Covenant
security solutions

The Integration of SOPHIA with the People, Process, and Technology

The Convergence and collaboration of perfect arguments

February 15, 2016

Covenant Security Solutions, Inc.
Danyetta Fleming Magana
President/Founder
Covenant Security Solutions, Inc.

SHA-256 0dc9795c428e31ef8149403a345db5ad7fb0d477d8ea225bd1a1ecea20bfff66

SHA-512
e5e761b3ac069f41bad847ec8894ee4e3b340692735230ea0c9eb8edacca5c7e7592488a6d2cdbe27
8cf1eaa0947b33295fa315676830108734ae9b3bae54d0d

SHA-384
8a0d3b2a03cab8812d90809fc93cbe7ba03f09c06f1911e9efef906d24b9fcbe7651cda6f049815fee
cb85afd119e9cd

Abstract

The security industry continues to develop advanced hardware and software security tools as single point solution technologies in an attempt to protect sensitive assets. Specific known cyber-security threats such as viruses and worms adversely affect an organization's information and information systems. Advanced security devices working in collaboration with many other technologies often offer a "defensive layered approach" that is referred to as defense in depth and defense in breath. Nevertheless, many companies are increasingly coming under attack by new cyber-attacks at alarming rates. The substantial growth of the internet and the extraordinary contribution of intelligent devices connected to our corporate networks have changed the way a majority of businesses fundamentally conduct day to day operations to complete critical business tasks. Many traditional functions in the physical world have become morphed in cyber-space using technology. In return, this has created scores of opportunities for the bad guys to commit traditional crimes in cyber space. This paper examines strategies to improve an organization's overall cyber-security posture and manage risk by converging physical and cyber security by collecting real time data on the organizations people, systems, and processes using Covenant Security Solutions Security Operations and Intelligence Analysis (SOPHIA). The goal is to be proactive with regards to the detection of threats and implement processes to mitigate the threats. This paper first examines the importance of protecting a company's assets from a business perspective. Then we emphasize the need for understanding

risk of the people, process, and technology, as opposed to only a security tool (system). We finish our discussion with giving an overview of SOPHIA, what it does and how to integrate it within the organization.

Introduction

Technology accelerates a company's business processes. Most businesses cannot survive without technology. The market is making it increasingly challenging for businesses to solve business problems without technology solutions to handle big data, mobility, and software defined networks[1]. These technology demands create risk; dare we say challenges for the data a business must protect. To remain competitive and relevant in today's society, the majority of companies leverage the power of social media. The best way to attract customers and sell your product is online. [2] Dr. Dwayne Hodges, in his TEDx talk, echoed retired 4-Star General Keith Alexander and former Director for the National Security Agency and head of United States Cyber Command, when he stated in his speech "between Facebook and virtual worlds they represent over a billion users, if this were a country it would be the third largest country in the world - China, India, and then Facebook". In an increasingly technology dependent world where businesses use technology to perform day to day tasks to accomplish end state business goals, the attack surface gets bigger, more attack vectors blossom, and what a business gains in convenience they lose in security[3]. The disruption of services from technology could lead to a

[1] http://responseit.ca/our-blog/critical-areas-of-focus-for-it-leaders/
[2] https://www.youtube.com/watch?v=X9jSFRiJX_k
[3] https://www.secureworks.com/blog/general-apt-attacks-new-defenses-against-advanced-malware

