



Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permitted without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Managing Cybersecurity Initiatives & Effective Communication (Cybersecurity L
at <http://www.giac.org/registration/gcpm>

Risky Business

SimpleRisk: Enterprise Risk Management Simplified

GIAC (GCPM) Gold Certification

Author: Robert Sorensen, rssoren@gmail.com
Advisor: Stephen Northcutt

Accepted: June 06, 2014

Abstract

Risk Management is often an overlooked aspect of any Cybersecurity program, however, without it, the potential of a major incident increases. The challenges associated with risk management are figuring out how to identify, prioritize, track, and mitigate risk. This paper will explore a framework of managing risk by utilizing an open source program called SimpleRisk. A case study involving GIAC Enterprises, will explain the features and advantages of using such a tool to manage risk.

1. Introduction

Risk Management has evolved just like many other aspects of IT Security. Risk management, or threat modeling, requires a methodical approach or framework. In Adam Shostack's new book, *Threat Modeling: Designing for Security*, he introduced a way to look at threats by focusing on four key questions: "What are you building? What can go wrong? What should you do about those things that can go wrong? Did you do a decent job of analysis?" (Shostack, 2014, p. 5).

While this may seem like a simple concept, identifying, managing, and more important, mitigating risk is where IT Security professionals truly earn their keep. In their book, *Managing Cybersecurity Resources: A Cost-Benefit Analysis*, Lawrence Gordon and Martin Loeb point out, "given the unpredictable nature of breaches, cybersecurity decisions are often based on gut instinct rather than sound economic analysis" (Gordon, 2006). Gut instincts are not enough to combat the many challenges presented by the sophisticated threat actors in today's world.

Risk management is an integral part of project management. Project risk management is one of 10 key project management knowledge areas as defined by the Project Management Institute. As outlined in the *Project Management Body of Knowledge PMBOK Guide, 5th Ed.*, "Risk Management is the process of defining how to conduct risk management activities for a project. The key benefit of this process is that it ensures that the degree, type, and visibility of risk management are commensurate with the risks and the importance of the project to the organization." (A Guide to the Project Management Body of Knowledge, 2013, p. 467).

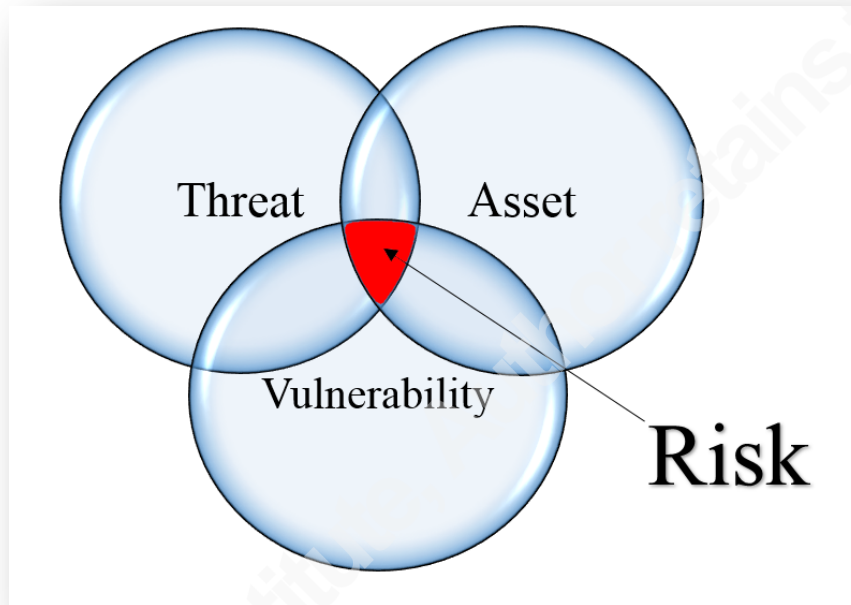
This paper will explore the concepts of risk management, introduce SimpleRisk open source framework, and finally, illustrate the power of SimpleRisk through a detailed case study involving GIAC Enterprises.

2. Risk Management Concepts

While the concept of risk is well known, it can still present challenges for IT Security professionals. According to Gartner, by 2010, 30% of global 2000 companies will have been directly compromised by an independent group of cyber activists or cyber criminals (George, 2014). This prediction is not surprising given the aggressive approach used by cyber foes.

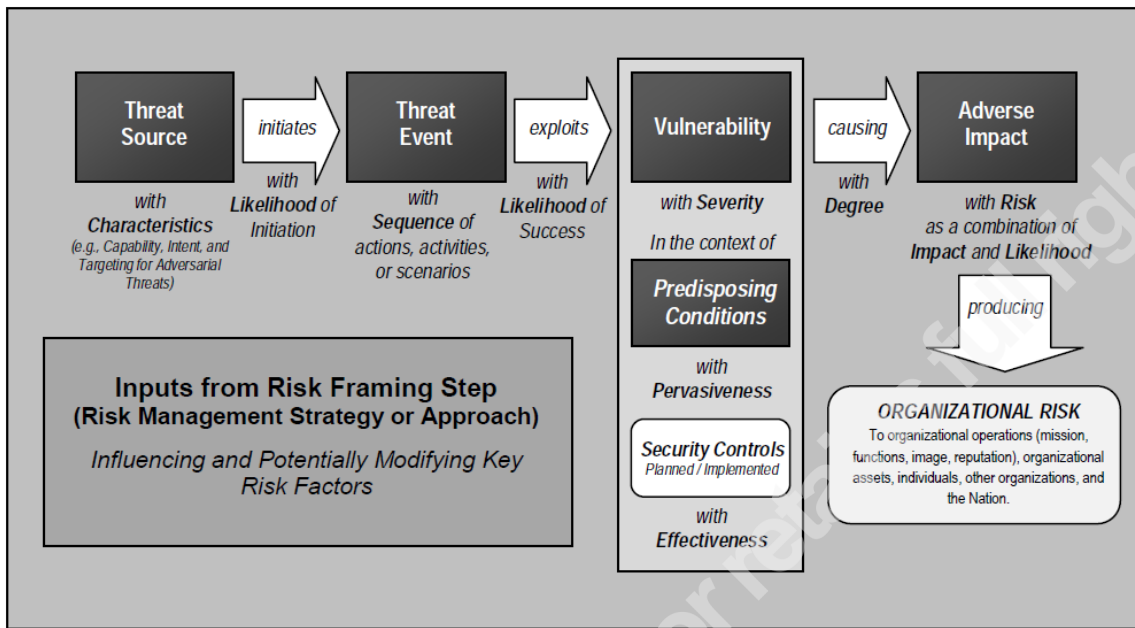
Robert Sorensen, rssoren@gmail.com

Security risk is often represented as any event that could compromise the assets, operations and objectives of an organization. In order for an 'event' to occur and expose a risk, two conditions are required: First, a vulnerability must exist such as a software flaw or poor programming technique, business operations insecurity, and employees not following access and usage policy; Second, a threat must exploit that vulnerability. This is well represented in the following diagram:



2.1. Risk Model

As described in the NIST Special Publication 800-30 Revision 1, a risk model defines the risk factors to be assessed and the relationships among those factors. A generic risk model with key risk factors is illustrated in the following figure (SP 800-30r1, p. 12).



As shown, risk is a function of the likelihood of a threat event's occurrence and potential impact should the event occur. It also shows relationships and degrees of impact. For example, loss of current or future business due to a potential loss of proprietary data or the unavailability or degradation of information systems.

2.2. Threats

Threat sources can be categorized as adversarial, accidental, structural, or environmental. Adversarial threats can be described as individuals, groups, organizations, or states that seek to exploit the resources of an organization. Accidental threats can be described as erroneous actions taken by individuals in the course of performing their everyday tasks. Structural threats can be a failure of equipment, environmental controls, or software. Finally, environmental threats could consist of natural disasters and failures of critical infrastructure on which the organization depends but which are outside the control of the organization. Appendix A provides additional detail as defined by NIST (SP 800-30r1, p. D-2).

2.3. Threat Events

There are many different penetration vectors or threat events. They can be categorized or grouped as such:

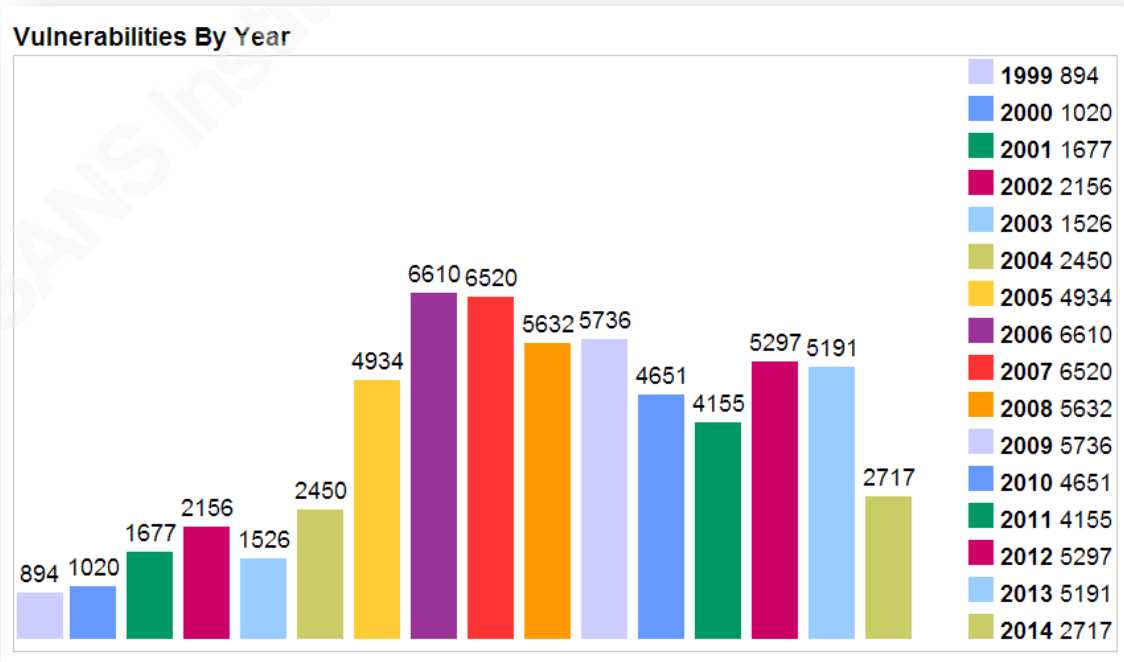
Robert Sorensen, rssoren@gmail.com

- Perform reconnaissance and gather information
- Craft or create attack tools
- Deliver/insert/install malicious capabilities
- Exploit and compromise
- Conduct an attack (direct/coordinate attack tools or activities)
- Achieve results (cause adverse impact, obtain information)
- Maintain a presence or set of capabilities
- Coordinate a campaign

These threat events are important to understand as they provide an insight for potential risk mitigation. Appendix B provides additional detail as defined by NIST (SP 800-30r1, pp. E-2-6).

2.4. Vulnerabilities

A quote from John Pescatore, who was a Vice President at Gartner, Inc. at the time, sums up things nicely in regards to vulnerabilities, "There is no such thing as the unstoppable attack in cybersecurity. Every attack, in order to succeed, needs to exploit a vulnerability" (Infosecurity-magazine.com, 2011). As of May 30, 2014, there have been 2,717 new vulnerabilities reported to the Common Vulnerabilities and Exposures (CVE) database just in 2014 alone! As shown in the chart below, there will always be new vulnerabilities (Cvedetails.com, 2014).



The most recent zero-day Internet Explorer vulnerability affecting versions of IE dating back to version 6.0 immediately received the attention of Microsoft when Adrienne Hall, General Manager, Microsoft Trustworthy Computing stated, “The security of our products is something we take incredibly seriously. When we saw the first reports about this vulnerability we decided to fix it, fix it fast, and fix it for all our customers” (Zeltzer, 2014).

What security professional has not heard of or been affected by the recent Heartbleed OpenSSL cryptographic library vulnerability that allows attackers to invisibly read sensitive data from a web server? This was a big deal as it was estimated that approximately 66% of the Internet or two-thirds of the web servers could be using this software (Powledge, 2014).

Adobe Flash is always an exploit vector as they again just had to release an emergency update amid new zero day drive-by attacks (Goodin, 2014).

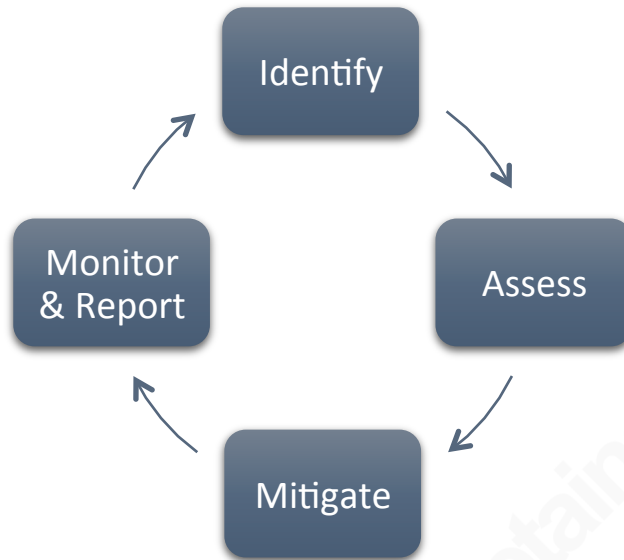
The few examples just mentioned provide the Threat Actors with plenty of ammunition in which to focus their attacks.

