**Incident Response – Distributed Denial of Service (DDoS), Web Defacement, and Cross-site Scripting for Webpage**

Marcel Njighe Tezeh

Wilmington University

SEC6060

Dr Fraley

August 22, 2021

# **Incident Response – Distributed Denial of Service (DDoS), Web Defacement, and Cross-site Scripting for Webpage**

# **Part I: Introduction**

## **Impact Statement**

The following will outline recommendations for incident responses for handling a compromise or violation of an organization’s security in support of the Wilmington University (Wilmu) mission (Kral, 2012; "Library Mission, Vision, and Values," 2019).

* Collecting and facilitating access to information in multiple formats.
* Linking to global networks.
* Providing adaptive learning spaces and the technologies to support research and the creation of knowledge.
* Preserving the scholarly record and unique content of the University.

**Part II: Design of Plan**

## **Purpose**

The Wilmu Library is critical to the student's and faculty's continued support, providing significant scholastic and administrative resources to keep the University's academic and operational systems functioning. The Incident Response Plan (IRP) provides the framework and the foundation for handling incident responses (Kral, 2012). An IRP helps an organization prepare for the operational part of responding to an inevitable security breach (Johnson 2014; Kral, 2012). The IRP outlines how to respond and mitigate an incident, the business criteria for recovery, key indicators for normal business operations, and follow-up activities (Johnson 2014; Kral, 2012). The incident response supports detecting incidents and managing these incidents to minimize damages and downtime (Johnson 2014). In addition, the IRP will show that Wilmu Library has due care and due diligence in place when there is a security breach (Johnson 2014).

**Objectives**

The following are key objectives of the IRP (King & Moore, 2018).

* Identify and prioritize critical Wilmu Library processes
* Define plans to restore services within defined key performance indicators
* Document the various key roles and responsibilities to support this IRP

The IRP provides a framework for the Wilmu employees to enable the responses within this document (King & Moore, 2018). When an event occurs, the business impact found in this document lists processes in priority to help reduce the risk and reduction in the University Library from providing services to students (King & Moore, 2018).

## **Use of the IRP**

The IRP will provide a mechanism to focus training and restoration efforts in an emergency (Johnson 2014). The IRP helps an organization prepare for the operational part of responding to an inevitable security breach utilizing the following stages (Johnson 2014).

* Preparation;
* Identification;
* Containment;
* Investigation;
* Eradication;
* Recovery; and
* Follow-up.

The Wilmu employees and Wilmu’s contractors should use the IRP stages and their training to minimize damage and restore services while maintaining the evidence from the incident (King & Moore, 2018). To prosecute an attacker, the forensics team must provide evidence to connect the attacker to an incident (Thiruvaazhi & Alex, 2012).

## **Assumptions**

The following assumptions address the criteria of this IRP of Distributed Denial of Service (DDoS), Web Defacement, and Cross-site Scripting for Webpage.

* Wilmu has incident response capabilities such as monitoring and network logging (Johnson 2014).
* Wilmu has the appropriate resources: employees, third-party partners, software, and hardware to respond to an incident (Kral, 2012).
* A clear understanding of severity definition to support the incident response (Johnson 2014).
* The Business Impact Analysis (BIA) assists in outlining the priorities and timeframes for restoring operations (Johnson 2014).

## **Development**

Wilmu co-chairs work with the Wilmu CIO and appropriate essential resources/roles in defining and developing the Wilmu Library IRP ("MIT Business Continuity Plan," 1995). The essential resources/roles are the ongoing maintenance of the critical process areas for functional business processes are the key resources/roles ("MIT Business Continuity Plan," 1995).

## **Testing**

Testing scenarios need to represent actual cases to train employees and third parties how to react to and deal with security incidents and their processes to resolve these incidents. The tabletop exercises provide a safe environment to focus and train everyone to respond to a specific cyber incident. There are two different types of tabletop exercises.

* Technical Tabletop Exercise is for Wilmu and the third-party technical security team. The exercise outputs help the team understand how to respond and refine IRP to respond to security incidents better.
* Executive Tabletop Exercise is for the executive-level employees. The tabletop exercise will walk through the decisions to support the IRP for man-made security incidents. The outcome is that the executive employees understand the various roles, processes, and internal and external communication approaches during a security incident.

Testing of the IRP will occur on an annual basis unless significant software or infrastructure changes occur.

## **Maintenance**

Maintenance includes the ongoing updating and revising of this living document to reflect ongoing changes to software, infrastructure, new or removal of functionality, changes in Cloud providers, or the addition of new forensic testing tools (*"MIT Business Continuity Plan,"*1995; Snedaker & Rima, 2014). All changes need to adhere to the following Change Management process (Snedaker & Rima, 2014).

* Changes require testing to ensure these operate correctly
* Changes to critical business processes require a review and approval from the Wilmu Emergency team
* Update the revision number
* Update training and testing materials
* Communicate the changes and perform training as required
* Distribute the plan to the appropriate people

# **2. Organization of Disaster Response and Recovery**

## **Business Continuity Management Team**

This Business Continuity Management Team (BCMT) is responsible for responding in the event of a disaster. The response includes assessing potential damage to the Wilmu Library facility and enacting the Wilmu Library's Wilmu Library Coordinator Center. Including taking the lead responsibility to ensure that the Wilmu Library can function effectively during a crisis and resume business operations as quickly as possible (refer to Figure 1).

The Business Continuity Management Team (BCMT) is responsible for implementing and executing the IRP ("MIT Business Continuity Plan," 1995). In this case, the Library BCMT will focus the IRP on cyber hacks, Denial-of-Service attacks, and data compromises. Responsibilities include responding and implementing the corresponding IRP ("MIT Business Continuity Plan," 1995). As such, the Library IRP will outline the employees requirements and actions to respond to Distributed Denial of Service (DDoS), Web Defacement, and Cross-site Scripting for Webpage attacks and the required timeframes to restore critical business processes (Hout, 2020).

