

Safeguarding the Enterprise through SIEM and Security Analytics (SA)

Contents

Overview:	1
The Logon Process	2
What is required to protect our enterprise and society?	3
How should an enterprise implement their security management system?	5
Security Analytics	6
Creating a Chief Information Security Officer (CISO) position.....	8
Defining the needs and responsibilities of an Enterprise Security System	9
Defining Security and Technology threats and assigning Responsibilities	10
Information Security Responsibilities	10
Approaches to developing an Enterprise Security System	10
Threat based approach to implementing Enterprise Security Management	11
Risk based approach to Enterprise Security Management	11
Cloud Risk and Security Protection	12

Overview:

Ever since the new era of Information technology (IT) was introduced in the 1960's (remember IBM 360 Mainframes) there has always been a concern about safeguarding information from unauthorized intrusion and the loss of critical data.

At first, physical security (now referred to as a Physical Access System – PAS) was employed to stop unauthorized people from entering the data center where the computers were housed, and for a long time physical security proved to be sufficient. But then Information technology was expanded to include Communications between the computer and the end-user and physical security no-long proved sufficient. It



Figure 1: Tom Bronack, author of White Paper – bronackt@gmail.com

was necessary to create a new type of security system that would be used to control who had access to programs (referred to as Applications with a short hand name of Applid's to identify them) and from which locations. The concept grew into a three tiered Access Control System based on Applid, Userid, Password, commonly referred to your logon.

The Logon Process

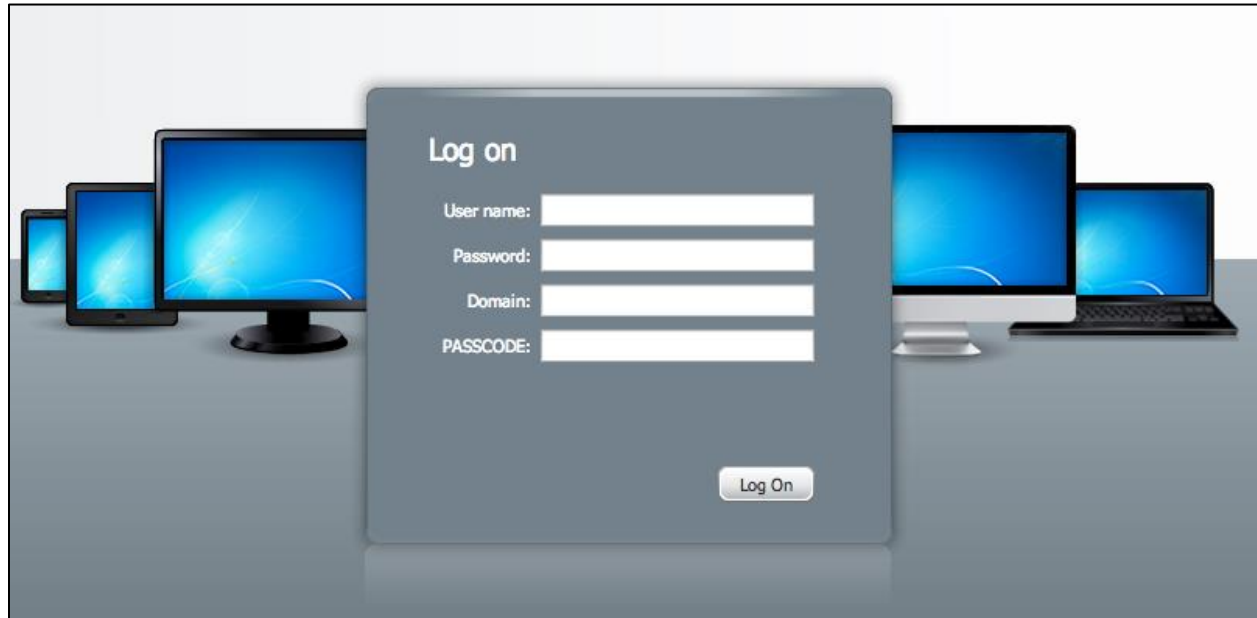


Figure 2: The Logon Function of Applid, Userid, Password (with a Domain Passcode included)

Again, this approach satisfied most requirements to safeguard information and locations, but times changed and people got smarter in the use of computers. Eventually, Hackers started to get curious about what was hidden in the mainframe that they could play with and an entire revolution began with “**Black Hats**” trying to gain unauthorized access and “**White Hats**” trying to block their attempts. Now, the entire computer field is like the “Wild Wild West” because of the World Wide Web (WWW) and the Internet.