disaster for a business and have devastating consequences. What a Chief Executive Officer and his/her senior management care most about is: how and when a disruption of any time sensitive critical business function will occur, what the damage will cost the company in momentary value or reputation, and how long it will take to get that function back up and running again to prevent them from losing more money. They generally do care about other items such as employee safety and regulatory requirements of privacy of data. We just used less than 50 words to describe any disruption on technology that could range from a cyber-attack, accidental technology failure, intentional insider threat, or a natural disaster. The consequences are all the same and we never once mention malware, server, hardware, or any tech-talk. Industry jargon isn't necessary when speaking to a CEO or senior management unless they ask a specific question. You really don't have to be a subject matter expert in technology when you are trying to understand the strategies for how to lay the ground work for what is referred to as a business impact analysis (Tipton, 2007). A critical error for many cyber-security experts is to find the new tool on the market, or go with the "internet recommendation" on Google, and apply it to the problem. This is not the way to go. Understanding the security triad that includes confidentiality, Integrity, and availability for each asset that needs to be protected is implied, but is not covered in detail in this paper. Instead, what we do not focus on is looking for technology point solutions and defense in depth with technical, administrative, and physical controls; however, we place greater emphasis towards improving the companies culture using a risk framework posture by looking at the people and processes, and by identifying what, why, where, how, and when they interact with the physical and cyber-domain within the organization. This includes, but is not limited to, using security tools and trying to identify anomalies within those systems and process. In this paper we will illustrate the importance of examining risk management and threat identification by examining the potential threats and vulnerabilities that exist on the *people, process, and technology,* as they apply to the three pillars of security: confidentiality, integrity and availability (Tipton, 2007). Gordon (2015) stated *"a well-structured enterprise wide information security program must ensure that the core concepts of availability, integrity, confidentiality, are supported by adequate security controls design to mitigate or reduce the risk of loss, disruption, or corruption of information" (p.7)* It is critical that organizations take a granular look at each leg (people, process, and technology) and sub-processes within those legs and evaluate them separately using risk management techniques on a security triangle to determine the true impact of a disruption to process, people, and technology. It is important to examine any relationships and dependencies that exist, where the loss of one component could create a disruption to the other two components. Understanding events and unusual occurrences is a result of cyber security and physical security baselining of people, system and processes within an organization. This is illustrated in figure 1 of page 7 at a holistic level. The evaluation of all three is so critical that Tipton (2007) actually calls this a *"winning combination"* (p.389). We agree with Harold Tipton and maintain that many organizations depend on layer 3 security devices too much. In addition, many organizations are too dependent on security technology devices to resolve their cyber-security issues to the exclusion of the human and processes component of the triad. Technology point solutions do not work. You cannot protect today's threats with yesterday's programs, processes, training, and policies. Using technology alone is a practically impossible and cyber-security protection requires the convergence of physical security and cyber-security. Three critical steps will help secure the integrity of business data and processes:

- Preparation

- Detection
- Protection

These protective measures involve identification of assets, real time monitoring, threat modeling, and methods of resiliency and most importantly, the customization of cyber security measures. One major reason why technology by itself does not work is because technology by itself is often not the problem. For example, many statistical reports will report a high number of "hardware or software failure" as the cause and leave the cause of the disruption and downtime in the category as "IT failure". We find this to be misleading and off base when many vendors have the ability to provide metrics such as Mean Time to Failures (MTTF), Mean Time to Repair (MTTR) and most importantly businesses can have a sound SLA describing what the vendor can and cannot do during a disaster to support the business if their product is not working for any reason. What is more common is that businesses do not have a solid disaster recovery plan or service level agreement with a vendor. As a result, the businesses end up with cheap equipment that is not configured or installed correctly. The absence of MTTF, MTTR with SLA is never a good thing. What we are getting at is when these things are not addressed, this is "human error" not an "IT failure". Many IT devices from an IT vendor with an SLA that have good people and processes will endure a storm. Our next illustration defending IT is about encryption. It is very difficult to take an enormous semi prime number in the finite field and try to figure out the two original primes with today's computer processing power. When I say large, I am talking about a stack of paper 17,000 pages. The larger the semi prime, the harder it is to compute the original primes. To be candid, algorithms such as RSA 2048, named after its inventers, Rivest-Shamir-Adleman may be nearly impossible to break and the work factor and cost is so high, that unless you have tons of gold and the world's best secrets, you are more than likely not worth hacker's time and effort. He would not be able to pull it off using traditional crypto analysis methods such as brute force and dictionary attacks. However, they are typically not going after a key or one station for a piece of data. With these attacks, the attackers want all the data and all the stations. Therefore, what would be easier is for the attacker to try to exploit a poorly designed or implemented crypt system, exploit the use of poor password, account management system, or perhaps exploit the people that work for the company. This was the case when RSA, a top security company that sells security for more than 40 million businesses was attacked. [4] RSA is believed by many to be one of the finest security companies in the world and produces some great security products; however, people are your weakest link to security. The fact that RSA provides SecureID two factor authentication products along with the manner of the attack, suggest that there was a lot of social engineering in the attack that focused on the "people and processes" of RSA, and not the technology. Although, some security experts doubt this was a sophisticated attack[5], it is clear that attackers felt confident they could send a phishing email with a stimulating attachment [6] with high hopes inquisitive users would click it. This approach is more ideal than performing a brute force attack on a password for one account. It is important to note that although the attacker hacked RSA, their golden nugget was RSA customers. Understanding who the attacker is, what they want, how they want it, and mapping this model to the people, technology, and processes of your customers, is a leap forward in cyber-security that will help you build better protection for your processes. This is what Covenant Security Solutions aims to do. *See figure 1 below*