**Figure 1**

*Business Continuity Management Team (BCMT)*



## **Incident Response**

In the age of the digital revolution, cyber-attacks can be crippling. Proper and efficient incident response to such attacks is critical in restoring network services to normal function with little to no interruption. Once a cyber-attack is detected, it is crucial to identify the type of attack, contain the attack to support the forensics investigation (Johnson, 2014).

## **Disaster Detection and Determination**

With technological advancements, there are more ways in which those advancements can be compromised. The implementation of disaster detection and determination are critical in maintaining security. When detection abilities are in place, that helps prevent a disaster from happening as the employees is notified of possible threat attempts. Determination of disasters is important in ensuring that the disaster is responded to in a reasonable amount of time and so additional disasters can be prevented. Wilmu Library employees should be aware of detection and discovery of disasters and update security as needed.

## **Disaster Notification**

In the event of a disaster, employees and students should receive an alert via email or text message letting them know what occurred and how they might have been affected. It is also necessary to include how Wilmu Library has solved/is solving the incident.

# **3. Initiation of the Incident Response Plan**

## **Activation of a Business Continuity Site**

As Wilmu Library contains many resources both in the physical locations and on the website, it is crucial to have a backup of their resources in an incident that disrupts these resources. Having remote backups will provide a mechanism to ensure constant connectivity to Wilmu employees and students.

## **Dissemination of Public Information**

Wilmu Library must respond promptly, confidently, and accurately during an emergency, especially when there is media coverage for the situation.

During a Data breach, Wilmu Library should first solve the problem and then send out information to all the individuals whose data is compromised and what actions they can take to avoid further damage.

For example, a denial-of-service in the Wilmu Library online platform requires a quick update to Wilmu employees and students with a potential return to regular service date. When the cyberattack impacts Wilmu's finances and compromises personal data requires the notification of the proper authorities and then the public.

## **Disaster Recovery Strategy**

Organizations of all sizes generate and manage massive amounts of data; much of it is mission-critical. The impact of corruption or data loss from human error, hardware failure, malware, or hacking can be substantial. Therefore, it is essential to have the IRP as part of the Business Continuity Plan (BCP) and the disaster recovery plan to restore business data from a data backup image while recovering evidence from the attack (Kelly, 2020).

## **Emergency Phase**

This phase occurs in the immediate aftermath of a disaster. Organizations must focus their attention on addressing immediate threats to people, property, and business (Kelly, 2020).

In the case of Wilmu Library, forming a team and focusing on the emergency right away should be the first step. A level of preparedness prepares the Wilmu Library for these events.

# **4. Scope of the Incident Response Plan**

## **Overview**

As defined in the business continuity strategy, an Incident Response Plan includes procedures for all the phases. The scope will focus on human-made disasters such as cyber risk, denial of service, and data compromise. Incident Response Plan is limited in scope to recovery and business continuity from a severe disruption of human-made activities due to the non-availability of library facilities. The Incident Response Plan includes procedures that align with recovery processes in the Business Continuity Strategy. This plan will not cover major regional or national disasters such as regional earthquakes, war, or nuclear holocaust. However, it can provide some guidance in the event of such a large-scale disaster.

This risk category identifies applications with the highest priority and must be restored within hours of a disaster disabling a functional area. Specifically, each function of these systems includes an evaluation to ensure the appropriate allocations are in place for these risk categories, as described below.

## **Category I- Critical Functions**

Some of the critical functions of this Incident Response Plan include the following.

* Emergency Management: In different situations, the employee should know how to respond to a cyber hack or data breach.
* Security: Protecting physical and intellectual property, data records, and other sensitive materials from damage, theft, or loss is another critical function of the Incident Response Plan.
* Information Technology: The security and protection of the entire system are critical to maintain operations. In the event of an IT disruption, there could be no access to the system available.

## **Category II- Essential Functions**

Disaster Recovery: It is essential to store the essential records, data, and plans almost solely electronically, protecting the security and sanctity of IT systems.

## **Category III- Necessary Functions**

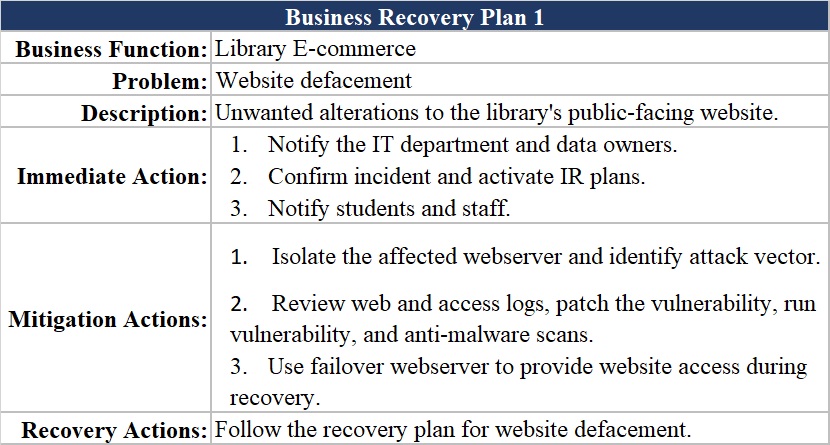
Knowledge Management: Knowledge management covers the distribution of trade secrets, passwords, and other pertinent business knowledge so that business can survive beyond the lifetime of any one particular team member.

## **Category IV- Desirable Functions**

Health and Safety: Beyond the business function, customers' and employees' health and safety are paramount. As we are dealing with Cyberattack and Data breaches, health and safety will not be as much and will not be a critical function to address. Refer to Figure 2 for examples of business recovery plans. The IRP needs to align and integrate with the Wilmu Library's existing Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) (Sher-Jan, 2012).

