Using Information Security as an Auditing Tool

Adi Sitnica

USING INFORMATION SECURITY AS AN AUDITING TOOL

GIAC GSNA Gold Certification

Author: Adi Sitnica, adi.sitnica@gmail.com

Advisor: Richard Carbone

Accepted: July 11, 2016

Abstract

As cyber-attacks are gaining visibility within mainstream media, what once was knowledge for information security expertise is now a concern of everyday individuals. With solutions and information readily available, where does one start in the pursuit of information security? The understanding of the organization's system and network infrastructure is required, but what type of approach can be taken? Investigation leads to using information security as an auditing tool to analyze and report on an organization's strengths, weaknesses and needs. As a result, the organization inherently gains visualization of the current posture, its gaps and a method for continuous remediation.

1. Objective

As part of information security needs, information gathering in the form of an audit will be done across the organization. The goal of this paper is to gather knowledge about an organization to understand what keeps it in business. This in turn will allow for delegation of risk, appropriately based on veracity rather than perceived importance. As a result, concentrated efforts can be made to increase the information security posture with a direct correspondence to lowering precisely only the confirmed risk factors, thereby drastically reducing resources and time consumption while improving the organization's stance in the most effective and financially reinforced context.

This will be made possible using information security auditing as a tool, which will be explained throughout this paper, commencing with simple internal investigations, leading towards multifaceted research that can be tied together to form a robust information security and business-centric infrastructure.

2. Introduction

Over the past few years we have seen emphasis given on cyber-attacks and breaches within the mainstream media. Truth is that they have been around since the 20th century, but only recently, through mainstream media, has the public started to understand and be aware of its existence. This is primarily due to the age we live in, where everything is interconnected, from our phones to our cars, even our washing machines processing an order through Amazon for a detergent refill. Even in 2016, many organizations may see the information security threat, but since it has not yet affected them, it is not a priority. The reality is that the cyber-attacks and breaches we see in the media are just the tip of the iceberg. A good visual to understanding that the threats are real and quantifiable is to look at the Verizon Data Breach and Investigations Report (DBIR), released annually with in-depth analytics on the threat posture across various industries. However, even the DBIR and other such reports, the threats covered are based on data through available and shared channels and knowledge, with the bulk of information security threat vectors being mostly unknown or undisclosed, at least until somebody is attacked or breached, and the malicious activity detected.

Adi Sitnica, adi.sitnica@gmail.com

Each organization deals with information security differently; some are bound by law to improve on their information security posture, some are pro-active, some ignore it, some are driven by business needs, while some are waiting for somebody within their industry to be attacked to take notice or action. No matter where an organization falls in this spectrum, interacting with digital technology one is bound to be involved with information security at some level, if not already. So the question is what can an organization do to protect themselves? With all of the hype around information and cyber security, where does one start?

The growth rate of vendors trying to sell information security, whether as a service or product to enhance an organization's information security posture has expanded exponentially, where a research project is required just to understand high-level options. The cybersecurity market report by Cybersecurity Ventures for Q4 of 2015 shows that the worldwide cyber security market is estimated to grow from $75 billion in 2015 to $170+ billion by 2020 (Cybersecurity Ventures, 2015). With all of this information and internal business necessities competing for resources, what can be done? Understanding one's organization and its business drivers, including information security context and what risks and impact it brings to the table, are the most important factors. To do this, research is essential. To gain a better understanding one can use information security as an auditing tool.

3. Context

Regardless of what industry one is in, if technology is part of it, then it is susceptible to cyber-attack, or "An attack, via cyberspace, targeting an enterprise's use of cyberspace for the purpose of disrupting, disabling, destroying, or maliciously controlling a computing environment/infrastructure; or destroying the integrity of the data or stealing controlled information" (National Institute of Standards and Technology, 2013). Before researching any type of information security-related solutions or the threats a specific organization may face, one must first understand the infrastructure and information that makes it tick, or from a financial perspective, be profitable and in business.

Once understood, the criticality of items within the organization can be assigned and prioritized. These prioritizations can be used to dictate effort and planning, and a

self-assessment or self-audit can be used to obtain this information. Swanson (2001) describes a self-assessment as a method to determine the status of information security posture and a means for improvement through visibility of gaps. Use the following questionnaire to put together a high-level dataset that can steer an organization in the right direction:

- Does the organization have any digital assets? In other words, does the organization leverage the use of internal technology or external 'third-party' technology such as the cloud?
    - If so, does the organization have a list available and can account for all of the digital assets throughout the organization?
    - Is this list kept up-to-date?

  Examples of these are a list of assets, a standardized software and hardware list traced to the list of assets, and tools used to maintain these assets.
- Does the organization have policies and procedures in-place for technology? Examples of these are acceptable use policy, information security awareness policy, software and hardware procurement policy, etc.
- Does the organization employ individuals that have an information security background? Example of these are a group of individuals specializing in information security, such as analysts, incident response and security awareness champions.
- What are the limitations in terms of information sharing within the organization through the use of technology? Examples of these are chat room, forums, SharePoint, and other collaborative work-spaces.

