5
7.2	Fire	Homeless	6	7	5
8.1	Vandalism	Graffiti	4	7	4
9.1	Animal	Animal bite	6	9	4
10.1	Nat. Disaster	Earthquake	9	4	10
10.2	Nat. Disaster	Fire	7	5	4
			7.0	6.2	7.3

Figure 11.
Values for the risk threat matrix.

The area that represents each threat index relates to the speed of onset. The speed at which the threat is enacted is critical from a reaction time perspective. With a rapid speed of onset, the ability to mitigate the loss and de-escalate the event after the act has been initiated is very low. Consequently, the losses will be higher when this threat is enacted as illustrated in the **Figure 12** below. The values reflected by the risk loss matrix are set by the local security team and may be agreed to by leadership

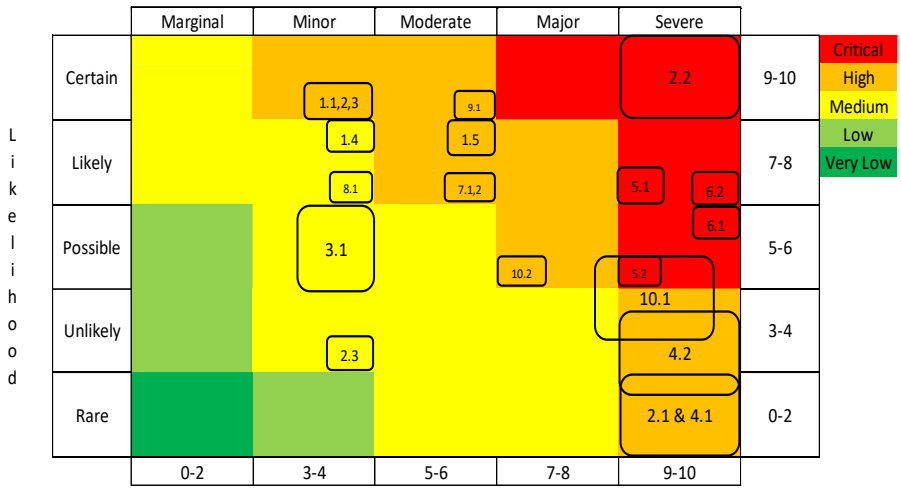

Figure 12.
Risk loss matrix heat map.

The risk loss matrix above is the current state prior to augmented controls. The impact of more powerful controls will reduce the speed of onset (the box size around the number) while shifting the location of the box in the heat map from redder to greener. In other words, the box around the number will shrink as the enhanced control increases the time of onset. The number and its shrinking box will move towards the left as the augmented control reduces the impact of an exploited vulnerability. And, the number with its box will move downwards as the likelihood of the exploited vulnerability occurring is reduced. A reduction in the RPN ultimately indicates the management of the threatscape and the reduction in vulnerability at the facility. The movement of risk threats making them less likely, less impactful, and having a longer onset time takes fo

cused ongoing leadership within the organization. Having the right leadership for change activities is critical [50-53]. An effective leader needs to be an articulate and enthusiastic conceptualizer who is good at grasping strategies and explaining them [50]. Leadership includes prioritization, deployment, and measurement against established goals.

If outcome measurements indicate that effort has fallen short of a target, a leader may initiate a limited improvement cycle as a remediation. Additionally, a framework review may be prudent due to project duration and environmental turbulence. A framework conceived during a time of stability may not be applicable during, or following, a time of volatility [10].

Once the framework design has been fine-tuned and verified as being appropriate by the facility security team, an accountable leader should initiate a repeat scan to refresh the gap analysis data. Continuous improvement is an aggressive leadership activity allowing an organization that embraces learning to keep pace with a rapidly evolving environment [54, 55].

4.6. Multi-Site Scaling

With a single facility having achieved a strong or mature posture, the controls adopted by the facility can now be leveraged for other facilities. The table below shows how this can be accomplished. Along the column headings are the list of facilities and a column that relates to the cost of each control item. Each site may have different control requirements.

These requirements are listed on the rows and are grouped into three classes. A facility that handles high value assets and needs strong controls would need to achieve compliance with regard to all three control categories. Other facilities that handle lower value assets may only have to achieve the first category. Under each site column a simple 'Y' or 'N' can be used to

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 2, No. 1: 280-290, 2018
DOI: 10.33805/2576-8484.155

indicate if the control is in place. If it is not, the cost to achieve the control can be listed. This allows leadership to know why the achievement of the control would cost. The overall cost of compliance is then added up at the bottom of the column as shown in **Figure 13** below.