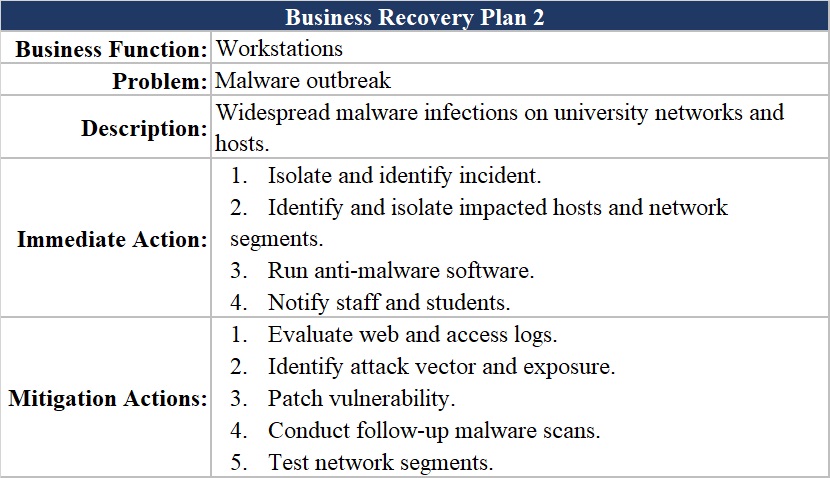
**Figure 2**

*Two Business Recovery Plan Examples*



**Figure 2**

*Two Business Recovery Plan Examples (continued)*

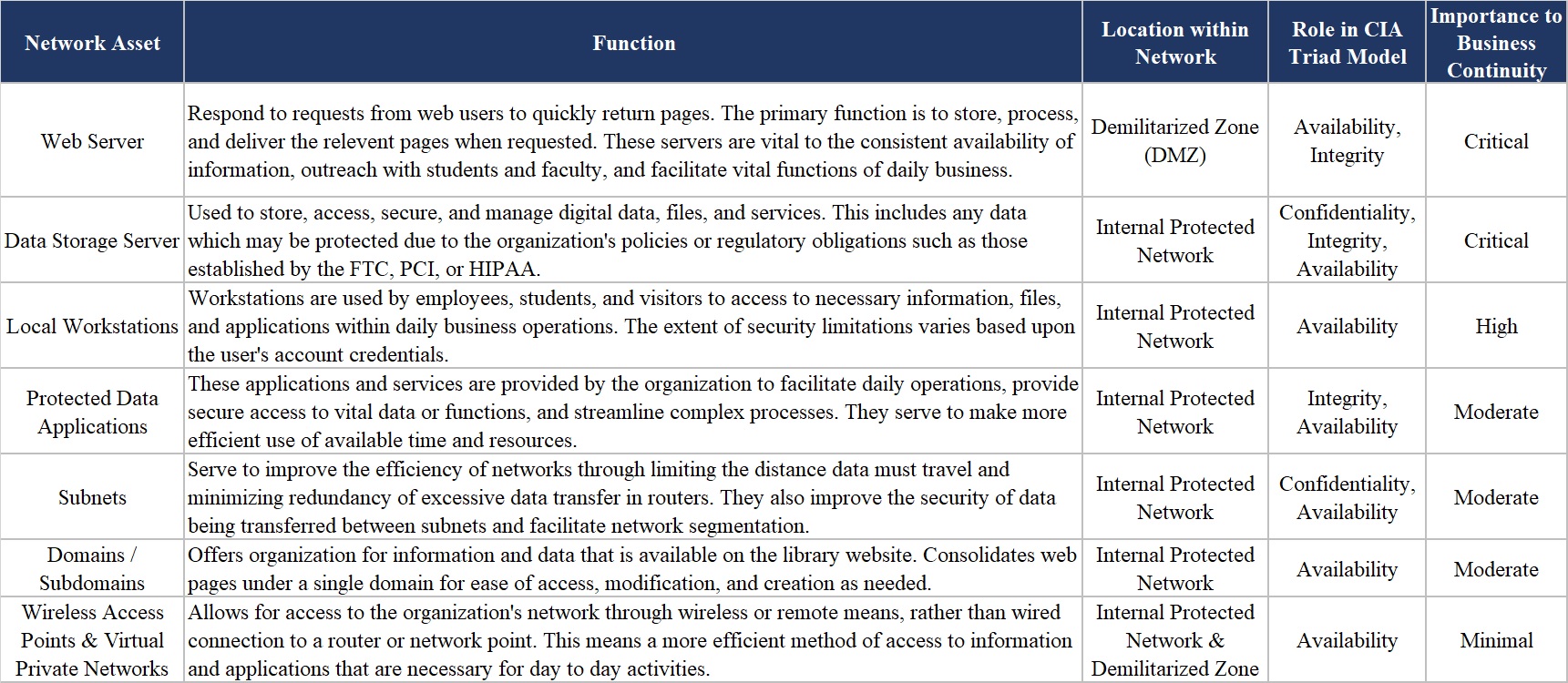


## **Business Impact Analysis**

An essential step in preparing incident response procedures is to conduct business impact analysis (BIA). This analysis aims to identify assets within an organization's network and predict the likelihood and consequences of disruption of business functions. The result is an understanding of the relevant assets, their relevant business function, and their importance to business continuity (Weber, 2019). Thus, allowing for a holistic assessment of the business functions facilitates prioritizing network security for the most vulnerable or vital assets. Refer to Figure 3 for the asset enumeration for the Wilmu Library.

