Cybersecurity Incident Response Procedure

This procedure document:

1. Groups threats into one of four defined threat-levels.
2. Establishes responsibilities for cybersecurity incident response.
3. Provides action steps for users who may be targets or victims of these attacks.
4. Guides those who must report, identify, investigate, and respond to these threats.

Cyberattacks are often unexpected and can suddenly become a very high priority, regardless of the day or time they are discovered or when they are ultimately resolved and mitigated. Generally, early identification and prompt action in response to these attacks is the most effective measure available.

Like criminals who steal physical items, cyber criminals often succeed by gradually elevating the severity of their attacks. A criminal who wants to break into your house may begin by simply monitoring your house and the activity around it. A next step might be for them to surreptitiously make attempts to gain access by checking for unlocked doors and unlocked windows, maybe even late at night or when no one is expected to be home. An even more invasive step might be to access that unlocked window or door to gain access. A final step might involve stealing your keys to the house so they can eat the food in your fridge, read your diary, and take your valuables.

A cyber-criminal follows this same pattern and uses each cyber-attack is an attempt to gradually gain more information and access so they can commit progressively more harmful and damaging acts. The goal is often some financial reward (*transfers of money, access to bank accounts, etc.*) but the goal can also be to simply cause harm and disruption.

To effectively defend against and respond to these attacks, every user must understand these risks as well as the best response to them. Those charged with assisting users with these threats (IT support staff) need pre-defined tasks to complete so that a prompt and efficient response can be implemented when needed. These procedures establish clear responsibility and define threat-level groups, while also providing detailed actions for targeted users, support staff, and senior administrators involved with cybersecurity incident response. While these detailed procedures focus specifically on phishing attacks, an effective cybersecurity response procedure must be adaptable to a broad range of threat tactics and techniques, as can be found in up-to-date online knowledgebases (MITRE ATT&CK, n.d.).

This procedure categorizes threats using **four levels** to define their severity. **Threat Level 1** is the **least severe** threat and **Threat Level 4** is the **most severe**. All threats require prompt action and are considered very high priority issues to resolve. Each targeted user plays a critical role in the overall effectiveness of the response to each threat. Our IT support staff plays a critical role too, by documenting the details of each incident, communicating throughout the incident, and assisting in the resolution of each incident.

All threats require prompt action and are considered very high priority issues to resolve. Targeted users play a critical role in the overall effectiveness of the response to each threat by promptly reporting issues. The IT support staff plays a critical role too, by promptly documenting the details of each incident, communicating throughout the incident, and assisting in the resolution of each incident. Senior management is also responsible and accountable for ensuring that procedures are

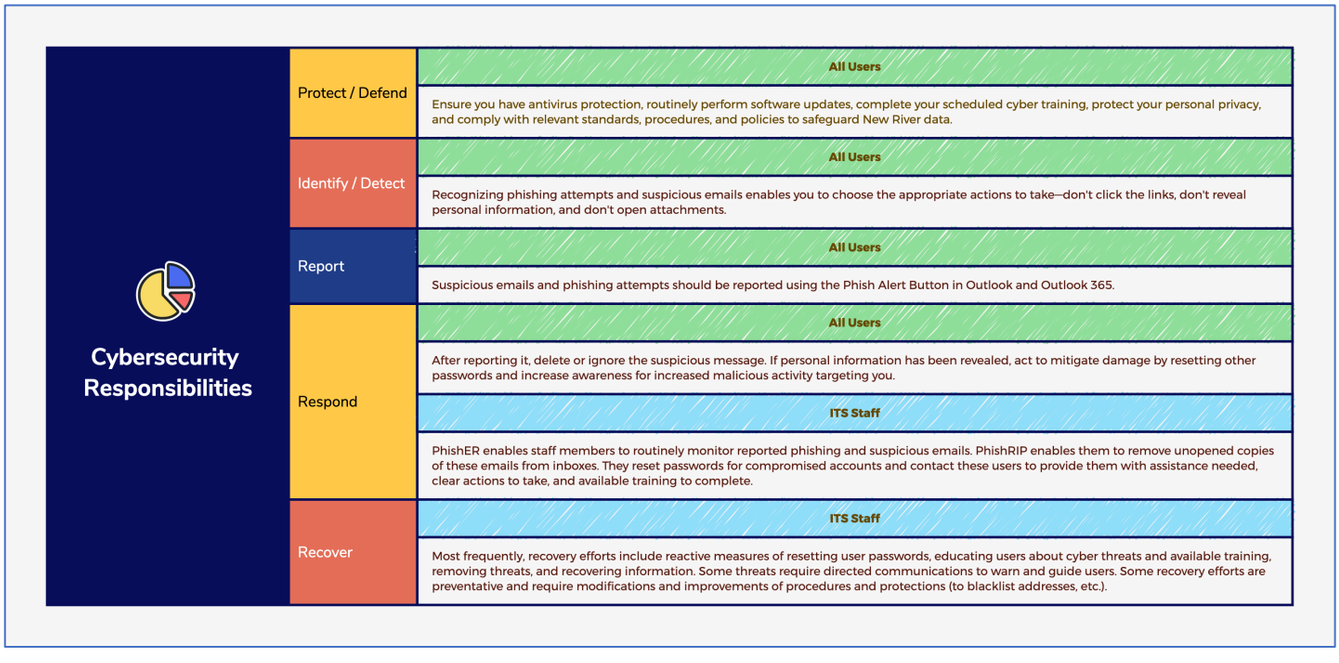
followed to effectively report and respond to these incidents. Not all incidents can be resolved internally though, since the most severe threats must be reported to external agencies.