Most will have answered these questions and found out that part or all their organization is run by technology or with technology interaction, and that digital assets are not accounted for properly or kept up to date. This is one of the primary gaps with most organizations these days: the basic accountability and knowledge of one's own technology and assets is incomplete. By understanding what technology is used within the organization, one can take a risk-based approach to analyzing a solution. To perform this type of action will require the organization to perform internal auditing, or "Independent review and examination of records and activities to assess the adequacy of

system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures" (National Institute of Standards and Technology, 2013).

Auditing can take many forms, but the goal is always the same; to assess something. "The audit dates in Britain from at least medieval times, when the auditor on landed estates literally heard the accounts read out and checked on the lord's behalf that his steward had not been negligent or fraudulent. Then as trading and manufacturing companies multiplied in the eighteenth century, accountants were commonly employed as auditors to check that all was in order with the investments of partners or shareholders" (Matthews, 2006). Even in the 21st century, auditing has remained largely unchanged, and can be applied in the same manner, except in this case against an organization digital assets.

Using the output from the aforementioned questionnaire provides a high-level understanding of an organization, and that can be used to understand the current information security posture and gaps. For example, leveraging auditing to understand what type and how many servers are used within it. In a fictitious example, Company XYZ has 50 servers accounted throughout the organization after an audit. Of those 50 servers, 35 run Microsoft operating systems, and 15 Red Hat operating systems. From an analytical perspective, this provides information to an organization on how many servers are being used, and what types of operating systems are running. If this is expanded to encompass all digital assets an organization uses, one can then account for all the technologies used throughout it, how many and what type. This type of audit report can then be used for various means, including presenting facts to management, trying to obtain funding, limiting the scope of projects and understanding the demographic of technology from an information security perspective.

Consider the data from the audit report for all digital assets; that information can be used to create a baseline of technology in use within the organization, which can then be used as a comparative means to self-assess in a continuous manner, providing visibility of technology use, then and now. Going one step further, use the audit report data of all digital assets to further delve into the analytical risks associated with that technology. One can eliminate risk associated with technology that is not in-use within an

organization, and instead concentrate efforts on applicable risks. In our fictitious example of Company XYZ, that would limit the risk analysis to only Microsoft and Red Hat operating systems. This drastically decreases the need to research unnecessary data, or solutions for risk that does not apply, which in turn lowers the financial burden of information security. Continuing with further risk analysis, one would delve into researching the vulnerabilities, which in this case would be limited to Windows and Linux only, instead of other operating systems that are not used throughout the organization such as VxWorks or iPhone Operating System (iOS). This provides a focused path towards the next step, which is investigating threats against that specific technology, and associating it with threat-intelligence.

To start the investigation one must gather available knowledge about the vulnerabilities of said operating systems. These can be found at various locations on the Internet, but one should start with the vendors themselves, and build the portfolio from there. Publically available knowledgebase from the vendors about specific products can help visualize the current state of vulnerabilities. Examples of some vulnerability information sources are the United States Computer Emergency Readiness Team (US-CERT) with technical alerts and vulnerability bulletins, and the Common Vulnerabilities and Exposures (CVE) with an archive of publically known information security vulnerabilities and exposures. While vulnerabilities can be further examined for applicability towards the organization and its usage and application of the technology, they are omitted from this paper and will instead be presented at a high-level.

Once the vulnerabilities are gathered and documented, the next step is to investigate the threats associated with the organization, its industry and the vendor products themselves. For example, malware built to leverage vulnerabilities on Windows XP in most cases will not work on Red Hat. There are exceptions, but that is a more complex issue. Based on information security industry expertise, simple threat vectors are used more often than not, because a secure and limited threat vector target generally ends up not being worth the effort for the attacker. For those more complex attack scenarios, an organization will require defense-in-depth or multiple defensive layers in order to deter, protect or slow down and detect the attacker.

The threats one faces should be based on internal responses to incidents and known attack scenarios that required the organization to react. These scenarios, due to the details documented during the analysis and response phase, can act as the best means to obtain funding to further develop information security. They can be directly attributed to a financial loss for the organization, and thus would have the highest of visibility. A step beneath, from a prioritization sense, would be threat-intelligence gathering through various sources. Webroot. (n.d.) defines threat-intelligence as "evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice, about an existing or emerging menace or hazard to assets that can be used to inform decisions regarding the subject's response to that menace or hazard." Threat-intelligence can help paint a picture of the organization's industry or information security threat vectors overall. Some of these include the Verizon DBIR, the Symantec Threat Report, the Kaspersky Security Bulletin and the SANS Internet Storm Center. Note that consideration of demographics should be made when gathering knowledge; data gathered from the western part of the globe will differ from eastern-gathered. Use this as an advantage, and investigate the same topics from various sources throughout the world. This in turn provides improved oversight of the threat-intelligence currently affecting the organization or industry, from various perspectives.