People can stay hidden behind walls and communicate over telephone lines and satellites to computers all over the world. Some of these people are attempting criminal activities to steal a person's identity or access their bank account, with many succeeding. Even worse, are the State Sponsored Cyber Attacks aimed at stealing intellectual property, military secrets, or interfering with the infrastructure of other countries. These attacks could lead to a cyber-war that could end with everybody losing computer services, control over the infrastructure, and suffering a generational impact that would devastate society. We could all be living in the 19th century again and who wants that – who could even do the things people did then to survive. We have all grown too accustomed to using computers and we may have lost our ability to survive without them.

Now you have an idea of why information security is so important. The loss of computers would have a dramatic impact on society and drive people back to a time they are not prepared to live in again.

What is required to protect our enterprise and society?

Obviously, protecting our computerized world is a prime directive for society in order to continue to move forward. Could you imagine a world without Google, or Facebook, or email and Instant Messages? Heck, people would have to talk to each other again face-to-face and everything presently controlled with the help of a computer would have to be controlled and serviced manually.

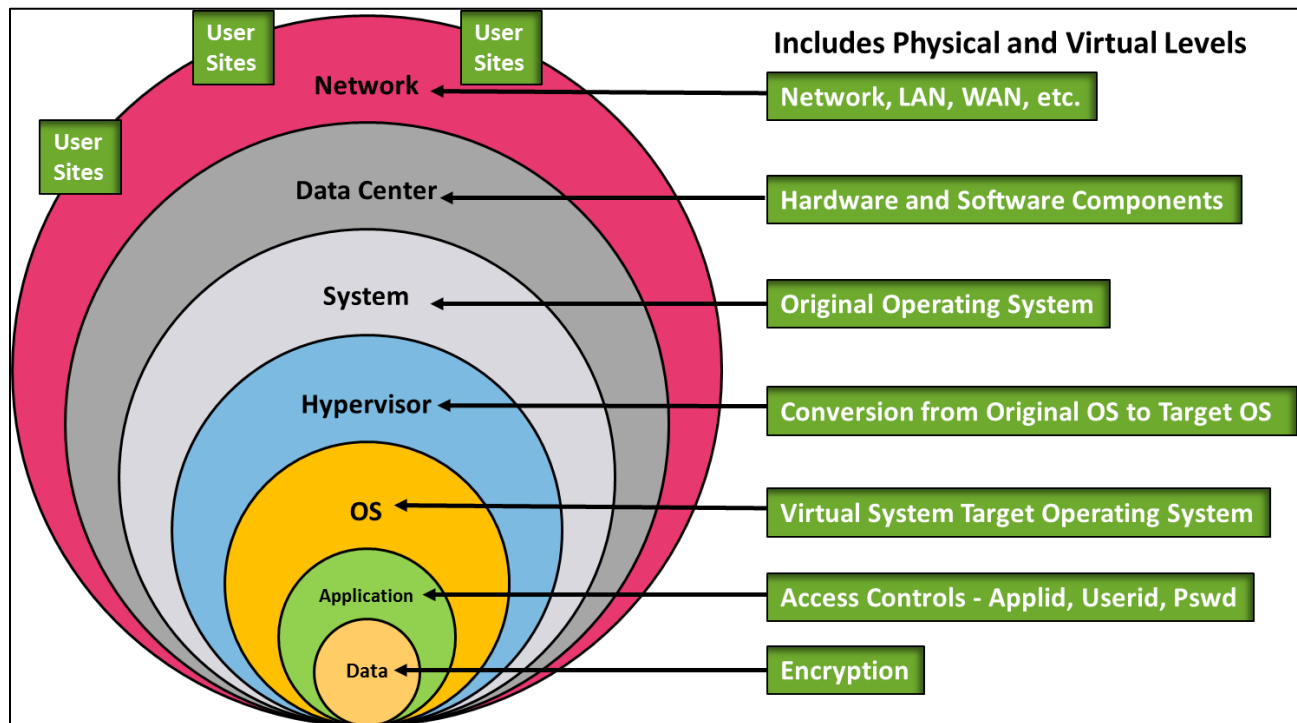


Figure 3: Protecting Enterprise Data from outside intrusion with layers of protection

