Global Information Assurance Certification Paper

Alternative Risk Assessment for True Risk
Michael Thibdeau
9/15/2004
GIAC Security Essentials Certification (GSEC)
Practical Assignment
Version 1.4c

Abstract

Risk Assessments are classically performed with regard for only Information Technology systems and personnel. Often, the simple business ramifications from the perspective of a non-IT practitioner are not taken into consideration. Nor are the results of risk assessments from other portions of a business correlated into IT risk assessment. Using elements from different leading risk assessment methods, such as the OCTAVE® approach, the COBRA philosophy and guidelines developed by the GAO. The proposed method fills gaps and increases the reach of these other guidelines to form a comprehensive enterprise risk map, which illustrates the risks facing all different facets of an organization. With this type of risk assessment, any deficiency with the HIPAA Security rule or SysTrust Accreditation will be apparent.

Introduction

The purpose of this document is to outline potential threats and their associated risk values to the Company and its' Security Committee. Threats and Risks are constantly changing; there are no absolute values for the probability of an event occurring. Is the power more likely to go out when the sky is clear and birds chirping, or during a hurricane? Are more viruses released in the immediate days following patch day, or before? The impact itself may not be changed, but as the likelihood of an event increases, so does the risk. So the moment a 'stateful' risk assessment is performed, it is out of date, therefore leading to inaccurate understanding of risks and even perhaps lowered concern for certain risks. To counter this possible inaccuracy, the arbitrary likelihood of an event happening is determined by the people directly involved with the risk.

This document is the white paper for a risk assessment method catered to a for profit insurance related organization. The objective of this method is to perform a risk assessment that is HIPAA Security compliant, and be suitable for SysTrust Accreditation. [9] First the proposed method itself is discussed in detail. The method outlines the philosophy of the assessment, in that it provides a framework for an organizational assessment while leaving the department level able to perform their own assessments. These department assessments are then aggregated into the Risk Map, to determine an overall compliance and security overview. The concept of a consequence and a threat vector is introduced and defined to illustrate risk.

Following the method detail is a comparison to some of the current leading Risk Assessment methods and where the proposed method builds on the ideas of other Risk Assessment processes and improves upon them. How legislation affects security and risk assessments. Where the legislation requirements and risk assessment activities overlap. The closing argument presents some situations where the proposed method improves upon other methods, and support for performing this type of risk assessment.

The steps necessary to complete the assessment are presented, however a complete walkthrough is not provided, as much of the method requires independent thought and a thorough understanding of the organization that is being assessed. This is intended to be a paper to support the proposed method and a guideline to carry out that method.

Method Design

The Risk Map is designed to serve as the risk assessment along with being the audit trail of security and policy compliance. The Risk Map will be the framework for a risk assessment for the organization as a whole, along with aggregating the individual business unit assessments. The first step involves documenting the organizations business structure and identifying the consequences, which will have the largest impact on operations. This will begin to outline what business units are responsible for preventing certain consequences.

Often an assessment is limited in scope, only focusing on a specific location or department. This analysis method relies on considering the entirety of the organization that is being assessed first, then carry the risk mitigation to the departmental level. At this point, those creating the strategic overview of risks and consequences can choose which results would be most detrimental to the operation of the business. This is done without considering the specific threat that could be invoked to cause that result. The association of the consequence vs. threat vector will be judged by the operational units throughout the business, or by knowledgeable associates, but the consequences are sorted at the strategic level. The business units will then perform their own individual risk assessments according to the strategic outline. The consequence types to be used:

Consequences

Loss of Power
Loss of Systems/Data
Loss of Physical Security Controls
Loss of Associates
Damage to Client/Partner
Disclosure of PHI
Loss of Assets
Loss of Ability to Process
Loss of Ability to Do Business
Loss of Prestige/Reputation
Regulatory Breach
Loss of Backup Systems/Data
Physical Security Breach
Network Security Breach
Loss of Network Security Controls
Breach of Policy
Illegal Activity
Breach of Contract

For the most part, the consequences are general, so that the strategic choice of which consequences need to be avoided is made. Then assign resources and responsibility where necessary. This assists in the determination of the organizations overall security posture. It is not necessary for the senior management to determine what departments in the organization must play a role in preventing undesirable consequences.