Once the threat vectors are investigated and the data documented, start piecing together the puzzle, including all of the previously researched information and correlating the data appropriately to pin point risk. For example, take Company XYZ, which falls under the Accommodation industry. Research shows its usage of the Windows operating system, further expanded with documented vulnerabilities against it. Now, take into account the threats and threat-intelligences and further position the risk. Pulling the information from the Verizon DBIR 2015, Point of Sale attack threat vectors represent 91% of all Accommodation breaches, while 1% represent Web App Attacks. From a risk perspective, the vulnerabilities that are specific to Point of Sale application would be prioritized over Web App Attacks.

After all information has been investigated and gathered, analytics and reporting must be compiled. The report should highlight an organization's assets, the details of those assets, the industry threat-portfolio as well as the asset threat-portfolio. Note that

when using information security as an auditing tool, one should not attempt to tackle too large of an effort. Instead, a concentrated risk based approach should be taken. SANS Institute (2014, p. 128) describes a vulnerability scan performed against 'everything,' which results in a negative outcome. On the other hand, the SANS Institute (2014, p. 130) showcases a concentrated effort which provides much better results. With all of those details, a process must now be created and enforced in order to increase the information security posture in a recurring manner using continuous remediation. This process then becomes the baseline, and can be used for external audits, compliance tracking, and presentation or reporting to management. This leads to the next question, how to obtain funding to start such a complex undertaking?

There is a very real problem in today's organizations to obtain funding to pursue information security and its solutions. This is because within information security the return on investment is not viewed as direct revenue, but prevention against possible attacks/risks. Depending on the industry an organization is in, this can cause efforts to go in vein before getting anywhere. To eliminate this possible obstacle before it takes root, take advantage of the following lessons learned:

- Gather analysis reference publications/papers from various sources such as the Ponemon Institute, Q1 Labs (now IBM), Gartner and others.
- Investigate own industry and available information on cyber security breaches, especially with competitors; use that as an advantage to fund the efforts.
- Leverage any internal-knowledge of malicious incidents (viruses, etc.) and the actions that had to be taken to resolve those incidents.
- If third-party vendors were brought in to investigate and resolve incidents, use the cost associated with these, including the reports the vendors left in terms of a gap analysis.
- Investigate external drivers to enhance information security (US-CERT, FBI, etc.)

Loaded with this information, an organization is now on the right path for enhancing its defense-in-depth strategy, a term that is used to describe, "Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and dimensions of the organization" (National Institute of Standards and Technology, 2013). Proper planning to enhance an

organization's security posture is not only the correct path, but also an obvious one, if it is to stay active as a business. More and more organizations are looking for products and vendors that can provide assurance that they have information security handled, whether that is through direct regulatory compliance or through use of supply chain security.

Without the procurement of additional tools and expertise, one can leverage individuals within an organization to get started using information security as an auditing tool. This will support building a representation of the current security posture, as well as help understand the demographic, risks and needs of the organization.

4. Information Security as an Auditing Tool

Consider the previously used information and definitions of information security and auditing. How would one use that knowledge to enhance the information security posture of the organization? Try to think of information security as a goal to understanding one's own organization and knowing the risks associated with it. To understand one's own organization one must perform a self-assessment. That in turn will identify and quantify assets and risks associated with it. In addition to highlighting the risk, it would also provide a gap analysis and a means to track the information security posture of the organization over time.

Take a vehicle as an example. If procuring a new or used vehicle an investigation or analysis, or for comparison reasons, an audit will be performed. Is it the right size? How much does it cost? What kind of engine does it have? Based on the audit's investigation and answers, a more definitive vehicle can be chosen, one that fits the needs. Next, we look at the industry's known issues. Is the manufacturer known for something, positive or negative? What do other individuals say about the manufacturer, or specifically the exact vehicle? Collection of all of this information over time provides an oversight of what is being considered. This can be used as a baseline, and further investigation can be adapted and compared to the baseline, thereby eventually getting to the selection based on set criteria that would be acceptable, or in this case, a risk that is acceptable.

There are no standard set of questions that can be used as each industry is different, but there is commonality in terms of information security regardless of the

industry. This is where we can start. An example of general information security knowledge, regardless of industry, is the Center for Internet Security (CIS), an organization concentrating in cyber security that is driven by a global community of public and private sectors with a common goal to enhance the defenses against cyber-attacks. Part of the CIS products and services portfolio includes the CIS Critical Security Controls (Center for Internet Security, 2016), available publically for free, which provides a standardized set of controls, based on global input from the information security community, in a living-document. Specifically, a threat-intelligence driven and tested set of best practices, including key threat vectors and how to defend against them, documented threat paths, and a forum for information sharing and knowledge which can be used to identify and solve new information security problems. This in turn produces a focused response for meeting controls/requirements that have been tested and validated by diverse experts across a plethora of industries. What was established is a proven approach to make organizational changes in a feasible way, and usable for compliance with one's own industry information security requirements. It is an approach taken by the global information security community to provide guidance to organizations to enhance their defense-in-depth and information security posture, all with direct lessons learned from various industries and individuals. This provides a proven and hardened pathway towards enhancing its security posture against a framework that is kept up-to-date by a legion of information security professionals.