Compliance Status by Site

		Site 1	Cost	Site 2	Cost	Site 3	Cost	Site 4	Cost	Site 5	Cost	Site 6	Cost	Site 7	Cost	Site 8	Cost	...	Cost	Site N	Cost
Class 1	Control 1	N	$ 7,009	Y		N	$ 11,878	N	$ 9,072	N	$ 12,119	N	$ 9,987	N	$ 12,236	N	$ 10,580			N	$ 6,887
	Control 2	N	$ 7,842	N	$ 6,290	N	$ 7,185	N	$ 14,099	N	$ 5,028	N	$ 9,689	N	$ 13,389	N	$ 14,390			N	$ 11,232
	Control 3	N	$ 10	N	$ 14,401	N	$ 5,619	N	$ 13,966	N	$ 7	N	$ 11	N	$ 13,397	N	$ 5,992			N	$ 13,762
	Control 4	N	$ 5,985	N	$ 12,838	N	$ 11,923	Y		N	$ 12,258	N	$ 5,490	N	$ 5,530	N	$ 5,493			N	$ 11
	Control 5	N	$ 12,213	N	$ 9,152	N	$ 6,244	N	$ 13,355	N	$ 6,460	N	$ 11,762	Y		Y				N	$ 14,968
	Control 6	N	$ 6,347	N	$ 12,930	Y		N	$ 13,231	N	$ 6,341	N	$ 9,374	N	$ 13,765	N	$ 9,899			N	$ 11,432
	Control 7	N	$ 8,912	N	$ 9,701	N	$ 62	N	$ 5,305	N	$ 9,850	N	$ 10,041	Y		N	$ 7			N	$ 14,312
	Control 8	Y		N	$ 14,998	N	$ 6,771	N	$ 8	N	$ 62	N	$ 5,871	N	$ 5,906	N	$ 9,904			N	$ 12,104
	Control 9	N	$ 6,819	Y		N	$ 8,281	N	$ 5,374	N	$ 9,852	N	$ 13,573	N	$ 5,741	N	$ 11,220			N	$ 5,055
	Control 10	Y		Y		N	$ 8,319	N	$ 7,786	N	$ 7,548	N	$ 6,512	N	$ 11,069	N	$ 11,296			N	$ 11,844
	Compliance %	20%		30%		10%		10%		0%		0%		20%		10%				0%	
	Cost of Compliance		$ 55,137		$ 80,310		$ 66,282		$ 82,196		$ 69,525		$ 82,310		$ 81,033		$ 78,781				########
Class 3	Control 21	N	$ 12,744	N	$ 6,028	N	$ 8,661	Y		Y		N	$ 13,412	Y		N	$ 8,859			Y	
	Control 22	N	$ 10,888	Y		Y		Y		Y		N	$ 7,963	N	$ 14,284	N	$ 8,427			N	$ 11,338
	Control 23	Y		Y		Y		Y		N	$ 6,504	Y		Y		Y				N	$ 13,078
	Control 24	Y		N	$ 14,999	N	$ 13,550	N	$ 5,487	N	$ 9,719	Y		N	$ 10,314	Y				Y	
	Control 25	Y		Y		N	$ 11,041	N	$ 6,618	Y		N	$ 8,243	Y		Y				Y	
	Control 26	Y		N	$ 6,478	N	$ 7,357	Y		Y		N	$ 10,932	Y		N	$ 9,635			N	$ 14,306
	Control 27	N	$ 7,979	Y		Y		Y		Y		Y		N	$ 6,511	Y				Y	
	Control 28	N	$ 10,189	Y		Y		Y		N	$ 11,873	Y		Y		Y				N	$ 7,641
	Control 29	Y		Y		Y		N	$ 13,779	N	$ 11,339	Y		N	$ 9,674	N	$ 6,250			N	$ 10,981
	Control 30	Y		Y		Y		N	$ 8,314	N	$ 13,373	Y		N	$ 7,058	N	$ 12,994			Y	
	Compliance %	60%		70%		60%		60%		50%		60%		50%		50%				50%	
	Cost of Compliance		$ 41,800		$ 27,505		$ 40,609		$ 34,198		$ 52,808		$ 40,550		$ 47,841		$ 46,165				$ 57,344
Class 5	Control 41	Y		Y		Y		Y		Y		Y		Y		Y				Y	
	Control 42	Y		Y		Y		Y		Y		Y		Y		Y				Y	
	Control 43	N	$ 6,690	Y		Y		Y		Y		Y		Y		Y				Y	
	Control 44	Y		Y		Y		Y		Y		Y		Y		Y				Y	
	Control 45	Y		Y		Y		Y		Y		Y		Y		Y				Y	
	Control 46	Y		Y		Y		Y		Y		Y		Y		Y				Y	
	Control 47	Y		Y		Y		Y		Y		Y		Y		Y				Y	
	Control 48	Y		Y		Y		Y		Y		Y		Y		Y				Y	
	Control 49	Y		Y		Y		Y		Y		Y		Y		Y				Y	
	Control 50	Y		Y		Y		Y		Y		Y		Y		Y				Y	
	Compliance %	90%		100%		100%		100%		100%		100%		100%		100%				100%	
	Cost of Compliance		$ 6,690		$ -		$ -		$ -		$ -		$ -		$ -		$ -				$ -

Figure 13.
Control assessment and costs.

