UBC Incident Response Plan

Contents

1. Rationale

Centralised notification and control of security incident investigation is necessary to ensure that immediate attention and appropriate resources are applied to control, eliminate and determine the root cause of events that could potentially disrupt the operation of the university or compromise university data.

2. Objective

The goal of this plan is to:

- Identify accountability for responding to computer security incidents
- Ensure appropriate escalation
- Ensure effective administrative response to computer security incidents
- Streamline the response process
- Secure and protect data in order to minimise the organisational impact of a computer security incident

3. Application

This plan applies to computer security incidents that affect UBC's information technology facilities, infrastructure or data assets, including but not limited to servers, workstations, firewalls, routers, and switches.

4. Definitions

A computer security incident, for the purposes of this plan, includes events where there is suspicion that:

- Confidentiality, integrity or accessibility of UBC data has been compromised
- Computer systems or infrastructure has been attacked or is vulnerable to attack

4.1 Types of Incidents

Security incident types include but are not limited to:

- *Malicious code attacks* - attacks by programs such as viruses, trojan horse programs, worms, rootkits, and scripts to gain privileges, capture passwords, and/or modify audit logs to hide unauthorised activity.

- *Unauthorised access* - includes unauthorised users logging into a legitimate account, unauthorised access to files and directories, unauthorised operation of “sniffer” devices or rouge wireless access points.

- *Disruption of services* - includes erasing of programs or data, mail spamming, denial of service attacks or altering system functionality.

- *Misuse* - involves the utilization of computer resources for other than official purposes.

- *Espionage* - stealing information to subvert the interests of a corporation or government entity.

- *Hoaxes* - generally an e-mail warning of a nonexistent virus.

- *Unusual Events* – includes erratic and persistent unusual system behaviour on desktops, servers or the UBC network. Inexplicable lock out of user accounts or the existence of a strange process running and accumulating a lot of CPU time.

4.2 Incident Severity

Incidents will be classified by the CSIRT Coordinator based on the perceived impact on university resources:

- *Minor* -incidents for which there are routine solutions. Sensitive information has not been exposed or accessed by unauthorised parties.

- *Medium* - incidents that do not have routine solutions but are limited in scope and consequences.

- *Severe* - incidents that involve significant personal data leakage, compromised institutional data, or that impacts a significant number of users, all of which has significant consequences

4.3 Information Security Unit

The Information Security Unit led by the Information Security Officer (ISO), reports to the Chief Information Officer (CIO), and has responsibility for the IT security infrastructure on campus.

4.4 CSIRT Coordinator

The CSIRT Coordinator is part of the Information Security Unit, and is charged with managing an incident.

4.5 Computer Security Incident Response Team (CSIRT)

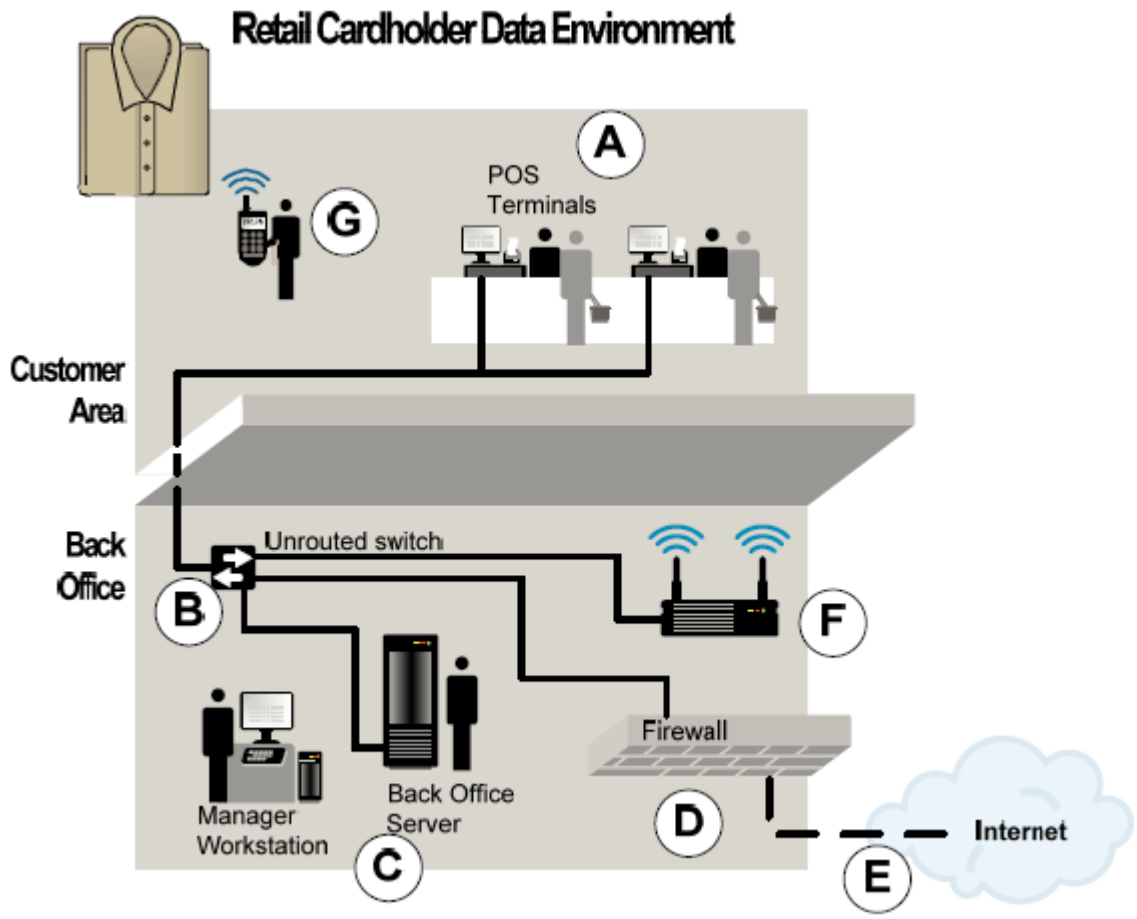
A CSIRT is assembled by the ISO, and is drawn as appropriate, from the following groups (or their delegates):