CIS, along with an organization's own information security requirements, whether internal or industry driven, can be used to generate a set of questions to facilitate a means to enhancing the information security posture of the organization. With that in mind, start with a high-level analysis of the organization. The answers to these following questions will provide insight towards the path that needs to be taken in order to succeed with information security:

- How many employees does the organization have?
- Does each employee own or lease a computer/laptop?
- Is a network infrastructure identified and monitored?
- Is the network segregated physically or virtually?
- Have the critical needs of the organization already been prioritized?

- How many separate organizational divisions are there?
- Is there an Information Technology team? Is it organizational or divisional?
- Is there an Information Security team? Is it organizational or divisional?
- Is the computer support outsourced, or is it done in-house?
- Is there a division of responsibilities chart beneath each team?

Depending on which industry the organization is in, one may have access to specific security frameworks or standards. A framework is "a basic structure underlying a system, concept or text" (Oxford, n.d.). A standard is "a published statement on a topic specifying characteristics, usually measurable, that must be satisfied or achieved in order to comply with the standard" (National Institute of Standards and Technology, 2013). In certain cases, the industry may already be under a set of information security requirements, frameworks or standards that are mandatory. These are usually provided in a general manner, followed by guidance documentation that explains or shows a path to meet those requirements, in a detailed level description.

Once a high-level representation is established, based on the responses from the questionnaire, a risk-based approach can be of much benefit. This can be tied to the information security requirements of the organization. That is, what is the real risk to the organization? The organization can protect itself against many possible threat vectors, but if some have no impact, then why invest further? An attack-tree analysis can provide a visual of the various types of threats that can have a direct impact, and highlight what threat vectors must be protected. This method also provides a means for directing efforts, which provide a resilient stance when presented to management detailing the path that needs to be taken, or alternatively, the risk sign-off that management has to accept to not pursue the path.

A pathway to properly estimate the risks and visualize them is to use an attack-tree analysis. An attack-tree analysis is a graphical method to highlighting or visualizing attack vector(s) against an asset or component that the organization is trying to protect. According to Schneier (1999), "Attack trees provide a formal, methodical way of describing the security of systems, based on varying attacks." An example depiction is shown in Figure 1, which describes various methods to burglarize a house. It visualizes

possible methods how a burglar can enter the house. From the depiction one can then further analyze the risks with various threat vectors; for example, if the house has reinforced glass with vibration alarms, the risk associated with that pathway may be lower than through the garage which has no security. If the risk for a garage attack is higher, then from an analytical perspective one can enhance the defense-in-depth of the garage threat vector; installing sensors, a locked door between the garage and the house, and other means to enhance the security against that specific threat vector. This in turn provides a means to visualize threat pathways, including responses as to why a certain effort is being made to enhance, in this case, the security of the garage.

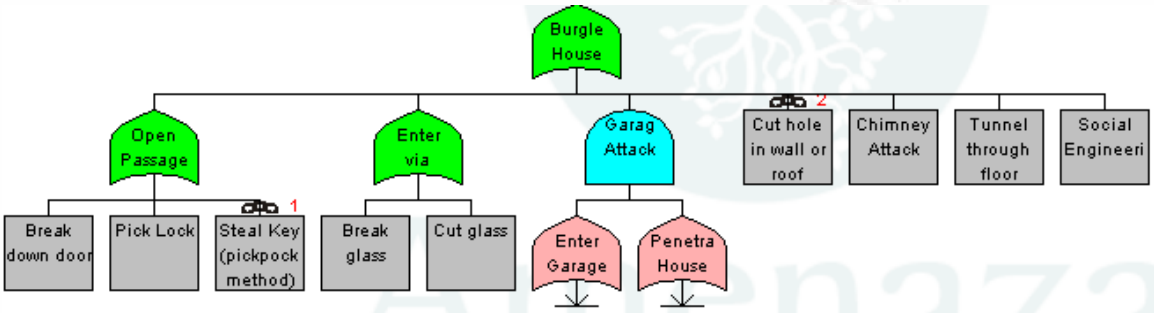

Figure 1. Attack Tree Example (Source: Amenaza)

Attribution to requirements that are laid out in frameworks, standards or organization-specific instances, and what controls help meet them, provide an insight to how the organization is performing. The next step of evolution is to take the information and keep it up to date, providing statistics and analysis over time in a report-like structure. This can then be used to present to management, organization, industry or external auditing, to highlight the current information security posture of the organization.