This table can then be combined with the individual facility Risk Register that indicates the Risk Priority Number for the facility in relation to the threat vectors. This new RPN is what would be expected with the control listed in place.

With this construct a leader can know the impact of the investment in the controls in the facility. This section will also show the impact of the investment across all facilities. With these tools in place, leadership can decide how to invest in the vulnerability mitigation posture of all facilities in the global supply chain as shown in **Figure 14**.

Compliance Status by Site

		Site 1	Cost	Site 2	Cost	Site 3	Cost	Site 4	Cost	Site 5	Cost	Site 6	Cost	Site 7	Cost	Site 8	Cost	...	Cost	Site N	Cost
Class 1	Control 1	N	$ 10,516	Y		N	$ 8,779	N	$ 12,461	N	$ 10,493	N	$ 5,537	N	$ 10,670	N	$ 12,757			N	$ 8,912
	Control 2	N	$ 8,346	N	$ 14,512	N	$ 9,032	N	$ 9,069	N	$ 11,506	N	$ 7,157	N	$ 14,540	N	$ 14,572			N	$ 8,182
	Control 3	N	$ 10	N	$ 5,267	N	$ 10,948	N	$ 10,791	N	$ 7	N	$ 11	N	$ 10,300	N	$ 8,215			N	$ 10,027
	Control 4	N	$ 9,827	N	$ 9,105	N	$ 11,673	Y		N	$ 14,641	N	$ 7,600	N	$ 11,549	N	$ 12,581			N	$ 11
	Control 5	N	$ 8,646	N	$ 13,905	N	$ 14,787	N	$ 10,037	N	$ 6,734	N	$ 9,718	Y		Y				N	$ 6,620
	Control 6	N	$ 5,169	N	$ 11,680	Y		N	$ 14,365	N	$ 6,437	N	$ 10,800	N	$ 8,691	N	$ 14,931			N	$ 11,000
	Control 7	N	$ 7,410	N	$ 9,854	N	$ 62	N	$ 10,100	N	$ 13,692	N	$ 10,029	Y		N	$ 7			N	$ 14,171
	Control 8	Y		N	$ 14,617	N	$ 14,988	N	$ 8	N	$ 62	N	$ 11,638	N	$ 14,206	N	$ 6,418			N	$ 5,849
	Control 9	N	$ 14,932	Y		N	$ 10,925	N	$ 8,129	N	$ 11,113	N	$ 8,127	N	$ 10,202	N	$ 12,901			N	$ 13,160
	Control 10	Y		Y		N	$ 12,254	N	$ 12,971	N	$ 10,760	N	$ 8,980	N	$ 13,736	N	$ 10,204			N	$ 5,906
	Compliance %	20%		30%		10%		10%		0%		0%		20%		10%				0%	
	Cost of Compliance		$ 64,856		$ 78,940		$ 93,448		$ 87,931		$ 85,445		$ 79,597		$ 93,894		$ 92,586				$ 83,838
Class 3	Control 21	N	$ 14,288	N	$ 6,696	N	$ 10,330	Y		Y		N	$ 13,928	Y		N	$ 7,638			Y	
	Control 22	N	$ 11,529	Y		Y		Y		Y		N	$ 14,881	N	$ 13,141	N	$ 14,896			N	$ 8,442
	Control 23	Y		Y		Y		Y		N	$ 11,637	Y		Y		Y				N	$ 6,139
	Control 24	Y		N	$ 7,230	N	$ 12,327	N	$ 7,925	N	$ 8,093	Y		N	$ 5,316	Y				Y	
	Control 25	Y		Y		N	$ 6,789	N	$ 12,052	Y		N	$ 9,743	Y		Y				Y	
	Control 26	Y		N	$ 10,891	N	$ 7,139	Y		Y		N	$ 7,430	Y		N	$ 12,153			N	$ 12,236
	Control 27	N	$ 13,628	Y		Y		Y		Y		Y		N	$ 6,572	Y				Y	
	Control 28	N	$ 14,505	Y		Y		Y		N	$ 12,664	Y		Y		Y				N	$ 14,444
	Control 29	Y		Y		Y		N	$ 11,815	N	$ 10,323	Y		N	$ 10,705	N	$ 8,158			N	$ 5,966
	Control 30	Y		Y		Y		N	$ 7,188	N	$ 14,348	Y		N	$ 11,023	N	$ 10,147			Y	
	Compliance %	60%		70%		60%		60%		50%		60%		50%		50%				50%	
	Cost of Compliance		$ 53,950		$ 24,817		$ 36,585		$ 38,980		$ 57,065		$ 45,982		$ 46,757		$ 52,992				$ 47,227
Class 5	Control 41	Y		Y		Y		Y		Y		Y		Y		Y				Y	
	Control 42	Y		Y		Y		Y		Y		Y		Y		Y				Y	
	Control 43	N	$ 10,709	Y		Y		Y		Y		Y		Y		Y				Y	
	Control 44	Y		Y		Y		Y		Y		Y		Y		Y				Y	
	Control 45	Y		Y		Y		Y		Y		Y		Y		Y				Y	
	Control 46	Y		Y		Y		Y		Y		Y		Y		Y				Y	
	Control 47	Y		Y		Y		Y		Y		Y		Y		Y				Y	
	Control 48	Y		Y		Y		Y		Y		Y		Y		Y				Y	
	Control 49	Y		Y		Y		Y		Y		Y		Y		Y				Y	
	Control 50	Y		Y		Y		Y		Y		Y		Y		Y				Y	
	Compliance %	90%		100%		100%		100%		100%		100%		100%		100%				100%	
	Cost of Compliance		$ 10,709		$ -		$ -		$ -		$ -		$ -		$ -		$ -				$ -