Once the strategic security posture has been identified, the information can be turned over to those who can determine what departments play a role in the resulting

consequences. For example, the Call Center can easily disclose PHI, whereas the Server Security group does not directly interact with external customers, is less likely to cause such a thing. This approach can rely either on business leaders or technology experts, but it is guided by the strategic determination of the worst consequences. (See Appendix A.)

With a basic table of what consequences are the greatest to which departments and locations, the threat vectors can be added to this table. To continue the Call Center and Server Security analogy, where the Call Center isn't very likely to have an Administrator go AWOL or need to protect their portion of the network from an intrusion. However the Call Center would be very susceptible a regulatory compliance failure, by disclosing PHI.

At this point, only the consequences will have been associated with the departments, locations or organizational units. The next step in the process will be to associate the threat vectors with the consequence and location. This only determines what threats and consequences a location may or may not be susceptible to, not what departments are responsible for mitigating that risk. This is to create understanding of the overall security stance, and what departments are affected by a consequence.

After determining what consequences are associated with the relevant areas, they can be separated to focus on the specific threats, and the person responsible for that area can perform the risk analysis. The threat vectors that will be used are as follows:

Threat Vectors

Natural Disaster
Electricity Disabled/Destroyed
Hardware/Software Failure
Hardware/Software Malfunction
Physical Security Control Failure
Physical Security Control Malfunction
Network Security Control Failure
Network Security Control Malfunction
Malicious Persons
Employee
Unknown User Infiltration - Network
Unknown User Infiltration - Physical
Corporate Policy Breach
Regulatory Compliance Failure
Administrator
Trusted Third Party
Consultant
Unknown User
Malicious Software
Evil Internet
Theft/Embezzlement
Burglary
Unauthorized Access

These Threat Vectors cover almost the entire range of threats that would be faced by an organization that is connected to the Internet. They are vague, and that is to leave flexibility to individual departments in crafting and implementing policies and procedures to address possible repercussions from the threat. (See Appendix B.)

Now the assessors determine what threat vectors can be mitigated enterprise wide and what threats have to be mitigated at a lower level such as the department or area. Many threats will require coordinated action from the associate level to the enterprise level. This exercise determines what risks can be focused on at a strategic level, and what risks will have to be driven by individuals or departments at a tactical level. For instance the Billing Department is susceptible to a hardware/software failure, however it isn't responsible for contingency planning so that they themselves can replace the affected hardware. This step only identifies potential risks and what areas may be responsible for them, leaving the actual mitigation actions left to the specific department or individual.

To continue with the Billing Department example, the threats they are able to mitigate could be, Malicious Employee, Theft/Embezzlement, Unauthorized Access, and Corporate Policy Breach. Controls and separation of duties are necessary to prevent a single employee from committing theft, along with audit trails and records that state what users have accessed whose information, so there is a trace back to any information that is accessed. Unauthorized access is prevented by using permission-based applications which are protected (password or otherwise) and only grant access based on responsibility. (See Appendix C.)

The end result of this exercise will be an outline of consequences and threat vectors that are associated with a department. The associations made will be the beginning of the responsibility mapping which now assigns the 'risk' to the appropriate party. Risk is defined in this case as a combination of the consequences and threat vectors grouped with the affected department. The business leaders of the organization have driven the process, and what they feel are the direst consequences, leaving subject experts or department supports to actually implement the procedures and policies to mitigate these risks. Traditional threat cases can be built if necessary according to the department that the assessment is taking place in.

To continue the process, it is necessary to determine what operating areas will be responsible for mitigating risks. This section assigns the mitigation responsibilities to the proper department. Using a variety of questions and exercises, each location, department or area is assigned to guard against possible risks. This approach makes any gaps in policy apparent by showing what threats have no department responsible for them, what threats need to be dealt with on an enterprise level, and which can be focused on at the department or local level. This step is not designed to create actual strategies for dealing with risks and threats, but what sections will ultimately be responsible for developing and implementing those strategies. This exercise will be used for the planning stages of risk mitigation. (See Appendix D.)