Threat Level	**Threat Example**
Threat Level 1	*A targeted user receives a phishing email.*
Threat Level 2	*A targeted user receives a phishing email and accidentally clicks the link (or replies to the message) and **reveals personal information** (perhaps even a password).*
Threat Level 3	*A targeted user receives a phishing email with an attachment (or hyperlink) and accidentally downloads the attachment (or clicks the link) that **may contain a virus or malware**.*
Threat Level 4*	*A targeted user is infected with **ransomware** or suspects their **identity has been stolen**.*

This RACI matrix identifies who is **R**esponsible, **A**ccountable, **C**onsulted, and **I**nformed for the given general tasks associated with incident response:

RACI Matrix of Responsibilities for Incident Response					
Tasks	*CIO – Ayersman*	*CISO – Davis*	*CTO – Garris*	*CEO - Copenhaver*	*All Users*
Incident Reporting	I	I	I	-	R
Incident Identification and Logging	I	A	A	-	I
Investigation	A	R	R	-	C
Diagnosis and Response	A	R	R	I	I
Resolution and Recovery	A	R	R	I	I
External Reporting	R	C	C	C	-

The following table summarizes the responsibilities at each crucial level of cyber defense:



THREAT LEVEL 1

A targeted user receives a phishing email.

Explanation
Phishing emails are identified by multiple criteria that may include:

1. You weren't expecting the email about this topic from this user.
2. The message contains oddly worded content, phrases, or errors.
3. There is urgency to the message, and it is asking you to quickly act.
4. You don't recognize the sender, or the message doesn't include a valid signature identifying the sender.
5. Mousing over links in the message (*without clicking them*) reveals suspicious URLs.

The purpose of phishing emails is for bad actors to obtain personal information from targeted users. There is no inherent threat posed by a phishing email **if the targeted user takes no action that reveals personal information** (like clicking a link or filling out a form or replying to the email and providing information that has been requested).

User — Actions to Take

1. **Report** the phishing email to IT by using the **Phish Alert Button** (or by forwarding a copy to an IT staff member).
2. **Delete** the message (without clicking any links, downloading any attachments, or replying to the sender and providing them with any personal information).

Actions Explained
All phishing emails should be reported (using the **Phish Alert Button** in Outlook is the preferred method). Once reported, the targeted user can safely delete the message (since reporting it has provided IT a copy to be used for analysis). If the targeted user receives and reports a phishing email (*and doesn't click the links, download the attachments, or reply to the email to expose personal data*) then there is no need to change passwords or scan your computer for viruses and malware, but there is certainly **no harm** in taking these precautions and **we recommend you do**.

*This is like having a stranger knocking on your door or window and you act quickly to **make sure your doors and windows are locked**.*

Help Desk Technician — Actions to Take

1. **Locate** and identify the reported phishing attempt in the **PhishER** interface of **KnowBe4**.
2. **Search** for copies of the message using criteria that match the (a) subject of the message, (b) the sender, and (c) perhaps even the body of the message.
3. **Remove** these messages out of inboxes by using the **PhishRIP** solution which moves these messages to a Quarantine folder for each user.

Actions Explained
When a phishing email is not successful (*the phishing victim has not revealed any personal information*) very little harm is done, but the message may be only one of many that New River users are receiving. If we don't act quickly, one of those other copies of the phishing email may result in more victims and a much bigger problem.

THREAT LEVEL 2

A targeted user receives a phishing email and accidentally clicks the link (or replies to the message) and ***reveals personal information*** *(perhaps even a password).*

Explanation
Links in phishing emails may take you to a fake login page where you provide your own credentials to the bad actor, or they may link to a script that contains a virus, malware, or ransomware. Attachments included with phishing emails may contain executable files that contain viruses, malware, or ransomware. Replying to a phishing email may inform the bad actor that your account is active, and you may reveal additional information that can cause you future harm.

By phishing, bad actors can obtain enough information to access the accounts of phishing victims so they can retrieve more personal information or impersonate the victim as they engage in progressively more threatening activities (*including financial transactions*).

User — Actions to Take

1. **Report** the phishing email to IT by using the **Phish Alert Button** (or by forwarding a copy to an IT staff member and explaining that you clicked the link, replied to the message, or downloaded the attachment).
2. **Delete** the message.
3. **Change** your password.
4. **Increase** your awareness for additional phishing emails that you may soon receive (they know you are active now).

Actions Explained
Remember, receiving a phishing email is harmless until you are tricked into acting inappropriately. You should:

1. **Never** click links in suspicious emails.
2. **Never** open attachments included with suspicious emails.
3. **Never** reply to suspicious emails.

This is like having a stranger knocking on your window or door and you ***open*** *the door or window for them.*

Help Desk Technician — Actions to Take

1. **Login** using the phishing victim's username and by trying the default password we assign (N + ID +r). If that password gains you access, it should be **changed** as it may be compromised. If that login fails, then login to the AD and **change** the user's password (to the default) and then login as that user.
2. **Check** Outlook for any malicious Rules and if found, delete them.
3. **Report** the message using the Phish Alert Button (if it hasn't already been reported). You may also delete the Sent or Received messages relevant to this phishing attack from the phishing victim's Inbox and Sent items folders.
4. **Logout** of the phishing victim's account.
5. A KnowBe4 Administrator (CISO or CIO) will receive the PAB notification and will use the information to create a **PhishRIP** script to quarantine any emails matching those criteria

(*before more users can open them*).

6. **Remove** any restrictions that might have been created by **Microsoft 365 Defender**. If the phishing victim's account has been restricted by **Microsoft 365 Defender** for sending too many emails, then an Administrator must remove that restriction.
7. **Contact** the phishing victim by phone to inform and educate them about the incident and provide them their new default password.

Actions Explained
When a phishing email is successful, the phishing victim has revealed some personal information. Often, this includes the phishing victim's own username and password (*if the link takes the phishing victim to a fake login page to collect the information*).

Microsoft 365 Defender alerts are triggered if a user sends too many emails in a short amount of time. The CISO receives these alerts as emails and SMS messages to his phone. He's able to then gather information about the issue to help resolve it.

Malicious Outlook rules are created using traditional email phishing methods. The targeted user receives an email appearing to be from an existing contact or an organization known to them. A link in the phishing email takes the targeted user to a fake Office 365 login page where the targeted user enters credentials. Once provided, the bad actor can log in as the targeted user with the credentials provided by the targeted user (*who is now a phishing victim*). The bad actor then creates a Rule in the victim's Outlook to generate more phishing emails, hoping to create more victims.

> **How to Detect and Remediate Outlook Rules and Custom Forms Injections Attacks**
> https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/detect-and-remediate-outlook-rules-forms-attack?view=o365-worldwide

THREAT LEVEL 3

*A targeted user receives a phishing email with an attachment (or hyperlink) and accidentally downloads the attachment (or clicks the link) that **may contain a virus or malware**.*

Explanation
Malicious emails may deliver a payload in the form of (1) an attachment or (2) a hyperlink in the message. Either method requires the targeted user to act by clicking the link or opening the attachment. If the targeted user takes no action or simply reports the message (using the **PAB**) and then deletes the message, the payload is typically not delivered. Payloads may contain a virus, malware, or ransomware. Any of these may be severely debilitating and may pose a threat beyond the targeted user to include others who share (or have shared) information with the targeted user. Once the targeted user is compromised, then the emails, address book, files, and other information available to that user are likely to also be compromised.

User — Actions to Take

1. **Report** the phishing email to IT by using the **Phish Alert Button** (or by forwarding a copy to an IT staff member and explaining that you opened the attachment).
2. **Delete** the message.
3. **Change** your password.
4. **Scan** your computer for viruses and malware.

5. **Increase** your awareness for additional phishing emails that you may soon receive (they know you are active now).

Actions Explained
Remember, receiving a phishing email is harmless until you are tricked into acting inappropriately. You should:

1. **Never** click links in suspicious emails.
2. **Never** open attachments included with suspicious emails.
3. **Never** reply to suspicious emails.

*This is like having a stranger knocking on your window or door and you (1) **open the door** or window for them and (2) **invite them in**.*

Help Desk Technician — Actions to Take

1. **Confirm** the user has **scanned** for viruses and malware using current antivirus definitions and assist them with **changing their password**.
2. **Verify** the user has no **malicious rules** in Outlook (these do not appear in antivirus scans).
3. **Report** this incident to WVHEPC within 30 days (*to be done by the CIO and CISO*).

Actions Explained
If the phishing email convincingly appears to be from a New River email address, then we should reset the password for that account too (just in case it has been hacked), then contact the account holder to inform them of the password change. Resetting a user's password won't prevent spoofing, but it will prevent a bad actor who has hacked into the targeted user's account from further access.

1. **Spoofing** simply means a bad actor is impersonating the New River account holder and is pretending to be them. This is usually a precursor to phishing, once you trust them, they trick you. There isn't much a user or a Help Desk Technician can do to prevent spoofing.
2. **Hacking** means the bad actor has gained access to a New River account and is now able to act on behalf of the New River user.

THREAT LEVEL 4

*A targeted user is infected with **ransomware** or suspects their **identity has been stolen**.*

Explanation
In either of these two situations, the targeted user (phishing victim) is no longer in control of their own information and someone else is. Ransomware is malicious software (malware) that prevents you from accessing your computer files and demands you pay a ransom to regain access. You can unknowingly download ransomware by opening an email attachment or by clicking a malicious link on a web page (or in an email). You may not even know you are infected until you receive a message demanding a ransom payment.

User — Actions to Take

1. **Report** the incident to IT by phone.
2. **Report** ransomware to the FBI (*the CIO and CISO can help you with this*).

3. **Report** identity theft to the Federal Trade Commission (FTC) (*the CIO and CISO can help you with this*).

Actions Explained
Once ransomware has infected your computer it is unlikely your files can ever be recovered. New River follows state and federal guidelines to never pay the ransom, as this is not a guarantee of the files being restored and incentivizes further ransomware attacks. Instead, we reformat the computer to eliminate the ransomware. If the victim has copies of files in the Cloud (OneDrive, Dropbox, Google Drive, etc.), it may be possible to recover these files and IT can assist with this effort.

*Unfortunately, ransomware and identity theft are like having a stranger knocking on your window or door and you (1) **open the door** or window for them, (2) **invite them in**, and (3) **give them the keys** to the house (relinquishing control to them).*

Warning Signs of Identity Theft
- Credit card charges for items you didn't purchase.
- Debt collection notices for accounts you didn't open.
- Denials for loan applications you didn't apply for.

Help Desk Technician — Actions to Take

For a computer infected with ransomware, take these actions (*listed in order of importance*):

1. **Disconnect** the infected computer from the network (*ethernet*) or by powering it off (*wireless*).
2. **Reset** the victim's password in the AD.
3. **Collect** relevant information in a trouble ticket to describe the incident and to aid others (*law enforcement*) in understanding the issue.
4. **Assist** the user with reporting ransomware to the FBI and identity theft to the FTC (*guide them to the reporting information in Appendix A and the CIO and CISO will assist them with the reporting*).
5. **Report** this incident to WVHEPC within 30 days (*to be done by the CIO and CISO*).

Actions Explained
By disconnecting the computer from the network, you deny the bad actor any further control of that device and you reduce the risk to other devices on the same network. By resetting the victim's password, you deny the bad actor any further access to that account. Further actions should focus on documenting the issue so that it can be officially reported.

REFERENCES

MITRE ATT&CK. (n.d.). *MITRE ATT&CK®*. Retrieved March 26, 2022, from https://attack.mitre.org/

APPENDIX A — REPORTING RANSOMWARE AND IDENTITY THEFT

Threat Level 3 and Threat Level 4
Incidents **must** be reported to **WVHEPC** using the 7-page **Cybersecurity Incident Response Form** within 30 days of the occurrence. The CIO and CISO will submit this report using the information collected by the Help Desk.

WVHEPC Cybersecurity Incident Response Form
https://web.newriver.edu/procedures/Post-Cyber-Incident-Response-Form-Blank.docx

Threat Level 4
Incidents must also be reported to the FBI or the FTC.

Ransomware — Federal Bureau of Investigations
https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware

Identity Theft — Federal Trade Commission
https://www.usa.gov/identity-theft