Number	Event Type	Description	RPN	PRPN	RPN	PRPN	RPN	PRPN	RPN	PRPN	RPN	PRPN	RPN	PRPN	RPN	PRPN	RPN	PRPN	RPN	PRPN	RPN	PRPN
1.1	Burglary	Instruments	40	5	29	6	31	21	17	14	30	30	48	26	32	18	37	29	15	19	41	29
1.2	Burglary	Cash	40	5	41	31	49	18	23	12	25	14	26	21	40	8	28	24	32	12	15	20
1.3	Burglary	Computers	40	5	32	14	21	32	28	29	17	29	47	15	24	6	40	11	21	29	42	21
1.4	Burglary	Servers	40	5	17	32	28	18	21	16	41	17	26	27	45	21	31	25	49	11	33	32
1.5	Burglary	Copper	40	5	23	14	48	18	23	28	42	27	48	12	47	31	48	22	40	21	50	22
2.1	Assault	Active shooter	24	16	36	8	16	8	38	26	40	11	49	23	50	28	50	17	41	6	29	12
2.2	Assault	Armed robber	24	8	46	18	32	22	28	21	23	27	25	21	36	21	40	28	32	18	27	22
2.3	Assault	Fight	15	6	31	16	16	28	28	12	46	27	33	14	17	9	31	14	20	17	26	7
3.1	Injury	Fall	25	15	17	21	21	18	49	6	15	15	43	19	45	8	29	14	49	30	45	27
4.1	Terrorism	Vehicle ram	24	21	28	6	46	28	29	21	20	28	49	6	42	8	25	32	15	32	33	8
4.2	Terrorism	Shooting	24	8	46	26	32	20	44	23	34	14	48	24	43	11	46	13	37	14	16	16
5.1	Sexual assault	Bathrooms	25	0	32	9	39	9	32	10	38	12	39	28	23	16	17	9	22	9	23	31
5.2	Sexual assault	Outside	25	10	30	27	49	6	24	31	22	26	39	25	27	8	37	24	22	11	49	32
6.1	Abduction	Customer	24	0	28	7	48	24	46	18	20	19	28	9	32	21	47	6	38	19	47	32
6.2	Abduction	Employee	24	16	31	22	45	7	22	27	19	22	36	8	22	16	18	21	41	7	41	17
7.1	Fire	Arson	24	9	50	8	22	19	49	20	49	18	42	17	16	13	47	11	31	11	48	10
7.2	Fire	Homeless	24	0	17	23	19	15	23	7	28	11	26	7	29	19	15	20	41	13	26	32
8.1	Vandalism	Graffiti	15	3	23	19	42	13	33	27	35	14	44	24	40	14	31	6	26	31	27	7
9.1	Animal	Animal bite	40	10	40	17	25	13	39	13	22	16	16	7	45	13	34	23	17	17	16	15
10.1	Nat. Disaster	Earthquake	40	15	35	8	47	8	45	19	15	10	22	17	20	23	18	30	22	14	48	28
10.2	Nat. Disaster	Fire	40	6	46	11	43	18	50	18	19	7	50	22	47	29	35	7	38	19	16	7
		Total RPN	417	143	536	246	542	256	579	299	445	277	589	271	534	257	520	275	492	268	517	303
		dRPN		274		290		286		280		168		318		277		245		224		214
		dRPN%		65.7%		54.1%		52.8%		48.4%		37.8%		54.0%		51.9%		47.1%		45.5%		41.4%
		GTRPN		5171																		
		GTdRPN		2576																		
		GTdRPN%		49.8%																		

Figure 14.
Linking the RPN to costs related to facility vulnerability mitigations.

5. Conclusion

Clarity around strategic planning is needed for better organizational outcomes. Through collective sharing, predictive learning, and reflection, leaders can enhance their ES techniques by using meaningful tools. Quick wisdom generation is needed in a fast-paced environment; however, sometimes these efforts to collect information are hampered by constraints imposed by internal and external sources. For example, the availability of critical information may be a challenge for a decision maker due to a lack of an organizational intelligence gathering capability or from an incomplete awareness of legal constraints. By increasing the 'speed to wisdom', strategic enactment potential is heightened and a more secure posture is achieved. Practically, an information collection capability coupled with an adaptive culture can be helpful in turning wisdom into action, as long as data is collected and recorded accurately, and can be extracted in a meaningful format [6, 56].