Past attempts at computer security have provided a foundation to move forward and protect our computerized resources, but it only takes one really big virus to infect thousands of computers so we have to be vigilant and constantly aware of “**New Day**” threats (i.e., those threats that have not been experienced before). The sheer volume of computerized traffic has surpassed man’s ability to monitor and mitigate threats already, so tools are now being used to safeguard against threats. These tools include:

1. Intrusion Detection (who is entering the system and from where)
2. Firewalls (are they allowed entry and access to requested resources)
3. Anti-Virus and Anti-Malware systems
4. Security Event Management (Access Logs)
5. Security Information Management (Data Usage Logs)
6. Security Event Information Management (SIEM)
7. Security Analytics
8. Role Based Access Control (RBAC) systems and Entitlements

9. Threat Management
10. Risk Management
11. GRC – Governance, Regulations, and Compliance
12. Disaster and Business Recovery Management
13. Enterprise Resiliency
14. Corporate Compliance

The list can go on forever, but we are now at a point where we can detect, record, and track security events from the user end-point, through the network, to the computer. Unfortunately, we are not humanly able to analyze the vast amounts of data being presented. We need help doing that in the form of the SIEM and Security Analytics approach, combined with Security Visualization.

Ideally, we could use a Security Operations Center (SOC) that can monitor and display all security related events through dashboard screens that are color coded and equipped with thresholds and alarms to alert us of unauthorized activity or potential threats. This is in process today with improvements constantly being made to include machine learning and artificial intelligence, so that lessons learned can be instantly applied with the goal of detecting and mitigating security and technology threats in near real-time. This technique is called Continuous Diagnostic and Mitigation (CDM) and it is being employed by private and public sector enterprises as we speak.




Figure 4: Security Operations Center (SOC)

The technology growth in the security field is spectacular, but it still needs input from man in order to know who is using the system and what their authorization is, based on their job title and functional responsibilities (**Role Based Access Control**). RBAC is associated with the resources (both physical and logical) that an individual is **Entitled** to use to satisfy their current functional responsibilities. If they leave the organization, or change functional responsibilities, then their level of entitlement is changed to reflect their new needs, so RBAC and Entitlements are a key part of security, but how about a person's behavior. We all know people who have suffered life altering experiences, even disgruntled employees who are unhappy with their job, the company, or management. Sometimes these people can inflict worse harm than a Hacker and precautions should be included in your security management system that takes behavior into account, otherwise you may have a saboteur or active shooter situation to contend with.

As you can see, implementing an enterprise-wide security management system can be a very difficult task, but one whose goals must be met in order to continue business in today's world. You can also derive a two prong approach to security management, one based on technology improvements and the other based on personnel management. Although technology and personnel are considered different disciplines, it is pretty hard to assign security controls that allow people access to what they need if you don't know their entitlements, as defined in their functional responsibilities. Hence, implementing a security management system requires an enterprise to have personnel and technology work together to achieve successful results. Of course, Legal, Risk Management, Compliance, and Auditing must all have seats at the table to define your vulnerabilities, rate them on criticality, and prioritize their resolution.

The goal of a Continuous Diagnostic and Mitigation Dashboard Project is to:

- **Provide** a **Continuous Diagnostic and Mitigation (CDM) Dashboard System** that communicates cyber-crime and technology threats and Error Detection information between the Enterprise Security Operation Center (SOC) and the end user **through these five steps**:

- 
- **Collect** - via a set of sensors and collection devices (Network based Firewalls, Intrusion Detectors, Access Rules and Controls, and SIEM (Security Information Event Management)) and tools collectively known as the Network Dashboard;
 - **Process** - the collected information is compare with Sensor and Scanner Rules to determines if security policies have been violated and are also used to identify risk information and filter non-threat information,
 - **Provide** - a Summary Reports to Enterprise Management and distribute the report to end points and department heads on a periodic basis (at least every 72 hours), or on-demand;
 - **Analyze** - **Threat and Defect information** to provide the department heads and end points with a **Threat Report** consisting of sorted **"Worse Case" Threats by priority of impact**;
 - **Use to** - **coordinate a Threat Response** by all Departments / Agencies, in **"Worse Case"** order, so that all pertinent information needed to address the **"Root Cause"** of the threat and reduce / eliminate the **"Threat Impact"** can be acted on.