Once the mapping of enterprise responsibility is complete, the process of developing actual strategies and actions to mitigate the risks identified begins. Continuing with the philosophy of top down, begin at the enterprise level. Determine what broad policies will counteract risks at the enterprise level. The objective at this point is to create

strategies that will speak to compliance, threat mitigation and security, while leaving room for the specific procedures created by the locations, departments and other areas to operate. After creating outline policies for the enterprise, the creation of procedures and policies for the next level begins. This could be physical locations, geographic or regional, or even the departments themselves. If it's a large area, something like the European Union, the policies and procedures developed will still be very general, but there may be policies in place regarding privacy and data safeguarding, that are not necessary in the US [7]. The flexibility allows the enterprise to create the specific procedures necessary for operating in that environment.

This process will be continued throughout the entire organization. Once the overall enterprise and regional policies have been developed, security and risk responsibilities can be filtered down to specific departments and operating areas. In this stage the individual departments now create solutions for their requirements, and implement the enterprise wide or regionally mandated policies or procedures. The Risk Map explains how risk is spread across the organization, and where departments fit into the corporate security program. This functions as both a planning tool and educational tool.

With the flexibility of this approach, there will be plenty of room for non-security units to implement their own specific policies and procedures to address the risks and threats that they are responsible for. These department or unit level procedures can be as specific or broad as necessary, but must adhere to the corporate wide policy on the matter, if there is one. An example of this could be the Web Development team has web application security testers. While they are not a part of the full time security unit, they are performing a security duty. Through using the risk map, web application security is assigned to the web security portion of the web development team and the security team will perform the auditing.

To avoid redundant policies and procedures, they are worked down the chain of command in the first steps, so that corporate strategic decisions can be made. After the local departments and areas have created their working procedures, they are sent back up the chain for a review of adherence to corporate policy and strategy. Once this review has been completed, the working areas should be left with clear procedures to follow, which were designed and created by those operating units themselves.

The end results of this risk assessment and analysis are HIPAA Security compliance as well as SysTrust accreditation, which validate the integrity, confidentiality and availability of data in the environment.

Current Methods

Many risk assessments follow the path of considering threat cases from a limited knowledge base, and of focusing on general mitigation factors (or controls) as opposed to associating the threats and risks with the corresponding responsible party, which could be anything from the entire organization, or a single associate. Without knowing who or what is responsible for specific types of threats leads to risks being considered

out of context. To create guidelines to considering threats, the concept of Threat Vectors is used. A Threat Vector is a potential avenue for the cause of a consequence. The value in this type of threat consideration is the vectors cover all types of possible threats, and can be used in department risk assessments by business unit leaders. By using these types of threat vectors you can create an organizational driven risk assessment program, which incorporates the particular goals of the organization but is not limited to the reactive nature of different threat cases. This grants the ability to perform many different and flexible types of risk assessments within each business unit.

For example, the COBRA philosophy is similar to a threat case based method, in that they use a set of pre-defined questions that illustrate and explain possible risk, educate the user and determine how one would answer or mitigate such a threat. The strengths of this method lie in both the education and the involvement of many different levels of the organization to create the risk state. The weakness of this method is that the framework for the threat mitigation is not clearly articulated, nor is it guided and created by the people responsible for the operation of specific business units. Instead relying upon a knowledge base compiled through customer interactions and case specific scenarios. [1]

With this in mind, these risk assessment guidelines have been created with the intention of using threat vectors and responsible parties, for risk analysis that can be performed by people at any level in the organization and should be performed at every level. Guidelines created by strategic decision makers set the boundaries and direction of the assessment and resolutions. The assessment guides the user, to determine what the greatest risks are to a specific organization, department, location, person or asset using an outline of threat vectors. These vectors cover all types of potential threats and are not limited to a type of knowledge base. This will determine the current risk state by using the answers and reactions from the people/department responsible for the mitigation of that threat vector as well as audits performed by the assessors. This is intended to create an analysis that will accurately reflect constantly changing threats and their risk levels, which can also be used to audit compliance of resulting initiatives.