Strategic agility enables an organization to achieve desired outcomes [57, 58] while sustaining organizational success [10]. Potentially strategic agility can be expressed in an algorithm as follows:

Strategic Agility = ES Accuracy x Agility x Adaptability

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 2, No. 1: 280-290, 2018
DOI: 10.33805/2576-8484.155

To elaborate, Scanning Accuracy is simply the capability to obtain and exploit knowledge of an organization's situation in its environment; current and future. Agility is the ability to minimize the negative influence of obstacles on momentum needed for adaptation. Adaptability is an organization's ability to transform itself to stay ahead of threats, thereby preserving or increasing the organizations viability and efficacy [21].

In some cases, strategic planning is ad hoc with a dependency on serendipity that may or may not be forthcoming [12, 13, 15]. Alternatively, some organizations see value in planning and execution [59]. Organizations that plan may underestimate the complexity that exists between the environment and aspect of the organization. Even a mature organization may not appropriately understand or leverage the links between domains that can improve outcome potential. For example, a control to mitigate vulnerability in one area may have a positive or negative impact in another. To understand this better, a confident organization, inviting of criticism, may allow their concerned employees, department leaders, and members of the security team to influence their framework design, its weighting, and the metrics that are being applied to have a better understanding of the complex and dynamic environment [11].

Task selection within a threat domain directly impacts domain specific goal achievement [60]. These tasks are aligned with goals imposed on a situation. Ambiguity, uncertainty, and an understanding of residual risk in a system are critical aspects of environments in transition [53, 61]. Specifically, Perceived Environmental Uncertainty (PEU) is the difference between information needed to make a decision about a task and information available [62]. PEU tends to mask composite measures sought after during scanning activities [63] that drive task creation. Concurrently, leaders tend to act on a perceived environment [64] with a goal of achieving a desired adaptation to a more secure posture [14, 21]. Task leaders must also know that environmental variation relates to changes that may occur independent of a leaders' ability to notice, comprehend, or interpret environment related data [65]. Consequently, organizations tuned into their environment, while allowing for discovery, are more likely to succeed because they are able to respond predictively through meaningful action and contingencies to a wide range of signals [66]. Leaders must understand that the security locus of control includes those who attend the facility and those who live or work nearby.

When direct (employees) and indirect (neighbors of the facility) stakeholders know that a strategic plan is thorough, and when they are given opportunities to influence the plan [49], they are more inclined to be cooperative and in alignment with the objectives. Engaged stakeholders are also more likely to follow a meaningful path laid out for the organization, even if sacrifice is involved [11]. Even so, it is better to achieve a goal through strategy than through sacrifice. Although complexity is intensified with the diversity that exists within stakeholder population, methods discussed in this article aid in efficient and timely ongoing accomplishment of organizational postural transitions necessary in turbulent and evolving risk environments [12, 15, 67-70].

6. Implications and Limitations

This article attempted to provide theoretical models for the listing and assessment of threats, along with the power of the mitigating controls currently in place. The model also allows for improvement on the threatscape through quantitative control augmentation. While each situation is different, this case study shows that the opportunity to exploit vulnerabilities can be reduced significantly using the tools presented. Clearly, more research is needed to enable facilities, and other similar organizations, to rapidly evolve their threat governance capabilities so that risk-based loss is averted. As threats continue to evolve, rigidity of approach by facility leaders puts lives and property at risk. Conversely, predictive leaders, through the use of suitable ES tools can reduce risk loss through posture adaptations.

This article is based on a facility-based global supply chain case study that can be considered as informational to other locations. Some limitations on generalizability exist as all locations are not the same, however, the general structure can be applied in a multi-site organization. Even though many facilities are unique, the tools presented are transferrable and with minor modifications could be practically used. While some leaders in facilities are taking significant measures to protect their employees, many others believe that the risks they could incur are tolerable. Some of this risk comes from threat sources, while other sources are risks associated with a lack of compliance with policy. To understand this better, leaders must understand what the threats are, how well they are being mitigated, and have an interest to mitigate the residual risk that exists. The residual risk is the type and magnitude of the threat that has not yet been addressed. This risk continues to be carried by the leadership of the facility and should be known to them.

References

[1] S. Solis, *Ringling Bros. Circus closing after 146 years*. USA, 2017.