This in turn can provide a better representation of the enhancements that are required, and those that are not. For example, if one is trying to protect an isolated server without any network capability, then the threat vectors related to network penetration or leverage of network vulnerabilities are not applicable. With this information one can pinpoint the threat vectors, and based on assignment of risk can properly implement a defense-in-depth strategy with a risk-based approach. Cole (2013) states, “In order for an organization to make sure they are focusing in on the right areas, threat needs to drive the

risk equation." SANS Institute (2012, p. 37) uses the following formula: Risk = Threat * Vulnerability. "Organizations should be focusing in and fixing vulnerabilities that are tied to high risk items, not just fixing any vulnerability that does not have an actual threat tied to it" (Cole, 2013, p. 13). This, in its finalized state can be used as a cost effective, compliant and analytics-based pathway to information security.

When an audit process is in place, it can be reused in a recurring manner. It can help identify shortcomings as well as critical needs within an organization, and it can be used to provide an ongoing report to management that highlights the posture, where it is lacking, and where it is properly implemented. With the recurring report, over time the organization will gain visibility into the transient efforts within, and will be able to better assess risks. That is, understanding the organization's critical needs, and what parts have to be prioritized over others in relation to business operations and continuity. The report will also shed light on items that are underfunded or understaffed, which may require supplementary support.

From an audit and risk-based approach, the security posture gaps of the organization should start to become evident, through the process of analysis and prioritization. In this case, the security posture gaps are vulnerabilities across the spectrum of the analysis, including assets, policies, processes and staff.

Based on the risk posture an organization can investigate and assign staff, resources and proper planning to enhance the defense-in-depth, and lower the threat vector space of those risks. This information can be used to discuss funding and task assignment with management and technical leaders. Further continuous analysis and auditing can highlight results, over time. In detail, now that a process is in place that can be used in a recurring manner, proper planning must be done to keep the process active and current. This requires building a self-analysis or self-auditing process for the organization at a high-level, with standards including frequency, process, expectations and requirement-based compliance control tracking. These can be internal or based on a framework or standard.

Adi Sitnica, adi.sitnica@gmail.com

5. Fictional (example) Approach

Now that the overall process of using information security as an audit tool is presented, what does this look like in a completed state? Revert to the fictitious example of Company XYZ used in previous sections. Company XYZ had 35 servers that are Windows-based and 15 that are Red Hat-based. Taking the guided approach used by this paper, Company XYZ does indeed have digital assets, in the form of servers. They do not use any third-party technology, and are limited to 20 employees. Only the datacenter technology is accounted for, not the components that are used by the employees for their work. This includes their laptops, the networking that keeps their assets connected to the datacenter equipment, and the test lab. The software used within has been standardized, and is accounted for across all boundaries. A set of policies and procedures is in place; however it does not cover information security in detail. There is an acceptable use policy, but no security awareness or procurement policies. Only 2 of the 20 employees have a background in information security but are not specialized in that area of expertise. Microsoft Office suite is used for documentation, and Slack, a communication and collaboration platform is used to work together, online and offline.

With this knowledge, one can create a baseline of the organization, spanning from individuals and their roles, to policies and procedures that they have to adhere to, including assets used to run the business, specifically the hardware and software. From this baseline, an investigation can be made into the assets' vulnerabilities. In this case, Windows and Red Hat operating systems, and Microsoft Office suite and Slack as a means of doing business. Note this is a high-level example; a real world example would include all of the detailed hardware and software that is used within the organization including routers, switches, third-party applications and commercial off the shelf software.

Delving deeper into the Windows operating system, Company XYZ uses Windows 2008 R2. Leveraging the information sources such as US-CERT and CVE, one can locate a set of vulnerabilities against these specific operating systems and their versions. Verification can be done to see what patches, if any, have been applied to limit the vulnerabilities that are known. Once recorded, one has a baseline and an analysis that highlights the current posture of the organization. The next step is to investigate the

threat-intelligence. Take for example the Verizon DBIR 2015. Considering Company XYZ is in the Accommodation industry, the Verizon DBIT 2015 states that point of sale (POS) attacks represent 91% of all Accommodation breaches (Verizon, 2015). Based on the POS analysis, Company XYZ would fall into the 'small' category as seen in Point-Of-Sale Intrusions Section within the DBIR. Specifically, for smaller organizations, the POS devices were directly targeted, normally by guessing or brute forcing the passwords. From a risk analysis perspective, taking that information into account the organization would concentrate the effort to enhance the password, possibly introducing multi-factor authentication, eliminating any default passwords, and changing the user IDs to something non-standard. There are more threat vectors explained, but this is meant to illustrate the direction of using information security as an auditing tool.