One of the more important assumptions of this method is the support of senior executives. At this point in time, security, performing risk assessments and safeguarding confidential data have all been legislated in major industries, and organizations, and more importantly senior executives, are now responsible for this protection. Particularly in the health care arena, which has had both its privacy and security legislated, at least in the United States. This has led to increased awareness and support from senior management who are now responsible for compliance with such regulations. The pure quantitative assessment is no longer necessary to defend and support security spending. [2]

The introduction of the Sarbanes-Oxley Act of 2002 has several security ramifications. [5] The necessity of internal control structures to monitor and audit the actions of the organization in the financial context are carried over to other portions of the business. As separation of duties has now been legislated, along with the statute that requires

these controls be audited by an external firm, it's another point that security processes and Information Security in general can assist in complying and maintaining compliance of this law. Taken from Section 404 of the Sarbanes-Oxley Act; [6]

> *(1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting; and*
>
> *(2) contain an assessment, as of the end of the issuer's fiscal year, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.*

These types of controls and assessments would be best served by adding them to the risk assessment, as they are potential risk points, and the mitigation factors need to be documented and controls and policies implemented to mitigate the risks and non-compliancy. The Act also mandates that the results, procedures and controls be audited by an external organization, which does not have ties to the organization being assessed.

Another assessment program to consider, which is most similar to the proposed method, is the OCTAVE® Approach [4], which considers many of the strengths and weaknesses of other risk assessments. The focus is more directed towards an overall strategic risk management program, which does not focus solely on information technology and the systems surrounding it. The approach guides the assessor, which is non-expert led, to use the common business sense to calculate and determine risks and mitigation factors. Combined with a large threat case set, this can provide a very comprehensive assessment, which speaks to many of the different business needs as well as the technical requirements. However, it is designed to be driven by a small group, and does not advocate for enterprise wide security policies which are designed from a high level view of the organization. The combination of both C level and line unit policies and procedures is necessary for education and comprehensiveness.

Currently most risk assessment methodologies rely on focusing on just a particular system or set of systems that are deemed to be the most important or are chosen because they are most visible. While the majority of the solutions identified through risk assessment are implemented by a small group of security professionals, there is no education throughout the organization of what is being done, and how it affects each user or even what the efforts are intended to accomplish.

In the Information Security Risk Assessment Practices of Leading Organizations [8] the GAO outlines similar steps to the proposed method. In particular, holding the business units responsible for assessments. However the proposed method goes slightly farther, by also holding them responsible for some of the security controls and processes that need to be put in place. Another addition over the GAO method reviewed is the overall Risk Map framework, which allows for a comprehensive security view of an organization, but can be carried out in the localized manner that the GAO identified.

The overall assessment also covers the hierarchal nature of responsibility for different risks and threats. All departments are not responsible for protecting entry and exit from its' operational area, yet each would be responsible for keeping patient records in locked storage, while access to the entire building must be supervised. Another department does that. Using this process outlines the interdependencies of responsibility between each operational sector of the organization, which then enables those different groups to take steps to mitigate their portion of the risk, while educating them on the overall responsibility for that risk

It is possible to consider the above physical access risk posed to the whole of the enterprise, but it is mitigated in different ways at different physical locations. So the breakdown of the policy to mitigate that risk could be as follows: There is a corporate wide policy stating that no unauthorized access is to be granted to users/visitors. One location may use biometric identification, while another could use magnetic card readers. This now splits into location responsibility, and the specific policy or procedure for each location. The HR department is responsible for granting and terminating access. The reception office is responsible for opening the door when an authorized visitor arrives, and denying when necessary. Each individual is responsible for reporting suspicious, unauthorized or unknown visitors.