**Figure 3**

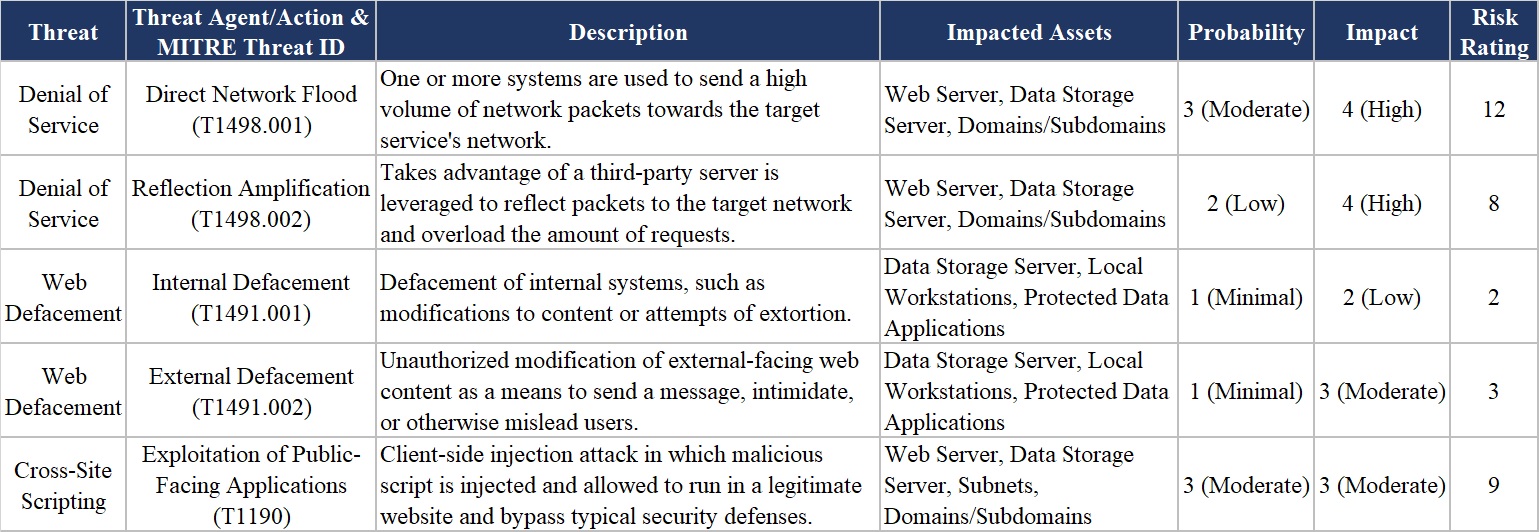
*Asset Enumeration for the Wilmu Library*



With the inventory taken of the network's assets and their relevant business functions, the incident response team can begin conducting a risk assessment and understanding the risks presented through quantitative grading. Grading uses the simple equation of Risk = Impact x Probability (Woerner, 2017). Potential impact can take many forms, such as the loss of sales, delayed income, increased expenses for recovery, regulatory fines, contractual penalties, client dissatisfaction, or negative brand publicity (Ready.gov, 2021). The impact of these factors can vary from one organization to another or differ from one time to another, so consistent assessment is vital to maintain a realistic view of threats and risks. The table below (refer to Figure 4) outlines the prospective risks of methods used for denial of service, web defacement, and cross-site scripting, as dictated by the MITRE ATT&CK threat database.

**Figure 4**

*MITRE ATT&CK Threat Risk Ratings*



# **PART III TEAM DESCRIPTIONS**

## **1. Business Continuity Management Team**

### ***Overview***

Section III outlines the key organizations and responsibilities across the BCMT, sub-teams, and functional areas such as support teams (*"MIT Business Continuity Plan,"* 1995).

### ***Roles/Responsibilities***

During an emergency, it takes various people/roles across Wilmu to ensure the appropriate actions to rectify the human disaster (*"MIT Business Continuity Plan,"* 1995). Refer to Appendix A for contact information for the following roles.

* College President – Mostly informational, but the President will assist when there is a requirement for emergency budget approvals.
* Library Director and Assistant Library Director – oversees the library's day-to-day activities and needs to assist in all recovery efforts.
* Librarian – supports the Library Director and can be the go-to role for the support teams to address questions to restore the library systems.
* Chief Information Officer – oversees the IT operations and is a key contact to ensure the correct people on the IT/Datacenter teams are part of the recovery efforts.
* Library Public Services and Communications Specialist or the Director Public Relations – supports both internal and external communications.
* Library Technician II – an expert in the Wilmu library systems and provides information to the IT/Datacenter teams.
* Vice President, Administrative and Legal Affairs – oversees Wilmu legal operations and ensures the correct people on the legal operations teams are part of the recovery efforts.
* Operations Manager – support anything to do with the Wilmu facilities.
* Library Resources and Systems Manager – deep understanding of key Wilmu library business processes, can provide information to the IT/Data Center teams and support testing.
* Learning Commons Assistant – deep understanding of key Wilmu library business processes can provide information to the IT/Data Center teams and support testing.
* Instruction Librarian – deep understanding of key Wilmu library business processes, can provide information to the IT/Data Center teams and support testing.
* Chief Human Resources Officer – oversees HR operations and ensures the correct people on the HR operations teams are part of the recovery efforts.

## **2. Organization Support Teams**

The following is a list of the various teams to assist with human-made disasters such as cyber risk, denial of service, and data compromise.

* Human Capital Management sub-team – assists with all employee matters.
* Insurance Team – supports the Wilmu to ensure payment dispersion for all applicable coverage areas per the Wilmu policy.
* IT/Data Center sub-team(s) – assist in the restoration of disrupted services.
* Legal/Contract sub-team(s) – help clarify and ensure all partners adhere to the current contract(s) and support any potential ligations due to the disaster.
* Physical Security team – limit or prevent access to any computer system on a Wilmu campus site to prevent any other human-made disaster.
* Public Information sub-team – communicate to the Wilmu employees, students, and the public as required about the current disaster, schedule for updates, and when systems are returning to normal operations.
* Student and Alum teams – supports the direction of the BCMT to ensure students are cared for during the disaster.

# **PART IV RECOVERY PROCEDURES**

## **1. Notification List**

* Refer to Figure 1, Business Continuity Management Team (BCMT) for the contact information.
* A review of the contact list needs to occur during the annual IRP review.
* The contact list needs updating when there are changes in the organization.

## **2. Action Procedures**

### ***Distributed Denial of Service (DDOS)***

Denial of Service (DoS) is typically a severe event since the goal is to prevent anyone from accessing a service such as a web server bringing a business to a halt (Mölsä, 2005). A few types of DoS include flooding, distributes, and logic to be aware of when developing an IRP (Mölsä, 2005). A DoS attack can flood the target host or network with traffic until the target cannot respond or crashes, preventing legitimate users' access (CISA, 2009). The Distributed Denial of Service (DDoS) uses a flood approach but in a coordinated fashion across several services simultaneously (Mölsä, 2005).

Intrusion Detection Systems (IDS) alerts can trigger an Incident Response (IR) (Mölsä, 2005). An additional sign that can trigger IR response includes the following (CISA, 2009).