2.5. Risk Management Cycle

Now that risk has been defined with the relationship between assets, threats, and vulnerabilities, it is important to recognize the risk management cycle. As mentioned, risks first need to be **Identified**. This can be based on a vulnerability scanning, management review of process and procedures, type of assets and potential vectors of exploits based on operating system and applications that are being used. Next, the need to **Assess** the risk based on the likelihood, impact and potential loss of reputation or goodwill or associated costs. The next key point is **Mitigation**, or taking the steps to reduce risk to an acceptable level. Risk cannot be mitigated if it has not been identified or understood. Risks can be avoided, transferred, mitigated, or just plainly accepted. The **Monitor & Report** step is to help management perform reviews and access the progress of risk mitigation projects defined and implemented in the mitigation step.

Of course, this is a continual cycle of circling back to identify potentially new, or the evolution of current risks. The ***Risk Management Cycle*** is illustrated below:

Robert Sorensen, rssoren@gmail.com



3. SimpleRisk

SimpleRisk was developed by Josh Sokol, who ran into many barriers and budget constraints in regards to tools to manage risk. Very few companies can afford the expensive IT Governance, Risk and Compliance (GRC) tool sets that can assist an analyst in managing risk. However, as pointed out by Michael Rasmussen, President of Corporate Integrity, “People are doing IT GRC whether they are calling it that or not, but they are document-centric [solutions], using spreadsheets and other documents. Spreadsheets are a recipe for disaster. Eventually, they outgrow this; they don’t have proper audit trails and it becomes unmanageable” (Roiter, 2011).

Josh decided to do something about it and developed SimpleRisk based entirely on open source technologies and using the Mozilla Public License 2.0. It is highly configurable and includes dynamic reporting with the ability to tweak risk formulas on the fly. It is under active development, and new features are being added all the time. SimpleRisk is truly Enterprise Risk Management simplified (SimpleRisk).

3.1. SimpleRisk Installation

For testing, SimpleRisk was installed on an Ubuntu 14.04 virtual machine with a full LAMP stack. Three very detailed installation guides (*SimpleRisk Installation Guide*, *SimpleRisk Upgrade Guide*, and *SimpleRisk Installation Guide*) are available from the simplerisk.org/documentation website (Sokol). In a recent *toolsmith* column in ISSA Journal,

Robert Sorensen, rssoren@gmail.com

Russ McGree also provides some quick installation notes (McGree, 2014). Following his quick install steps will eliminate the need to create/populate the SimpleRisk database via PHPmyadmin utility.

One note of interest in relation to the install is to make sure the SimpleRisk Web bundle is untarred under the active 'www' root in Ubuntu. For example, when Ubuntu 14.04/LAMP was installed, the default root directory for the web server was /var/www/html.

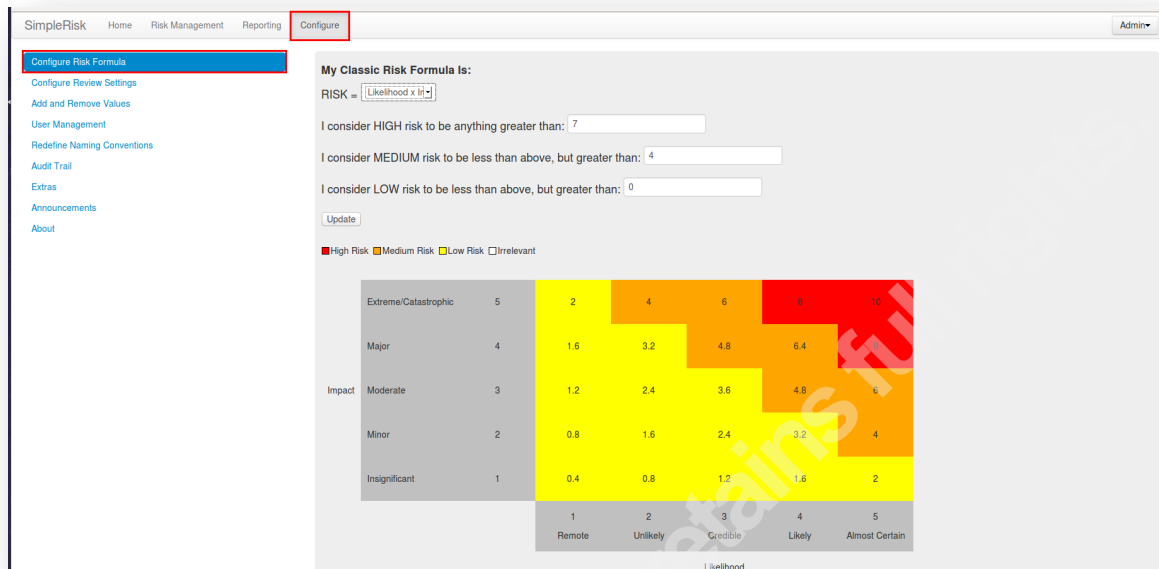
3.2. SimpleRisk Configuration

Once SimpleRisk is installed, there are configuration settings that may need to be made. Here are the configuration options:

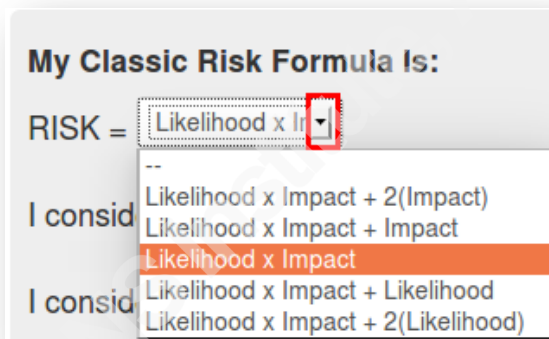
- Configure Risk Formula
- Configure Review Settings
- Add and Remove Values
- User Management
- Redefine Naming Conventions
- Audit Trail
- Extras
- Announcements
- About

3.2.1. Configure Risk Formula

The *Configure Risk Formula* configuration option provides a means to define the nature of risk. By default, High Risk is defined to be anything greater than 7. Medium Risk to be less than above (High Risk), but greater than 4. Low Risk is defined to be less than above (Medium Risk), but greater than 0. These can be changed if the need warrants. The chart below defines Impact (1. Insignificant/ 2. Minor/ 3. Moderate/ 4. Major/ 5. Extreme Catastrophic) vs. Likelihood (1. Remote/ 2. Unlikely/ 3. Credible/ 4. Likely/ 5. Almost Certain) and how each degree defines where the risk falls, i.e., High/Medium/Low.



The **Classic Risk Formula** defaults to *Likelihood x Impact* as shown in the drop-down menu associated with this setting.



The Risk table changes based on the risk formula selected. For example, selecting the formula $RISK = Likelihood \times Impact + 2(Impact)$ gives a much different risk profile. This formula adds more weight to the impact, thus increasing the risk.

My Classic Risk Formula Is:

RISK = Likelihood x Impact + 2(Impact)

I consider HIGH risk to be anything greater than:

I consider MEDIUM risk to be less than above, but greater than:

I consider LOW risk to be less than above, but greater than:

☒ High Risk
 ☒ Medium Risk
 ☒ Low Risk
 ☐ Irrelevant

Impact		1	2	3	4	5
		Remote	Unlikely	Credible	Likely	Almost Certain
Extreme/Catastrophic	5	4.3	5.7	7.1	8.6	10
Major	4	3.4	4.6	5.7	6.9	8
Moderate	3	2.6	3.4	4.3	5.1	6
Minor	2	1.7	2.3	2.9	3.4	4
Insignificant	1	0.9	1.1	1.4	1.7	2

Likelihood

3.2.2. Configure Risk Settings

The *Configure Risk Settings* option determines the number of days High, Medium, or Low risks are reviewed. The defaults are shown in the screenshot below.

SimpleRisk Home Risk Management Reporting **Configure**

[Configure Risk Formula](#)
Configure Review Settings
[Add and Remove Values](#)
[User Management](#)
[Redefine Naming Conventions](#)
[Audit Trail](#)
[Extras](#)

I want to review HIGH risk every 90 days.

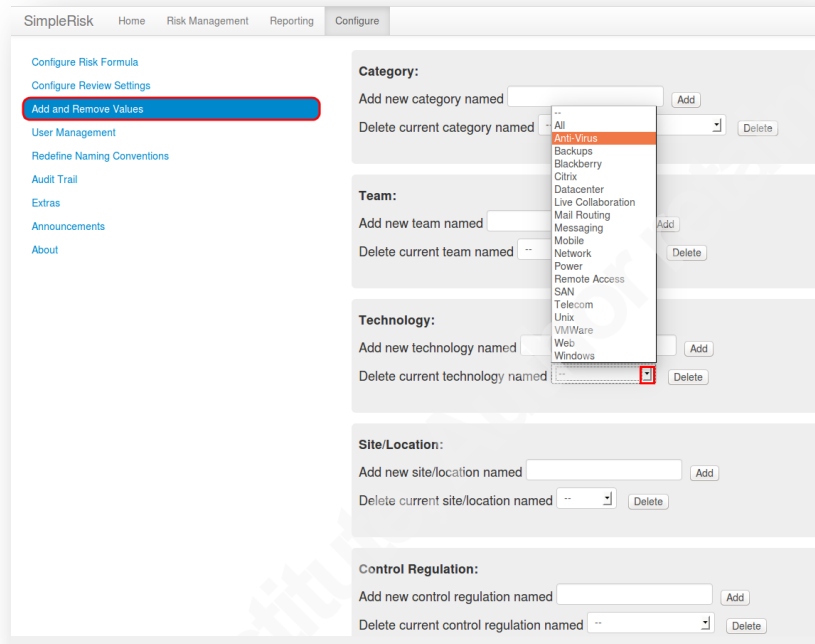
I want to review MEDIUM risk every 180 days.

I want to review LOW risk every 360 days.

Robert Sorensen, rssoren@gmail.com

3.2.3. Add and Remove Values

The *Add and Remove Values* option allows for very granular tracking and configuration of all aspects of tracking and managing risk. The ability to add/delete different values provides a risk manager the details that would not normally be tracked. Values include Category, Team, Technology, Site/Location, Control Regulation, Risk Planning Strategy and Close Reason. An example of the configuration setting is shown below.



3.2.4. User Management

The *User Management* option allows the SimpleRisk admin to create users with very specific roles. For example, the admin could define users that are only allowed to submit a new risk, modify existing risks, close risks, plan mitigations, review low/medium/high risks, or allow access to “Configure” menu. Certain roles can also be assigned based on teams(s) assignments. For example, an admin on the Network team could be assigned the responsibility to review and/or specific mitigate risks. Auditors are very keen on the separation of duties as Kevin Coleman, Technolytics Institute pointed out, “Separation of duties is a key concept of internal controls and is the most difficult and sometimes the most costly one to achieve. This objective is achieved by disseminating the tasks and associated privileges for a specific security process among multiple people” (Coleman, 2008).