The proposed method standardizes the criteria of threats and risks so that local supports are able to effectively mitigate the risks specific to their department or area and give the enterprise the ability to detect what risks have not been given ample attention or resources. This is accomplished by creating a risk map that takes into account the organizations structure and the responsibilities of each portion of the organization while focusing on the specific risks that can be mitigated by each of those departments.

Whereas the weakness in today's common methods would be the focus on specific threat cases, that are met by specific security elements which are very broad, and almost wholly the responsibility of the professional security team. The result is that threat cases which are considered only in the context of Information Security and how the threats are mitigated by those means, without concern for how those types of threats affect other areas of operation. For this reason, along with the fact that many risk assessments will leave out threat cases, or not consider them from the view of a non-security operations unit. If there is no documentation as to why they are not considered, it cannot be known whether the threat was mitigated, not of concern, or just ignored. The proposed method will result in a comprehensive security view, not only including the why of the threat cases considered, but the why not of the cases left. Without this information, an analysis has limited itself, and could lead to unnecessarily lower or higher levels of risk.

Method Outline

1. Determine organizations business structure. Use this as the framework for departmental risk assessments.

2. Determine which Consequences have the most detrimental effect to the operation of the business.

3. Determine what portions of the organization are the most affected by a particular consequence.

4. Determine which Threat Vectors are relevant to departments throughout the organization.

5. Complete the Risk Map that organizes threat vectors, consequences and departments that will account for mitigating the threats and consequences.

6. Use the Risk Map to guide the creation of controls and policies to mitigate risks where appropriate.

References

1. C & A Security Risk Analysis Group. "The Risk Assessment Process." Introduction to Security Risk Analysis & Security Risk Assessment. http://www.security-risk-analysis.com/introduction.htm (6/16/2004).

2. Merrit, James W. "A Method for Quantitative Risk Analysis." 10/1999. http://csrc.nist.gov/nissc/1999/proceeding/papers/p28.pdf (6/16/2004).

3. Office of the Secretary. “Health Insurance Reform: Security Standards; Final Rule” Final. 2/20/2003. http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf (6/19/2003).

4. Alberts, Christopher. Dorofee, Audrey. Stevens, James. Woody, Carol. “Introduction to the OCTAVE® Approach” August 2003. http://www.cert.org/octave/approach_intro.pdf (6/21/2004).

5. One Hundred Seventh Congress of the United States of America. “Sarbanes-Oxley Act of 2002”. 01/23/2002. http://news.findlaw.com/hdocs/docs/gwbush/sarbanesoxley072302.pdf (6/21/2004).

6. AICPA. Summary of Sarbanes-Oxley Act of 2002. 2002. http://www.aicpa.org/info/sarbanes_oxley_summary.htm (6/21/2004).

7. European Parliament. Directive 95/46/EC. 11/23/1995. http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31995L0046&model=guichett (6/28/2004).

8. General Accounting Office. 11/1999. http://www.gao.gov/special.pubs/ai00033.pdf (6/29/2004).

9. AICPA/CICA. AICPA/CICA Trust Services. 4/1/2003. http://www.aicpa.org/assurance/systrust/princip.htm (6/29/2004).

Definitions

Threat Vector – A potential avenue for the cause of a consequence

Consequence – An unfavourable result of the exploitation of a threat vector

Risk – The combination of Threat Vector and Consequence

Risk Map – The outline of an organizations risk mitigation strategy

Threat Mitigation – The implementation of policies, procedures or controls to decrease the likelihood or impact of a consequence.

Location - The geographic or logical area where the consequence, threat vector or risk is being considered.

Department - The units assigned to develop policies and procedures to mitigate risk caused by specific threat vectors and consequences.

Impact - The alleged impact of the consequence or event occurring.

Likely - The likelihood of an event occurring under the specified circumstances.