- The Enterprise must define **Entitlements** associated with Personnel Job Functions, so that a **Role Based Access Control (RBAC)** security system can be implemented.

Figure 5: The Goals of a Continuous Diagnostic and Mitigation (CDM) Dashboard System

How should an enterprise implement their security management system?

Like any other major project, there are specific phases that must be achieved in order to implement the best security management system for your enterprise. The basic phases are:

1. **Needs Analysis – to fully define all of your enterprise’s protection and compliance needs, including:**
 - a. Physical and Logical needs (i.e., Physical Access System, Logical Access System);
 - b. Critical Systems and Resources;
 - c. Network, Computer, and storage management considerations, both physical and virtual;
 - d. Enterprise Resiliency and Corporate Certification;
 - e. Risk Management and Insurance;
 - f. Business Continuity Management; and,
 - g. Human Resource Management and Information Technology.
2. **Architectural Diagrams**
 - a. Physical Environment;
 - b. Logical Environment;
 - c. Present vs. Future requirements.
3. **Engineering Diagrams**
 - a. Present Equipment and Infrastructure;
 - b. Future Equipment and Infrastructure Requirements;
 - c. Roadmap to move from present to future environment.
4. **Request for Proposal (RFP) issuance**
 - a. Define the needs for assistance in a Request For Proposal (RFP);
 - b. Locate qualified vendors who can provide the needed services and products;

- c. Forward the RFP to selected vendors and coordinate their responses;
 - d. Select vendors to assist in accomplishing goals;
 - e. Initiate the project by creating a universal Project Plan.
- 5. Execute the Project Plan and monitor status**
- a. Kick-off project;
 - b. Monitor and report on status of project;
 - c. Make necessary project adjustments;
 - d. Accomplish Project Goals.
- 6. Integrate Project Deliverables within everyday functions**
- a. Completely document project results and provide needed manuals;
 - b. Along with Awareness Programs from project conception through implementation, deliver Documentation and Training to personnel as needed;
 - c. Conduct Training Upgrades as the environment evolves;
 - d. Ensure that personnel job functions are included in new system, so that events are tracked and recorded to insure adherence to Standards and Procedures;
 - e. Conduct periodic reviews and Post Mortems to gain Lessons Learned and develop Teaching Events as needed;
 - f. Integrate Support and Maintenance to resolve encountered problems;
 - g. Integrate Change and Release Management to implement changes and enhancements to the system in a controlled manner through Version and Release Management.

This six-step process should get you on your way, but every enterprise is different and modifications may be needed to best suit your needs.

Security Analytics

Security Analytics (SA) has evolved over time as described below.

1. **Initially** security management was concerned with perimeter defense and relied on Physical Security in the form of Guards, Locked Doors with Key Passes, and fenced off areas that evolved into concentric circles around critical resources. These defenses were based on Security Event Management (SEM) for area access categories that were prevalent at the time.
2. **The second phase** of security management was based on Security Information Management (SIM) and incorporated logical precautions as dictated by Compliance Laws and Regulations. These requirements were initially developed by the enterprise, but later became government and industry requirements. Over time, the volume and time requirements associated with compliance resulted in the need for a better way of detecting and responding to security events that impacted information.
3. **The current phase** of security management incorporates methods for visualizing security events and information impacts and is named Security Incident Event Management (SIEM), which is a rapid method for examining security logs to detect and repair known security incidents, while bypassing new events and reporting them to the proper authorities. With the use of Big Data Analytics and Visualization techniques, the newly established Security Operations Center (SOC) could best identify, rate, and respond to flaws that posed cyber and technology threats.

In order for Security Analytics to succeed, it is necessary to implement tools and procedures that can be employed quickly enough to respond to security intrusions in near real-time. Without SA tools, the enterprise would have a very difficult time defending itself against hackers and cyber-attacks.