To further build upon this, let us consider Company ABC. Company ABC is a multi-national large organization with 5000+ employees within the Manufacturing industry. Company ABC does not currently have all of their assets accounted for, but tracing the procurement of the business leads to a baseline identification of assets that were purchased. Company ABC also uses the cloud through a third-party provider to store some of their intellectual property. However Company ABC does have policies and procedures in place for technology, including a dedicated information security set. It also has a dedicated information security staff with expertise. The boundaries of the Company ABC information sharing are limited through the use of isolation and firewalls. The generation business portion is separated from the corporate portion, limiting the threat vectors to the generation. It uses Google for work, including Apps and Cloud services. Based on these responses, Company ABC is required to further investigate its relation to its assets; use the baseline identification of assets and correlate them to the usage throughout the organization. Eliminate unused (but procured) assets, and build a new baseline of assets for the organization. From that baseline further investigate and create a standard list of software that is used. Create a software baseline, and locate the baseline information in living documents. Validate that the current policies and procedures do not require adjustment based on the investigation. Once validated or adjusted, as necessary, take a look at the vulnerabilities against the updated baseline. Based on these vulnerabilities look for industry or asset specific threats and research threat-intelligence.

Adi Sitnica, adi.sitnica@gmail.com

Because Company ABC is within the Manufacturing industry, the Verizon DBIR 2015 showcases that 60% of attacks are attributed to Cyber-espionage, and 34% to crimeware. Based on this and further information gathering, an approach can be taken to highlight where Company ABC is with its baseline, and what has to be done to enhance its information security posture using the researched information, including baseline organization information, the vulnerabilities, threats and threat-intelligence.

With these two high-level examples, let us delve into a low-level scenario using the methods previously described. Take for example a fictional data center, located in Company ABC. Within this data center, consider four divisions housed there: application development, help desk management system, electronic documentation system (where the intellectual property is stored), and development environments. Based on research and analysis performed internally against the organization's prioritization of assets, the electronic documentation system is the most critical and houses the organization's intellectual property, with the development environment being the second because it is here where the intellectual property data is created, tested and validated. The other two are less critical and will be omitted from this scenario. Based on the previous audit, one has a list of assets housed under the electronic documentation system, including current security posture associated with it. From that information, an attack tree can be built, and the threat vectors can be properly assigned a risk level. Take for example the access to the electronic documentation system; it is done via the organization's intranet using the resources available to end-employees (laptops, desktops, mobile phones). From the three resources only two have access to the electronic documentation system, thereby eliminating the third, in this case mobile phones, from the threat vector space. The laptops use Wi-Fi to connect to the intranet and can be used from external locations. The desktops can only be used at the organization's sites. Thus, the desktop threat vectors are limited to physical connections, excluding Wi-Fi, and excluding any external access without pivoting. In this case, the term pivoting is used to describe a threat vector path that is restricted; however, by using a compromised system on the internal demilitarized zone (DMZ) one can bypass safety measures which would otherwise stop the attacker. Using these methods to delve into the attack scenarios, one can visualize possible threat vectors, and based on analysis and research, both internal and external, can prioritize risk

in a document format. Using the output of this risk, one can request funding and associate it with direct risk, completely researched from top to bottom, leaving little reason, except to accept the risk by management or to fund the information security solutions to eliminate or lower those risk vectors.

Next, without incorporating the funding request pathway as described, let us delve into how the research and analysis can be used to provide a status report for compliance and/or current gap analysis, in a recurring fashion. If we take the research done against Company ABC and XYZ, we will have available the baseline information. As noted, the two companies have different baseline information; for example, Company XYZ has the software list standardized and accounted for, while ABC does not. The two baselines can be represented using a comparative depiction, as shown in Table 1.

Table 1: Baseline Analysis

Audit:	**Company ABC**	**Company XYZ**
Employees	5000+	20
Assets accounted for:	No	Sub-set
Assets:	Only procured asset list is available	35 Windows Servers, 15 Red Hat Servers
Assets missing:	All	Employee laptops, test lab equipment, and networking equipment

The stage(s) where one should start depend on prioritization of the information that is researched, and can be based on risk acceptance vectors. In this case, we will make a fictional prioritization for accounting all of the assets of the organization. For Company ABC the baseline is unknown, and must be created as a first step; this can be done as previously described by using the procurement asset list and building an internal list of active and used assets. For Company XYZ, this is accounted for within the datacenter, but is missing information concerning employee laptops, test lab equipment and networking equipment. For the first phase of using information security as an auditing

tool, we can showcase our current stance in terms of assets between the companies. The approach would first be to fulfill the detail required to have all assets accounted for. Thus, at current date a report can highlight the status and what is currently accounted for. Using the funding further research will be done to locate all of the companies' assets and record them properly within 6 months. At the 6 month period, Table 1 can be further updated as shown in Table 2.

Table 2: Baseline Analysis + 6 months

Audit:	**Company ABC**	**Company XYZ**
Employees	5000+	20
Assets accounted for:	Yes	Yes
Assets:	6375 laptops, 1350 servers, 433 network equipment assets, 255 mobile phones, 830 workstations	35 Windows Servers, 15 Red Hat Servers, 40 laptops, 3 servers, 10 switches, 6 routers, 4 firewalls, 5 test servers, 8 test workstations
Assets missing:	Unable to locate active in comparison to procurement list: 76 servers, 172 laptops, 12 network equipment assets,	None.

