UBC Incident Response Plan V2.0

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, merchant systems, firewalls, routers, and switches.

4. Reporting a Computer Security Incident

All suspected computer security incidents must be reported immediately to UBC IT via the IT Service Centre (ITSC) at security@ubc.ca or 604-822-6141.

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.

5. Managing the Security Incident

5.1. All Incidents

The ITSC will:

- Create an incident file
- Escalate to the CSIRT Coordinator

The CSIRT Coordinator will:

- Coordinate the incident with the ITSC staff and/or any other relevant personnel
- Escalate as required to SCOR and/or the Associate Director of Information Security Management (AD ISM)
- Ensure that relevant information is captured in the incident file; regardless of the technical resources assigned to "work" the incident. These resources may include SCOR, the ITSC, University IT Support Staff or other personnel as required
- Close the incident file

SCOR will:

- Investigate to determine if a breach has occurred:
  - Until confirmed it is to be classified as an incident; and
  - If a breach is confirmed, then declare the severity of the breach.
- 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 Securing and Preserving Electronic Evidence guideline
- Report, as needed, to the appropriate UBC department for further action; in some cases this may include discipline. Note: The type of information involved may dictate mandatory reporting requirements

5.2. Medium and Severe Incidents

This section covers additional procedures for incidents classified as "Medium" or "Severe", which must be followed in addition to the procedures for "All Incidents".

The AD ISM will:

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

The 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

5.3. *Severe Incidents*

This section covers additional procedures for incidents classified as “Severe”, which must be followed in addition to the procedures for “Medium and Severe Incidents”.

The AD ISM will:

- Escalate the incident to the CIO
- Ensure that the CSIRT includes the CIO and the relevant owner(s) of the data or services affected

The CIO will:

- Brief the Provost and any other relevant UBC Executives
- Ensure risk is managed in consultation with the Provost and any other relevant 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 UBC Executives that assisted in the management of the incident

5.4. *Merchant Incident Handling Process*

This section covers additional procedures for Merchant (Payment Card Industry) incidents, which must be followed in addition to the procedures for “All Incidents”.

The ITSC will:

- Merchant incidents are any where the following examples of Merchant processing systems are included in the report:
  - PIN pad tampering
  - Rogue wireless access point detected
  - Any incident involving credit card processing such as Visa, Mastercard, Amex, etc.
  - Any incident where PCI or merchant processing are reported
  - Acquirer references such as TD, Chase, Moneris, Beanstream, etc.
  - Merchant website compromise
- Escalate the incident to the “Financial Analyst - UBC PCI Compliance” 604-822-0259; If no response from or if the Financial Analyst - UBC PCI Compliance is away, contact:
  - Manager, Revenue Accounting 604-822-6779
  - Director, Financial Reporting 604-822-3584

The Financial Analyst – UBC PCI Compliance will:

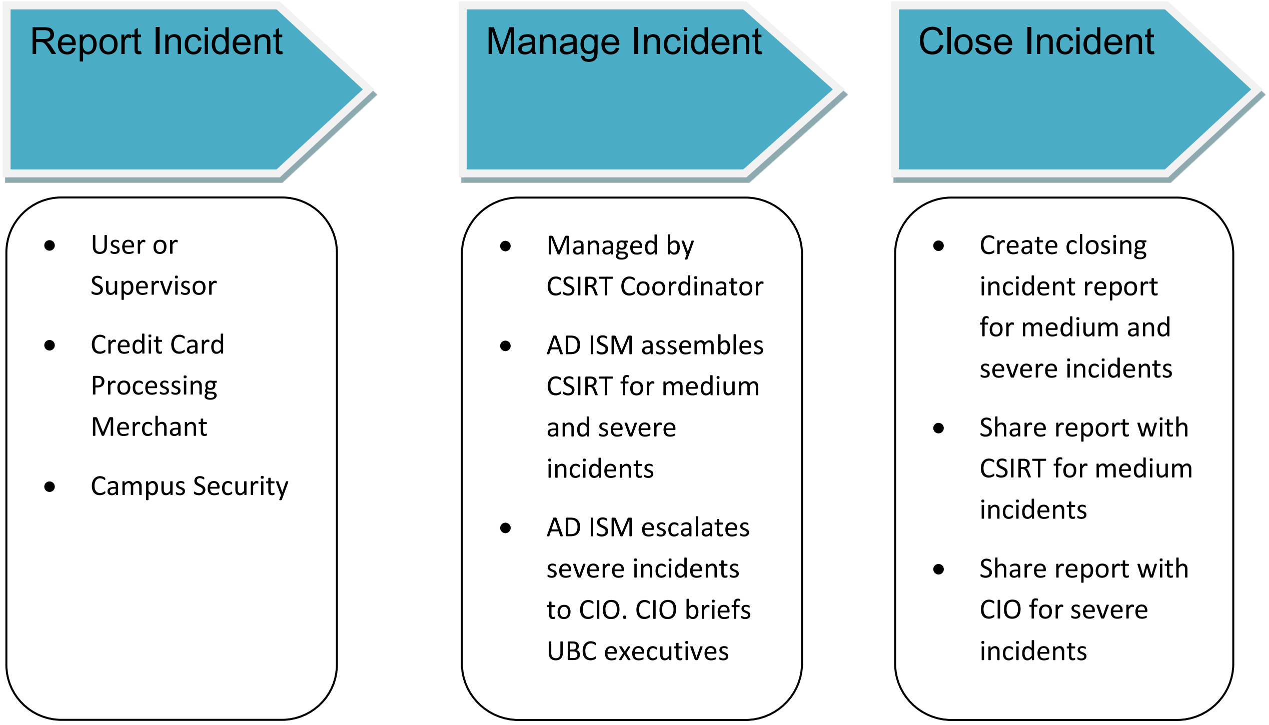
- Contact the merchant to coordinate the incident
- Coordinate with the CSIRT Coordinator
- Coordinate with PCI Working Committee as required
- Coordinate any contact with Acquirer/Card companies