Robert Sorensen, rssoren@gmail.com

SimpleRisk Home Risk Management Reporting Configure

Configure Risk Formula
Configure Review Settings
Add and Remove Values
User Management
Redefine Naming Conventions
Audit Trail
Extras
Announcements
About

Add a New User:

Type: SimpleRisk

Full Name:

E-mail Address:

Username:

Password:

Repeat Password:

Team(s)

Information Security
IT Systems Management
Network
Unix
Web Systems

User Responsibilities

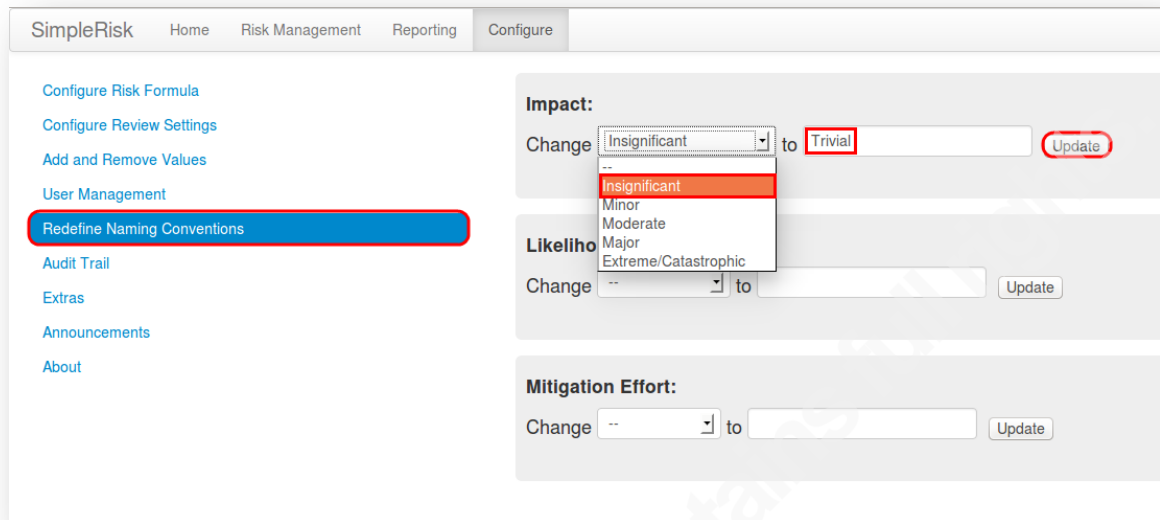
- ☐ Able to Submit New Risks
- ☐ Able to Modify Existing Risks
- ☐ Able to Close Risks
- ☐ Able to Plan Mitigations
- ☐ Able to Review Low Risks
- ☐ Able to Review Medium Risks
- ☐ Able to Review High Risks
- ☐ Allow Access to "Configure" Menu

Multi-Factor Authentication

☒ None

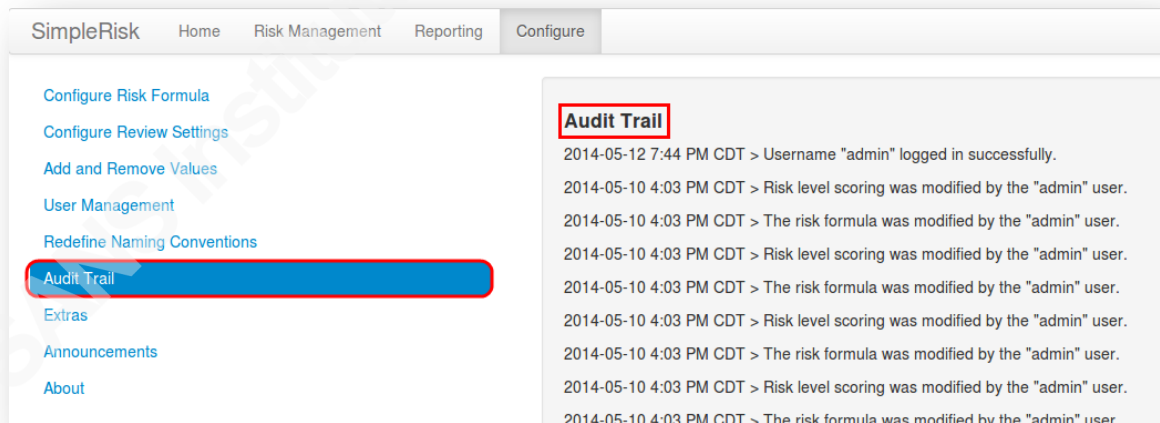
3.2.5. Redefine Naming Conventions

The *Redefine Naming Conventions* provides a means of redefining the meaning of Impact, Likelihood, and Mitigation Effort. For example, under Impact, a risk manager might want to change 'Insignificant' to 'Trivial'.



3.2.6. Audit Trail

The *Audit Trail* option is pretty self-explanatory. It keeps a detailed audit trail of all actions taken while working in SimpleRisk.



3.2.7. Extras

The *Extras* option provides premium add-ons to the core SimpleRisk platform which enhances and provides more functionality. The cost is reasonable and offers a perpetual license:

- **Cost authentication extra:** Currently provides support for Active Directory

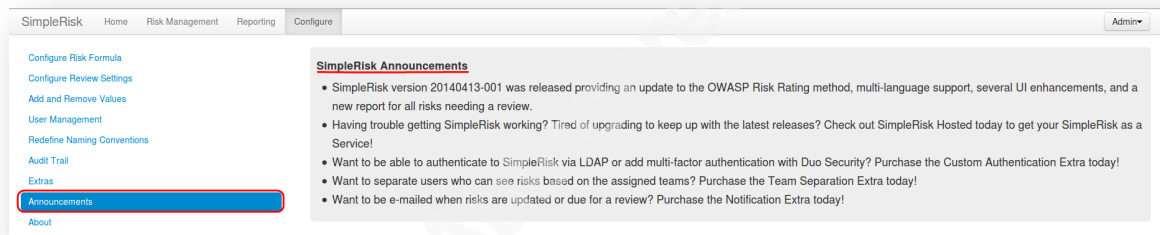
Robert Sorensen, rssoren@gmail.com

Authentication and Duo Security multi-factor authentication, but will have other custom authentication types in the future.

- **Team-Based Separation:** Restriction of risk viewing to team members the risk is categorized as.
- **Notification:** Sends email notifications when risks are submitted, updated, mitigated, or reviewed and may be run on a schedule to notify users of risks in the Unreviewed or Past-due state.
- **Encrypted Database:** Encryption of sensitive text fields in the database.

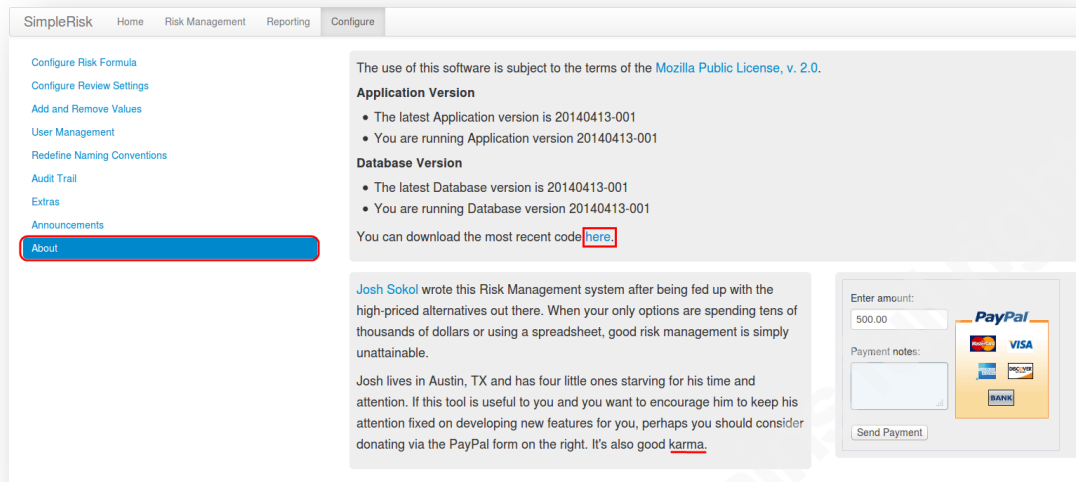
3.2.8. Announcements

The *Announcements* option provides the latest information related to SimpleRisk development and extra enhancement options.



3.2.9. About

The *About* option provides version information and informs admins when a new update is available along with a download link. Josh also provides a means of supporting his effort and earning some much needed karma.



4. SimpleRisk Case Study

4.1. Background

GIAC Enterprise (GIAC-E) is a small to medium-sized growing company. It employs 900 workers, including a small group of business and IT workers at corporate HQ, with the rest of the remote workforce distributed worldwide. They also have various support contracts in place to assist with day-to-day help desk, and commodity security products such as anti-virus/anti-malware. The company is the largest supplier of fortune cookies scripts or proverbs in the world and prides itself on a rich history as well as cutting edge original research. The current primary product of GIAC-E is the content of the fortunes themselves, i.e., the data. Data is handled at corporate headquarters.

GIAC-E current infrastructure services include the data center, networking, and central services such as Oracle and Exchange back ends. A firewall is deployed with a standard DMZ and Internal segments. Otherwise, the network is flat. This model has worked well for years so there is no real incentive to change this model. Like many other fledging businesses, GIAC-E employs minimal security practices and has no centralized security group. They do not see the need to spend a large percentage of their scarce resources on security since the current configuration seems to be doing a fine job. IDS/IPS is not deployed considering all workstations have anti-virus installed. Patching is spotty since it is the responsibility of the individual user to maintain their equipment.

Robert Sorensen, rssoren@gmail.com

Due to the competitive nature of the fortune cookie business, it is critical for GIAC-E to look for other means of distributing the fortunes. The tried and true method of having the cookies distributed from a central datacenter is no longer sufficient. By having all the data in one location also introduces additional risks associated with potential denial of service attacks or data loss due to sophisticated hacker attacks.

Research and development has continued to refine the development of fortune cookie sayings and have developed a propriety algorithm that has incorporated the explosion of social media. They have also developed the design of a fortune telling machine and its associated manufacturing process. This is the edge they need to stay a step ahead of their competition. Unfortunately, security was not integrated in the development/testing phases.

To their shock and surprise, GIAC-E's main competitor, Golden Dragon Fortunes, LLC, just announced a fortune telling machine that looked almost identical to their own. Not only that, the fortunes themselves showed characteristics of the new fortune-saying generation algorithm. How could this have happened since this was such a top secret project? Was GIAC-E compromised? So many questions with so few answers.

4.2. Identifying Risks

GIAC-E had never experienced a security breach like this before and did not have the in-house expertise to deal with such an incident. They immediately hired an external consultant, Security HD, Inc., to assist them. Security-HD, Inc. prides themselves in documenting and managing risks. They have integrated SimpleRisk to assist them in managing the risks exposed during the breach root cause analysis and after action report.

After a thorough investigation of the incident, Security-HD, Inc. identified the following risks that contributed to the breach:

1. GIAC-E.com website was discovered to have 12 Medium, and two High vulnerabilities including:
 - a. Cross-Site Request Forgery vulnerability was discovered that allowed remote attackers to hijack the authentication of administrators.
 - b. Multiple SQL injection vulnerabilities were discovered that allowed remote attackers to execute arbitrary SQL commands.

Robert Sorensen, rssoren@gmail.com

2. Lack of Log review on web server:
 - a. Log review is not taking place on web server or the platform operating system enabling the breach to go unnoticed.
3. Lack of review of data on website:
 - a. Information on website listed key GIAC-E personnel, thus providing the opportunity for social engineering attacks.
4. Employees had no IT Security training:
 - a. Lack of basic IT Security awareness training left employees more susceptible to social engineering attacks.
5. Lack of Network Access Control:
 - a. An imposter from Golden Dragon Fortunes posed as a vendor. During a bathroom break, the vendor plugged a laptop into the internal network and sent an internal memo posing as the CEO to all employees containing a malicious link to a Blackhole exploit kit server's landing page.
6. Key administrative account was compromised via social engineering/crafted spear phishing attack:
 - a. Publically accessible information about GIAC-E was gathered. A key administrator was identified and a targeted spear phishing email was sent that contained a malicious attachment.
7. Third-Party access restrictions not enforced:
 - a. GIAC-E had a contract with a Third-Party vendor that helped develop the hardware for the new fortune teller machines at their Research Park location. A key engineer's account was compromised which allowed full and unrestricted access to GIAC-E's internal development network.
8. Remote Access did not require two-factor authentication:
 - a. An employee's password (which did not have a lockout mechanism after a set number of unsuccessful logins) was cracked and used to VPN into the protected network.
9. Recently terminated employee account was not immediately removed from the server:
 - a. Logs indicated this employee account was accessed from Golden Dragon Fortunes network space.
10. IDS/IPS was not installed:
 - a. Data breach was effective by installing malware on the file server via

phishing attack. This process went unnoticed for months due to the lack of IDS.

11. Lack of Incident Response:

- a. The GIAC-E IT staff was at a loss of what to do when they were notified of a possible data breach. They decided to keep it quiet so they did not get in trouble. This lasted for six weeks until the true nature of the breach was revealed.

12. Lack of Mobile Device Policy:

- a. GIAC-E deployed new Android tablets to key employees for testing the new fortune cookie generation algorithm via a new app. Employees were not properly trained on the proper use of mobile devices and downloaded source code for the new app and stored it on their mobile device for review at home. Tablet was stolen and did not have full-disk encryption.

Security-HD, Inc. could easily have found additional risks but realized that they had a good starting point. By identifying these risks, GIAC-E will now be able start to mitigate them, thus helping to protect their critical intellectual property.

4.3. Document Identified Risks using SimpleRisk

Security-HD, Inc. opened up SimpleRisk and realized that there is a need to add some values in order for fully document GIAC-E's corporation by clicking on the **Configuration | Add and Remove Values** tab and proceeded to add the following values:

- Technology: Account Management, Authentication, IDS/IPS, Encryption, Logging
- Team: Remote and Mobile Users, Content Management
- Location: GIAC-E Headquarters, Remote Sites, Research Park

Security-HD, Inc. proceeded to enter the risks identified. Here is an example of the entry screen in SimpleRisk as shown in the screenshot below:

I. Submit Your Risks

II. Plan Your Mitigations

III. Perform Management Reviews

IV. Prioritize for Project Planning

V. Review Risks Regularly

Document a New Risk

Use this form in order to document a new risk for consideration in the Risk Management Process.