The Support and Security Operation Center

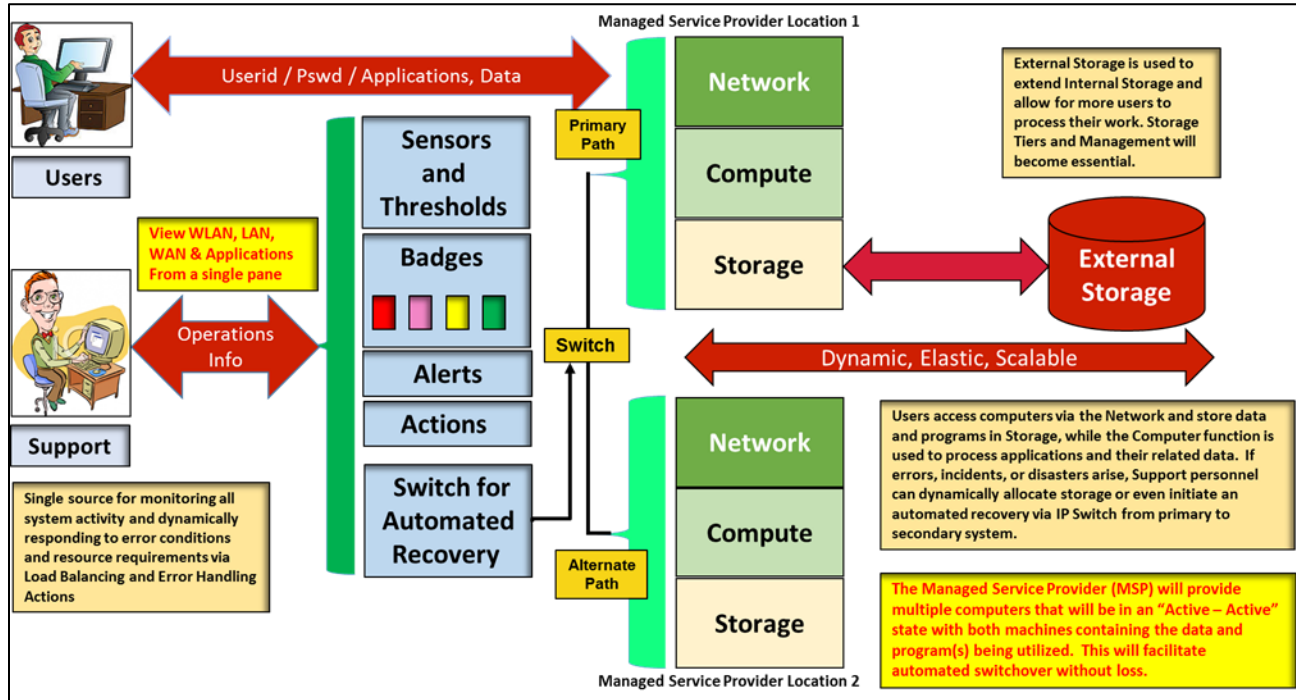


Figure 6: Load Balancing and Error Handling for a Virtual Environment with Automatic Recovery

When errors are detected through Threshold Sensors and Network Scanners, Alerts are initiated, and automated Actions taken to bypass failing components and maintain operations

This process is included in Virtual Systems that have eliminated all "Single-Points-Of-Failure" and programmed secondary paths as problem circumventions. Active / Active environments will maintain applications and data in sync across the primary and secondary facility to eliminate any interruption to production operations. This configuration can switch from primary to secondary facility automatically and will be transparent to the end user.

In the real-world, security management systems must be integrated within your everyday environment and have the capability to sense, rate, alert, and take immediate actions to safeguard the enterprise. This is accomplished in the following manner:

1. Establish Thresholds to define security categories like Good, Poor, or Bad.
2. Assign color codes to the categories like, Good (Green), Poor (Yellow), and Bad (Red).
3. Develop an Alarm mechanism that will notify the Security Operations Center (SOC) Staff of abnormalities when they occur, both going from good to bad and returning from bad to good.
4. Implement an Alert Mechanism that would notify people when a security flaw occurred or is resolved. This can consist of emails, problem tickets, phone calls, or bells and sirens.