[2] A. Cuervo-Cazurra, L. Ciravegna, M. Melgarejo, and L. Lopez, "Home country uncertainty and the internationalization-performance relationship: Building an uncertainty management capability," *Journal of World Business*, vol. 53, no. 2, pp. 209-221, 2018. https://doi.org/10.1016/j.jwb.2017.11.002

[3] J. Müllner, "From uncertainty to risk—A risk management framework for market entry," *Journal of World Business*, vol. 51, no. 5, pp. 800-814, 2016. https://doi.org/10.1016/j.jwb.2016.07.011

[4] R. Baker, H. Anderson, S. Bishop, A. MacLeod, N. Parkinson, and M. Tuffen, "The UK Plant Health Risk Register: A tool for prioritizing actions," *EPPO Bulletin*, vol. 44, no. 2, pp. 187-194, 2014. https://doi.org/10.1111/epp.12130

[5] F. D. Patterson and K. Neailey, "A risk register database system to aid the management of project risk," *International Journal of Project Management*, vol. 20, no. 5, pp. 365-374, 2002. https://doi.org/10.1016/s0263-7863(01)00040-0

[6] V. Choudhury and J. L. Sampler, "Information specificity and environmental scanning: An economic perspective," *MIS Quarterly*, pp. 25-53, 1997. https://doi.org/10.2307/249741

[7] W. M. Cohen and D. A. Levinthal, "Absorptive capacity: A new perspective on learning and innovation," *Administrative Science Quarterly*, pp. 128-152, 1990. https://doi.org/10.2307/2393553

[8] J. R. Hough and M. A. White, "Scanning actions and environmental dynamism: Gathering information for strategic decision making," *Management Decision*, vol. 42, no. 6, pp. 781-793, 2004. https://doi.org/10.1108/00251740410542348

[9] R. C. May, W. H. Stewart Jr, and R. Sweo, "Environmental scanning behavior in a transitional economy: Evidence from Russia," *Academy of Management Journal*, vol. 43, no. 3, pp. 403-427, 2000. https://doi.org/10.5465/1556402

[10] R. A. D'Aveni, G. B. Dagnino, and K. G. Smith, "The age of temporary advantage," *Strategic Management Journal*, vol. 31, no. 13, pp. 1371-1385, 2010. https://doi.org/10.1002/smj.897

[11] M. De Pree, *Leadership is an art*. New York, USA: Random House, 2004.

[12] F. Aguilar, *Scanning the business environment*. New York: Macmillan Co, 1967.

[13] D. Hambrick, "Environmental scanning, organizational strategy, and executive roles: A study in three industries," Unpublished Doctoral Dissertation, Pennsylvania State University, Pennsylvania, 1979.

[14] D. C. Hambrick, "Specialization of environmental scanning activities among upper level executives," *Journal of Management Studies*, vol. 18, no. 3, pp. 299-320, 1981. https://doi.org/10.1111/j.1467-6486.1981.tb00104.x

[15] A. Kefalas and P. Schoderbek, "Scanning the business environment: Some empirical results," *Decision Sciences* vol. 4, pp. 63-67, 1973.

[16] D. S. Elenkov, "Strategic uncertainty and environmental scanning: The case for institutional influences on scanning behavior," *Strategic Management Journal*, vol. 18, no. 4, pp. 287-302, 1997. https://doi.org/10.1002/(sici)1097-0266(199704)18:4%3C287::aid-smj865%3E3.0.co;2-b

[17] G. Jogaratnam and K. K. Wong, "Environmental uncertainty and scanning behavior: An assessment of top-level hotel executives," *International Journal of Hospitality & Tourism Administration*, vol. 10, no. 1, pp. 44-67, 2009. https://doi.org/10.1080/15256480802557275

[18] L. G. Hrebiniak and W. F. Joyce, "Organizational adaptation: Strategic choice and environmental determinism," *Administrative Science Quarterly*, vol. 30, no. 3, pp. 336-49, 1985. https://doi.org/10.2307/2392666

[19] W. M.-H. Tsai, I. C. MacMillan, and M. B. Low, "Effects of strategy and environment on corporate venture success in industrial markets," *Journal of Business Venturing*, vol. 6, no. 1, pp. 9-28, 1991. https://doi.org/10.1016/0883-9026(91)90003-v

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 2, No. 1: 280-290, 2018
DOI: 10.33805/2576-8484.155

[20] M. A. Carpenter and J. W. Fredrickson, "Top management teams, global strategic posture, and the moderating role of uncertainty," *Academy of Management Journal*, vol. 44, no. 3, pp. 533-545, 2001. https://doi.org/10.5465/3069368

[21] S. Davis and C. Meyer, *Blur: The speed of change in a connected economy*. New York, USA: Warner Books, 1998.

[22] L. J. Bourgeois III, "Strategic goals, perceived uncertainty, and economic performance in volatile environments," *Academy of Management Journal*, vol. 28, no. 3, pp. 548-573, 1985. https://doi.org/10.5465/256113

[23] R. M. Beal, "Competing effectively: Environmental scanning, competitive strategy, and organizational performance in small manufacturing firms," *Journal of Small Business Management*, vol. 38, no. 1, pp. 27-47, 2000.