* Slow network performance
* System unavailability, or
* Unable to access any website.

**DDoS Defense.**

There are different attack types, Indirect, Direct, and Reflection (Pandya, 2015). The Indirect attack uses zombies and bots to hide the attacker's origin (Pandya, 2015). Versus a Direct attack targets a specific host (Pandya, 2015). The Reflection attack hides the attacker's identity by using an intermediate host (Pandya, 2015).

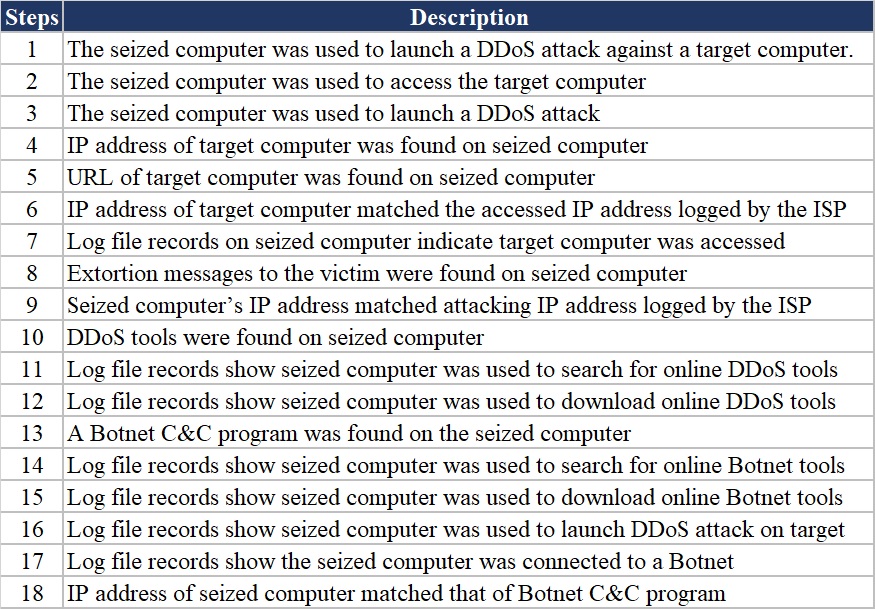
A company needs to plan a defense for each attack type using software and hardware (Pandya, 2015). In addition, the DDoS incident management process needs to be part of the overall company incident management process (Pandya, 2015). The overall DDoS defense will support the forensic response by protecting potential evidence and using software tools such as monitors, a flow monitor, and logs during the forensic analysis (Pandya, 2015).

Once it is known there is a DDoS attack underway, it is vital to follow the DDoS incident management process and engage resources from the forensics team to preserve any potential evidence (Thiruvaazhi & Alex, 2012). An organization can deploy several mitigation strategies depending on its size and budget once identifying a DDoS attack (Lyon, 2017). Amazon and Microsoft continue to enhance their service offerings with packet filtering, employing a blocking proxy and blacklisting known bad network traffic, load balancing, and redundancy (Chen et al., 2017; Joelle & Park, 2018). During the DDoS attack, Wilmu can reroute employee and student traffic using the Domain Name System (DNS) Service (SRV) records, the Name Authority Pointer (NAPTR) records to route the requests to the backup server (Chen et al., 2017). In addition, Wilmu could purchase access to scrubbing centers at providers such as AWS or Google to block DDoS traffic due to volumetric and application-based attacks (Orans, 2017).

To prosecute an attacker, the forensics team must provide evidence that can connect the master-handler of the attacker to their command and control for the DDoS attack (Thiruvaazhi & Alex, 2012). The forensic team should perform key steps to preserve evidence and support post-attack forensics (Overill, 2013; Thiruvaazhi & Alex, 2012). Each forensic investigation is the same, and the use of templates assists in preserving DDoS evidence (Overill, 2013). The goal of using a template and standardized steps is to identify the PC with the DDoS command and control launch software (see Figure 3).

## **Figure 3**

*Template Data for Forensic Investigation of a Suspected DDoS Attack*



Wilmu Library will need to use a third party to perform a post-attack forensics review (Thiruvaazhi & Alex, 2012). A third party should have the ability to create a lab to mimic a safe environment using the computer identified for launching the DDoS attack to perform a traceback analysis (Thiruvaazhi & Alex, 2012). The goal of the traceback analysis is to identify the master-handler (Thiruvaazhi & Alex, 2012).

The team will need to review the monitoring logs from the Intrusion Prevention Systems (IPS), firewalls, and flow monitor to help recreate an attack (Overill, 2013; Thiruvaazhi & Alex, 2012). Depending on the test lab will directly impact the ability to do a traceback analysis (Thiruvaazhi & Alex, 2012). The team will place the attack code on some systems and launch a small attack (Thiruvaazhi & Alex, 2012). The goal is to capture the information on the architecture of Handler Agent of DDoS attack using packet sniffers (Thiruvaazhi & Alex, 2012).

The next step is to test the disk images using tools to locate files executed during the attack (Thiruvaazhi & Alex, 2012). As long as there were no anti-forensic or file location was overwritten too many times, the team might identify the attack code leading to the master-handler (Thiruvaazhi & Alex, 2012). This information can help identify the systems used for launching the initial attack and, at times, the attack code (Thiruvaazhi & Alex, 2012). Finally, the team will perform network forensics (Thiruvaazhi & Alex, 2012). Leveraging the network logs and if a network analyzer was tunning its logs to find patterns in communication and unique IP addresses (Thiruvaazhi & Alex, 2012).

Using a repeatable procedure with both computer and network forensics can help the forensics team identify UP traceback to the master-handler used by the attacker (Overill, 2013; Thiruvaazhi & Alex, 2012). The evidence from the Wilmu Library and a third party will assist in prosecuting the attacker(s) (Thiruvaazhi & Alex, 2012).