5. Define Actions to be taken for the full range of security violations and associate them to alarms, so that actions to bypass security/failure conditions can immediately be taken, while personnel can follow-on with necessary repairs and mitigations.
6. Record all activities and follow-on incidents with a Post Mortem discussion to define the reason behind the failure, developing lessons learned and teaching events as needed.

Some of the characteristics of a Security Incident Event Management (SIEM) Security Analytics (SA) system are depicted below.

Key Characteristics of Security Incident Event Management (SIEM) and Security Analytics (SA) Platforms	
Characteristic:	Description:
Speed of Transaction Analysis	The ability to analyze a threat event and return a decision about it in near real-time, leading to an automated security control system
Amount of Data Analyzed	Petabytes requiring Big Data tools to analyze and report on encountered error conditions and their mitigations.
Big Data Infrastructure	Because of the diversity and volume of data it is necessary to utilize Big Data systems to analyze information.
Event Correlation Process	Context-based, adaptive, and risk-based threat detection
Integrated Platform	Platform must include the ability to capture network analysis and visibility (NAV), threat intelligence, Security User Behavior Analysis (SUBA) and SIM data to then present that information to authorized consoles.
Machine Learning	Supervised and unsupervised machine learning methods detect anomalous behavior without the need for pre-written rules.
Risk Computation Models	Statistical-based and rules-based risk and security event modeling
Entity and Link Analytics	Entity and Link Analytics - evaluating network, host, and endpoint devices linked together
Statistical Probability Methods	Probability models to determine the likelihood of a breach

Figure 7: Features of a SIEM and Security Analytics System

Creating a Chief Information Security Officer (CISO) position

Many enterprises have elevated Information Security to the 'C' level and announced the creation of a Chief Information Security Officer (CISO). In some cases, this position is assigned to individuals who have risen through the security technology ranks and have extensive hands-on experience identifying and resolving security threats. In other enterprises, the CISO position is more involved with legal, business, compliance, and business issues. The person holding the CISO position can therefore have a wide-range of backgrounds and qualifications, but in all cases the CISO is responsible for reporting to the enterprise on how best to protect resources, intellectual property, reputation, and the confidence of the client base. Other enterprises have addressed both needs by creating a Chief Security Officer (CSO) and a Chief Information Security Officer (CISO), with the CSO reporting to the CISO. This final approach seems to be the most adopted approach used by today's enterprise. Another 'C' level position of importance is the Chief Compliance Officer (CCO) who is responsible for insuring that the enterprise complies to all regulations and laws in the countries where the enterprise does business.