Appendix A

Location	Consequence	Impact	Explanation
Location 1	Loss of Power	Minor	If there is a loss of power greater than 3 days, it is declared a disaster and the DR plan is put into action.
Location 1	Loss of Systems/Data	Major	Would have a major impact on operations for a several hour period, non-critical systems loss would not affect overall operations.
Location 1	Loss of Backup Systems/Data	Major	Everyday operations would not be affected, however were there to be a loss of production systems/data the company would be in a disaster situation
Location 1	Disclosure of PHI	Minor	Current privacy policies mitigate this consequence by providing specific resolutions to disclosure.
Location 1	Loss of Ability to Process	Catastrophic	Claims, orders and customer service are all performed in this location, the loss of these services would critically damage the organization.
Location 1	Loss of Network Security Controls	Major	Would expose critical systems to attack or compromise, would have an affect on other areas of operation
Location 2	Loss of Power	Minor	If there is a loss of power greater than 3 days, it is declared a disaster and the DR plan is put into action.
Location 2	Loss of Systems/Data	Minor	Very little mission critical processing is performed at this location; systems would be restored while other locations pick up the workload.
Location 2	Loss of Backup Systems/Data	Minor	Potential for important client data to be lost, operations would be able to continue
Location 2	Disclosure of PHI	Minor	Current privacy policies mitigate this consequence by providing specific resolutions to disclosure. Very little PHI goes through this location.
Location 2	Loss of Ability to Process	Major	Would have greatest effect on marketing and sales, however business could continue to operate
Location 2	Loss of Network Security Controls	Minor	Area could be segregated from rest of business and repaired without compromising the security of the business as a whole.

Appendix B

Location	Threat Vector	Consequence	Severity	Explanation
Location 1	Hardware/Software Failure	Loss of Systems/Data	Major	The loss of the systems and data at this location would cause major disruption to business, would take several hours to recover from backup.
Location 1	Hardware/Software Failure	Loss of Backup Systems/Data	Major	Would make the organization unable to recover from an event that caused primary systems to cease functioning. Potential for catastrophic failure.
Location 1	Hardware/Software Failure	Loss of Network Security Controls	Major	Creates the potential for unauthorized access to Ephi and other confidential data.
Location 1	Hardware/Software Failure	Loss of Ability to Process	Catastrophic	Location ceases to function until backup systems restored, orders, claims, eligibility all stop.
Location 1	Hardware/Software Failure	Disclosure of PHI	Minor	Does not apply, if the hardware/software ceases to function, it will not return any information
Location 2	Hardware/Software Failure	Loss of Systems/Data	Minor	This location could continue functioning with minimal systems and data functioning.
Location 2	Hardware/Software Failure	Loss of Backup Systems/Data	Major	Could not recover important marketing, sales and financial data, effect would not be immediate.
Location 2	Hardware/Software Failure	Loss of Network Security Controls	Major	Would cause network segment to be shut down, affects new business, provider relations, marketing efforts to be disrupted.
Location 2	Hardware/Software Failure	Loss of Ability to Process	Major	Affects new client proposals, sales efforts and customer retention
Location 2	Hardware/Software Failure	Disclosure of PHI	Minor	Does not apply, if the hardware/software ceases to function, it will not return any information

Appendix C

Location	Threat Vector	Consequence	Department	Mitigation	Explanation
Location 1	Hardware/Software Failure	Loss of Systems/Data	System Services Server Administration Information Systems & Network Services	Enterprise	The respective departments will be required to document and outline the policies and procedures for the restoration, protection and repair of hardware and software systems for the entire enterprise.
Location 1	Hardware/Software Failure	Loss of Backup Systems/Data	System Services Server Administration Information Systems & Network Services	Enterprise	The respective departments will be required to document and outline the policies and procedures for the restoration, protection and repair of backup hardware and software systems for the entire enterprise.
Location 1	Hardware/Software Failure	Loss of Network Security Controls	Server Administration Information Systems & Network Services	Enterprise	Policies and procedures are developed along the guidelines specified in the Final Security Rule.
Location 1	Hardware/Software Failure	Loss of Ability to Process	System Services Server Administration Information Systems & Network Services Programming	Enterprise	These departments will create the policies and procedures so that the enterprise can continue to function. Each of these departments are responsible for their respective areas of operation.
Location 1	Hardware/Software Failure	Disclosure of PHI	All Privacy Office	Enterprise	All associates are trained and educated to be aware of the fact that a disclosure must be reported immediately and investigated. The Privacy Office is fully prepared to investigate and remedy any disclosures.
Location 2	Hardware/Software Failure	Loss of Systems/Data	Technical Support Information Systems & Network Services	Location 2	Location 1 provides the primary expertise, while Location 2 Technical Support, would perform the actual replace or repair if necessary.