[4] http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/?_r=0
[5] http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/?_r=0
[6] http://bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/?_r=0

SOPHIA and People, Process and Technology

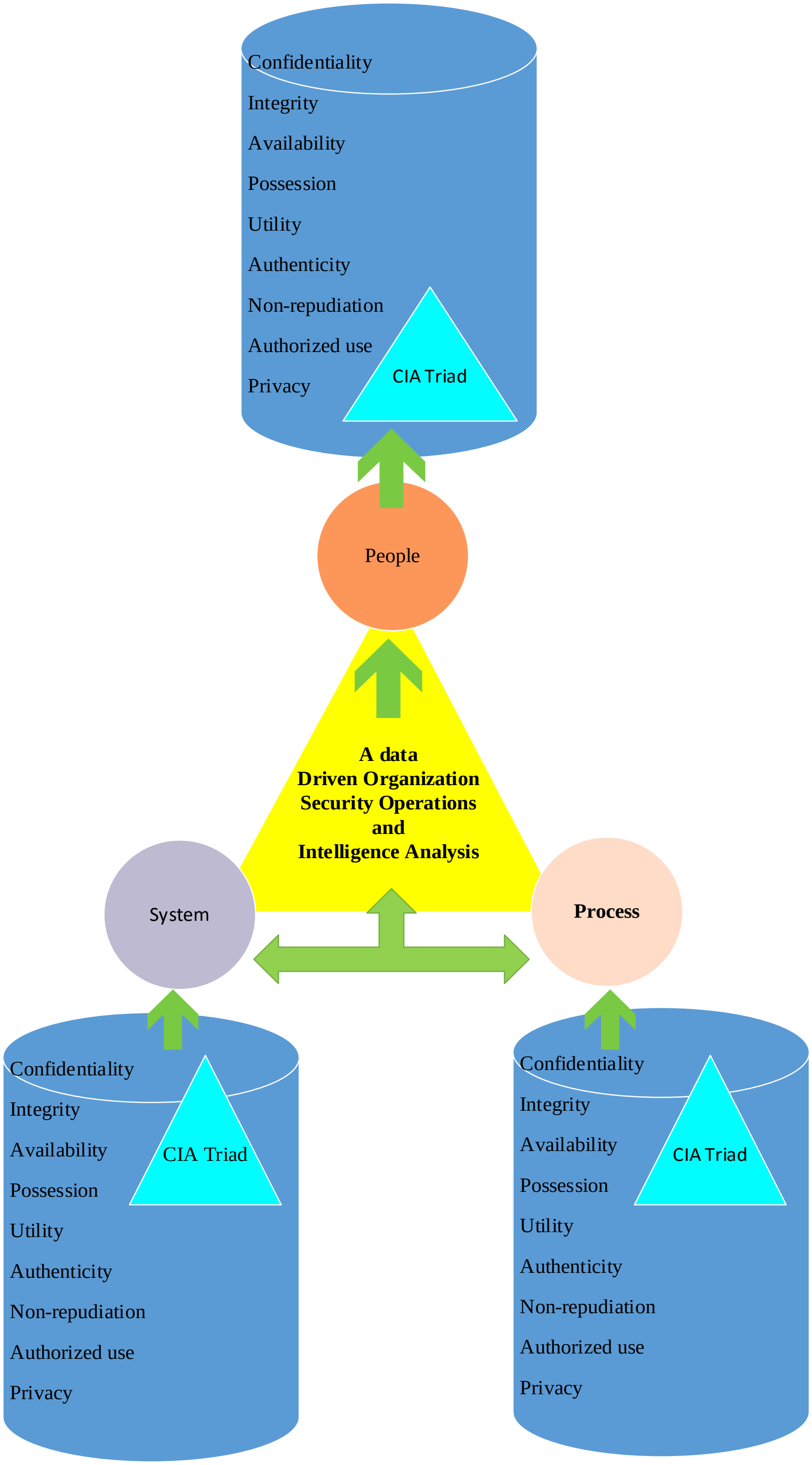


Figure 1

People, Process, Technology, the CIA Triad, and SOPHIA

Tipton (2011) suggests that there are nine core principles of the foundation framework to run security operations. Risk management is an ongoing process; whereas risk analysis has a start and stop point. We maintain that the nine core principles listed below should be applied to the people, process, and technology using SOPHIA. This is our version of the *"winning combination"*. The goal is to develop a tool to manage ongoing risk within an organization and conduct risk analysis on threats identified to mitigate the impact (Tipton, 2007). The Center of gravity for the following core principles are confidentiality, integrity, and availability. These three principles serve as the baseline for measurement for how a time sensitive or critical process, service, people, and technology, might be adversely affected. The cause is not discussed for the purpose of this paper. Rather, we recommend that the following nine core principles in the Information System Security Management Professional guide be evaluated for every leg using a *service oriented architecture* risk management based approach as illustrated in *figure 1*. They are as follows:

- Confidentiality
- Integrity
- Availability
- Possession
- Utility
- Authenticity
- Non-repudiation
- Authorized use
- Privacy

People

It is often though that the equipment is the most important part of an organization's IT security. However, people are the most important asset in an organization. The equipment is only as good as the people and processes that utilize them. A sever, computer, or any software is just lines of code that are predictable in nature and operate in black and white with a set of instructions (code). In the absence of corruption, manipulation of the code, or the code just not aligning with the new environment, the system should work as predicted. On the other hand, when subjected to human error or manipulation, an action as simple as downloading freeware from the internet will reduce the predictability of the operating system. It is possible that the antivirus program or intrusion detection program will be unable to respond appropriately. It is more likely that it will be an employee that will accidently or purposely engage in some activity that will sabotage the time sensitive critical server. There is also a possibility that it could be a malicious cyber-hacker from the outside, or even a natural disaster. Regardless of the cause, the consequence is the same and you need people to be well trained and experienced. Training and experience are more effective when combined with employee value such as ethics awareness. People are an organization's first line of defense in protecting the organization for many reasons (Tipton, 2007). Employees that are trained and informed on processes and technology and the threats associated with them, are less likely to make a mistake or break company policy. Holding people accountable for processes and ensuring they are trained on those processes will help to ensure constant communication between members of management and the employees. It also ensures that processes and technologies are being used in a manner that is consistent with cooperate security policy, allowing for the immediate investigation of incidents. This requires regular monitoring and reporting on the status of events in both the physical and cyber-spaces.

