BC HOUSING
Housing Provider Technology Support

Cyber Attack Incident Report Guidesheet

Detecting and dealing with a Cyber Attack is not only overwhelming for your society but can also take a significant toll on the person responsible in your organization for incident command. The first question will be "what do I do?", and there can be a tendency to panic.

This guide sheet has been created by the Housing Provider Technology Support team @ BC Housing to assist your organization through responding to an attack. If you already have an incident response plan in place, you are ahead the game and can utilize this guide sheet as a supplement.

Who Should I Inform?

It is important that the correct people are informed of the attack when it first happens. Relaying information beyond the list below does not need to take place immediately:

Who to Contact First

1. Your IT Department or IT Service Provider
2. Funder Relationship Managers (eg. BC Housing, AHMA, Health Authority)
3. BC Housing Tech Support Team - hptechbc@bchousing.org
4. OIPC if you have determined there has been a privacy breach

Once you have ascertained the parties that have been affected, they will also need to be informed utilizing your society's Privacy Breach process.

What Are Some Important Questions When Starting Your Incident Response?

Before started to respond to the Cyber Attack there are some important questions that should be answered:

Important Questions

1. **When** did the event happen?
2. **How** was it discovered and **Who** discovered it?
3. **What** is the scope of the compromise?
4. Do you know the **source/point of entry** of the attack?
5. **What** types of data have been encrypted, stolen or destroyed?

How Do I Know If We Are Engaging in the Right Process?

Formality is important when responding to a cyber attack. If your IT department or IT Service Provider are having difficulties, or would like verification that you are going down the right path, BC Housing can help:

BC HOUSING
Housing Provider Technology Support

Housing Provider Technology Support Resources @ BC Housing

- Advice from qualified IT Security professionals in incident repsonse
- Recommendations of 3rd party professional services for deeper assitance through an attack

What Are the Steps for Incident Response?

Below is a suggested incident response cycle based on best practices from the SANS Institute, one of the recognized world-wide leaders in security education and certification.

PICERL

Preparation > Identification > Containment > Eradication > Recovery > Lessons Learned

Prepare - Incident Response Plan

- If you have an Incident Response or Business Continuity Plan, initiate those.
- If you do not have these plans generated please reach out to the Housing Provider Technology Support team @ BC Housing and follow PICERL guidelines

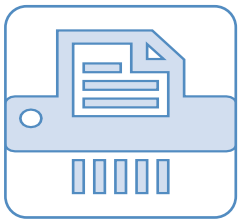
Identify

- Disconnect the affected networks/workstations from the current system
- Inform your Funder Relationship Managers and the Housing Provider Technology Support Team @ BC Housing
- Document the **important questions** - who/what/where/when/how?
- Gather and perserve information from various sources (log files, error messages)

Contain

- Identify and contain the issue using an antivirus program.
- Remove any accounts/programs left on the system by the cybercriminal.
- Ensure steps are being taken to contain the breach short term and long term.

BC HOUSING
Housing Provider Technology Support

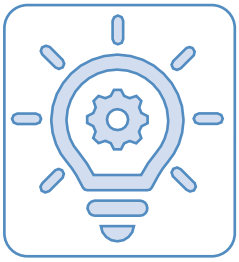


Eradicate

- Eliminate the root cause that lead to the breach.
- A malware removal tool like Malwarebytes might be needed to clear our the infestation.

Recover

- Complete steps above **BEFORE** entering the recovery stage.
- Determine if you have a trusted backup to restore from.
- Test, monitor and validate the system that is brought back into production.
- Change passwords that are recorded on the system - including any personal ones



Lessons Learned

- Document the incident as best as possible.
- Are you prepared for a future event?
- Do you have an incident response plan created?
- Do your employees/organization need further cyber security training?

The Housing Provider Technology Support team is available to help with Cyber-Security Awareness training and general Cyber-Security advice.