Location 2	Hardware/Software Failure	Loss of Backup Systems/Data	Technical Support Information Systems & Network Services Server Administration	Location 2	Location 1 provides the primary expertise, while Location 2 Technical Support, would perform the actual replace or repair if necessary.
Location 2	Hardware/Software Failure	Loss of Network Security Controls	Information Systems & Network Services Server Administration	Location 2	The security teams from Location 1 would do all of the necessary monitoring and maintenance for all Locations network security, and also are tasked with repairing any failures.
Location 2	Hardware/Software Failure	Loss of Ability to Process	Technical Support Information Systems & Network Services Server Administration System Services Programming	Enterprise	The Location 1 support groups would assist Location 2 Technical Support in restoring operation to that location by BCP and DR plans.
Location 2	Hardware/Software Failure	Disclosure of PHI	All Privacy Office	Enterprise	All associates are trained and educated to be aware of the fact that a disclosure must be reported immediately and investigated. The Privacy Office is fully prepared to investigate and remedy any disclosures.

Appendix D

Location	Threat Vector	Consequence	Department	Impact	Mitigation	Likely	Explanation
Location 1	Hardware/ Software Failure	Loss of Systems/Data	System Services Server Administration Information Systems & Network Services	Minor	Enterprise	3	During normal operation, the likelihood of this event occurring is constant.
Location 1	Hardware/ Software Failure	Loss of Backup Systems/Data	System Services Server Administration Information Systems & Network Services	Major	Enterprise	2	There are a few circumstances where the likelihood of this event occurring increases. These are, natural disasters, wars and malicious employees/admins
Location 1	Hardware/ Software Failure	Loss of Network Security Controls	Server Administration Information Systems & Network Services	Major	Enterprise	4	The chances of this event are increased when a vulnerability in a popular program is found and exploit code is released to the public before the vulnerability has been repaired by the vendor.
Location 1	Hardware/ Software Failure	Loss of Ability to Process	System Services Server Administration Information Systems & Network Services Programming	Catastrophic	Enterprise	1	This event can only occur if all backup systems fail, and the backup site has been destroyed.
Location 1	Hardware/ Software Failure	Disclosure of PHI	All Privacy Office	Minor	Enterprise	3	The most likely occurrence of this event is during system upgrades and maintenance. The approach of failing 'closed' to deny all data is taken.
Location 2	Hardware/ Software	Loss of Systems/Data	Technical Support	Major	Location 2	3	The likelihood of this occurring changes

	Failure		Information Systems & Network Services				depending on the local conditions, however the impact and resolution are the same.
Location 2	Hardware/ Software Failure	Loss of Backup Systems/Data	Technical Support Information Systems & Network Services Server Administration	Minor	Location 2	2	During normal operation, the likelihood of this event occurring is constant.
Location 2	Hardware/ Software Failure	Loss of Network Security Controls	Information Systems & Network Services Server Administration	Minor	Location 2	3	The chances of this event are increased when a vulnerability in a popular program is found and exploit code is released to the public before the vulnerability has been repaired by the vendor.
Location 2	Hardware/ Software Failure	Loss of Ability to Process	Technical Support Information Systems & Network Services Server Administration System Services Programming	Minor	Enterprise	2	This event can only occur if all backup systems fail, and the backup site has been destroyed.
Location 2	Hardware/ Software Failure	Disclosure of PHI	All Privacy Office	Minor	Enterprise	1	The most likely occurrence of this event is during system/software upgrades and maintenance. The approach of failing 'closed' to deny all data is taken.

Last Updated: July 27th, 2017

Upcoming Training

SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event