Subject: log review on web server

External Reference ID: 2

Control Regulation: ISO 27001

Control Number: 2

Site/Location: GIAC-E Headquarters

Category: Monitoring

Team: Web Systems

Technology: Logging

Owner: Admin

Owner's Manager: GIAC-E CIO

Risk Scoring Method: Classic

Current Likelihood: Credible

Current Impact: Moderate

Risk Assessment: Log review is not taking place on web server or the platform operating system enabling the breach to go unnoticed.

Additional Notes

Submit Reset

Security-HD, Inc. proceeded to input the remaining risks. SimpleRisk provides multiple ways to score risk to include the *Classic*, *CVSS*, *DREAD*, and *OWASP* methodology. Risk calculations can be somewhat subjective and that each scoring calculator derives scores differently. Most risks were scored by the classic model, but Risks 1a, 5a, and 8a were scored using the CVSS score method (first.org). Risk 6a was scored using the DREAD model (cisodesk.com). Finally, Risk 1b was scored using the OWASP method (owasp.org).

SimpleRisk comes with built-in calculators to assist in determining risk scores as shown in the example below using the SimpleRisk CVSS V2.0 Calculator:

7.6
(High)

Risk ID: 1001

Subject: GIAC-E.com web site was vulnerable to Cross-Site Request Forgery (CSRF)

Status: New

[Hide Risk Scoring Details](#)

Update CVSS Score

Base Score Metrics

Attack Vector: Network
Attack Complexity: High
Authentication: None
Confidentiality Impact: Complete
Integrity Impact: Complete
Availability Impact: Complete

Temporal Score Metrics

Exploitability: Undefined
Remediation Level: Undefined
Report Confidence: Undefined

Environmental Score Metrics

Collateral Damage Potential: Undefined
Target Distribution: Undefined
Confidentiality Requirement: Undefined
Integrity Requirement: Undefined
Availability Requirement: Undefined

Update

SimpleRisk CVSS Calculator - Mozilla Firefox

localhost/management/cvss_rating.php

SimpleRisk CVSS V2.0 Calculator

This page provides a calculator for creating CVSS vulnerability severity scores. The scores are computed in sequence such that the Base Score is used to calculate the Temporal Score and the Temporal Score is used to calculate the Environmental Score.

CVSS Score

CVSS Base Score: 7.6
Impact Subscore: 10
Exploitability Subscore: 4.9
CVSS Temporal Score: 7.6
CVSS Environmental Score: 7.6

Help Desk

None
There is no impact to the availability of the system.

Partial
There is reduced performance or interruptions in resource availability. An example is a network-based flood attack that permits a limited number of successful connections to an Internet service.

Complete
There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.

Base Score Metrics

Exploitability Metrics
Attack Vector: Network
Attack Complexity: High
Authentication: None
Impact Metrics
Confidentiality Impact: Complete
Integrity Impact: Complete
Availability Impact: Complete

Temporal Score Metrics

Exploitability: Undefined
Remediation Level: Undefined
Report Confidence: Undefined

Environmental Score Metrics

Collateral Damage Potential: Undefined
Target Distribution: Undefined
Impact Subscore Modifiers
Confidentiality Requirement: Undefined
Integrity Requirement: Undefined
Availability Requirement: Undefined

Submit

SimpleRisk provides a comprehensive report that shows all risk scoring methods and the risks scored using each. Select **Reporting** | **All Open Risks by Scoring Method** option as shown in the screenshot below:

SimpleRisk

Home Risk Management **Reporting** Configure

Admin

Risk Dashboard

Risk Trend

All Open Risks Assigned to Me by Risk Level
All Open Risks by Risk Level
All Open Risks Considered for Projects by Risk Level
All Open Risks Accepted Until Next Review by Risk Level
All Open Risks to Submit as a Production Issue by Risk Level
All Open Risks by Scoring Method
All Open Risks Needing a Review
All Closed Risks by Risk Level
Submitted Risks by Date
Mitigations By Date
Management Reviews By Date
Projects and Risks Assigned

This report shows all risk scoring methods and the risks scored using each.

Classic Risk Scoring			
ID	Subject	Risk	Date Submitted
1012	Lack of mobile device policy	6	2014-05-19 20:06
1009	Recently terminated employee account was not immediately removed from server	6	2014-05-19 18:47
1007	3rd-Party access restrictions not enforced	4.3	2014-05-19 19:24
1010	IDS/IPS was not installed	3.4	2014-05-19 19:53
1002	Lack of log review on web server	2.9	2014-05-19 18:54
1004	Employees had no IT Security training	2.6	2014-05-19 19:04
1011	Lack of Incident Response	2.3	2014-05-19 20:02
1003	Lack of review of data on GIAC-E.com web site	1.7	2014-05-19 18:56

CVSS Risk Scoring			
ID	Subject	Risk	Date Submitted
1001	GIAC-E.com web site was vulnerable to Cross-Site Request Forgery (CSRF)	7.6	2014-05-19 18:46
1008	Remote access did not require 2-factor authentication	6.7	2014-05-19 19:29
1005	Lack of Network Access Control	4.7	2014-05-19 19:09

DREAD Risk Scoring			
ID	Subject	Risk	Date Submitted
1006	Key administrative account was compromised via social engineering/crafted spear phishing attack	6	2014-05-19 19:14

OWASP Risk Scoring			
ID	Subject	Risk	Date Submitted
1013	GIAC-E.com web site was open to multiple SQL Injection vulnerabilities	4.9	2014-05-23 12:50

Custom Risk Scoring			
ID	Subject	Risk	Date Submitted

4.4. Manage/Mitigate Identified Risks using SimpleRisk

Now that the risks have been identified, it is time to come up with a game plan to manage and/or mitigate them. SimpleRisk sorts mitigation prioritization based on risk score. This provides a list of submitted risks that require mitigation planning. To show this list, click on **Risk Management** | **Plan Your Mitigation** as shown below:

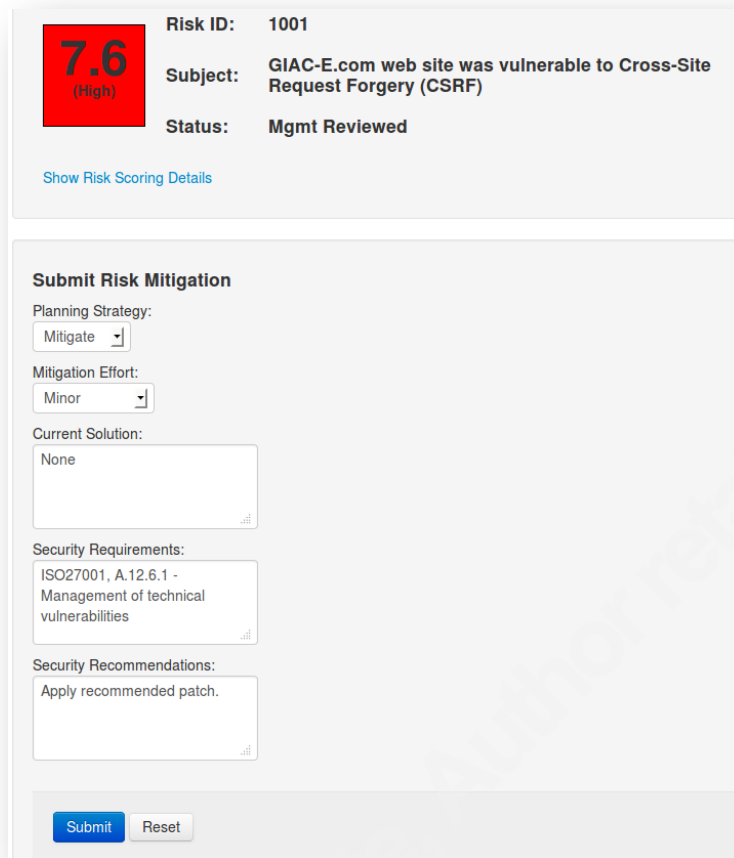
SimpleRisk Home **Risk Management** Reporting Configure Admin

I. Submit Your Risks
II. Plan Your Mitigations
 III. Perform Management Reviews
 IV. Prioritize for Project Planning
 V. Review Risks Regularly

Below is the list of submitted risks that require mitigation planning.

ID	Status	Subject	Risk	Submitted	Mitigation Planned	Management Review
1001	New	GIAC-E.com web site was vulnerable to Cross-Site Request Forgery (CSRF)	7.8	2014-05-19 19:46	No	No
1008	New	Remote access did not require 2-factor authentication	7.5	2014-05-19 20:29	No	No
1012	New	Lack of mobile device policy	7.1	2014-05-19 21:08	No	No
1009	New	Recently terminated employee account was not immediately removed from server	6.6	2014-05-19 20:47	No	No
1006	New	Key administrative account was compromised via social engineering/crafted spear phishing attack	6.2	2014-05-19 20:14	No	No
1013	New	GIAC-E.com web site was open to multiple SQL injection vulnerabilities	4.8	2014-05-23 13:50	No	No
1005	New	Lack of Network Access Control	4.7	2014-05-19 20:09	No	No
1007	New	3rd-Party access restrictions not enforced	4.3	2014-05-19 20:24	No	No
1010	New	IDS/IPS was not installed	3.4	2014-05-19 20:53	No	No
1002	New	Lack of log review on web server	2.9	2014-05-19 19:54	No	No
1004	New	Employees had no IT Security training	2.6	2014-05-19 20:04	No	No
1011	New	Lack of Incident Response	2.3	2014-05-19 21:02	No	No
1003	New	Lack of review of data on GIAC-E.com web site	1.7	2014-05-19 19:56	No	No

Security-HD, Inc. determines that there is a patch available for the Cross-Site Request Forgery (CSRF) and SQL injection vulnerability associated with the website and can be mitigated quickly at a minimal cost. By clicking 'No' under Mitigation Planned for ID 1001, it leads them to the *Submit Mitigation* page. They submit their planned mitigation as shown below:



Risk ID: 1001

Subject: GIAC-E.com web site was vulnerable to Cross-Site Request Forgery (CSRF)

Status: Mgmt Reviewed

[Show Risk Scoring Details](#)

Submit Risk Mitigation

Planning Strategy:
Mitigate

Mitigation Effort:
Minor

Current Solution:
None

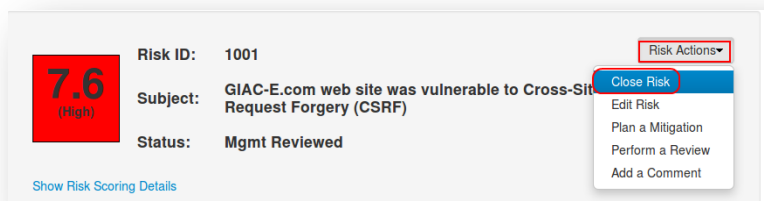
Security Requirements:
ISO27001, A.12.6.1 - Management of technical vulnerabilities

Security Recommendations:
Apply recommended patch.

[Submit](#) [Reset](#)

After the mitigation is accepted, Security-HD, Inc. then goes to the *Perform Management Review* phase where risk ID 1001 is reviewed with management. This is done by clicking the ‘No’ link under the *Management Review* column. The risk was approved and the next step, ‘*Submit as a Production Issue*’ was selected with directions to the sys admins to apply the patch as soon as possible.

It did not take the sys admins long to apply the patch and verify that the risk was resolved. Security-HD, Inc. proceeded to close this task by clicking ‘*id link 1001*’. From here, ‘*Close Risk*’ was selected from the drop down *Risk Actions* menu.



Risk ID: 1001

Subject: GIAC-E.com web site was vulnerable to Cross-Site Request Forgery (CSRF)

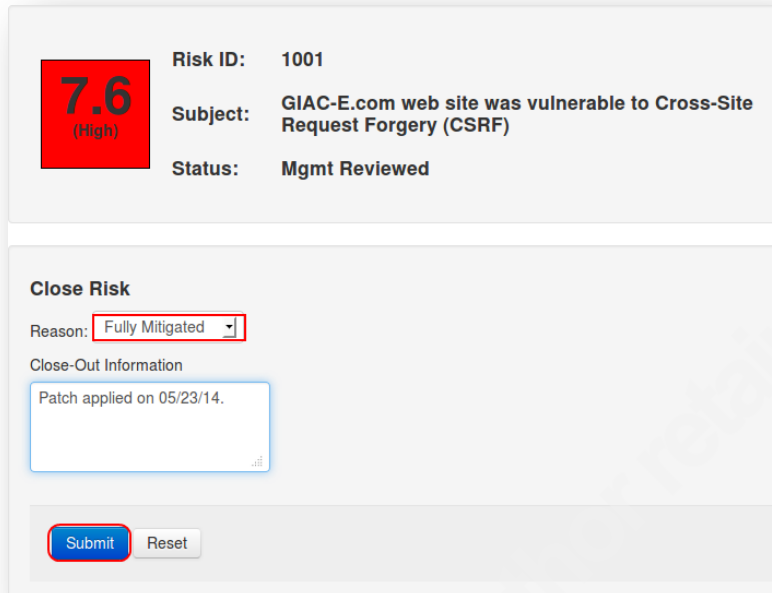
Status: Mgmt Reviewed

[Show Risk Scoring Details](#)

Risk Actions

- Close Risk
- Edit Risk
- Plan a Mitigation
- Perform a Review
- Add a Comment

Since the patch was applied, under the *Reason* drop down menu, '*Fully Mitigated*' was selected and the patch date was entered in the *Close-Out Information* box as shown.