### ***Web Defacement***

The unauthorized modification of web pages, including the addition, removal, or alteration of existing content, is referred to as website defacement (CywareLabs, n.d.). Threat actors may be motivated to deface a website for various reasons, including attempting to embarrass Wilmu or promoting alternative viewpoints. In some cases, a threat actor may deface a website by injecting malicious code that infects visitors' devices (Center for Information Security (CIS), 2021). The main consequence of this attack would be the loss of credibility of the hacked organization (Wilmu Library). In some cases, it leads to indirect economic losses because of the distorted web content conveyed by the hacked organization (Mao & Bagolibe, 2019).

**Web Defacement Defense.**

This plan is created with a general guideline to defend against and recover Wilmu University library from website defacements. Maintaining up-to-date software can reduce the risk of defacement of the Wilmu library website. In most cases, the defense against web defacement relies on monitoring websites and restoring the system after the incident (Mao & Bagolibe, 2019).

The time between the execution of the attack and the system's restoration time is highly dependent on the performance of the website's monitoring tool and the response capacity of the technical teams (Mao & Bagolibe, 2019). Most website defacement defense tools available on the market can, to some extent, the integrity of the data and the notification of the administrators when signatures change. This technique is more or less effective for static websites subjected to weak modification cycles (Mao & Bagolibe, 2019).

Wilmu security team should be involved when designing and developing its website. Wilmu security team will work closely with its development team to ensure that they are well trained in secure coding practices such as encoding outputs properly to prevent cross-site scripting attacks. Use specific coding alternatives to protect the website from Structured Query Language (SQL) attacks and HTTPS-only cookies to protect the website from hackers. Wilmu should also explore the following techniques to safeguard its website from defacement further:

* Implement the principle of least privilege on web servers
* User input validation
* Reverse proxies
* Deploying web application firewalls

**Identification and Notification.**

Wilmu should utilize third-party web content monitoring systems. Content monitoring systems like ESDS VTMSCAN enables security defacement monitoring to track a website before it is breached (Jadhav, 2020). While monitoring, the records are maintained by taking snapshots. In this phase, the genuine changes made by the Wilmu are captured and compared with the website's current state (Jadhav, 2020).

Wilmu Information Security Incident Response procedure should provide specific details of handling information security events within the Wilmu Library. The Wilmu administrative policy should require any individual, system monitoring team, and all Wilmu employees. Anyone who suspects that an information security incident has likely occurred needs to report it to the appropriate parties, including the Wilmu IR team, their manager, departmental representatives, information technology response employees, institutional risk management, and university communications.

**Web Defacement Incident Response.**

Wilmu should respond to website defacement attacks by first taking the website offline and activating the IR plan to remove the malicious code and patch the vulnerabilities. In the investigation and eradication phases, the Wilmu incident response and digital forensic plan should entail the team to:

* Contact the vendor if the Wilmu library is the third party hosting the website to report any abnormal activities.
* Replace the website with a maintenance page immediately.
* Wilmu CSIRT should inspect the contents and latest backups of the site for hidden malware and vulnerabilities.
* Inform relevant parties of the incident (e.g., students, instructors, suppliers, and third parties).
* Make a statement to the public to preserve Wilmu organizational reputation.
* Restore the Wilmu website with backups to ensure a quick recovery.
* Report the incident to the police.
* Have an external forensic technical expert investigate and analyze how the website was defaced and evaluate the response process (e.g., to improve for any future complications).

**Web Defacement Forensic Analysis.**

Both criminals, as well as investigators, use the internet. Every moment, a criminal leaves traces on a computer while using a web browser. The browser history, temporary files, index.dat, cookies, download files, unallocated space, and cache contribute to providing proof (Nalawade, & Bharne, & Mane, 2016). The private forensic investigator hired by Wilmu should use log files to find out critical information like when, how, and by whom accessed the Wilmu Library webserver. For example, a web server, most commonly, Apache HTTP Server, will provide two main log files – access.log and error.log. The access.log records all requests for files that the forensic expert (s) can use in their investigation.

### ***Cross-site Scripting for Webpage***

Cross-site scripting (XSS) attacks are malicious scripts injected into websites considered to be trustworthy and secure (Kirsten, 2020). In XXS attacks, an attacker uses a web application as a vehicle to distribute malicious code, typically via a browser side script, to the end-user. Flaws or vulnerabilities within the web application provide an opportunity for an attack anywhere there is the use of user input and the output it creates without validating or encoding it (Kirsten, 2020). There are four classifications of an XXS attack, stored (persistent), reflected (non-persistent), induced XXS, and Dom-based XXS (Wasef & Fitri, 2016).

**Detection and Notification.**

The most common methods of identifying vulnerabilities susceptible to XXS attacks within the web application are in the following categories: dynamic analysis, static analysis, and hybrid analysis (Wasef & Fitri, 2016). Static analysis can detect errors initially but is not accurate and can lead to several false positives. Dynamic analysis is when a security tool hits the operating application dynamically based on thousands of identified vulnerabilities and attack plans (Wasef & Fitri, 2016). Hybrid, a combination of the previously mentioned two, uses the dynamic analysis method combined with the false positives of the static analysis to provide more accurate results (Wasef & Fitri, 2016).

There should be routine manual testing, code review, and use of web application security scanners to determine if an attack has occurred. When there is suspicion that the Wilmu Library has identified an XSS attack, the protocol should include the notification of the University IT department.

**XSS Defense.**

Preventing XSS can be simple in some cases and complex in other cases. The meter of difficulty depends on the complexity of the application and its means of handling user-controllable data (PortSwigger, 2019). PortSwigger (PortSwigger, 2019) states that a combination of the following measures can effectively prevent XSS vulnerabilities:

* Filter user input as strictly as possible
* Encode the user-controllable data output
* Use headers to ensure browsers interpret the responses as they were intended
* Use a Content Security Policy (CSP) to minimize the severity of any XXS vulnerabilities that could occur

**Incident Response for XSS.**

The incident response to an XSS attack includes several phases. First, define the CSIRT, assets, and scope of the identified attack. Second, use the preliminary investigation to declare an incident (Nidecki, 2019). Including any intelligence necessary to assist in the declaration. Third, once the scope of the incident is determined, identify what assets to contain. Containment is necessary to eliminate affecting other assets. Next, eliminate the "poisonous" script and any such consequences of the incident. For example, fix all remaining vulnerabilities (Nidecki, 2019). Finally, in the recovery phase, reconnect the assets and complete any necessary communications and legal/compliance resources due to the incident (Nidecki, 2019).