From here, the threats and threat-intelligence can be further gathered and correlated to the organization's risk, based on an analysis done using risk prioritization, as described previously. Based on the risk assignment, one can create a roadmap for how to resolve the risk with the funding that has been previously obtained, and highlight it over time with improvement against the baseline. To make use of a gap analysis as part of the research conducted, one can use the following output:

Baseline-Q2-2016 audit phase:

- 37 Windows-based servers storing application data within the electronic documentation system.

- Uses single-factor authentication.
- Security hardening has not been completed.
- 3 servers use multi-homed network interface cards.

Gap Analysis:

- Lack of multi-factor authentication.
- Lack of log visibility, including alarms.
- Lack of security hardening configuration.
- Lack of network infrastructure visibility and host firewall configuration.

Using the gap analysis one can lay out a prioritization plan for fixing said gaps, based on risk analysis, vulnerabilities, business drivers, threats and threat-intelligence. Once completed based on a fictional assignment one can use the following output as example:

Baseline-Q3-2016 audit phase:

- 42 Windows-based servers storing application data within the electronic documentation system.
- Uses multi-factor authentication.
- Security hardening has not been completed.
- 5 servers use multi-homed network interface cards.
- Proper network configuration and visibility has been added.

Gap Analysis:

- Lack of log visibility, including alarms.
- Lack of security hardening configuration.

Based on the example, provided at a high-level, a path forward can be taken using a continuous effort against ever evolving analysis of risk, business needs, vulnerabilities, threats and threat-intelligence. This can be used for various reasons, including management presentation, compliance checks, requirement adherence, external governed audits against the organization, internal incident response and many more. This type of information can be used to visualize the security posture of an organization, and provide reporting, including metrics over time concerning the security posture and evolution of information security within the organization.

6. Conclusion

Using information security as an auditing tool provides benefits that span beyond the terminology itself; risk analysis, business drivers, management support, funding inquiries, compliance and requirement adherence, accountability, structure across multiple boundaries, and many others. Regardless of the need, a benefit lies within all stages of the laid out process whether it is for information security or different motives that support the improvement of the organization. The baseline justification to start the process is that investigation and research can be done without the procurement of any additional tools and services, and can be started internally by individuals who are seeking to improve themselves or the organization. If a properly laid out plan is put together for the process, it can be revised over time per the needs and newly uncovered information to formulate a recurring tactic for improvement by use of observable metrics.

Information security has evolved over the last decade, and information that can be a benefit for any organization can be found on the Internet via many of the resources mentioned herein and other such sources. What is required is a desire to improve, whether for oneself or the organization. One does not need an information security background to get started; what are required is vision and proper tracking and research. Many organizations are treating information security as an afterthought, some are ignorant until impacted, while others are performing minimal work. Instead, consider being proactive, give opportunity to those who want to learn about the organization that can benefit both the individual(s) and the organization by creating a pathway using information as an auditing tool to analyze the organization and its current business drivers and status.

Adi Sitnica, adi.sitnica@gmail.com

References

Amenaza Technologies Limited. (2014). SecurITree 4.1 - Build 006 - 2014/07/15 [Software]. Available from http://www.amenaza.com

Burns, J.M. (1978). Leadership, N.Y, Harper and Row.

Center for Internet Security. (2016). The CIS Controls for Effective Cyber Defense, Version 6.0. Retrieved from: http://www.cisecurity.org

Cole, E. (2013). Advanced Persistent Threat: Understanding the Danger and How to Protect Your Organization. Syngress.

Cybersecurity Ventures. (2015, Q4). Cybersecurity Market Report. Retrieved from http://cybersecurityventures.com/cybersecurity-market-report/

Fortune. (2009, July 8). Best advice I ever got. Jim Sinegal: Show, don't tell. (Kimes, M, Interviewer). Retrieved from http://archive.fortune.com/galleries/2009/fortune/0906/gallery.best_advice_i_ever_got2.fortune/2.html

Higson, AW and Saxon Harrold, S. (1987). A Survey of Corporate Donors' Views of Charities' Financial Statements, Charity Trends 1986/87.

Matthews, D. (2006). History of Auditing: The Changing Audit Process in Britain from the Nineteenth Century to the Present Day. London: Routledge.

National Institute of Standards and Technology. (2013, May). Glossary of Key Information Security Terms. Retrieved from http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Schneier, B. (1999, December). Attack Trees. Retrieved from https://www.schneier.com/academic/archives/1999/12/attack_trees.html

Swanson, Marianne. (2001). Security self-assessment guide for information technology systems. Gaithersburg, MD: U.S. Dept. of Commerce, Technology Administration, National Institute of Standards and Technology.