7.6
(High)

Risk ID: 1001

Subject: GIAC-E.com web site was vulnerable to Cross-Site Request Forgery (CSRF)

Status: Mgmt Reviewed

Close Risk

Reason: Fully Mitigated

Close-Out Information

Patch applied on 05/23/14.

Submit Reset

Each risk was reviewed, *Approved* or *Rejected*, and the next steps were considered (*Accept Until Next Review*, *Submit as a Production Issue*, or *Consider for Project*) as shown in the **Reporting | Management Reviews by Date** report below:

SimpleRisk	Home	Risk Management	Reporting	Configure	Admin▼
<div> Risk Dashboard Risk Trend All Open Risks Assigned to Me by Risk Level All Open Risks by Risk Level All Open Risks Considered for Projects by Risk Level All Open Risks Accepted Until Next Review by Risk Level All Open Risks to Submit as a Production Issue by Risk Level All Open Risks by Scoring Method All Open Risks Needing a Review All Closed Risks by Risk Level Submitted Risks by Date Mitigations By Date Management Reviews By Date Projects and Risks Assigned </div>					
This report shows all management reviews ordered by review date.					
ID	Subject	Review Date	Review	Next Step	Reviewer
1004	Employees had no IT Security training	2014-05-24 16:49	Approve Risk	Accept Until Next Review	Admin
1006	Key administrative account was compromised via social engineering/crafted spear phishing attack	2014-05-24 16:48	Approve Risk	Submit as a Production Issue	Admin
1003	Lack of review of data on GIAC-E.com web site	2014-05-24 16:45	Reject Risk	Accept Until Next Review	Admin
1002	Lack of log review on web server	2014-05-24 16:24	Approve Risk	Submit as a Production Issue	Admin
1012	Lack of mobile device policy	2014-05-24 16:20	Approve Risk	Consider for Project	Admin
1013	GIAC-E.com web site was open to multiple SQL injection vulnerabilities	2014-05-24 16:49	Approve Risk	Submit as a Production Issue	Admin
1011	Lack of Incident Response	2014-05-24 16:47	Approve Risk	Consider for Project	Admin
1009	Recently terminated employee account was not immediately removed from server	2014-05-24 16:33	Approve Risk	Submit as a Production Issue	Admin
1010	IDS/IPS was not installed	2014-05-24 16:24	Approve Risk	Consider for Project	Admin
1001	GIAC-E.com web site was vulnerable to Cross-Site Request Forgery (CSRF)	2014-05-24 17:25	Approve Risk	Submit as a Production Issue	Admin
1007	3rd-Party access restrictions not enforced	2014-05-24 16:48	Approve Risk	Accept Until Next Review	Admin
1005	Lack of Network Access Control	2014-05-24 16:45	Approve Risk	Submit as a Production Issue	Admin
1001	GIAC-E.com web site was vulnerable to Cross-Site Request Forgery (CSRF)	2014-05-24 16:31	Approve Risk	Submit as a Production Issue	Admin
1008	Remote access did not require 2-factor authentication	2014-05-24 16:22	Approve Risk	Consider for Project	Admin

Based on the remaining risks, Security-HD, Inc. recommends GIAC-E implement four projects. These projects will vastly improve their overall security program and help detect and reduce future compromises. Without proper IDS/IPS, it was difficult to determine the exact cause of the compromise. Also, without a formal Incident Response program, GIAC-E was not prepared to detect an intrusion much less be able to contain and mitigate it in a timely manner. After digging deep into logs and reviewing the mobile device configuration, Security-HD, Inc. determined that the major breach was a result of lack of two-factor authentication on compromised accounts and the lack of encryption of sensitive data on their mobile devices. Thus, the projects shown in **Reporting | All Open Risks Considered for Projects by Risk Level** were entered.

SimpleRisk Home Risk Management **Reporting** Configure Admin▼

Risk Dashboard
Risk Trend
All Open Risks Assigned to Me by Risk Level
All Open Risks by Risk Level
All Open Risks Considered for Projects by Risk Level
All Open Risks Accepted Until Next Review by Risk Level

This report shows all open risks considered for projects ordered by risk level.

ID	Status	Subject	Risk	Submitted	Mitigation Planned	Management Review
1008	Mgmt Reviewed	Remote access did not require 2-factor authentication	7.5	2014-05-19 20:29	Yes	Yes
1012	Mgmt Reviewed	Lack of mobile device policy	7.1	2014-05-19 21:08	Yes	Yes
1010	Mgmt Reviewed	IDS/IPS was not installed	3.4	2014-05-19 20:53	Yes	Yes
1011	Mgmt Reviewed	Lack of Incident Response	2.3	2014-05-19 21:02	Yes	Yes

These projects were entered in the *Risk Management | IV. Prioritize for Project Planning* option of SimpleRisk.

SimpleRisk Home **Risk Management** Reporting Configure Admin▼

I. Submit Your Risks
II. Plan Your Mitigations
III. Perform Management Reviews
IV. Prioritize for Project Planning
V. Review Risks Regularly

1) Add and Remove Projects
Add and remove projects in order to associate multiple risks together for prioritization.
Add new project named
Delete current project named

2) Add Unassigned Risks to Projects
Drag and drop unassigned risks marked for consideration as a project into the appropriate project tab.

2-Factor Authentication

Incident Response

Mobile Device Management

IDS/IPS

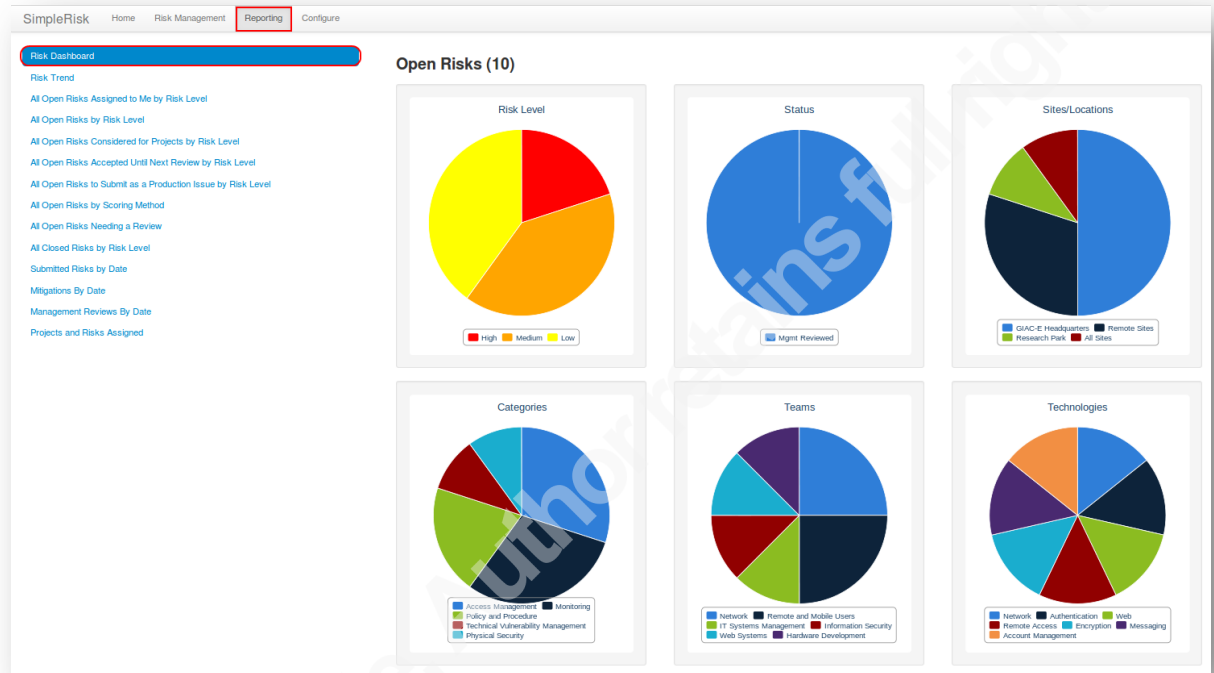
3) Prioritize Projects
Move projects around and change the order of prioritization. Once finished, don't forget to press the "Update" button to save your changes.

2-Factor Authentication

Incident Response

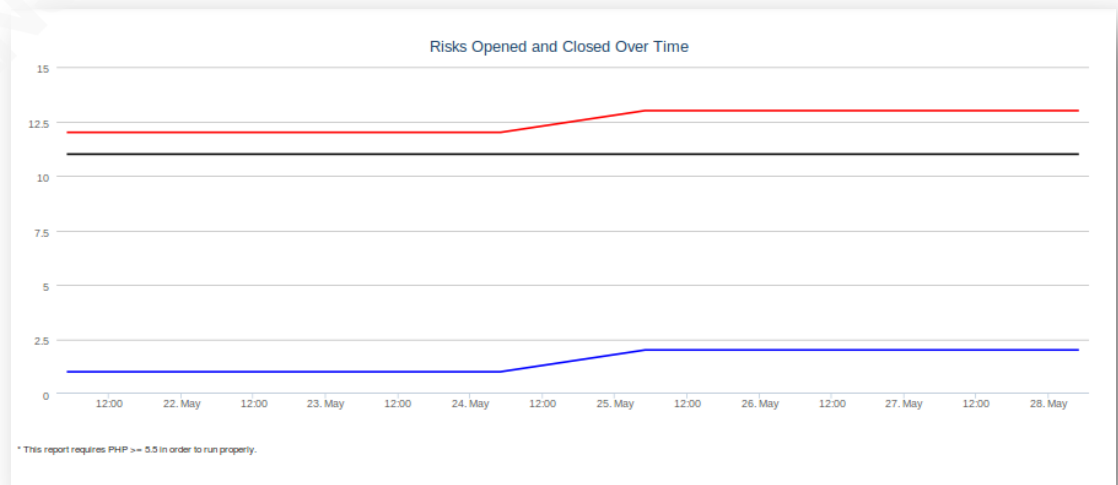
4.5. Reporting functions of SimpleRisk

SimpleRisk provides an executive dashboard and detailed reporting functionality. The **Reporting | Risk Dashboard** provides a comprehensive overview of the risks entered.



Other reports help drill down to more detailed view of the risks. The report options are shown below:

➤ Risk Trend



➤ All Open Risks Assigned to me by Risk Level

This report shows all open risks that have the current user as the owner or manager associated with the risk ordered by risk level.

ID	Status	Subject	Risk	Submitted	Mitigation Planned	Management Review
1008	Mgmt Reviewed	Remote access did not require 2-factor authentication	7.5	2014-05-19 20:29	Yes	Yes
1006	Mgmt Reviewed	Key administrative account was compromised via social engineering/crafted spear phishing attack	6	2014-05-19 20:14	Yes	Yes
1005	Mgmt Reviewed	Lack of Network Access Control	4.7	2014-05-19 20:09	Yes	Yes
1010	Mgmt Reviewed	IDS/IPS was not installed	3.4	2014-05-19 20:53	Yes	Yes
1002	Mgmt Reviewed	Lack of log review on web server	2.9	2014-05-19 19:54	Yes	Yes
1011	Mgmt Reviewed	Lack of Incident Response	2.3	2014-05-19 21:02	Yes	Yes

➤ All Open Risks by Risk Level

This report shows all open risks ordered by risk level.

ID	Status	Subject	Risk	Submitted	Mitigation Planned	Management Review
1008	Mgmt Reviewed	Remote access did not require 2-factor authentication	7.5	2014-05-19 20:29	Yes	Yes
1012	Mgmt Reviewed	Lack of mobile device policy	7.1	2014-05-19 21:08	Yes	Yes
1009	Mgmt Reviewed	Recently terminated employee account was not immediately removed from server	6	2014-05-19 20:47	Yes	Yes
1006	Mgmt Reviewed	Key administrative account was compromised via social engineering/crafted spear phishing attack	6	2014-05-19 20:14	Yes	Yes
1005	Mgmt Reviewed	Lack of Network Access Control	4.7	2014-05-19 20:09	Yes	Yes
1007	Mgmt Reviewed	3rd-Party access restrictions not enforced	4.3	2014-05-19 20:24	Yes	Yes
1010	Mgmt Reviewed	IDS/IPS was not installed	3.4	2014-05-19 20:53	Yes	Yes
1002	Mgmt Reviewed	Lack of log review on web server	2.9	2014-05-19 19:54	Yes	Yes
1004	Mgmt Reviewed	Employees had no IT Security training	2.6	2014-05-19 20:04	Yes	Yes
1011	Mgmt Reviewed	Lack of Incident Response	2.3	2014-05-19 21:02	Yes	Yes

➤ All Open Risks Considered for Projects by Risk Level

This report shows all open risks considered for projects ordered by risk level.