[24] M. Yasai-Ardekani and P. C. Nystrom, "Designs for environmental scanning systems: Tests of a contingency theory," *Management Science*, vol. 42, no. 2, pp. 187-204, 1996. https://doi.org/10.1287/mnsc.42.2.187

[25] D. F. Jennings and J. R. Lumpkin, "Insights between environmental scanning activities and Porter's generic strategies: An empirical analysis," *Journal of Management*, vol. 18, no. 4, pp. 791-803, 1992. https://doi.org/10.1177/014920639201800411

[26] B. Czarniawska, "Complex organizations still complex," *International Public Management Journal*, vol. 10, no. 2, pp. 137-151, 2007. https://doi.org/10.1080/10967490701323662

[27] R. Duncan, "Characteristics of organizational environments and perceived environmental uncertainty," *Administrative Science Quarterly*, vol. 17, pp. 313-327, 1972. https://doi.org/10.2307/2392145

[28] J. E. Dutton and S. E. Jackson, "Categorizing strategic issues: Links to organizational action," *Academy of Management Review*, vol. 12, no. 1, pp. 76-90, 1987. https://doi.org/10.5465/amr.1987.4306483

[29] B. P. Ebrahimi, "Environmental complexity, importance, variability and scanning behavior of Hong Kong executives," *International Business Review*, vol. 9, no. 2, pp. 253-270, 2000. https://doi.org/10.1016/s0969-5931(99)00039-6

[30] J. Thompson, *Organizations in action*. New York, USA: McGraw-Hill, 1967.

[31] P. Anderson and M. L. Tushman, "Organizational environments and industry exit: The effects of uncertainty, munificence and complexity," *Industrial and Corporate Change*, vol. 10, no. 3, pp. 675-711, 2001. https://doi.org/10.1093/icc/10.3.675

[32] L. Fahey and V. K. Narayanan, *Macroenvironmental analysis for strategic management (The west series in strategic management)*. St. Paul, Minnesota: West Publishing Company, 1986.

[33] I. Goll and A. M. Rasheed, "Rational decision-making and firm performance: The moderating role of the environment," *Strategic Management Journal*, vol. 18, no. 7, pp. 583-591, 1997. https://doi.org/10.1002/(sici)1097-0266(199708)18:7%3C583::aid-smj907%3E3.0.co;2-z

[34] N. Snyder, "Environmental volatility, scanning intensity, and organizational performance," *Journal of Contemporary Business*, vol. 10, pp. 5-17, 1981.

[35] S. A. Zahra, "Corporate strategic type, environmental perceptions, managerial philosophies, and goals: an empirical study," *Akron Business and Economic Review*, vol. 18, no. 2, pp. 64-77, 1987.

[36] K. M. Sutcliffe, "What executives notice: Accurate perceptions in top management teams," *Academy of Management Journal*, vol. 37, no. 5, pp. 1360-1378, 1994. https://doi.org/10.5465/256677

[37] R. Y. Lau, S. S. Liao, K. Wong, and D. K. Chiu, "Web 2.0 environmental scanning and adaptive decision support for business mergers and acquisitions," *MIS Quarterly*, vol. 36, no. 4, pp. 1239-1268, 2012. https://doi.org/10.2307/41703506

[38] W. J. Ferrier, K. G. Smith, and C. M. Grimm, "The role of competitive action in market share erosion and industry dethronement: A study of industry leaders and challengers," *Academy of Management Journal*, vol. 42, no. 4, pp. 372-388, 1999. https://doi.org/10.5465/257009

[39] F. J. Milliken, "Three types of perceived uncertainty about the environment: State, effect, and response uncertainty," *Academy of Management Review*, vol. 12, no. 1, pp. 133-143, 1987. https://doi.org/10.5465/amr.1987.4306502

[40] R. L. Daft, J. Sormunen, and D. Parks, "Chief executive scanning, environmental characteristics, and company performance: An empirical study," *Strategic Management Journal*, vol. 9, no. 2, pp. 123-139, 1988. https://doi.org/10.1002/smj.4250090204

[41] N. Venkatraman, "The concept of fit in strategy research: Toward verbal and statistical correspondence," *Academy of Management Review*, vol. 14, no. 3, pp. 423-444, 1989. https://doi.org/10.5465/amr.1989.4279078

[42] W. M. Lindsay and L. W. Rue, "Impact of the organization environment on the long-range planning process: A contingency view," *Academy of Management Journal*, vol. 23, no. 3, pp. 385-404, 1980. https://doi.org/10.5465/255507

[43] R. B. Robinson Jr, "The importance of "outsiders" in small firm strategic planning," *Academy of Management Journal*, vol. 25, no. 1, pp. 80-93, 1982. https://doi.org/10.5465/256025

[44] M. Valencia, *The gods strike Back: A special report on financial Risk*. Economist Newspaper, 2010.

[45] I. I. Mitroff and J. R. Emshoff, "On strategic assumption-making: A dialectical approach to policy and planning," *Academy of Management Review*, vol. 4, no. 1, pp. 1-12, 1979. https://doi.org/10.5465/amr.1979.4289165

[46] S. Isaac and W. Michael, *Handbook in research and evaluation educational and industrial testing services*, 3rd ed. San Diego, California, 1997.