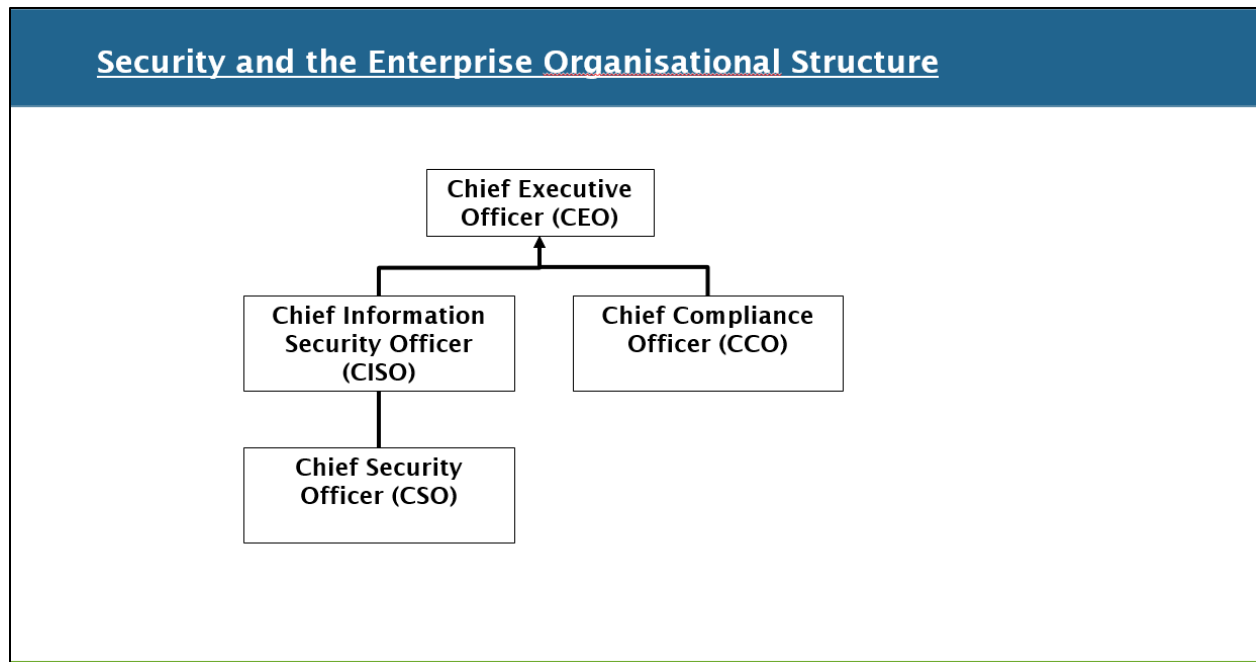


Figure 8: The enterprise security and compliance organizational structure

Defining the needs and responsibilities of an Enterprise Security System

You must first define the range of responsibilities associated with the enterprise security environment, then define a Threat Based Approach to implementing security precaution, and finally a Risk Based Approach to implementing security precautions. Once these issues have been defined, rated, and evaluated you must then define functional responsibilities, tools, displays, alerts, and actions to be taken to mitigate encountered cybercrimes and technology threats. A Continuous Diagnostic and Mitigation (CDM) system has been found as best suited to satisfy the security deterrence needs of the enterprise.

The approach presented here will provide four areas to consider when establishing an enterprise security system and the roles that should be integrated to support security and technology threats. They are:

1. Responsibilities included in establishing an Enterprise Information Security Environment
2. Threat based approach to implementing Enterprise Security Management
3. Risk based approach to Enterprise Security Management
4. Cloud Risk and Security Protection

Defining Security and Technology threats and assigning Responsibilities

Information Security Responsibilities

Information Security Responsibilities	
<ul style="list-style-type: none"> Physical Security Data Security Intellectual Property GRC – Governance, Regulation, Compliance Risk Management Forensics and Investigations Business Continuity Management Data Privacy and Entitlements Strategic Security initiatives Audit Universe and Audit Schedules Threat Intelligence Capabilities Situational Awareness Continuous Diagnostics and Mitigation (CDM) Ownership of Risk and Security in the Cloud Cyber Threat Intelligence: <ul style="list-style-type: none"> Cyber Security National Action Plan Cyber Security Policies Network Security – SIEM Encryption, Cryptography, and Bio-Metrics <ul style="list-style-type: none"> PIV, PIV-I, CAC Interfacing with Professional Organizations Documentation, Awareness, Training, and Certification of staff 	<ul style="list-style-type: none"> Firewalls, Intrusion Detection, Anti-Virus and Malware IT Security Tools and Products Threat Intelligence Capabilities: <ul style="list-style-type: none"> Data from Systems, Applications, and Network Intrusion Detection and Prevention systems Endpoint Anti-Virus and Security Controls Firewalls and Anti-Malware Scanner and Sensor Rules and Results Tracking Role Based Access Controls (RBAC) PIV / PIV-I and Entitlements HWAM, SWAM, Vulnerabilities, and Configuration vulnerability detection and protection of Technical Environment SPLUNK data collection and analysis tools, et al Prioritize identified Gaps and Exposure Risks Unified Security Intelligence Management System combining Log Management, endpoint and network monitoring, SIEM and Security Analysis, Reporting and Mitigation Action Plans Develop a Three Step Approach: <ol style="list-style-type: none"> Infrastructure Protection Entitlements and staff Behavior Analysis

Figure 9: Defining Security and Technology Threats and Assigning Responsibilities

Approaches to developing an Enterprise Security System

The range of problems faced by an enterprise is extensive, but all of the subjects listed above should be identified, rated, and included in the Enterprise Security System that you develop to safeguard the intellectual properties and assets of your business.

There are two approaches presented on the following pages, the Threat Based Approach and the Risk Based Approach. Both have merit, and in fact, both should be performed to fully defined the needs of your enterprise. A third topic is included to identify the special needs of companies utilizing Cloud Based services.