ID	Status	Subject	Risk	Submitted	Mitigation Planned	Management Review
1008	Mgmt Reviewed	Remote access did not require 2-factor authentication	7.5	2014-05-19 20:29	Yes	Yes
1012	Mgmt Reviewed	Lack of mobile device policy	7.1	2014-05-19 21:08	Yes	Yes
1010	Mgmt Reviewed	IDS/IPS was not installed	3.4	2014-05-19 20:53	Yes	Yes
1011	Mgmt Reviewed	Lack of Incident Response	2.3	2014-05-19 21:02	Yes	Yes

➤ All Open Risks Accepted Until Next Review by Risk Level

This report shows all open risks accepted until next review ordered by risk level.

ID	Status	Subject	Risk	Submitted	Mitigation Planned	Management Review
1007	Mgmt Reviewed	3rd-Party access restrictions not enforced	4.3	2014-05-19 20:24	Yes	Yes
1004	Mgmt Reviewed	Employees had no IT Security training	2.6	2014-05-19 20:04	Yes	Yes

➤ All Open Risks to Submit as a Production issue by Risk Level

This report shows all open risks submitted as production issues ordered by risk level.

ID	Status	Subject	Risk	Submitted	Mitigation Planned	Management Review
1009	Mgmt Reviewed	Recently terminated employee account was not immediately removed from server	6	2014-05-19 20:47	Yes	Yes
1006	Mgmt Reviewed	Key administrative account was compromised via social engineering/crafted spear phishing attack	6	2014-05-19 20:14	Yes	Yes
1005	Mgmt Reviewed	Lack of Network Access Control	4.7	2014-05-19 20:09	Yes	Yes
1002	Mgmt Reviewed	Lack of log review on web server	2.9	2014-05-19 19:54	Yes	Yes

➤ All Open Risks by Scoring Method

This report shows all risk scoring methods and the risks scored using each.

Classic Risk Scoring			
ID	Subject	Risk	Date Submitted
1012	Lack of mobile device policy	7.1	2014-05-19 21:08
1009	Recently terminated employee account was not immediately removed from server	6	2014-05-19 20:47
1007	3rd-Party access restrictions not enforced	4.3	2014-05-19 20:24
1010	IDS/IPS was not installed	3.4	2014-05-19 20:53
1002	Lack of log review on web server	2.9	2014-05-19 19:54
1004	Employees had no IT Security training	2.6	2014-05-19 20:04
1011	Lack of Incident Response	2.3	2014-05-19 21:02

CVSS Risk Scoring			
ID	Subject	Risk	Date Submitted
1008	Remote access did not require 2-factor authentication	7.5	2014-05-19 20:29
1005	Lack of Network Access Control	4.7	2014-05-19 20:09

DREAD Risk Scoring			
ID	Subject	Risk	Date Submitted
1006	Key administrative account was compromised via social engineering/crafted spear phishing attack	6	2014-05-19 20:14

OWASP Risk Scoring			
ID	Subject	Risk	Date Submitted

Custom Risk Scoring			
ID	Subject	Risk	Date Submitted

➤ All Open Risks Needing a Review

This report shows all open risks needing a management review.

UNREVIEWED					
ID	Status	Subject	Risk	Days Open	Next Review Date
1001	New	GIAC-E.com web site was vulnerable to Cross-Site Request Forgery (CSRF)	7.6	6	UNREVIEWED
1002	New	Lack of log review on web server	2.9	6	UNREVIEWED
1003	New	Lack of review of data on GIAC-E.com web site	1.7	6	UNREVIEWED
1004	New	Employees had no IT Security training	2.6	6	UNREVIEWED
1005	New	Lack of Network Access Control	4.7	6	UNREVIEWED
1006	New	Key administrative account was compromised via social engineering/crafted spear phishing attack	6	6	UNREVIEWED
1007	New	3rd-Party access restrictions not enforced	4.3	6	UNREVIEWED
1008	New	Remote access did not require 2-factor authentication	7.5	6	UNREVIEWED
1009	New	Recently terminated employee account was not immediately removed from server	6	6	UNREVIEWED
1010	New	IDS/IPS was not installed	3.4	6	UNREVIEWED
1011	New	Lack of Incident Response	2.3	6	UNREVIEWED
1012	New	Lack of mobile device policy	7.1	6	UNREVIEWED
1013	New	GIAC-E.com web site was open to multiple SQL injection vulnerabilities	4.8	2	UNREVIEWED

➤ All Closed Risks by Risk Level

This report shows all closed risks ordered by risk level.

ID	Status	Subject	Risk	Submitted	Mitigation Planned	Management Review
1001	Closed	GIAC-E.com web site was vulnerable to Cross-Site Request Forgery (CSRF)	7.6	2014-05-19 19:46	Yes	Yes
1013	Closed	GIAC-E.com web site was open to multiple SQL injection vulnerabilities	4.8	2014-05-23 13:50	Yes	Yes
1003	Closed	Lack of review of data on GIAC-E.com web site	1.7	2014-05-19 19:56	Yes	Yes

➤ Submitted Risks by Date

This report shows all risks ordered by submission date.

ID	Subject	Submission Date	Calculated Risk	Status	Team	Submitted By
1013	GIAC-E.com web site was open to multiple SQL injection vulnerabilities	2014-05-23 13:50	4.8	Closed	Web Systems	Admin
1012	Lack of mobile device policy	2014-05-19 21:08	7.1	Mgmt Reviewed	Remote and Mobile Users	Admin
1002	Lack of log review on web server	2014-05-19 19:54	2.9	Mgmt Reviewed	Web Systems	Admin
1005	Lack of Network Access Control	2014-05-19 20:09	4.7	Mgmt Reviewed	Network	Admin
1008	Remote access did not require 2-factor authentication	2014-05-19 20:29	7.5	Mgmt Reviewed	Remote and Mobile Users	Admin
1011	Lack of Incident Response	2014-05-19 21:02	2.3	Mgmt Reviewed	Information Security	Admin
1001	GIAC-E.com web site was vulnerable to Cross-Site Request Forgery (CSRF)	2014-05-19 19:46	7.6	Closed	Web Systems	Admin
1004	Employees had no IT Security training	2014-05-19 20:04	2.6	Mgmt Reviewed		Admin
1007	3rd-Party access restrictions not enforced	2014-05-19 20:24	4.3	Mgmt Reviewed	Hardware Development	Admin
1010	IDS/IPS was not installed	2014-05-19 20:53	3.4	Mgmt Reviewed	Network	Admin
1003	Lack of review of data on GIAC-E.com web site	2014-05-19 19:56	1.7	Closed	Content Management	Admin
1006	Key administrative account was compromised via social engineering/crafted spear phishing attack	2014-05-19 20:14	6	Mgmt Reviewed	IT Systems Management	Admin
1009	Recently terminated employee account was not immediately removed from server	2014-05-19 20:47	6	Mgmt Reviewed		Admin

➤ Mitigation by Date

This report shows all mitigations planned ordered by mitigation date.

ID	Subject	Mitigation Date	Planning Strategy	Mitigation Effort	Submitted By
1009	Recently terminated employee account was not immediately removed from server	2014-05-24 14:37	Mitigate	Considerable	Admin
1010	IDS/IPS was not installed	2014-05-24 16:18	Research	Significant	Admin
1003	Lack of review of data on GIAC-E.com web site	2014-05-24 15:52	Watch		Admin
1006	Key administrative account was compromised via social engineering/crafted spear phishing attack	2014-05-24 15:06	Research	Significant	Admin
1011	Lack of Incident Response	2014-05-24 14:44	Mitigate	Significant	Admin
1001	GIAC-E.com web site was vulnerable to Cross-Site Request Forgery (CSRF)	2014-05-24 14:26	Mitigate	Minor	Admin
1001	GIAC-E.com web site was vulnerable to Cross-Site Request Forgery (CSRF)	2014-05-24 17:18	Mitigate	Minor	Admin
1005	Lack of Network Access Control	2014-05-24 16:00	Mitigate	Minor	Admin
1002	Lack of log review on web server	2014-05-24 15:09	Mitigate	Minor	Admin
1012	Lack of mobile device policy	2014-05-24 14:48	Research	Significant	Admin
1008	Remote access did not require 2-factor authentication	2014-05-24 14:28	Mitigate	Significant	Admin
1013	GIAC-E.com web site was open to multiple SQL injection vulnerabilities	2014-05-24 16:12	Mitigate	Minor	Admin
1007	3rd-Party access restrictions not enforced	2014-05-24 15:18	Mitigate	Considerable	Admin
1004	Employees had no IT Security training	2014-05-24 15:03	Mitigate	Considerable	Admin

➤ Management Reviews by Date

This report shows all management reviews ordered by review date.

ID	Subject	Review Date	Review	Next Step	Reviewer
1002	Lack of log review on web server	2014-05-26 07:51			Admin
1002	Lack of log review on web server	2014-05-26 07:52	Approve Risk	Submit as a Production Issue	Admin
1004	Employees had no IT Security training	2014-05-24 16:49	Approve Risk	Accept Until Next Review	Admin
1006	Key administrative account was compromised via social engineering/crafted spear phishing attack	2014-05-24 16:48	Approve Risk	Submit as a Production Issue	Admin
1003	Lack of review of data on GIAC-E.com web site	2014-05-24 16:45	Reject Risk	Accept Until Next Review	Admin
1002	Lack of log review on web server	2014-05-24 16:24	Approve Risk	Submit as a Production Issue	Admin
1012	Lack of mobile device policy	2014-05-24 16:20	Approve Risk	Consider for Project	Admin
1013	GIAC-E.com web site was open to multiple SQL injection vulnerabilities	2014-05-24 16:49	Approve Risk	Submit as a Production Issue	Admin
1011	Lack of Incident Response	2014-05-24 16:47	Approve Risk	Consider for Project	Admin
1009	Recently terminated employee account was not immediately removed from server	2014-05-24 16:33	Approve Risk	Submit as a Production Issue	Admin
1010	IDS/IPS was not installed	2014-05-24 16:24	Approve Risk	Consider for Project	Admin
1001	GIAC-E.com web site was vulnerable to Cross-Site Request Forgery (CSRF)	2014-05-24 17:25	Approve Risk	Submit as a Production Issue	Admin
1007	3rd-Party access restrictions not enforced	2014-05-24 16:48	Approve Risk	Accept Until Next Review	Admin
1005	Lack of Network Access Control	2014-05-24 16:45	Approve Risk	Submit as a Production Issue	Admin
1001	GIAC-E.com web site was vulnerable to Cross-Site Request Forgery (CSRF)	2014-05-24 16:31	Approve Risk	Submit as a Production Issue	Admin
1008	Remote access did not require 2-factor authentication	2014-05-24 16:22	Approve Risk	Consider for Project	Admin

➤ Projects and Risks Assigned

This report shows all projects and the risks assigned to them.

2-Factor Authentication			
ID	Subject	Risk	Date Submitted
Incident Response			
ID	Subject	Risk	Date Submitted
Mobile Device Management			
ID	Subject	Risk	Date Submitted
IDS/IPS			
ID	Subject	Risk	Date Submitted

This is a very comprehensive set of reports that can be used to manage an enterprise risk program. In addition to the reports available, an *Audit Trail* is generated for every action performed for each risk. For example, ID 1001 shows that the following actions have occurred for this risk to include closing the task (this is a very beneficial feature of SimpleRisk, one that auditors will love.):

Robert Sorensen, rssoren@gmail.com

Audit Trail

2014-05-26 7:22 AM CDT > Risk ID "1001" was marked as closed by username "admin".

2014-05-24 5:25 PM CDT > A management review was submitted for risk ID "1001" by username "admin".

2014-05-24 5:18 PM CDT > A mitigation was submitted for risk ID "1001" by username "admin".

2014-05-24 5:08 PM CDT > Risk mitigation details were updated for risk ID "1001" by username "admin".

2014-05-24 4:31 PM CDT > A management review was submitted for risk ID "1001" by username "admin".

2014-05-24 2:26 PM CDT > A mitigation was submitted for risk ID "1001" by username "admin".

2014-05-23 1:41 PM CDT > Scoring method was changed for risk ID "1001" by username "admin".

2014-05-23 1:41 PM CDT > Risk details were updated for risk ID "1001" by username "admin".

2014-05-23 1:40 PM CDT > Scoring method was changed for risk ID "1001" by username "admin".

2014-05-23 1:40 PM CDT > Risk scoring for risk ID "1001" was updated by username "admin".

2014-05-23 1:40 PM CDT > Scoring method was changed for risk ID "1001" by username "admin".

2014-05-23 1:19 PM CDT > Scoring method was changed for risk ID "1001" by username "admin".

2014-05-23 1:18 PM CDT > Risk details were updated for risk ID "1001" by username "admin".

2014-05-19 8:01 PM CDT > Risk scoring for risk ID "1001" was updated by username "admin".

2014-05-19 7:51 PM CDT > Risk details were updated for risk ID "1001" by username "admin".

2014-05-19 7:46 PM CDT > A new risk ID "1001" was submitted by username "admin".

4.6. Maintenance of SimpleRisk

SimpleRisk is a great open source project for managing risk. One thing that is missing from the program is the ability to backup and restore the MySQL database. This could be critical, especially before upgrading SimpleRisk.