These are two features that Covenant Security Solutions offers with our Security Operations and Intelligence Analysis (SOPHIA) tool that allows management to stay current in real time with the security posture of the organization. Our alert generation tool with SOPHIA and our Covenant Awareness Training, and Education Resource tool and training program that can be integrated as a corrective measure mapped to people and processes through the matrix library via SOPHIA, assists our clients with placing the focus back on its employees to enforce the required education, training, and computing environment specific training for each process. For example, if you wanted to consider having a tutorial video in Covenant Awareness Training, and Education Resource tool that tells users how to respond to phishing attempts and block spam users, this would be accessible through SOPHIA simultaneously after reporting the phishing attempt as a corrective action for all users to be alerted of suspect phishing email attempt on company employees.

Process

Processes should be looked at from a holistic perspective within an organization's cyber-security policy and should include guidelines, best practices, and step by step procedures. The organization's that are serious about security will look at the processes and have a specific system policy for processes or systems that could create disruption. For example, the IoT, and many companies adopting the Bring your own device (BYOD) to work concept. This concept may save the company a lot of money, but it also creates a host of new threats to the organization. As a result, best practice suggests a system specific policy that addresses protocol on specific areas such as how to handle corporate email and data. Something as simple as using a mobile device manager (MDM) may seem like a good idea, but doing so just adds a new security risk to the organization's Enterprise Security Network resulting in some authentication issues. This is not to say that these things can't be done, because they can. This is to raise the point that the CIA triad must be applied to other system(s), people(s), and process(s) in a deliberate manner that supports the corporate security policy. This is referred to as process security (Triton, 2007). Every organization has unique applications and processes. The reliance on technology and IP communication devices in most organizations makes it necessary to scrutinize the system, people and processes that use these special technologies. Cyber-Security can be achieved with service-oriented architecture by applying the CIA triad on each of the processes. The ability to understand the sensitive nature of an organization's programs, services, applications, processes, and software and apply it to the CIA triad, allows the organization to determine a threat source, determine what is normal and then determine how to respond. The security triangle dictates that all systems, people, and processes are mapped separately to the CIA triad (Figure 1) to identify any threats, risk, or vulnerabilities. Each leg of the CIA triad must be mapped to each leg of the security triangle with the appropriate cyber-security controls required to address those threats. Figure 2 extends beyond figure 1 and covers others areas of security (Tipton, 2011). We believe these are robust models for evaluation on the people, process, and technology.