Oxford Dictionaries (n.d.). Dictionary, Thesaurus, & Grammar. Retrieved from http://www.oxforddictionaries.com

Adi Sitnica, adi.sitnica@gmail.com

Ponemon Institute, LLC. (2011, April). State of IT Security: Study of Utilities & Energy Companies. Retrieved from http://www.ponemon.org/local/upload/file/Q1_Labs%20_WP_FINAL_3.pdf

SANS Institute. (2012c). Domain 3 Information Security Governance and Risk Management. The SANS Institute.

SANS Institute. (2014c). 507.2 Effective Network and Perimeter Auditing/Monitoring. The SANS Institute.

SANS. (2016). SANS Critical Security Controls Poster. Retrieved from https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

SANS. (2016). SANS Security Awareness Report, Awareness Is Hard: A Tale of Two Challenges. SANS Securing The Human.

Symantec. (2016, April). Internet Security Threat Report, Volume 21. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Verizon. (2015). 2015 Data Breach Investigations Report. Retrieved from http://www.verizonenterprise.com/DBIR/2015/

Webroot. (n.d.). Threat Intelligence: What is it, and How Can it Protect You from Today's Advanced Cyber-Attacks? (Issue 1) Retrieved from https://webroot-cms-cdn.s3.amazonaws.com/6114/5452/9864/gartner-threat-intelligence-what-is-it-and-how-can-it-protect-you-from-todays.pdf

Last Updated: August 20th, 2019

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Tampa-Clearwater 2019	Clearwater, FLUS	Aug 25, 2019 - Aug 30, 2019	Live Event
SANS Copenhagen August 2019	Copenhagen, DK	Aug 26, 2019 - Aug 31, 2019	Live Event
SANS Philippines 2019	Manila, PH	Sep 02, 2019 - Sep 07, 2019	Live Event
SANS Munich September 2019	Munich, DE	Sep 02, 2019 - Sep 07, 2019	Live Event
SANS Brussels September 2019	Brussels, BE	Sep 02, 2019 - Sep 07, 2019	Live Event
SANS Canberra Spring 2019	Canberra, AU	Sep 02, 2019 - Sep 21, 2019	Live Event
SANS Network Security 2019	Las Vegas, NVUS	Sep 09, 2019 - Sep 16, 2019	Live Event
SANS Oslo September 2019	Oslo, NO	Sep 09, 2019 - Sep 14, 2019	Live Event
SANS Dubai September 2019	Dubai, AE	Sep 14, 2019 - Sep 19, 2019	Live Event
SANS Paris September 2019	Paris, FR	Sep 16, 2019 - Sep 21, 2019	Live Event
Oil & Gas Cybersecurity Summit & Training 2019	Houston, TXUS	Sep 16, 2019 - Sep 22, 2019	Live Event
SANS Rome September 2019	Rome, IT	Sep 16, 2019 - Sep 21, 2019	Live Event
SANS Raleigh 2019	Raleigh, NCUS	Sep 16, 2019 - Sep 21, 2019	Live Event
SANS Bahrain September 2019	Manama, BH	Sep 21, 2019 - Sep 26, 2019	Live Event
SANS San Francisco Fall 2019	San Francisco, CAUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS London September 2019	London, GB	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS Dallas Fall 2019	Dallas, TXUS	Sep 23, 2019 - Sep 28, 2019	Live Event
SANS Kuwait September 2019	Salmiya, KW	Sep 28, 2019 - Oct 03, 2019	Live Event
SANS Northern VA Fall- Reston 2019	Reston, VAUS	Sep 30, 2019 - Oct 05, 2019	Live Event
SANS Cardiff September 2019	Cardiff, GB	Sep 30, 2019 - Oct 05, 2019	Live Event
SANS Tokyo Autumn 2019	Tokyo, JP	Sep 30, 2019 - Oct 12, 2019	Live Event
SANS DFIR Europe Summit & Training 2019 - Prague Edition	Prague, CZ	Sep 30, 2019 - Oct 06, 2019	Live Event
Threat Hunting & Incident Response Summit & Training 2019	New Orleans, LAUS	Sep 30, 2019 - Oct 07, 2019	Live Event
SANS Riyadh October 2019	Riyadh, SA	Oct 05, 2019 - Oct 10, 2019	Live Event
SIEM Summit & Training 2019	Chicago, ILUS	Oct 07, 2019 - Oct 14, 2019	Live Event
SANS October Singapore 2019	Singapore, SG	Oct 07, 2019 - Oct 26, 2019	Live Event
SANS Lisbon October 2019	Lisbon, PT	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS San Diego 2019	San Diego, CAUS	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS Baltimore Fall 2019	Baltimore, MDUS	Oct 07, 2019 - Oct 12, 2019	Live Event
SANS Doha October 2019	Doha, QA	Oct 12, 2019 - Oct 17, 2019	Live Event
SANS Denver 2019	Denver, COUS	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS Seattle Fall 2019	Seattle, WAUS	Oct 14, 2019 - Oct 19, 2019	Live Event
SANS New York City 2019	OnlineNYUS	Aug 25, 2019 - Aug 30, 2019	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced