Guidepost

www.guidepostsolutions.com

"PREDICTIVE INTELLIGENCE AND INTELLIGENCE FUSION – MOVING FROM THE DEMO TO REALITY"

Create a compelling vision, build a solid business case and transform your security department from a cost center to a value center.

September 2016

WHITE PAPER

Table of Contents

Executive Summary

Today's threat environment is evolving at an alarming rate. Global and domestic acts of terror are occurring on a more frequent basis with catastrophic outcomes that resonate at a very visceral level within the corporate fabric, from key executives to line employees.

Competing for headlines with these heinous acts are the continual data breaches that erode the financial integrity fabric and brand value of major enterprises.

The profile of the perpetrators of acts of terror and corporate security breaches continues to change, with self-radicalization topping the present day list of motivation for attacking innocent victims. In a similar fashion, the profile and motivation for the cyber-related offender has shifted from a shadowy figure simply looking to skim some easy money to sophisticated rings of hackers looking to not only obtain financial gain but to cause irreparable reputational harm in the process.

Security leaders tasked with the protection of the personnel and assets of leading corporate organizations are being assailed on a daily basis by providers of technology and operational solutions that are purported to address these threats.

The challenge lies in separating the true enterprise risk reduction value offered by these solutions from the slick presentations and exhaustive lists of generalized benefits being pitched by the solution sales teams.

There is no silver bullet, and no single solution will address the specific needs of a global organization. A pragmatic, integrated approach must be taken to identify the solutions that resonate with each company's unique risk profile, corporate culture and level of executive support for the security function. Once the optimum solutions are identified, they must be implemented in a cohesive, relevant and collaborative fashion (a process of "fusion") that delivers the maximum real-world value from the predictive intelligence and risk-reduction investment, and this value must be linked to key business functions that have a material and significant impact to the company's bottom line.

The key concept to grasp in this environment, where the security department's value has been tied to critical business functions that represent millions to billions of dollars in risk, is that you are reframing the entire financial discussion with your leadership from "how much money are we going to save" to "how much risk are we going to avoid". When you deliver on this monetary risk reduction the ROI received by the company and the perception of the security function as a cornerstone of corporate shareholder value will be significant and measurable.

The Problem: Defining Your Intelligence Fusion Vision

Most security executives realize that their command and control environment and delivery mechanisms require an upgrade to stay in pace with today's evolving threat landscape. The first step in this process is moving command and control from "Alarm Monitoring Centers" charged with viewing and managing information feeds from access control, video management and intrusion detection platforms to "Intelligent Command Centers" that broaden this reach to include the actual global risks that can have a material effect on the enterprise. The problem in this fundamental shift in focus lies in creating a clear, multi-faceted vision for what the optimal operating environment will look like. Key questions that need to be answered to define this vision include:

- What specific threats will be addressed?
- How will technology be leveraged to address these threats?
- What are the operational challenges surrounding implementing these technologies and managing the increased level of information handling?
- What specific skill sets will be required from the operators and analysts charged with managing this information flow?
- How will this optimized environment be dramatically different from today's operating model?
- How will this environment deliver definable and measurable initial monetary risk reduction to the enterprise showing return on investment (ROI) for the initial capital expenditure investment?
- What are the key metrics that will support this environment year after year from a total cost of ownership (TCO) perspective ensuring support for the ongoing operation expenditure investment?

This vision can only be shared with executive leadership in an exciting and compelling fashion once all aspects are clearly defined by the security leader responsible for the upgrade initiative. With a solidified vision in place, gaining funding for the initiative and long-term support for the program from executives becomes a natural process and the true value from the intelligence fusion investment can be realized.

"This vision can only be shared with executive leadership in an exciting and compelling fashion once all aspects are clearly defined by the security leader responsible for the upgrade initiative. With a solidified vision in place, gaining funding for the initiative and long-term support for the program from executives becomes a natural process and the true value from the intelligence fusion investment can be realized."

The Market Gap

Having a clear vision of what an optimized future-state environment will look like is a key first step in an upgrade process. The next challenge in today's market is sourcing the solutions that will bring this vision to reality.

Solution providers have developed many new and innovative technology platforms that are driven more by their ability to provide compelling features and benefits in a demonstration setting or in a marketing brochure than in the real-world environment of a global security operations center charged with corporate enterprise risk management.

Having multiple intelligence feeds hurling information at command center operators on global activist activity, social media postings, travel alerts, civil unrest, severe weather and crime trends all popping up on a GIS-enabled world map may seem like an environment that could deliver actionable risk-reduction solutions.

The inverse of this envisioned state is the reality that is most often experienced within corporate environments attempting to implement these feature-rich solutions.

Turning on multiple information feeds and having command center personnel whose skill sets reside in the previous "Alarm Monitoring Center" work flow of identifying an alert, applying a notification protocol to this alert, opening up an incident on their screen and sending out a communication to the field sets up both the center and the operator for failure.

Intelligence feeds seldom contain information that is as "black and white" as alerts from a security system platform. A door is either forced open or it isn't. An exit alarm is either active or it's not. There is either video activity on a camera or there's nothing happening in the field of view. Black and white.

Intelligence feeds are full of "shades of grey". Weather feeds can be pretty specific as to the expected timing of an event, its level of severity, the impact radius of the event and its expected duration. Applying these same metrics to activist activity, social-media heat mapping and potential governmental instability is where the gap between the demo, the marketing brochure and the real world becomes apparent.

Fulfilling the initial vision will require the implementation and optimization of these "shades of grey". Just because the solution is challenging and difficult doesn't mean that we can stay in our old, safe environment. We simply need to understand what the challenges are to fulfill the vision, apply a focused approach to addressing each challenge and remain agile in solving new challenges as they arise.

How "Intelligent" is Your Intelligence?

We've all seen the warning on a menu that states, "Consuming raw or undercooked meats, poultry, seafood, shellfish, or eggs may increase your risk of foodborne illness".

Many security operation centers currently enable a dizzying array of multiple sources of intelligence, without a robust program to filter down the quantity and quality of data and alerts that can assail their operators.

The point is that consuming large quantities of this raw intelligence data can significantly impact the health of your command center.

Every potential feed of intelligence information should undergo the following list of requirements prior to being selected for the center and ultimately being deployed and presented to operators:

- What is the business threat and/or enterprise risk that will be diminished by viewing this feed?
- What is the anticipated *quantity* of daily alerts from this feed?
- What is the anticipated *quality/applicability* of the alerts from this feed?
- What will the potential impact be from a false positive alert from this feed?
- What will the potential impact be from missing an alert from this feed?
- Where does this feed fall in its priority level (mission critical, regionally critical, background information only, etc.)?
- Can an operator act directly upon information from this feed, or is it interdependent on other data sources to drive an action?
- Will alerts from this feed include tag data (geocodes, meta data, keywords, etc.) to allow for automated functional/regional distribution or are they text alerts that need to be read in full by an operator to determine subsequent actions?
- How can the raw data from this source be filtered and analyzed prior to being communicated to the center based upon your specific business needs?

- Can this feed mitigate other enterprise risks to the company beyond the needs/scope of the security organization?
- Who will be the target audience (regional security managers, business unit leaders, C-suite executives, etc.) when alerts from this feed reveal a credible threat that will require action?
- How will information from this feed need to be packaged to be readily understood and acted upon by these audience members?

The answers to these requirements will drive a selection process that will trim down the quantity of raw data coming over the transom within the command and control environment. Once the final list of intelligence feeds is established, the process enters a secondary phase of determining the level of outsourcing to be utilized in filtering and pre-analysis to deliver a higher degree of actionable intelligence to the center operator.

> *"This secondary phase requires a high level of diligence and a moderate level of cynicism. The demonstrations and marketing literature from the feed providers will make another big play at this phase, and the fusion center team needs to look beyond the buzz words and focus on real-world use cases where the correct, actionable data is delivered while the clutter is successfully removed."*

This secondary phase requires a high level of diligence and a moderate level of cynicism. The demonstrations and marketing literature from the feed providers will make another big play at this phase, and the command center team needs to look beyond the buzz words and focus on real-world use cases where the correct, actionable data is delivered while the clutter is successfully removed.

"Analysts" Versus "Operators"

We've used the term "operator" up to this point to describe the role of the personnel charged with monitoring the data feeds that fuel the command center and taking action on this information.

An "operator" in this context has a job description that is inline with the position title. Like a telephone operator, this person is essentially occupying a call center workstation where they follow a script that dictates their actions in a specific set of circumstances. Excellent communication and customer service skills are required for this position, but a deep understanding of the underlying applications and business risks being managed are not. Professional, motivated and diligent operators are a key component in the staffing of a command center since they are the critical "man-machine interface" between the outside world of threats and alerts and the internal corporate world of reaction and mitigation. An operator's world is objective in nature.

Sourcing of operators is typically done on a contract basis utilizing providers of security guard services. It is critical to work with the guard service provider to ensure they understand the difference between a fixed post/roving security officer and a command center operator. Some leading guard service providers have independent divisions that focus solely on staffing command centers and this can be an excellent choice in making the selection of a command center operator provider.

An “analyst” performs a higher-level function in support of the command center. Analysts review the alerts being received and determine their severity and applicability to the specific corporate function or entity that could be impacted by content of the alert. Analysts assign priorities and follow escalation protocols to ensure that the correct level of incident reaches the corresponding level of leadership so that business decisions can be made and remediation efforts can commence. This is a delicate balance since the command center never wants to be viewed as an annoyance by senior leadership, clogging up their inbox with routine communications. On the other hand, key executives will also be frustrated and challenge the need for the center if they were not informed of an incident that they feel would have required their participation. The analyst’s world is subjective in nature. These are the experts that will assimilate the “shades of grey” in alerts and determine the “black and white” response actions to be taken.

Sourcing of analysts can be accomplished via three different channels. The first is the outsourcing of analyst functions to the intelligence feed service provider(s) as previously mentioned. This “pushes” the analysis out of the internal command center and relies upon a pool of analysts employed by the provider(s) to predetermine (as best as they can) the information that is pertinent to your needs. Depending upon the complexity of the data being processed, this can be an excellent choice to limit the amount of incoming data and leverage the investment from the provider in their pool of analysts that specialize in their specific area of risk mitigation (i.e. only receiving travel alerts covering countries where you do business or have active itineraries instead of receiving information on the entire world and sorting/prioritizing the information using internal analysts.).

The second channel for analyst sourcing is through your guard services provider. Some providers understand the distinction between “operators” and “analysts” and can provide you with candidates that may fulfill your business requirements. Review, approval and oversight for these contracted resources requires a higher level of internal management commitment than the operator function due to the criticality of the information being processed and the visibility to executive leadership of the actions being recommended and the escalation decisions being made by the analyst.

The third channel is to hire internal head count to staff the analyst positions. This can be an excellent choice if ideal candidates can be identified and recruited and they can be compensated and motivated at a level that ensures a long-term commitment to the command center team. Internal personnel can have a greater level of influence with stakeholders outside of the security organization as opposed to contract personnel which may gain a higher level of buy-in for the command center function.

Many companies will end up with a “hybrid” of these three channels for the analyst function depending upon the size and complexity of their command center organization. A balance can be struck between leveraging the expertise of the intelligence service provider’s analysts to limit the amount of data being transmitted to the center, leveraging the staffing resources of the guard service provider to provide a greater number of front-line analysts, and internally hiring one or more senior analysts to provide the oversight only a company employee can deliver.

Rear View Mirror Versus the Windshield

At CSO conferences and roundtable discussions across the country, a consistent statement from the podium for the past couple of years has been, "If you're looking at guns, guards and gates you're looking in the rear view mirror".

This statement will normally get several nods of approval around the audience, or even a round of applause.

This is a bold statement, and it has serious ramifications for the future of the security function within the global corporate environment as it pertains to a corporation's overall "situational awareness".

The problem lies in the gap between the bold statement and the actual security command and control operating environment. Many corporate security departments today are still outfitted with very elaborate and expensive rear view mirrors.

Keeping a tight focus on physical security systems in today's threat environment is very similar to focusing on the rear view mirror while speeding down a highway.

We are certainly charged with the effective monitoring and administration of access control and video management systems that can represent millions of dollars of capital investment by the company. These systems are primarily in place as deterrent and crime prevention assets. The types of incidents they are deployed to detect occur on an infrequent basis and their level of visibility to the core business functions of the company and their enterprise risk impact are negligible. The inverse of this infrequency is also true from this information feed. This area is the source of the greatest amount of "false positive" traffic in any command and control environment. The number of door held open alerts, access denied notifications and door forced open alarms that are equipment-related as opposed to actual intrusions can number in the range of hundreds to thousands daily at a busy command center.

Ignoring the view in the rear view mirror is not an option, and checking on what's happening in this area of risk is still a critical function. Normalizing these data and applying an aggressive program of alarm reduction and appropriate response are ongoing and necessary initiatives to maintain the delivery of an effective security integrity process. However, having the rear view mirror as your primary focus is also not a productive option. You will always be viewing "what's already happened" instead of "what's coming".

The key concept to assist in this stratification of enterprise risk is answering these simple questions relating to what you are monitoring from this channel:

- If your office in Paris got broken into in the middle of the night and the perpetrators stole a couple of large-screen monitors from a conference room, would this get reported in the news the following morning?
- Would there be any effect on the company's revenue or reputation?
- Would the company's stock price go down on the next day's trading?

It is highly unlikely that there would be a positive answer to any of these questions. Security system alerts are about loss prevention, not shareholder value.

The two critical risk areas that are visible when you shift your focus from the rear view mirror to the windshield that *do* wreak havoc upon a company's revenue, reputation and brand value are business disruption and IT-related breaches or denial of service. Incidents that fall into these categories have the potential to have an immediate material effect on the health of the organization and can drive a loss in market capitalization that is far beyond the actual loss of revenue or information.

Critical Risk #1 - Business Disruption

Let's look at these critical risks one at a time. Business disruption and the mitigation of business disruption risk is distinctly different from business continuity. Business continuity is a reactive set of measures put in place to allow the company to recover from an incident and resume operations in an orderly fashion. Any established company has a robust business continuity program in place and has a cadre of full-time staff devoted to this process.

Business disruption mitigation is a proactive set of work flows and business rules that apply predictive intelligence to identified precursors that could have a credible impact on business operations. When these precursors become active, the command center can apply pre-planned measures to notify business units that may be impacted with not only the type of incident that has a credible chance of occurrence but with a set of remediation actions that will either minimize or eliminate the downstream disruption of profitable business conduct.

> *"Business disruption mitigation is a proactive set of work flows and business rules that apply predictive intelligence to identified precursors that could have a credible impact on business operations. When these precursors become active, the command center can apply pre-planned measures to notify business units that may be impacted with not only the type of incident that has a credible chance of occurrence but with a set of remediation actions that will either minimize or eliminate the downstream disruption of profitable business conduct."*

In order for this work flow to be successful, the command center analysts need to completely understand the external threats to the enterprise. They also must be tasked with gaining a high-level understanding of the internal operations of the business to be able to overlay these threats and relate them to potential business risks. Collaboration between security leadership and key stakeholders from the company's primary business units can empower this knowledge transfer. This knowledge-sharing should culminate in the development of specific scenarios of potential business disruption risk, the establishment of the work flows to manage these scenarios, the definition of the roles and responsibilities of both the security team and the management of the business unit and the protocols to monitor the evolution of an incident from precursor to conclusion.

A business disruption mitigation program must be global in nature, even if the company utilizing the program is a domestic entity. Most command centers that monitor data feeds beyond security systems have some mechanism to overlay alerts from these feeds and apply them to the company's real estate portfolio. This process allows analysts to see how alerts could affect operations at these company-centric locations. While this is a key feature of situational awareness, it is a small piece of the business disruption puzzle.

A business is only as sound as its supply chain and its mobile assets. A command center must have the capability of overlaying threat information not only to the fixed assets of a company, but to the extended business landscape of interdependent suppliers, materials in transit and personnel assets on travel to gain a true risk management perspective.

Receiving an alert that there is a potential governmental meltdown in a specific international city in a previously stable country that could be heading to instability, followed by alerts of planned civil disobedience and unrest within this city can have severe ramifications for getting employees to their workplace and getting product finished, out the door and to its intended destination.

If the scope of vision for the command center is only focused on company-owned or leased facilities, this type of alert could be acknowledged and catalogued with no follow-up action required if there are none of these facilities in the expected impact radius.

The fact is that while your company may not have any facilities in this city, it could be a major manufacturing and distribution hub for one of your key suppliers, and you may have a dozen or more of your employees embedded at this supplier's facility to oversee their operations as they relate to providing you goods and services.

Upon review of the overall evolving threat scenario, you determine the timing of the potential disruption is ten days out pending the results of a local election. Activist plans show they are intent on disrupting governmental operations, staging marches that will impact traffic in both the central business district and in the commercial district, and they want to shut down the airport.

This alert could have a more significant business impact than a similar set of threats just down the street from your headquarters. Having some of your employees stuck in traffic and not be able to make it to this week's wellness training due to a protest is not ideal. This type of incident pales in comparison to millions of dollars in mission-critical supplies being held up for a week or more in our hypothetical troubled city. We could also have employees that are seeking reassurance in this location confirming they are either safe to stay in place or there is a swift extraction plan in the works.

A workflow for this alert could include the following:

- Notify the business unit leader who is reliant on the materials of the impacted provider.
- Assist in determining if it would be feasible to request advance shipment of finished goods from the supplier to an alternate location outside the projected area of impact.
- Determine whether the possibility of disruption is severe enough to temporarily have employees remain in their domicile prior to the events.
- Have employees temporarily relocated to an adjacent country with a lower risk profile to allow them to return in short order if the threat doesn't materialize or once an acceptable level of in-country stability is achieved.

This level of proactive information-sharing and coordination with stakeholders from other business units deliver measurable financial results from the command center function far in excess of the capital and expense investment to fund the center.

Expanding the scope and reach of your situational awareness to handle business disruption mitigation is primarily an exercise in internal procedure development and applying best practices as opposed to an expansion of technology or intelligence feeds. The information you need will be within your data sources. Your processes that cover what information to look at, how to stratify this across the global interdependency landscape and how to respond to specific incidents is where the real work will need to be performed and where the real rewards will be realized.

> *"This level of proactive information-sharing and coordination with stakeholders from other business units deliver measurable financial results from the fusion center function far in excess of the capital and expense investment to fund the center."*

Critical Risk #2 - Information Security and Integrity

Our second critical risk is much larger and potentially much more dangerous to the company and its overall enterprise value. Just the appearance of an IT-related breach or denial of service can drive a company's stock price and total market capitalization into a tailspin, even if no actual data loss or service disruption has occurred.

The proactive work flow from the command center in this arena is twofold. The first area of support to the CISO and the IT function is the sharing of global situational awareness monitoring intelligence that could show the credible potential of an increased threat to their cyber assets.

This could come from sentiment analysis of social media feeds showing unrest around a specific business decision emanating from your company (outsourcing plans, a reduction in force, increased pricing for a product, support for a political cause, etc.). Posts could be detected stating that your company is mentioned in chatter among groups you have profiled to represent a credible threat (these could either be civil unrest groups who stage protests or physically disrupt operations or hacktivist groups who disrupt network services or operations). The traffic indicates these groups are trying to find a way to disrupt your business, diminish your reputation, or both. These are "dual-vector" threats, meaning they could evolve into a physical disruption of your business, a cyber-attack, or both.

These types of alerts aren't typically on the radar of the IT security team. Through their security information and event management (SIEM) platform, they have in-depth alerting of specific threat scenarios for firewall penetration, denial-of-service (DoS) or malware viruses embedded in e-mails, phishing scams involving e-mails or cloned websites and mass data assaults on their webservers from automated surfing programs.

Moving from these general threats to the notification of a more specific alert can assist them in deploying proactive tactics to focus their countermeasures on specific areas of the enterprise by way of elevating logging related to inbound IP addresses, content, activation of baseline traffic dashboards, keywords to monitor, data loss prevention (DLP) sensors, denial-of-service routing and possibly leading to the triggering of the business continuity/disaster recovery (BCDR) standby procedures.

The most effective process to enable this sharing of situational awareness intelligence is to provide a seat for an information security analyst within the command center environment. This creates a true "J-SOC" function (joint security operations center) that is handling both physical and network security functions within one facility. The determination of what types of alerts rise to the level of an IT-centric threat and the stratification of the contents of these alerts across the information security landscape is very subjective, and a skilled analyst who is on the front line of intelligence visibility can be the key catalyst to ensure the proper countermeasures are identified and deployed in a rapid fashion.

The second area of support in the IT security arena involves getting your own house in order. While the chief security officer or security director at a company is typically not responsible for information security, the physical security function and its attendant deployment of protective devices has evolved in recent years to create a significant level of information security vulnerability to the enterprise.

This vulnerability involves the deployment of IP-enabled end-devices, panels, video servers, application servers and workstations. On a frequent basis (if you know where to look) alerts are being broadcast of potential vectors of breach or compromise impacting these devices.

As previously stated, a specific security manufacturer's IP-enabled intercom station failing a penetration test is not going to show up on the SEIM feeds utilized by the IT organization. This type of information is very industry-specific and doesn't rise to the level of a broad vulnerability that will typically show up on the various subscription-oriented common vulnerabilities and exposures (CVE) feeds provided by anti-virus, anti-malware or US-CERT feeds, at least not within sufficient context for the analyst to take specific action.

If you receive a notification of a vulnerability on one of your device types (of which you may have hundreds of instances of this device attached to the network), your key metric will be your mean time to remediate (MTTR) this vulnerability. Remediation in this context is defined as removing the vulnerability completely and/or deploying satisfactory compensating controls surrounding the vulnerability from all instances of the device as they are currently deployed. A single instance of a vulnerable device remaining connected to the network is one too many from a cyber integrity standpoint.

Developing and deploying a robust database of all instances within your physical security deployment of IP-enabled devices is a crucial step in diminishing this threat. A simple test case can help you determine if you have this function in place.

Let's assume you've received an alert that a specific IP-enabled video camera has been found to have a hard-coded factory password that cannot be changed and if used could compromise the functionality of the device and your video platform and could provide back-channel access to your production network.

How quickly could you determine:

- Do we have any of these devices installed within our system?
- How many do we have?
- What specific facilities are they in globally and what is their physical location within these facilities?
- What is the specific network IP address these devices are connected to?
- What is the remediation required to address this vulnerability (i.e. a simple firmware upgrade "push" across the network that could take hours, or the physical replacement of the devices which could take days)?

- How long will it take to address the vulnerability at all devices (MTTR)?
- What will it cost per device?
- What is the total remediation cost?

If you determine that it would take more than an hour to answer these questions you have a serious problem. At many global companies, it could take days to gather all of this information from all of the business units and area managers involved.

We don't have the luxury of taking days to close a potential network security threat vector. The bad news is that once we know a device is vulnerable, the miscreants that would seek to exploit this vulnerability know about it as well.

The point is to embed a rapidly-deployable work flow into the command center fabric supported by agile and dynamic database tools that will drive the MTTR surrounding these types of vulnerabilities to hours instead of days.

This combination of proactive intelligence-sharing combined with aggressively managing a potential point of internal IT vulnerability will link the command center's function to both key aspects of the IT Security critical risk.

"Cost Center" to "Value Center"

It is critical for us to shift our focus within the Intelligent Command Center environment from an alarm monitoring center perspective to a much broader vision that includes key areas of revenue, reputation and market capitalization protection. This shift empowers the fundamental change in perception by executive leadership of the entire security department from a "cost center" to a "value center".

The "blocking and tackling" functions of managing employee access, unlocking doors, viewing cameras and responding to intercom calls are typically viewed at a senior level at most companies as no more significant than the facility-centric costs of watering plants and changing light bulbs. This perception groups security into a cost environment that doesn't inspire future investment. In many cases, there is leadership pressure to continue to drive these fixed costs down on an annual basis.

You can shift this perception overnight when you make the credible business case that future investment in the command center concept will deliver measurable returns in shareholder value protection.

In the "cost center" environment, requests for funding would typically have to end up as a "zero sum" equation within the security department budget (i.e. "Give me a million dollars of capital next year, and I'll reduce guard costs by $330k a year for a 3-year ROI"). These type of straight-line budget requests are always based upon, "How much money are we going to save?" The problem with this circular investment strategy is your capacity for funding is based upon the overall security budget which is a very small number (a few million dollars annually, even at the largest companies).

In the "value center" environment, you will transition your business cases and budget requests in a framework of "How much risk are we going to avoid?" as opposed to "How much money are we going to save?"

You are now going to tie your service delivery to business disruption mitigation, which in each instance carries a risk reduction of several million dollars. You'll show a credible tie-in to IT security breach protection and denial of service reduction. Each instance of these types on incidents have an attendant cost impact of several million dollars. Ultimately, since these types of incidents can affect the company's market perception and stock price, you are offering protection of shareholder value. A security-related incident that moves the company's stock by just a few points can have an impact of several billion dollars in market capitalization.

> *"The key concept to grasp in this environment, when the Intelligent Command Center's value has been directly tied to critical business functions that represent millions to billions of dollars in risk, is that you don't need to be* ***right every time****. If you are just right* ***once a year*** *and help steer your ship proactively and avoid an iceberg, the fusion center has more than paid for itself. If you are right* ***once a month****, the ROI received by the company and the perception of the security function as a cornerstone of corporate shareholder value will be significant and measurable."*

It does sound a bit presumptuous to say to the C-suite, "Give me a couple of million in capital to upgrade my command center and an additional million in expense per year to staff it, and I'll provide you risk reduction at ten times this amount."

The command center business case has a little more subtlety than this sentence, but this is the underlying truth of your overall value proposition to the company.

Enterprise risk *management* exists as a significant and critical entity within any company of considerable size. Risk *management* is primarily an underwriting function and by its very semantics is reactive in nature. Incidents occur, the damage is assessed, claims are made and the company is reimbursed for losses over the self-insured limits it carries. Proactive risk *management* entails modeling the company's underwriting profile to balance coverages carried to the frequency of losses and claims. A very crucial process for the health of the business.

Through the command center, you will be offering enterprise risk *monitoring.* This function is proactive in nature and is tasked with forecasting near-future potential threats and directing mitigating measures before an incident occurs. This is not providing *insurance* to cover the company after a loss, this is providing some level of *assurance* that a loss can be avoided.

There is a time-honored adage in the federal agency and major metropolitan police department environment that states, "The perpetrators only have to be right once. We have to be right 100% of the time."

Federal agencies and leading police departments have thousands of personnel and billions of budget dollars to accomplish this mission. Corporate security departments have a handful of people and have to fight for every budget dollar. The key concept to grasp in this environment, when the Intelligent Command Center's value gets directly tied to critical business functions that represent millions to billions of dollars in risk, is that you don't need to be *right every time*. If you are just right *once a year* and help steer your ship proactively and avoid an iceberg, the command center has more than paid for itself. If you are right *once a month,* the ROI received by the company and the perception of the security function as a cornerstone of corporate shareholder value will be significant and measurable.

Sticking your neck out and making this business case may sound like too far of a reach for many security leaders. This is a "land grab" for responsibilities that may be out of the scope and purview of your position as it is defined today. The truth is that taking on some level of visibility and responsibility for these threats, risks and mitigation plans is a very natural extension of the corporate security function. One "gift" that is given to security leadership is that the company (even a relatively small company) will pay for security to put people in front of computers and monitors on a 24 x 7 basis to manage threats and risks. All you are doing in the command center model is putting information on these computers and monitors that manage the actual *fiscal* risks to the company. Once you have this information, you can share it with the risk management team to lower the overall corporate risk profile and reduce underwriting costs. You'll include corporate compliance executives to bolster your regulatory position and avoid potential fines or service delivery disputes. Your information-sharing will assist your legal department in strengthening their litigation avoidance posture for employee-safety related matters and customer service level delivery challenges. Working in concert with these other business leaders and helping them apply your actionable intelligence to their challenges makes you a catalyst for overall corporate business integrity and profitability.

Another key concept in this shift from cost to value is determining where a robust security integrity program and highly-visible investment in intelligence fusion adds to your company's client-facing value proposition. We've seen data center companies use this investment as a prime feature in their overall service offering. Software and cloud providers leverage this security investment to bolster client and prospect confidence in the protection of their critical data. Oil and gas companies have leveraged this program to demonstrate the protection of shareholder value in increased safety in their operations and the protection of confidential information. Pharmaceutical companies demonstrate increased value for their shareholders through enhanced regulatory compliance and supply-chain integrity. Make your fusion initiative compelling to your executives and then make your center a "showcase" for your sales and marketing team and you will become a core component of your company's sales pitch.

Returning millions of dollars to the bottom line on an annual basis through risk reduction along with increasing revenue is a far cry from being lumped in with watering plants and changing light bulbs.

Some Assembly Required

The upgrade of a command and control center environment to a fully-integrated and operational command center is a complex undertaking. The business case you've made involves a broad array of technologies and solutions that need to be vetted, procured, delivered, installed, integrated and commissioned.

This process is very much like heading to the hobby store and picking up their top-of-the-line scale model of a battleship. You get it home, open the box, pull out the hundreds of parts and find out there's no instructions and no glue.

You're smart, and over time with a lot of trial and error and test-fitting of parts and looking at the picture on the front of the box you could probably assemble something that looks like a battleship. With no glue, all of the parts would be somewhat in their correct place, but the slightest impact would see your battleship fall to pieces.

Unfortunately, you don’t have time for trial and error and test-fitting, and your model will need to be rock-solid and be able to survive impacts both minor and major. Your command center will need to be prepared to fight battles the day you turn the key and say you are in a “go live” state.

In the command center realm, policies, procedures, business rules, work flows and protocols are your “instructions”. To fulfill your vision and the ultimate business case for the command center, these need to be fully developed, distributed to any stakeholders they will affect, and be reviewed and approved prior to deployment. Upon deployment into the command center environment, operators and analysts need comprehensive initial training on their roles and responsibilities when executing these documents combined with operational drills and tabletop exercises to ensure they can follow a work flow under pressure in a simulated environment. The level of critical incidents that are to be managed require a commensurate level of pre-planning and documentation to deliver the premium professional services expected by the business units the center will be interfacing with and supporting.

This collection of documentation also cannot be printed out and stored in binders. This type of “static” documentation is too rigid and time-consuming to be effective in the dynamic environment of a command center. A robust data repository needs to be deployed and maintained to ensure current information is available to all operators and analysts and that this information is updated constantly with new work flows and compliance directives to keep pace with the evolving threat and corporate landscape. Holistic measures for document updating and version controls need to be put in place and monitored on a scheduled basis.

This on-line delivery of policies and protocols will empower the “call center experience” for operators so they will have ready access to response, communication and escalation directives that cover the incidents they are most likely to see on a daily basis. An automated program for incident/case management needs to surround this environment to capture cradle-to-grave documentation of the intelligence received, the actions taken, and the outcomes of these actions for retention and process improvement purposes.

The “glue” for your command center is integration. Integration in the command center environment occurs in two distinct areas.

The first is the internal security department integration of all of the technologies, data sources and mitigation controls deployed. This involves the linking of alerts between data sources to identify threats that have multiple vectors that can affect the company. It also involves the linking of alerts to geospatial displays to gain a visual representation of what the alerts are, their expected impact radius, and the company/supply chain/personnel assets that are within this impact radius. Integration can also include the automated alerting of events to assets based upon predetermined business rules and the geocoding of alerts.

The second area of integration is the deployment of the command center assets within the technology architecture and fabric of the company. The success of the center is reliant upon the stability and depth of the network and computing appliance infrastructure assets deployed to support it. Coordination with IT resources to build this infrastructure while working through the compliance requirements of the IT organization on this scale of an internal hardware/software initiative is a necessary and complex set of tasks that need to be performed in a cooperative and pragmatic fashion to obtain the level of resources and support the center will require. While providing some end-state support for the IT security function, this process of network provisioning for the center will also require an intense level of IT security coordination to ensure all applications and the solution architecture meet the security compliance requirements of the IT organization.

Many times in today's environment this level of application deployment will also require pushing certain aspects of the solution "to the cloud". You need to be prepared to coordinate the placement of some services, applications and functions within an environment such as Microsoft Azure or Amazon Web Services (AWS). Each instance of "cloud placement" will also require a level of documentation and compliance to meet the established IT protocols for the utilization of third-party data hosting providers.

> *"Many times in today's environment this level of application deployment will also require pushing certain aspects of the solution "to the cloud". You need to be prepared to coordinate the placement of some services, applications and functions within an environment such as Microsoft Azure or Amazon Web Services (AWS). Each instance of "cloud placement" will also require a level of documentation and compliance to meet the established IT protocols for the utilization of third-party data hosting providers."*

You will need help in the development and deployment of your instructions and your glue. Security organizations rarely have the internal resources to address these complex tasks while still performing the duties of their "day jobs". Also, "integration" tasks in the context of the command center are not services that can be sourced from your security "integrator". "Systems Integrator" is a label that has been self-applied by security systems contractors to themselves for years. These contractors do provide some compelling systems integration at the blocking and tackling level of the "black and white" environment of physical security systems. They are certainly capable of integrating platforms so when a door forced open alert is received a video image of a camera adjacent to the alert can be called up, a map of the affected area can be displayed, and an operator can be given instructions on who to call to manage the alert.

The level of true integration required to manage the "shades of grey" environment of intelligence fusion goes far beyond this level of internal linking of security system platforms. You will need support from professionals who can develop operation business rules, policies and procedures and can deploy them onto a dynamic data repository. You will also need a team with experience in selecting intelligence feed providers, normalizing the data from these providers and linking data between sources. Finally, you will need support in the coordination of integrating this solution suite within your corporate IT fabric, inclusive of all IT security requirements for both internal and cloud-based support initiatives.

All too often a security department finally gets the funding for a couple of new software packages, puts them on-line, and then decides to "see how it goes" as they start processing the new information that is popping up on their screens.

This piecemeal approach follows a thread of logic that says, "It is better to do something a little better than to do nothing at all."

> *"You request a suite of ten solutions and tell a great story on what all ten solutions will do and then get funding for two of them. An incident occurs, and you are challenged as to why, since you got some funding, you weren't able to address the incident in the way you represented when you asked for your full funding."*

Unfortunately, in the command center environment we are looking much more at an "all or nothing" approach. The danger of piecemeal solutions is that executive leadership tends to have a short memory. You request a suite of ten solutions and tell a great story on what all ten solutions will do and then get funding for two of them. An incident occurs, and you are challenged as to why, since you got some funding, you weren't able to address the incident in the way you represented when you asked for your full funding. Going back and forth with senior leadership and pointing fingers relating to who didn't fund what in the middle of a potential crisis is not a fun place to be and is not the foundation upon which a long and prosperous career is established.

Create the complete vision of the command center's end state solution suite, inclusive of instructions and glue, and build a business case upon the return to the company from this holistic initiative. And then dig in your heels. Half of a command center will not deliver half of the projected results. It may deliver none since a key component to bring the vision to reality and truly deliver may well have ended up in the unfunded half of your center upgrade project.

From Revolution to Evolution

Obtaining funding and buy-in for a command center, and then making the required investments and standing up this new solution will be a revolutionary change within your security department. The final key concept to keep in focus going forward is the command center project doesn't end on your "go live" date, it really just begins. Command centers must have the flexibility to evolve over time. There are multiple drivers for this evolutionary process.

The first driver is the fluid nature of the global threat landscape you are attempting to monitor. New types of threats will emerge. New groups will pop up that may have a special interest in your type of company. Countries where you have facilities or key supply chain assets will swing from stability to instability (or back the other direction). New acquisitions will be made, materially altering your company's global footprint and product mix.

These changes in the threat landscape and your company's asset portfolio will need to be captured and rolled into both your technical and operational platforms to keep pace with their evolution.

Concurrent with the evolution of threats, global regulations and compliance initiatives will continue to shift to keep pace with either new types of threats or new instances of corporate misconduct that governmental agencies feel require new legislation to mitigate. Regulatory compliance initiatives need to be constant internal work flows for the command center management team to keep pace with these policies.

We must also never lose sight of the fact that the entire command center is built upon a foundation of underlying technologies. Technology by its nature has a very short life cycle, and the more leading-edge the technology is that we deploy, the more rapid the innovations will occur within that technology sector to deliver new features and benefits.

This brings us full circle on the evaluation of technology and intelligence. When creating the vision for the command center you needed to move beyond the demonstration and marketing materials to determine what the optimal suite of solutions would be to empower the center prior to implementation. Once you are operational, you'll need to be pragmatic (and somewhat cautious) about what new technologies, software upgrades, additional feeds and additional features you'll want to embed within your center's fabric to stay abreast of new innovations.

To assist in this evolutionary environment, a comprehensive program of managed services should be woven into the command center solution environment. Your IT organization will be supportive of this since they seldom embark upon implementing a complex solution suite without a managed services program.

> *"With all aspects of a robust evolution management program in place, your fusion center will be positioned to fulfill its initial vision and continue to deliver enterprise value over time as your company continues to grow and its needs change over time."*

From an operational standpoint, a managed services team will provide professional analysts that will monitor the regulatory environment and assist in making the pertinent changes within your documentation suite to stay in pace with these requirements. They will work through your case management history to apply lessons learned from actual incidents and modify business rules and work flows to improve service delivery.

Within the technology space, a managed services team will keep all instances of technology integration running at optimal efficiency, and ensure patch management and version control across the multiple sources you're using to deliver your key functions. They will also work with both your internal IT stakeholders and any external cloud-based providers to keep your underlying network and appliance infrastructure running in a secure, high-availability state.

Finally, this team will be tasked with being on point for any performance issues or break/fix service ticket management covering the integrated platform. Intelligent Command Centers "fuse" multiple technologies from multiple sources to create a single, holistic work environment. The only problem with this multi-platform suite is identifying who to call when something doesn't work. A professional managed services team will be able to sift through all technologies involved in a malfunction, do a root cause analysis and bring the integrated platform back to full operation quickly.

With all aspects of a robust evolution management program in place, your command center will be positioned to fulfill its initial vision and continue to deliver enterprise value over time as your company continues to grow and its needs change over time.

Selection of an Intelligent Command Center Consultant

The holistic suite of services required to develop and implement a successful Intelligent Command Center have been developed and optimized by Guidepost Solutions through the performance of global initiatives for market leaders in technology, finance, telecommunications, critical infrastructure, healthcare, manufacturing, distribution/logistics, entertainment, and education.

Responding to our clients' needs, we combine the talents of experienced security management professionals, systems designers/engineers with our in-house experts in corporate IT, finance, regulatory compliance and operations. Our team includes former CSO/CISO/CIO level executives who truly bring the "owner's perspective" to our engagements and deliverables. We provide the following services in support of corporate Command Centers:

MASTER PLANS/BUSINESS CASES

Our team works closely with security executives to create the holistic vision for a Command Center, define the suite of solutions that will empower the Center and develop the specific fiscal metrics that drive a compelling business case for senior executives to embrace the solution and fund the initiative. We also provide a "health check" and gap analysis program for a client's current command and control environment, uncovering potential areas of improvement that can deliver greater enterprise value.

COMMAND CENTER ENVIRONMENT DESIGN

Guidepost Solutions provides a complete suite of services to design and manage the implementation of the comprehensive package of audio/visual technologies, workstations, telephony and network elements that empower a productive and collaborative Command Center work environment. This includes video walls, ergonomic work places/lines of sight, the provisioning of an Incident Command Room (ICR) and the network-based information-sharing between the Command Center, the ICR, and the C-suite.

INTELLIGENCE FEED MANAGEMENT

Guidepost Solutions has extensive experience across a broad landscape of intelligence feed services and providers and will assist in stratifying the proper feeds and level of pre-analysis supported by each potential provider to bring the optimum level of actionable intelligence into the Command Center. With the optimal suite of intelligence feeds selected, we assist with the integration and optimization of the overall intelligence data stream to ensure the correct alerts get analyzed and escalated to the proper team of stakeholders.

OPERATIONAL CONTENT DEVELOPMENT

A Command Center is only as effective as the operational protocols utilized to discharge its duties. Guidepost Solutions has the professional security operational background to assist in creating the comprehensive set of documentation that will empower incident management, escalation, remediation and retention. Once content is developed, we assist in the end-to-end training of operators and analysts inclusive of drills and tabletop exercises to ensure the content suite achieves its required objectives.

CYBER SECURITY EXPERTISE

Building a bridge between the physical security function and corporate IT security practices requires expertise across several areas of implementation. Our CISSP-certified IT security team members will interface with your IT organization to ensure the integrity of the Command Center solution and refine alerting and collaboration protocols to address key areas of overall corporate IT asset protection and breach mitigation.

PROTOCOL DATA MANAGEMENT

Concurrent with the development of operational content, our team of architects will empower a robust and agile data management platform to house and distribute all operational business rules, policies, procedures and work flows. This data repository will be structured to allow for "point and click" access to all actions that operators or analysts will use to perform their duties.

CLOUD SERVICES MANAGEMENT

Where required, Guidepost Solutions assists clients in the outsourcing of data storage and delivery of advanced computing services through cloud providers inclusive of Microsoft Azure and AWS. We manage the interface with the client's IT organization to ensure compliance with all cloud service security and service level requirements.

MANAGED SERVICES

Guidepost Solutions supports Command Center environments through our in-house Managed Services division which specializes in the health monitoring, version control and triage/service ticket management for complex, multi-platform solutions. This technical expertise is supplemented with ongoing operational protocol/data management support to ensure the client's protocols and business rules stay current with evolving threats and regulatory requirements.

Guidepost

Matthew V. Wharton

President, Security & Technology Consulting Group

Mr. Wharton serves as president for the Guidepost Solutions Security and Technology Consulting group and oversees its core services; cyber security, system design and project management, global command and control centers, security assessments and managed services. He is a career security professional with more than 30 years of experience leading security consulting and integration firms. He can be contacted at mwharton@guidepostsolutions.com

ABOUT GUIDEPOST SOLUTIONS LLC

In a world where change is certain, experience is the best protection. Guidepost Solutions offers global investigations, compliance and monitoring, and security and technology consulting solutions for clients in a wide range of industries. Our expert team provides leadership and strategic guidance to address critical client needs across the globe. With headquarters in New York, Guidepost Solutions maintains offices in key markets including Chicago; Dallas; Honolulu; London; Los Angeles; Oakland; Palm Beach; Sacramento; San Francisco; Seattle; Singapore; and Washington, D.C.; and has resources across the globe.

Experience guides us. Solutions define us.