Threat based approach to implementing Enterprise Security Management



Figure 10: Threat Based Approach to implementing an Enterprise Security System

Risk based approach to Enterprise Security Management

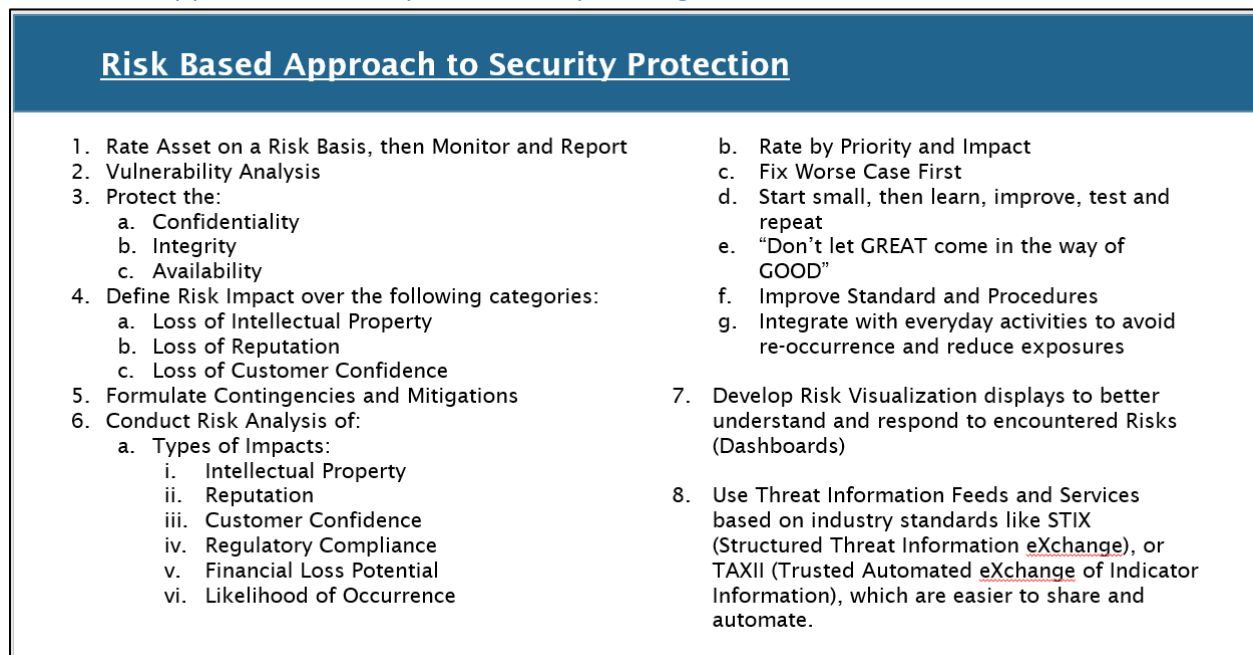


Figure 11: Risk Based Approach to implementing an Enterprise Security System

Cloud Risk and Security Protection

Cloud Risk and Security Protection

Cloud Risk and Security Reviews:

1. The enterprise is still responsible for Risk and Security, even when migrating to the Cloud – including Systems, Applications, and Data.
2. Cloud Service Provider supplied Risk and Security information is limited and not always accurate.
3. Compliance must be reviewed prior to migrating to a Cloud environment (Data Integrity).
4. You must review Legal and Vendor Agreements and Licenses for hidden costs and permissions.
5. In-House security practices may not work in the Cloud and should be scrutinized.
6. Additional Tools, Products, and Resources may be required to continue adherence to security and regulatory requirements.

Cloud Security Policy:

1. Clearly identified Executive Sponsor
2. Data Sensitivity and Cloud Data Protection Guidelines must be developed and adhered to.
3. Compliance mandates must be identified and adhered to.
4. Document Cloud Risk evaluation process and results, then obtain sign-off on results or corrective actions.

I hope this article helped you understand more about security management and how it is evolving in today's environment. Any comments or recommendations for improvement would be gladly accepted.

If you would like to discuss the information contained in this document, or believe my services could be helpful to your organization please do not hesitate to contact me at bronackt@gmail.com

Thank you,

Tom Bronack