6. 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

7. Summary of Incident Response Plan



Report Incident

- User or Supervisor
- Credit Card Processing Merchant
- Campus Security

Manage Incident

- Managed by CSIRT Coordinator
- AD ISM assembles CSIRT for medium and severe incidents
- AD ISM escalates severe incidents to CIO. CIO briefs UBC executives

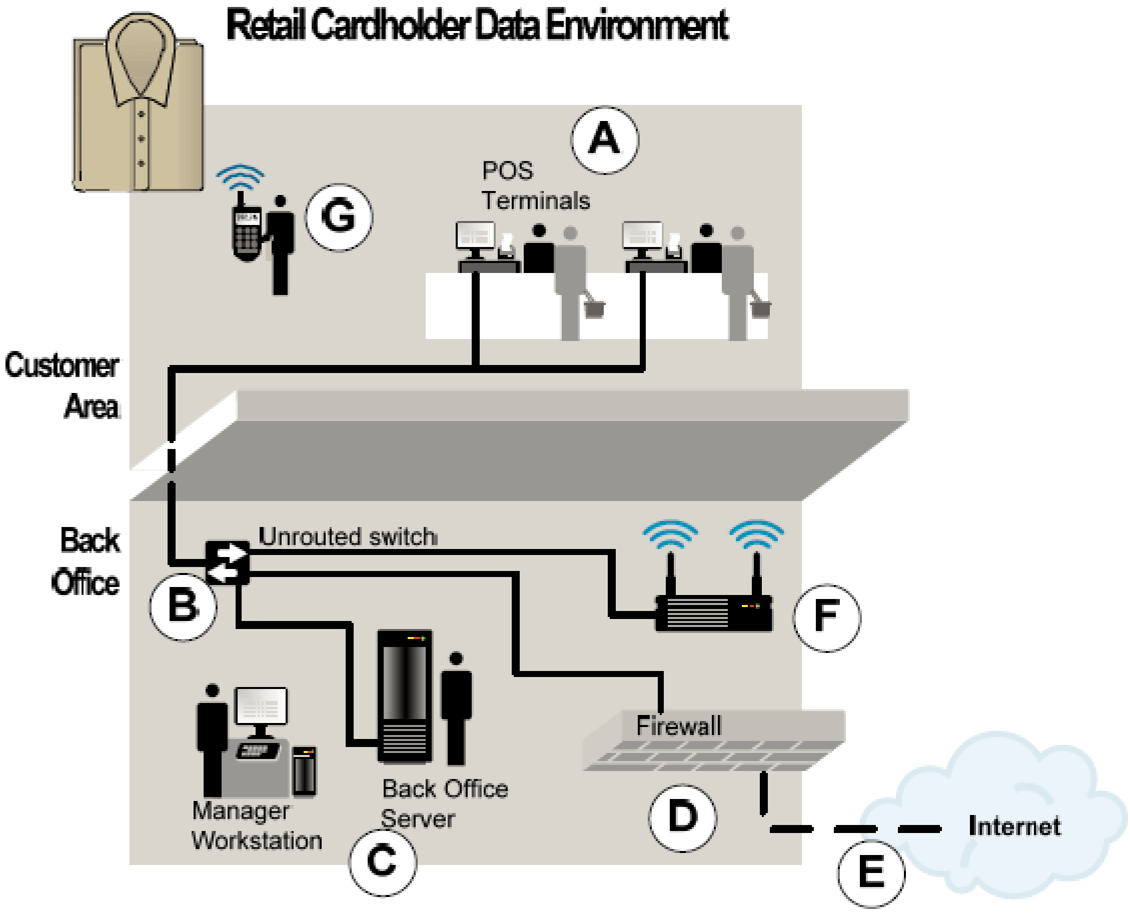
Close Incident

- Create closing incident report for medium and severe incidents
- Share report with CSIRT for medium incidents
- Share report with CIO for severe incidents

8. Glossary

9.1. *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.



9.2. *Computer Security Incident*

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

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

9.2.1. 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.

9.2.2. 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

9.3. *Computer Security Incident Response Team (CSIRT)*

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

- Campus Security
- Enrolment Services
- Finance
- Human Resources
- Information Technology
- Internal Audit

- Public Affairs
- Research
- Risk Management Services
- Treasury
- Unit/Department where incident occurred
- University Counsel

9.4. CSIRT Coordinator

The CSIRT Coordinator is the “Access and Identity Analyst”, who is part of the SCOR group, and is charged with managing an incident.