[47] T. Driouchi and D. Bennett, "Real options in multinational decision-making: Managerial awareness and risk implications," *Journal of World Business*, vol. 46, no. 2, pp. 205-219, 2011. https://doi.org/10.1016/j.jwb.2010.05.007

[48] N. M. Bandy, "Setting service standards: A structured approach to delivering outstanding customer service for the facility manager," *Journal of Facilities Management*, vol. 1, no. 4, pp. 322-336, 2002. https://doi.org/10.1108/14725960310808033

[49] D. Chrusciel, "Environmental scan: Influence on strategic direction," *Journal of Facilities Management*, vol. 9, no. 1, pp. 7-15, 2011. https://doi.org/10.1108/14725961111105691

[50] L. Bossidy and R. Charan, *Execution, the discipline of getting things done*. New York, USA: Crown Business, 2002.

[51] R. Heifetz, *Leadership without easy answers*. Cambridge, MA, US: Harvard University Press, 1994.

[52] K. G. Smith, W. J. Ferrier, and C. M. Grimm, "King of the hill: Dethroning the industry leader," *Academy of Management Perspectives*, vol. 15, no. 2, pp. 59-70, 2001. https://doi.org/10.5465/ame.2001.4614896

[53] D. Wilkinson, *The ambiguity advantage: What great leaders are great at*. London, UK: Palgrave Macmillan, 2006.

[54] H. Mintzberg, B. Ahlstrand, and J. Lampel, *Strategy safari: A guided tour through the wilds of strategic management*. New York, USA: Free Press, 1998.

[55] W. J. Ferrier, "Navigating the competitive landscape: The drivers and consequences of competitive aggressiveness," *Academy of management journal*, vol. 44, no. 4, pp. 858-877, 2001.

[56] G. Davis, *Management information systems: Conceptual foundations, structure, and development*. New York, USA: McGraw-Hill, 1985.

[57] D. Sull, "Competing through organizational agility," *The McKinsey Quarterly*, vol. 1, pp. 48-57, 2010.

[58] N. D. Barnard *et al.*, "Dietary and lifestyle guidelines for the prevention of Alzheimer's disease," *Neurobiology of aging*, vol. 35, pp. S74-S78, 2014.

[59] O. M. Welch, "Interrogating our practice: Enacting a" yes and" CPED agenda at Duquesne University," *Planning and Changing*, vol. 44, no. 3/4, p. 149, 2013.

[60] L. J. Bourgeois III, "Strategy and environment: A conceptual integration," *Academy of Management Review*, vol. 5, no. 1, pp. 25-39, 1980. https://doi.org/10.5465/amr.1980.4288844

[61] R. L. Daft and K. E. Weick, "Toward a model of organizations as interpretation systems," *Academy of Management Review*, vol. 9, no. 2, pp. 284-295, 1984. https://doi.org/10.5465/amr.1984.4277657

[62] J. Galbraith, *Designing complex organizations*. Reading, MA, US: Addison-Wesley, 1973.

[63] B. K. Boyd and J. Fulk, "Executive scanning and perceived uncertainty: A multidimensional model," *Journal of Management*, vol. 22, no. 1, pp. 1-21, 1996. https://doi.org/10.1177/014920639602200101

[64] B. K. Boyd, G. G. Dess, and A. M. Rasheed, "Divergence between archival and perceptual measures of the environment: Causes and consequences," *Academy of Management Review*, vol. 18, no. 2, pp. 204-226, 1993. https://doi.org/10.5465/amr.1993.3997514

[65] D. H. Doty, M. Bhattacharya, K. K. Wheatley, and K. M. Sutcliffe, "Divergence between informant and archival measures of the environment: Real differences, artifact, or perceptual error?," *Journal of Business Research*, vol. 59, no. 2, pp. 268-277, 2006. https://doi.org/10.1016/j.jbusres.2005.04.005

[66] R. A. Slaughter, "A new framework for environmental scanning," *Foresight*, vol. 1, no. 5, pp. 441-451, 1999. https://doi.org/10.1108/14636689910802331

[67] A. Buchholtz and D. Kidder, "Integrating agency and stewardship theories: The moderating role of the environment and time," presented at the Academy of Management, Chicago, IL, 1999.

[68] C. W. Choo, "The art of scanning the environment," *Bulletin of the American Society for Information Science*, vol. 25, no. 3, pp. 21-24, 1999.

[69] O. A. EI Sawy, "Personal information systems for strategic scanning in turbulent environments: Can the CEO go on-line?," *MIS Quarterly*, vol. 9, no. 1, pp. 53-60, 1985. https://doi.org/10.2307/249273

[70] T. McEwen, "Environmental scanning and organizational learning in entrepreneurial ventures," *The Entrepreneurial Executive* vol. 13, pp. 1-16, 2008.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 2, No. 1: 280-290, 2018
DOI: 10.33805/2576-8484.155