- Enrolment Services

- Human Resources
- Finance
- Campus Security
- University Counsel
- Public Affairs
- Internal Audit
- Research

4.6 Cardholder Data Environment (CDE)

A CDE is defined as the computer environment wherein cardholder data is transferred, processed, or stored, and any networks or devices directly connected to that environment.



5. Reporting a Computer Security Incident

All suspected computer security incidents must be reported immediately to UBC IT via the IT Service Centre (ITSC) at 604-822-2008.

Members of the university community must report a suspected computer security incident according to normal practice within their unit. This could be to their supervisor, to the IT service team for their unit or directly to the ITSC.

Where the computer security incident involves physical security issues in addition to computer security issues the incident must be reported to Campus Security who will in turn alert the ITSC.

6. Managing the Security Incident

6.1 All Incidents

Information Security will:

- Create an incident file
- Assign a CSIRT Coordinator
- Identify the scope and type of problem, including classification as minor, medium or severe
- Notify appropriate organizations internal and external to UBC (including relevant police agencies)
- Take corrective action as described in the guidelines for securing and preserving electronic evidence
- Report, as needed, to the appropriate UBC department for further action or discipline
- Close the incident file

6.2 Medium and Severe Incidents

Information Security Officer (ISO) will:

- Form a CSIRT to include the relevant owner(s) of the data or issue

CSIRT Coordinator will:

- Provide regular briefings to the CSIRT by e-mail at least once a day and more often at the outset - even if there has been “no change”

- Write a closing incident report that is shared with the CSIRT

6.3 Severe Incidents

Information Security Officer (ISO) will:

- Escalate the incident to the CIO

The CIO will:

- Brief the Provost and any other relevant senior UBC executives
- Receive regular reports on risks from the CSIRT and communicate them to the Provost and any other relevant senior UBC executives
- Ensure risk is managed in consultation with the Provost and any other relevant senior UBC executives
- Activate UBC's Disaster Response Plan (DRP) if the situation requires, based on the impact on persons, property, and the environment.
- Provide a closing incident report to the Provost and the other senior UBC executives that assisted in the management of the incident

7. Closing the Incident

A closing incident report shall be prepared by the CSIRT Coordinator for medium and severe incidents. The report shall include:

- Chronology of the incident and actions taken
- Scope of risk the university faced during the incident e.g. number of records, degree of exposure
- Description of action taken to mitigate and resolve the issue
- Communications that were taken
- Brief explanation of basis for key decisions
- Evaluation of whether response plan was followed
- Identification of internal improvements to infrastructure, systems, the incident response plan, and any other actions that are recommended

8. Managing Rogue Access Points

A centrally monitored system is used to continually detect unauthorised/rogue wireless devices within the university network. If a rogue access point is detected within 50 meters of a CDE an alert is generated and the applicable merchant(s) are contacted to investigate and if appropriate remove the wireless device.

9. Summary of Incident Response Plan