**Forensic Analysis of XSS.**

Obtain the digital evidence regarding an XSS attack using Wireshark, HashMyFile, and Mozilla extension Live HTTP Headers (Kurniawan et al., 2017). The analysis process has three phases, traffic analysis, hashing file analysis, and comparative analysis. Record and review all network traffic. Digital evidence gathered from the traffic header can provide communication information from the attacker, victim, and server (Kurniawan et al., 2017). Finally, use the backdoor-master.zip file downloaded by the victim and the backdoor.exe file on the server machine as digital evidence (Kurniawan et al., 2017).

## **Handling Evidence in Digital Forensics**

The handling of evidence that has been collected in a digital forensics investigation can make the outcome of an ensuing legal case. Because of this, there should be strict policies that gather how devices are collected and how the analysis is performed. The National Institute of Justice has noted that "digital evidence should be examined only by those trained specifically for that purpose" (Novak et al., 2018). Given that it is not unusual for digital forensics work to be outsourced to a contractor or specific government agencies to conduct. Despite this, there are guidelines that should be followed by all involved.

### ***Collection of Digital Devices***

**On the Scene.**

The digitally stored information is typically very sensitive and easily lost. Best practices such as the Scientific Working Group on Digital Evidence or the National Institute of Justice provide guidance on the proper handling of devices due to liquid, structural, or thermal damage (SWGDE, 2016). These best practices also include instructions on safely packing and transporting the devices to maintain integrity and efficient data retrieval. These guidelines dictate specific instructions for the handling of mobile devices and standalone computers or equipment.

**Mobile Devices.**

* Immediately turn off the device and remove the batteries. This preserved vital information such as cell tower location, call logs, and further manipulation of data on startup. The result is a reduction in the risk of remote destruction commands and other anti-forensics practices.
* When the device cannot be turned off, isolate it from nearby cell towers or outside interference. Setting the device to airplane mode, using a Faraday bag, or disabling Wi-Fi and Bluetooth capabilities can prevent outside interference.
* Transport the devices in antistatic packaging, such as paper bags or envelopes. Avoid using plastic containers due to their tendency to convey static electricity and humidity.

**Standalone Equipment.**

* Photograph the device's setting and note any current processes or connected hardware. If the computer is currently running, do not turn it off until it has been assessed. Evidentiary connections may be removed and lost if the device is shut down.
* If it is currently running destructive software, the device should be disconnected to prevent the deletion or removal of trace evidence within event logs.
* Nearby equipment should be assessed and seized as well. Connected devices such as copiers, scanners, surveillance cameras, and phones can contain evidence of suspected attack vectors.

**Performing Analysis.**

Once seizing the device(s), documenting the scene(s), and evidence is in the hands of the analysts, there are steps to maintain the integrity of this data.

**Prevent Contamination.**

Create devices images or work copies of the seized device before conducting any analysis. Use a clean piece of storage media to prevent any existing information from being analyzed and potentially contaminate the analysis's findings (Goodison et al., 2015). Storage media should be new or forensically wiped before use.

**Install Write-Blocking Software.**

Write-blockers prevent the working copy of the device from being subjected to any further manipulation. The data is only viewable and allows the analysis without altering the evidence (Asad, 2020).

**Select Ideal Extraction Methods.**

The variety of devices means that not every shred of evidence can be subject to the same extraction methods. Different software and operating systems vary in terms of encryption, whether full-disk, file-based or password-protected (Zbrog, 2019). Thus, allowing for an assessment on the best way to extract the data without hindering the analysis and investigation process.

While Wilmu does not necessarily possess the capability or expertise to carry out a full digital forensics' investigation, facets of the process are essential to understand. Adhering to best practices when examining digital or evidence or simply responding to an ongoing incident can drastically alter the outcome. There is an obligation to take these risks into account when formulating an incident response plan.

# **References**

Asad, S. (2020). Best Hardware Write Blockers for Digital Investigators. Linuxhint.com. https://linuxhint.com/best\_hardware\_write\_blockers/

Chen, W.-E., Tseng, L.-Y., & Chu, C.-L. (2017). An effective failure recovery mechanism for sip/ims services. Mobile Networks and Applications : The Journal of Special Issues on Mobility of Systems, Users, Data and Computing, 22(1), 51–60. https://doi.org/10.1007/s11036-016-0678-8

CIS (Center for Internet Security). (2021, June 15). Election Security Spotlight-Website Defacements. CIS. https://www.cisecurity.org/spotlight/cybersecurity-spotlight-website-defacements

CISA. (2009, November 4). Understanding Denial-of-Service Attacks. Cybersecurity and Infrastructure Security Agency CISA. https://us-cert.cisa.gov/ncas/tips/ST04-015

Cyware Labs. (n.d.). Web Defacement Attack Response | Incident Response | Retrieved August 13, 2021, from Cyware. https://cyware.com/use-case/web-defacement-response-automation

Goodison, S., Davis, R., & Jackson, B. (2015). *Digital Evidence and the U.S. Criminal Justice System Identifying Technology and Other Needs to More Effectively Acquire and Utilize Digital Evidence*. https://www.ojp.gov/pdffiles1/nij/grants/248770.pdf

Hout, O. (2020, September 28). 5 Essential Steps to Business Continuity Planning. Agility. https://www.agilityrecovery.com/article/5-essential-steps-business-continuity-planning

Jadhav, G. (2020, January 21). Monitor your Website Defacement Attacks with ESDS VTMScan Content Change Monitoring. ESDS BLOG |. https://www.esds.co.in/blog/monitor-your-website-defacement-attacks-with-esds-vtmscan-content-change-monitoring/#sthash.mDJsH646.dpbs

Joelle, M. M., & Park, Y.-H. (2018). Strategies for detecting and mitigating DDoS attacks in SDN: a survey. Journal of Intelligent and Fuzzy Systems, 35(6), 5913–5925. https://doi.org/10.3233/JIFS-169833