9.5. Merchant

Any University unit that accepts payment cards bearing the logos of any of the five members of the PCI-DSS (American Express, Discover, JCB, MasterCard or VISA).

9.6. Security Centre Operations Response (SCOR)

The SCOR group, led by the Associate Director of Information Security Management (AD ISM), reports to the Director of Infrastructure, and has responsibility for the IT security infrastructure on campus.

General Incident Response Outline:

1. IT: Verify that an incident has occurred
2. IT: Contain it to prevent further damages
3. IT: If there's the possibility that PI has been breached then activate the Privacy Breach Notification Process
4. IT: If there's a possibility that this incident involves merchant systems as they relate to the 5 brands (American Express, Discover, JCB, MasterCard or VISA) then follow the Merchant Incident Handling Process.
5. IT: If there's a possibility that this incident involves copyright infringement then follow the Copyright Infringement Handling Process.
6. IT: If there's a possibility that this incident may result in legal liability then consult with University Counsel via Chelsea Thompson.
7. IT: Identifies the vulnerability that led to the breach and closes it
    a. IT: if possible, also identify any other systems at UBC with the same vulnerability
    b. IT: where necessary, in consultation with communications, communicates the vulnerability information and remediation to affected parties
8. IT: identifies any Indicators of Compromise (IOCs) (e.g. IP addresses, web sites, ports, email addresses, etc.) and uses those to identify any other potentially compromised systems at UBC
9. IT: coordinates the restoration of service
10. IT: where valuable conducts a post-mortem
11. IT in consultation with the Affected Unit and other relevant units, such as UC and Public Affairs: files final report on the incident including recommendations to prevent a recurrence (if applicable)

Privacy Breach Notification Process (Activated When Incident Involves Potential Unauthorized Exposure/Alteration/Deletion of Personal Information(PI)):

1. IT: Gathers the following information and provides it to University Counsel (UC):
    a. Type of PI
    b. Amount of PI
    c. Relevant circumstances leading to potential unauthorized exposure/alteration/deletion

2. UC: Reviews information to determine whether notification is required in accordance with the BC Privacy Commissioner's Breach Notification Assessment Tool (https://www.ipc.on.ca/images/Resources/ipc-bc-breach-e.pdf) and Privacy Breaches: Tools and Resources (https://www.oipc.bc.ca/guidance-documents/1428). Notification of affected individuals and the Commissioner's Office is generally required where any of the following factors is present:
    a. Legislation requires notification
    b. Notification required to meet professional standards or certification standards
    c. Contractual obligation to notify
    d. Risk of identity theft
    e. Risk of physical harm
    f. Risk of hurt, humiliation, damage to reputation
    g. Risk of loss of business or employment opportunities

3. UC: Initial review is done by Paul Hancock in consultation with IT where further contextual information is required; this consultation may require the services of a forensics firm for either additional or independent analysis. If he believes that a privacy breach notification is required, then the matter is escalated to Hubert Lai for final determination.

4. UC: If notification is required, UC and UBC IT create a notification response team. For low severity breaches, this team will generally constitute only UC, UBC IT, and the affected unit. For higher severity breaches, the team will also include other support/stakeholder units including Public Affairs, Government Relations, the relevant Vice-President(s). The team will:
    a. Develop and approve communication plan for notification, web, press release, etc. – note that notification itself is generally delivered by the affected unit
    b. Determine supporting infrastructure (e.g. call centre, contact web page)
    c. Determine other supporting resources/compensation (e.g. credit monitoring, monetary compensation, specialized assistance)
    d. Assign spokesperson (if appropriate)
    e. Oversee notification process
    f. Assist with post-incident review as required

Copyright Infringement Handling Process:

1. IT: Copyright infringement (alleged) notice is received
2. IT: Is it possible to identify the individual who was using the IP address at the time of the allegation:
    a. Yes.
        i. IT: forwards the notice to the individual along with the letter provided by University Counsel, via Michal Jaworski, to the individual. Note: if the alleged infringer is an employee and the copyright material appears to be of the nature that the employee may have used the material for University Business then escalate the issue to the Library via Allan Bell; Allan will determine approach for engaging the employee.
        ii. IT: using a template provided by UC, IT notifies the party alleging the copyright infringement that the notice has been forwarded; IT does not provide any identifying information about the alleged infringer.
        iii. IT: keeps records relating to the incident for 6 months unless legal action is initiated; if legal action is initiated then records must be kept for 1 yr
    b. No.
        i. IT: using a template provided by UC, IT notifies the party alleging the copyright infringement that the notice could not be forwarded and provides reasoning as to why
        ii. IT: keeps records relating to the incident for 6 months unless legal action is initiated; if legal action is initiated then records must be kept for 1 yr
3. IT: if this incident requires additional legal advice, escalate to UC via Michal Jaworski. Possible reasons to escalate include: unusually formed notices of infringement, legal action being initiated, etc.