4.6.1. Backup/Restore SimpleRisk MySQL Database

A few simple scripts can accomplish this task easily. The first script will perform a backup of the MySQL database created for SimpleRisk.

```
#!/bin/bash

# $HOME/bin/sr_backup

# Define variables
bdate=`date '+%F_%H%M'`
backupdir=$HOME/backups
backupfile=$backupdir/simplerisk-backup_${bdate}.sql

echo -e "MySQL root password - \c"
mysqldump -u root -p simplerisk >$backupfile

if [ -f $backupfile ]
then
```

Robert Sorensen, rssoren@gmail.com

```

lcount=`cat $backupfile |wc -l`
if [ $lcount -gt 0 ]
then
    echo -e "\nBackup of SimpleRisk MySQL database was successfully completed.\n"
    ls -l $backupfile
else
    echo -e "\nBackup of SimpleRisk MySQL database failed. Please try again...\n"
fi
else
    echo -e "Failed to create backup of SimpleRisk MySQL database. Please try
again...\n"
fi

```

Here is an example of running this script:

```

risky@vb-riskyb:~/bin$ ./sr_backup
MySQL root password - Enter password:

Backup of SimpleRisk MySQL database was successfully completed.

-rw-rw-r-- 1 risky risky 58329 May 26 21:25 /home/risky/backups/simplerisk-
backup_2014-05-26_2125.sql
risky@vb-riskyb:~/bin$

```

Another script will be needed in order to restore the database. There may be multiple backups, so this script will present a menu of the available backups from which to select and restore the database.

```

#!/bin/bash

# $HOME/bin/sr_restore

# Define variables
backupdir=$HOME/backups

clear
echo -e '-----'
echo -e "                      AVAILABLE BACKUPS "
echo -e '-----\n'
PS3='..Select a backup to restore: '

select i in `ls -l $backupdir/*.sql | awk '{ print $9 }'`
do
    echo -e ""
    #PS3="Select a backup to restore: "
    hs="//`echo $i | awk -F, ' {print $1 }'` `echo $i | awk -F, ' { print $2 }'|sed
's/+/ /g'`"
    bfile=$i
    echo -e "Restoring backup $i...\n"
    echo -e "MySQL root password - \c"
    mysql -u root -p simplerisk < $bfile
    exit
done

```

Here is an example of running this script:

```
risky@vb-riskyb:~/bin$ ./sr_restore

-----
                        AVAILABLE BACKUPS
-----

1) /home/risky/backups/simplerisk-backup_20140519.sql
2) /home/risky/backups/simplerisk-backup_2014-05-22.sql
3) /home/risky/backups/simplerisk-backup_2014-05-23.sql
4) /home/risky/backups/simplerisk-backup_2014-05-24.sql
5) /home/risky/backups/simplerisk-backup_2014-05-26_2125.sql
6) /home/risky/backups/simplerisk-backup_2014-05-27_0750.sql
7) /home/risky/backups/simplerisk-backup_2014-05-27_1058.sql
..Select a backup to restore: 5

Restoring backup /home/risky/backups/simplerisk-backup_2014-05-26_2125.sql...

MySQL root password - Enter password:
risky@vb-riskyb:~/bin$
```

4.6.2. Upgrade SimpleRisk

Periodically, Josh provides an update to SimpleRisk. He has provided documentation on how to perform the upgrade (Sokol). Here is a quick overview of the steps:

1. `sudo bash` (perform operations as privileged user)
2. `cd /var/www/html` (web root)
3. `cp includes/config.php ~/backups` (make backup of config file)
4. `cd ..;rm -rf html; mkdir html;cd html` (remove/recreate html directory)
5. `tar xvfz ~/Downloads/simplerisk-en-2014-526-001.tgz`
6. `mv simplerisk/* .` (moves all SimpleRisk app files to the web root)
7. `rm -rf simplerisk` (removes the now empty simplerisk directory)
8. `cp ~/backups/config.php includes/` (restore config file)
9. Authenticate and upgrade the database
 - a. Open web browser and enter 'http://localhost/admin/upgrade.php
 - b. Login with an administrative user credentials
 - c. Verify upgrade is required, click *Continue*
 - d. See final message indicating that the SimpleRisk database upgrade is complete.

5. Conclusions

GIAC Enterprises learned many hard lessons by enduring a very costly breach of their intellectual property associated with their fortune cooking saying business. With the help of Security-HD, Inc., a Cybersecurity consultant, they realized the value of applying the principles of risk management.

To assist in managing the 12 risks identified, Security-HD, Inc. introduced GIAC-E management to the open source program called SimpleRisk. This framework provided them with a tool that truly helped them reduce future exposure by organizing, prioritizing, and funding projects.

A detailed case study illustrated all the functionality of SimpleRisk including, *Configuration, Risk Management, and Reporting*. Josh has provided the security community with a great resource in helping them manage risks in SimpleRisk – truly enterprise risk management simplified!

6. References

- A guide to the Project Management Body of Knowledge (PMBOK guide), Fifth Edition (5th ed.). (2013). Newtown Square, Pa.: Project Management Institute.
- Coleman, K. (2008, August 26). Separation of Duties and IT Security. Retrieved May 12, 2014, from <http://www.csoonline.com/article/2123120/it-audit/separation-of-duties-and-it-security.html>
- Cisodesk.com. (n.d.) DREAD – Risk Rating Model. Retrieved May 23, 2014, from <http://www.cisodesk.com/web-application-security/threat-modeling-risk-analysis/dread-risk-rating-model/>
- Cvedetails.com. (2014, May 6). Vulnerabilities by Year. Retrieved May 6, 2014, from <http://www.cvedetails.com/browse-by-date.php>
- first.org. (n.d.). A Complete Guide to the Common Vulnerability Scoring System Version 2.0. Retrieved May 22, 2014, from <http://www.first.org/cvss/cvss-guide.html>
- George, T. (2014, April 9). Security Threats: Risk's Often Neglected Step Child. Retrieved May 5, 2014, from <http://www.securityweek.com/security-threats-risks-often-neglected-step-child>
- Goodin, D. (2014, February 20). Adobe releases emergency Flash update amid new zero-day drive-by attacks. Retrieved May 6, 2014, from <http://arstechnica.com/security/2014/02/adobe-releases-emergency-flash-update-amid-new-zero-day-drive-by-attacks/>
- Gordon, L.A., & Loeb, M.P. (2006). *Managing Cybersecurity Resources: A Cost-benefit Analysis*. New York: McGraw-Hill.
- McRee, R. (2014, February). SimpleRisk: Enterprise Risk Management Simplified. *ISSA Journal*, 39-42. Retrieved May 2, 2014, from <http://holisticinfosec.org/toolsmith/pdf/february2014.pdf>
- Owasp.org. (n.d.). OWASP Risk Rating Methodology. Retrieved May 23, 2014, from https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology
- SimpleRisk. (n.d.) SimpleRisk: Enterprise Risk Management Simplified. Retrieved May 9, 2014, from <http://simplerisk.org/>.
- Shostack, A. (2014). *Threat Modeling: Designing for Security*. Indianapolis: John Wiley & Sons, Inc.
- Sokol, J. (n.d.) SimpleRisk Documentation Guides. Retrieved May 9, 2014, from <http://simplerisk.org/documentation>
- Robert Sorensen, rssoren@gmail.com

- SP 800-30r1. (2012, September). NIST Special Publication 800-30 Revision 1 – Guide for Conducting Risk Assessments. Retrieved May 5, 2014, from http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf
- Infosecurity-magazine.com. (2011, June 23). The hype, and the reality, behind advanced persistent threats. Retrieved May 6, 2014, from <http://www.infosecurity-magazine.com/view/18897/the-hype-and-the-reality-behind-advanced-persistent-threats/>
- Powledge, T. (2014, April 09). Heartbleed in OpenSSL: Take Action Now! Retrieved May 6, 2014, from <http://www.symantec.com/connect/blogs/heartbleed-openssl-take-action-now>
- Roiter, N. (2011, March 7). IT GRC tools: Control your environment. Retrieved May 9, 2014, from <http://www.csoonline.com/article/2127514/compliance/it-grc-tools--control-your-environment.html>
- Zeltzer, L. (2014, May 1). Microsoft issues fix for IE zero day. Retrieved May 6, 2014, from <http://www.zdnet.com/microsoft-issues-fix-for-ie-zero-day-7000029001/>

Appendix A – NIST Special Publication 800-30 Revision 1– Taxonomy of Threat Sources

Type of Threat Sources	Description	Characteristics
ADVERSARIAL - Individual - Outsider - Insider - Trusted Insider - Privileged Insider - Group - Ad hoc - Established - Organization - Competitor - Supplier - Partner - Customer - Nation-State	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting
ACCIDENTAL - User - Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects
STRUCTURAL - Information Technology (IT) Equipment - Storage - Processing - Communications - Display - Sensor - Controller - Environmental Controls - Temperature/Humidity Controls - Power Supply - Software - Operating System - Networking - General-Purpose Application - Mission-Specific Application	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.	Range of effects
ENVIRONMENTAL - Natural or man-made disaster - Fire - Flood/Tsunami - Windstorm/Tornado - Hurricane - Earthquake - Bombing - Overrun - Unusual Natural Event (e.g., sunspots) - Infrastructure Failure/Outage - Telecommunications - Electrical Power	Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization. Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).	Range of effects

Appendix B – NIST Special Publication 800-30 Revision 1– Representative Examples – Adversarial Threat Events

Threat Events (Characterized by TTPs)	Description
<i>Perform reconnaissance and gather information.</i>	
Perform perimeter network reconnaissance/scanning.	Adversary uses commercial or free software to scan organizational perimeters to obtain a better understanding of the information technology infrastructure and improve the ability to launch successful attacks.
Perform network sniffing of exposed networks.	Adversary with access to exposed wired or wireless data channels used to transmit information, uses network sniffing to identify components, resources, and protections.
Gather information using open source discovery of organizational information.	Adversary mines publically accessible information to gather information about organizational information systems, business processes, users or personnel, or external relationships that the adversary can subsequently employ in support of an attack.
Perform reconnaissance and surveillance of targeted organizations.	Adversary uses various means (e.g., scanning, physical observation) over time to examine and assess organizations and ascertain points of vulnerability.
Perform malware-directed internal reconnaissance.	Adversary uses malware installed inside the organizational perimeter to identify targets of opportunity. Because the scanning, probing, or observation does not cross the perimeter, it is not detected by externally placed intrusion detection systems.
<i>Craft or create attack tools.</i>	
Craft phishing attacks.	Adversary counterfeits communications from a legitimate/trustworthy source to acquire sensitive information such as usernames, passwords, or SSNs. Typical attacks occur via email, instant messaging, or comparable means; commonly directing users to websites that appear to be legitimate sites, while actually stealing the entered information.
Craft spear phishing attacks.	Adversary employs phishing attacks targeted at high value targets (e.g., senior leaders/executives).
Craft attacks specifically based on deployed information technology environment.	Adversary develops attacks (e.g., crafts targeted malware) that take advantage of adversary knowledge of the organizational information technology environment.
Create counterfeit/spoof website.	Adversary creates duplicates of legitimate websites; when users visit a counterfeit site, the site can gather information or download malware.
Craft counterfeit certificates.	Adversary counterfeits or compromises a certificate authority, so that malware or connections will appear legitimate.
Create and operate false front organizations to inject malicious components into the supply chain.	Adversary creates false front organizations with the appearance of legitimate suppliers in the critical life-cycle path that then inject corrupted/malicious information system components into the organizational supply chain.
<i>Deliver/insert/install malicious capabilities.</i>	
Deliver known malware to internal organizational information systems (e.g., virus via email).	Adversary uses common delivery mechanisms (e.g., email) to install/insert known malware (e.g., malware whose existence is known) into organizational information systems.
Deliver modified malware to internal organizational information systems.	Adversary uses more sophisticated delivery mechanisms than email (e.g., web traffic, instant messaging, FTP) to deliver malware and possibly modifications of known malware to gain access to internal organizational information systems.

Robert Sorensen, rssoren@gmail.com

Deliver targeted malware for control of internal systems and exfiltration of data.	Adversary installs malware that is specifically designed to take control of internal organizational information systems, identify sensitive information, exfiltrate the information back to adversary, and conceal these actions.
Deliver malware by providing removable media.	Adversary places removable media (e.g., flash drives) containing malware in locations external to organizational physical perimeters but where employees are likely to find the media (e.g., facilities parking lots, exhibits at conferences attended by employees) and use it on organizational information systems.