Johnson, L. R. (2014). Computer incident response and forensics team management: Conducting a successful incident response. Syngress

Kelly, M. (2020, April 14). *4 Phases of Disaster Management Explained (the Easy Way)*. BlackText-FullColor. https://home.akitabox.com/blog/4-phases-of-disaster-management

King, T., & Moore, B. (2018, May 9). University of New England Incident Response Plan 2018. Dixon Library IRP. https://www.une.edu.au/\_\_data/assets/pdf\_file/0003/286473/2018-Dixon-Library-IRP.pdf

Kirsten. (2020). Cross Site Scripting (XSS) | OWASP. Owasp.org. https://owasp.org/www-community/attacks/xss/

Kral, P. (2012, February 21). Incident Handler's Handbook. SANS Institute. https://www.sans.org/white-papers/33901

Kurniawan, A., Riadi, I., & Luthfi, A. (2017, April). (PDF) Forensic Analysis and Prevent of Cross Site Scripting in Single Victim Attack Using Open Web Application Security Project (OWASP) Framework. ResearchGate. https://www.researchgate.net/publication/315756005\_Forensic\_Analysis\_and\_Prevent\_of\_Cross\_Site\_Scripting\_in\_Single\_Victim\_Attack\_Using\_Open\_Web\_Application\_Security\_Project\_OWASP\_Framework

Library Mission, Vision, and Values. (2019). Library Mission | Wilmington University. https://www.wilmu.edu/library/mission.aspx

Lyon, B. (2017, September 21). Attackers are thinking about your application layer Security. are you? Forbes. https://www.forbes.com/sites/neustar/2017/09/21/attackers-are-thinking-about-your-application-layer-security-are-you/?sh=43bee66c4066

Mao, B., & Bagolibe, K. D. (2019, October). A Contribution to Detect and Prevent Website Defacement (No. 19232331). IEEE, https://doi.org/10.1109/CW.2019.00062

MIT Business Continuity Plan. (1995). MIT Recovery Plan Master. http://web.mit.edu/security/www/pubplan.htm

MITRE ATT&CK. (2019). *Defacement, Technique T1491 - Enterprise | MITRE ATT&CK®*. (2019). Mitre.org. https://attack.mitre.org/techniques/T1491/

MITRE ATT&CK. (2018) *Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK*. Mitre.org. https://attack.mitre.org/techniques/T1190/

MITRE ATT&CK, (2019). *Network Denial of Service, Technique T1498 - Enterprise | MITRE ATT&CK*. Mitre.org. https://attack.mitre.org/techniques/T1498/

Mölsä, Jarmo. (2005). Mitigating denial of service attacks: a tutorial. Journal of Computer Security, 13(6), 807–837

Nalawade, A., & Bharne, S., & Mane, V. (2016). September 1. Forensic analysis and evidence collection for web browser activity. IEEE Conference Publication | IEEE Xplore. https://ieeexplore.ieee.org/document/7877639

Nidecki, T. (2019, October 22). How To Build a Cyber Incident Response Plan. Acunetix. https://www.acunetix.com/blog/web-security-zone/cyber-incident-response-plan/

Novak, M., Grier, J., Gonzales, D. (2018, October 7).

*New Approaches to Digital Evidence Acquisition and Analysis*. National Institute of Justice. https://nij.ojp.gov/topics/articles/new-approaches-digital-evidence-acquisition-and-analysis

Orans, L. (2017, August 28). 3 ways to defeat DDoS attacks. Forbes. https://www.forbes.com/sites/gartnergroup/2017/08/28/3-ways-to-defeat-ddos-attacks/?sh=43750e27da78

Overill, R. E. (2013). Digital Forensonomics -- the Economics of Digital Forensics. The Pennsylvania State University. https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.307.5356&rep=rep1&type=pdf

Pandya, G. (2015, October 31). Preparing to withstand a DDoS Attack. Egnyte. https://sansorg.egnyte.com/dl/OzcvT28KCw

PortSwigger. (2019). What is cross-site scripting (XSS) and how to prevent it? Portswigger.net. https://portswigger.net/web-security/cross-site-scripting

Ready.gov (2021). *Business Impact Analysis | Ready.gov*. Ready.gov. https://www.ready.gov/business-impact-analysis

Rezaei Soufi, H., Torabi, S. A., & Sahebjamnia, N. (2019). Developing a novel quantitative framework for Incident Response Planning. International Journal of Production Research, 57(3), 779–800. https://doi.org/10.1080/00207543.2018.1483586

Sher-Jan, M. (2012, October 4). *7 best practices for a successful incident response plan*. Healthcare IT News. https://www.healthcareitnews.com/news/7-best-practices-successful-incident-response-plan

SWDGE. (2016, February 8). *SWGDE Best Practices for Collection of Damaged Mobile Devices*. Scientific Working Group on Digital Evidence. https://www.irisinvestigations.com/wp-content/uploads/2019/05/SWGDE-Best-Practices-for-Collection-of-Damaged-Mobile-Devices-020816.pdf

Thiruvaazhi, U., & Alex, E. (2012). A Forensic Mechanism to Trace the Master of Distributed Denial-of-Service Attack. ResearchGate. https://www.researchgate.net/publication/254307606\_A\_Forensic\_Mechanism\_to\_Trace\_the\_Master\_of\_Distributed\_Denial-of-Service\_Attack

Wasef, A., & Fitri, Z. (2016). Cross Site Scripting: Detection Approaches in Web Application. International Journal of Advanced Computer Science and Applications, 7(10). https://doi.org/10.14569/ijacsa.2016.071021

Weber, J. (2019, February 19). *What Is Business Impact Analysis & Why Is It Important?* ProjectManager.com. https://www.projectmanager.com/blog/business-impact-analysis

Woerner, R. (2017). *The real information security risk equation*. SearchSecurity; TechTarget. https://searchsecurity.techtarget.com/magazineContent/The-real-information-security-risk-equation

Zbrog, M. (2019). *Mobile & Digital Forensics: How Do Experts Extract Data from Phones?* Forensics Colleges. https://www.forensicscolleges.com/blog/guide-to-mobile-forensics