Technology

It is a critical error for any organization to consider technology as a silver bullet solution. In Madiant APT1 report, it was reported that scores of data were stolen from over 140 organizations using social engineering statics. These were passive attacks on people and processes. The attackers used various tactics which may have been initiated 1-3 steps prior to even touching the Vitim computer or network[7]. This is actually similar to the method that is

[7] Madiant Advance Persistent Threat PT 1 Report http://intelreport.mandiant.com/

used by many professionals when doing penetration testing by credited ethical hacking. Dell Secure networks calls this organized methodology the "kill chain".[8] The APT1 report shows an attack cycle of trained, skilled, and patient attackers using a variety of methods where organizations that may have used technology single point solutions for a line of defense may have learned it was impractical for and APT. Technology itself is strong, but does not hold well for the insider threat. Employees with nefarious intent and no supervision can do the greatest damage because they have the physical and logistical access control. However, using SOPHIA to enforce security activities such as least privileges and separation of duties while you collect data from the people, process, and technology will help mitigate the threat. This is a great first step, and organizations should go a step further to evaluate systems for additional security requirements and protection using a baseline and defense in depth on the people, technology, and operations. Tipton, (p.338, 2011) in his Information System Security Architecture Professional guide stated "to show what services are being provided and how they are being secured, a common security tactic for security professionals is to use defense depth (DiD) on technology by applying layers technical, physical, and administrative controls on technology." This is a good practice but only part of the battle. Covenant Security Solutions recommends applying the DiD strategy on the people and the process, an area that cannot be overlooked by security professionals and is easily achieved by applying controls such as service *oriented architect* for the processes and *education and training* for the people. The risk management approach of baselining systems (Technology) is identified using Engineering Principles for Information Technology Applied to Systems (NIST, 2004).

[8] https://www.secureworks.com/blog/general-apt-attacks-new-defenses-against-advanced-malware

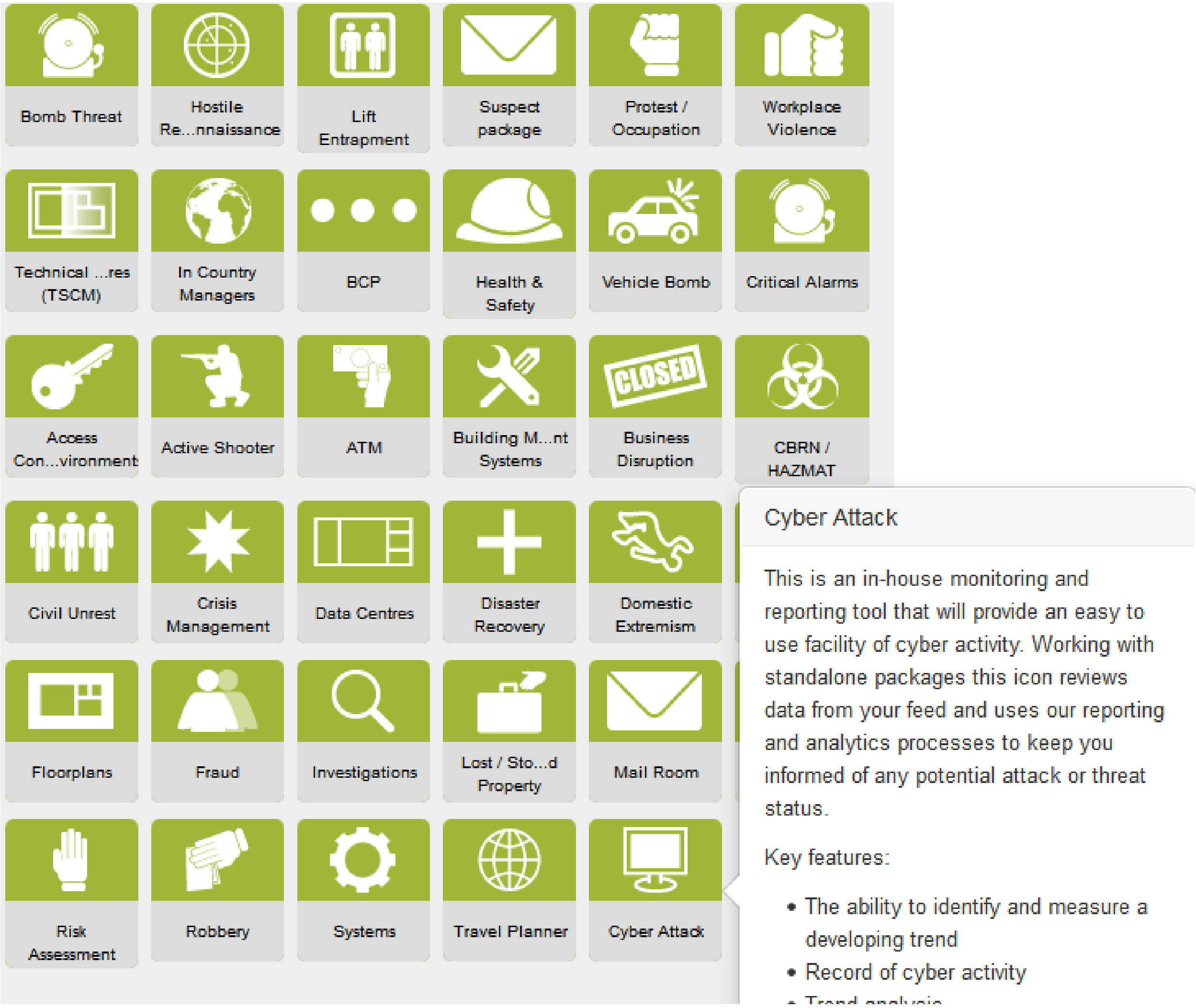
Data Driven Organization

Cyber-security and physical security within an organization should be driven by knowledge, and knowledge comes from data. Many organizations across different sectors lack the capability to track real time data and translate that data to useful information the organizations can use for the incident response and handling life cycle process, especially in a proactive manner. This is often because organizations are overwhelmed with the collection of too much data or collecting the wrong data and once they have the data, they do not know what to do with it. Data is derived from various sources, including security tools and data generated by the people and processes of the organization. The translation of data into intelligent information is a process called data analytics.

Security Operations and Intelligence Analysis (SOPHIA)

Covenant Security Solutions helps our clients by converging cyber-security and physical security data using our Security Operations and Intelligence Analysis (SOPHIA) tool and making customized based decisions on what data to trap, how to turn that data into information, how to transform that data into knowledge, and make better decisions from this knowledge. In a world of big data, SOPHIA works like a data tactical mart that collects the right data from various sources within an organization and turns it into intelligence. The theory behind this paradigm is to collect information and turn around intelligence to prevent an attack by collaborating with real time physical processes and cyber-assets. At the same time, we look for anomalies within the systems, people, and processes and generate alerts for human intervention. There is a complex set of relationships that exist and frequently change in data between systems, process, and people. Organizations should be proactive in the detection and risk reduction of threats, as opposed to being reactive and responding after the fact. If organizations operate in real time and manage all the constant changing patterns with the people, processes, and systems they may have a better understanding of how change in one area impacts other areas. SOPHIA closes that gap and works with various tools to offer a more proactive and collaborative security program that converges physical and cyber-security programs that account for *defense in depth* (Tipton, 2011). This is accomplished using risk profiles and monitoring specific areas of interest.

SOPHIA offers a menu of modular services (see figure 1) to capture data, monitor the organizations information and serve as a central nervous system with predefined tasks of what data to collect, where to collect this data, and what to do with the data once it has been collected. This paradigm of security using SOPHIA gives the organization more efficiency and reduces ambiguity with users. Therefore, maximum stakeholders and actors can use SPOPHIA. Security does not like complexity. IT users must be familiar with security in both the physical and cyber space realms to effectively protect the organization’s assets and time sensitive business processes. Furthermore, senior management must foster a culture that is receptive to operating as a data driven organization. This will require that all levels of the organization are consistently collecting and analyzing data from various sources including technology sensors, physical places, and humans. Organizations must be prepared to collect data and analyze data in a manner that allows for a conscious and deliberate enterprise security system.



Cyber Attack

This is an in-house monitoring and reporting tool that will provide an easy to use facility of cyber activity. Working with standalone packages this icon reviews data from your feed and uses our reporting and analytics processes to keep you informed of any potential attack or threat status.

Key features:

- The ability to identify and measure a developing trend
- Record of cyber activity
- Trend analysis

Figure 2- Expansion Modules

An inability to accurately collect and analyze data can result in an organization being reactive instead of proactive, which quickly places them on the offensive side. For organizations to mitigate and prevent attacks they need to be in the preparation, detection, and protection phase of the cyber-security frame work for incident response and handling[9]. This will place the

[9] Cyber Security Framework for Critical Infrastructure with categories, sub-categories, and informative references http://www.nist.gov/cyberframework/csf_reference_tool.cfm

organization in the position to anticipate threats, plan risk, establish policy, and have a corrective and recovery plan in place when threats do occur.

Covenant Security Solutions works with our clients to create custom security solutions to meet specific needs to mitigate the risk of threat and provide a process to deliver maxim protection for our client's information, systems, people, and processes. Our Security Operations and Intelligence Analysis (SOPHIA) software tool aggregates the appropriate data from the organization's physical security and cyber-security domain and centralizes the data for intelligent decisions to be made using a real time alerting system. The following is a sample of what some of the capabilities of SOPHIA are:

- Operating as a live notification tool to executive management during any incident
- Supporting fire evacuation planning and auditing
- Rolling stock inspections/security checks
- Contains intelligent station, depot and premises plans
- Sustains Health and Safety integration and compliance
- Delivers 'real time' incident flow management
- Assists in the prevention of hostile reconnaissance
- Informs trend and gap analysis
- Provides station/depot search plans
- Facilitates the management of protest and occupation incidents
- Provide control room solutions
- Guides Business Continuity Planning
- Assist in the integration of Access Control and CCTV
- Oversees the integration of fire control management

- Life Safety investigations
- Travel management
- Audit program for all events
- Smart alerting of trends and gap analysis
- Integrating with other platforms
- SOPHIA DEMO [10]

Security professionals will say there are no silver bullets in cyber-security; although many vendors and sales reps will commonly mispresent their security tools as the end all- be all to their security problems. Too many security tools can hurt an organization and not enough can hurt. Organizations must have a balance to have effective security with technology. This is referred to as redundancy to secure single points of failures and always aligns to the defense in dept. strategy (Tipton, 2011). This same model is applied and monitored for the people and process with SOPHIA.

At a minimum, using SPOHIA allows our clients to collect information from these areas on the people, system, and process, anticipate risk and detect threats against people, systems, and processes while following established cyber-security policies. This is the core concept of security operations of enterprise security management.

Conclusion

SOPHIA is a flexible and fluid life cycle approach with sectional capabilities to monitor the people, system, and process to alert key personnel, including technical staff, of precursors in the physical and cyber-security domains to assist them taking proactive measures. This includes

[10] https://www.secureworks.com/blog/general-apt-attacks-new-defenses-against-advanced-malware

providing corrective and recovery action, escalation actions, and restoration of business functions in accordance with the organization's cyber-security policy. The end goal is to help mitigate threats and protect assets, prevent disruptions of time sensitive business functions that would adversely impact a company's revenue, market shares, reputation, customer base, loss in future sales, and further result in any violation of regulatory and administrative laws leading to fines. SOPHIA is designed to work hand and hand with several security tools and polices including, the organization's cyber-security policy, disaster recovery plan, incident response plan, active shooter drill, System Admin Intrusion Detection System, System Admin Active Directory Windows Scheduler and other security tools. The goal of SOPHIA is to understand the normal environment for the organization's people, system, and processes and alert the organization when there is a health concern and send the appropriate organization actors into triage immediately to mitigate and prevent damage and keep all necessary stakeholders informed while following predefined steps.

References

Gordon, A. (2015). Official (ISC) 2 Guide to Certified Information System Security Professional Common Body Knowledge Fourth Edition: Taylor and Francis

Tipton, H. (2007). Information Security Handbook Six Edition: Taylor and Francis

Tipton, H. (2011). Official (ISC) 2 Guide to Information System Security Architecture Professional Common Body Knowledge: Taylor and Francis

Tipton, H. (2011). Official (ISC) 2 Guide to Information System Security Management Professional Common Body Knowledge: Taylor and Francis

NIST Special Publication 800-27 (2004) Engineering Principles for Information Technology Security (A Baseline for Achieving Security) Revision A