Threat Events (Characterized by TTPs)	Description
Insert untargeted malware into downloadable software and/or into commercial information technology products.	Adversary corrupts or inserts malware into common freeware, shareware or commercial information technology products. Adversary is not targeting specific organizations, simply looking for entry points into internal organizational information systems. Note that this is particularly a concern for mobile applications.
Insert targeted malware into organizational information systems and information system components.	Adversary inserts malware into organizational information systems and information system components (e.g., commercial information technology products), specifically targeted to the hardware, software, and firmware used by organizations (based on knowledge gained via reconnaissance).
Insert specialized malware into organizational information systems based on system configurations.	Adversary inserts specialized, non-detectable, malware into organizational information systems based on system configurations, specifically targeting critical information system components based on reconnaissance and placement within organizational information systems.
Insert counterfeit or tampered hardware into the supply chain.	Adversary intercepts hardware from legitimate suppliers. Adversary modifies the hardware or replaces it with faulty or otherwise modified hardware.
Insert tampered critical components into organizational systems.	Adversary replaces, through supply chain, subverted insider, or some combination thereof, critical information system components with modified or corrupted components.
Install general-purpose sniffers on organization controlled information systems or networks.	Adversary installs sniffing software onto internal organizational information systems or networks.
Install persistent and targeted sniffers on organizational information systems and networks.	Adversary places within internal organizational information systems or networks software designed to (over a continuous period of time) collect (sniff) network traffic.
Insert malicious scanning devices (e.g., wireless sniffers) inside facilities.	Adversary uses postal service or other commercial delivery services to deliver to organizational mailrooms a device that is able to scan wireless communications accessible from within the mailrooms and then wirelessly transmit information back to adversary.
Insert subverted individuals into organizations.	Adversary places individuals within organizations who are willing and able to carry out actions to cause harm to organizational missions/business functions.
Insert subverted individuals into privileged positions in organizations.	Adversary places individuals in privileged positions within organizations who are willing and able to carry out actions to cause harm to organizational missions/business functions. Adversary may target privileged functions to gain access to sensitive information (e.g., user accounts, system files, etc.) and may leverage access to one privileged capability to get to another capability.
Exploit and compromise.	
Exploit physical access of authorized staff to gain access to organizational facilities.	Adversary follows ("tailgates") authorized individuals into secure/controlled locations with the goal of gaining access to facilities, circumventing physical security checks.

Exploit poorly configured or unauthorized information systems exposed to the Internet.	Adversary gains access through the Internet to information systems that are not authorized for Internet connectivity or that do not meet organizational configuration requirements.
Exploit split tunneling.	Adversary takes advantage of external organizational or personal information systems (e.g., laptop computers at remote locations) that are simultaneously connected securely to organizational information systems or networks and to nonsecure remote connections.
Exploit multi-tenancy in a cloud environment.	Adversary, with processes running in an organizationally-used cloud environment, takes advantage of multi-tenancy to observe behavior of organizational processes, acquire organizational information, or interfere with the timely or correct functioning of organizational processes.
Exploit known vulnerabilities in mobile systems (e.g., laptops, PDAs, smart phones).	Adversary takes advantage of fact that transportable information systems are outside physical protection of organizations and logical protection of corporate firewalls, and compromises the systems based on known vulnerabilities to gather information from those systems.
Exploit recently discovered vulnerabilities.	Adversary exploits recently discovered vulnerabilities in organizational information systems in an attempt to compromise the systems before mitigation measures are available or in place.

Threat Events (Characterized by TTPs)	Description
Exploit vulnerabilities on internal organizational information systems.	Adversary searches for known vulnerabilities in organizational internal information systems and exploits those vulnerabilities.
Exploit vulnerabilities using zero-day attacks.	Adversary employs attacks that exploit as yet unpublicized vulnerabilities. Zero-day attacks are based on adversary insight into the information systems and applications used by organizations as well as adversary reconnaissance of organizations.
Exploit vulnerabilities in information systems timed with organizational mission/business operations tempo.	Adversary launches attacks on organizations in a time and manner consistent with organizational needs to conduct mission/business operations.
Exploit insecure or incomplete data deletion in multitenant environment.	Adversary obtains unauthorized information due to insecure or incomplete data deletion in a multi-tenant environment (e.g., in a cloud computing environment).
Violate isolation in multi-tenant environment.	Adversary circumvents or defeats isolation mechanisms in a multi-tenant environment (e.g., in a cloud computing environment) to observe, corrupt, or deny service to hosted services and information/data.
Compromise critical information systems via physical access.	Adversary obtains physical access to organizational information systems and makes modifications.
Compromise information systems or devices used externally and reintroduced into the enterprise.	Adversary installs malware on information systems or devices while the systems/devices are external to organizations for purposes of subsequently infecting organizations when reconnected.
Compromise software of organizational critical information systems.	Adversary inserts malware or otherwise corrupts critical internal organizational information systems.
Compromise organizational information systems to facilitate exfiltration of data/information.	Adversary implants malware into internal organizational information systems, where the malware over time can identify and then exfiltrate valuable information.
Compromise mission-critical information.	Adversary compromises the integrity of mission-critical information, thus preventing or impeding ability of organizations to which information is supplied, from carrying out operations.

Compromise design, manufacture, and/or distribution of information system components (including hardware, software, and firmware).	Adversary compromises the design, manufacture, and/or distribution of critical information system components at selected suppliers.
Conduct an attack (i.e., direct/coordinate attack tools or activities).	
Conduct communications interception attacks.	Adversary takes advantage of communications that are either unencrypted or use weak encryption (e.g., encryption containing publically known flaws), targets those communications, and gains access to transmitted information and channels.
Conduct wireless jamming attacks.	Adversary takes measures to interfere with wireless communications so as to impede or prevent communications from reaching intended recipients.
Conduct attacks using unauthorized ports, protocols and services.	Adversary conducts attacks using ports, protocols, and services for ingress and egress that are not authorized for use by organizations.
Conduct attacks leveraging traffic/data movement allowed across perimeter.	Adversary makes use of permitted information flows (e.g., email communication, removable storage) to compromise internal information systems, which allows adversary to obtain and exfiltrate sensitive information through perimeters.
Conduct simple Denial of Service (DoS) attack.	Adversary attempts to make an Internet-accessible resource unavailable to intended users, or prevent the resource from functioning efficiently or at all, temporarily or indefinitely.
Conduct Distributed Denial of Service (DDoS) attacks.	Adversary uses multiple compromised information systems to attack a single target, thereby causing denial of service for users of the targeted information systems.
Conduct targeted Denial of Service (DoS) attacks.	Adversary targets DoS attacks to critical information systems, components, or supporting infrastructures, based on adversary knowledge of dependencies.
Conduct physical attacks on organizational facilities.	Adversary conducts a physical attack on organizational facilities (e.g., sets a fire).
Conduct physical attacks on infrastructures supporting organizational facilities.	Adversary conducts a physical attack on one or more infrastructures supporting organizational facilities (e.g., breaks a water main, cuts a power line).
Conduct cyber-physical attacks on organizational facilities.	Adversary conducts a cyber-physical attack on organizational facilities (e.g., remotely changes HVAC settings).

Threat Events (Characterized by TTPs)	Description
Conduct data scavenging attacks in a cloud environment.	Adversary obtains data used and then deleted by organizational processes running in a cloud environment.
Conduct brute force login attempts/password guessing attacks.	Adversary attempts to gain access to organizational information systems by random or systematic guessing of passwords, possibly supported by password cracking utilities.
Conduct nontargeted zero-day attacks.	Adversary employs attacks that exploit as yet unpublicized vulnerabilities. Attacks are not based on any adversary insights into specific vulnerabilities of organizations.
Conduct externally-based session hijacking.	Adversary takes control of (hijacks) already established, legitimate information system sessions between organizations and external entities (e.g., users connecting from off-site locations).
Conduct internally-based session hijacking.	Adversary places an entity within organizations in order to gain access to organizational information systems or networks for the express purpose of taking control (hijacking) an already established, legitimate session either between organizations and external entities (e.g., users connecting from remote locations) or between two locations within internal networks.

Conduct externally-based network traffic modification (man in the middle) attacks.	Adversary, operating outside organizational systems, intercepts/eavesdrops on sessions between organizational and external systems. Adversary then relays messages between organizational and external systems, making them believe that they are talking directly to each other over a private connection, when in fact the entire communication is controlled by the adversary. Such attacks are of particular concern for organizational use of community, hybrid, and public clouds.
Conduct internally-based network traffic modification (man in the middle) attacks.	Adversary operating within the organizational infrastructure intercepts and corrupts data sessions.
Conduct outsider-based social engineering to obtain information.	Externally placed adversary takes actions (e.g., using email, phone) with the intent of persuading or otherwise tricking individuals within organizations into revealing critical/sensitive information (e.g., personally identifiable information).
Conduct insider-based social engineering to obtain information.	Internally placed adversary takes actions (e.g., using email, phone) so that individuals within organizations reveal critical/sensitive information (e.g., mission information).
Conduct attacks targeting and compromising personal devices of critical employees.	Adversary targets key organizational employees by placing malware on their personally owned information systems and devices (e.g., laptop/notebook computers, personal digital assistants, smart phones). The intent is to take advantage of any instances where employees use personal information systems or devices to handle critical/sensitive information.
Conduct supply chain attacks targeting and exploiting critical hardware, software, or firmware.	Adversary targets and compromises the operation of software (e.g., through malware injections), firmware, and hardware that performs critical functions for organizations. This is largely accomplished as supply chain attacks on both commercial off-the-shelf and custom information systems and components.
Achieve results (i.e., cause adverse impacts, obtain information)	
Obtain sensitive information through network sniffing of external networks.	Adversary with access to exposed wired or wireless data channels that organizations (or organizational personnel) use to transmit information (e.g., kiosks, public wireless networks) intercepts communications.
Obtain sensitive information via exfiltration.	Adversary directs malware on organizational systems to locate and surreptitiously transmit sensitive information.
Cause degradation or denial of attacker-selected services or capabilities.	Adversary directs malware on organizational systems to impair the correct and timely support of organizational mission/business functions.
Cause deterioration/destruction of critical information system components and functions.	Adversary destroys or causes deterioration of critical information system components to impede or eliminate organizational ability to carry out missions or business functions. Detection of this action is not a concern.
Cause integrity loss by creating, deleting, and/or modifying data on publicly accessible information systems (e.g., web defacement).	Adversary vandalizes, or otherwise makes unauthorized changes to, organizational websites or data on websites.
Cause integrity loss by polluting or corrupting critical data.	Adversary implants corrupted and incorrect data in critical data, resulting in suboptimal actions or loss of confidence in organizational data/services.
Threat Events (Characterized by TTPs)	Description
Cause integrity loss by injecting false but believable data into organizational information systems.	Adversary injects false but believable data into organizational information systems, resulting in suboptimal actions or loss of confidence in organizational data/services.
Cause disclosure of critical and/or sensitive information by authorized users.	Adversary induces (e.g., via social engineering) authorized users to inadvertently expose, disclose, or mishandle critical/sensitive information.

Cause unauthorized disclosure and/or unavailability by spilling sensitive information.	Adversary contaminates organizational information systems (including devices and networks) by causing them to handle information of a classification/sensitivity for which they have not been authorized. The information is exposed to individuals who are not authorized access to such information, and the information system, device, or network is unavailable while the spill is investigated and mitigated.
Obtain information by externally located interception of wireless network traffic.	Adversary intercepts organizational communications over wireless networks. Examples include targeting public wireless access or hotel networking connections, and drive-by subversion of home or organizational wireless routers.
Obtain unauthorized access.	Adversary with authorized access to organizational information systems, gains access to resources that exceeds authorization.
Obtain sensitive data/information from publicly accessible information systems.	Adversary scans or mines information on publically accessible servers and web pages of organizations with the intent of finding sensitive information.
Obtain information by opportunistically stealing or scavenging information systems/components.	Adversary steals information systems or components (e. g., laptop computers or data storage media) that are left unattended outside of the physical perimeters of organizations, or scavenges discarded components.
Maintain a presence or set of capabilities.	
Obfuscate adversary actions.	Adversary takes actions to inhibit the effectiveness of the intrusion detection systems or auditing capabilities within organizations.
Adapt cyber attacks based on detailed surveillance.	Adversary adapts behavior in response to surveillance and organizational security measures.
Coordinate a campaign.	
Coordinate a campaign of multi-staged attacks (e.g., hopping).	Adversary moves the source of malicious commands or actions from one compromised information system to another, making analysis difficult.
Coordinate a campaign that combines internal and external attacks across multiple information systems and information technologies.	Adversary combines attacks that require both physical presence within organizational facilities and cyber methods to achieve success. Physical attack steps may be as simple as convincing maintenance personnel to leave doors or cabinets open.
Coordinate campaigns across multiple organizations to acquire specific information or achieve desired outcome.	Adversary does not limit planning to the targeting of one organization. Adversary observes multiple organizations to acquire necessary information on targets of interest.
Coordinate a campaign that spreads attacks across organizational systems from existing presence.	Adversary uses existing presence within organizational systems to extend the adversary's span of control to other organizational systems including organizational infrastructure. Adversary thus is in position to further undermine organizational ability to carry out missions/business functions.
Coordinate a campaign of continuous, adaptive, and changing cyber attacks based on detailed surveillance.	Adversary attacks continually change in response to surveillance and organizational security measures.
Coordinate cyber attacks using external (outsider), internal (insider), and supply chain (supplier) attack vectors.	Adversary employs continuous, coordinated attacks, potentially using all three attack vectors for the purpose of impeding organizational operations.