Western
UNIVERSITY · CANADA

Western Process Documentation

Cybersecurity Incident Response Plan (CSIRP)

Engagement of the Cybersecurity Incident Response Team (CSIRT)

Version 2.4 | February 2024

Table of Contents

Section 1: Plan Framework

The Cybersecurity Incident Response Plan (CSIRP) is part of an overall cybersecurity strategy for Western University but may stand as a separate component for the purposes of operational implementation.

The purpose of this document is to make explicit an incident response methodology and clearly articulate the decision accountabilities along the process path.

The fact is that Western University, like other institutions in Canada and around the globe, is a target-rich environment for malefactors to engage. It is not a matter of IF Western University is the victim of a substantial cyber incident but more of a matter of WHEN. The defenses put in place through operational technological hardening or direct resourcing can be undermined by the simplest of actions on the part of an unwitting (or otherwise) actor. Even the best processes can be overcome with enough energy and time.

The Western Cybersecurity strategy is based on the National Institute of Standards and Technology (NIST) 800-53 reference framework and is predicated on balancing institutional readiness (technological, resource-oriented) with cultural resiliency (awareness, training).

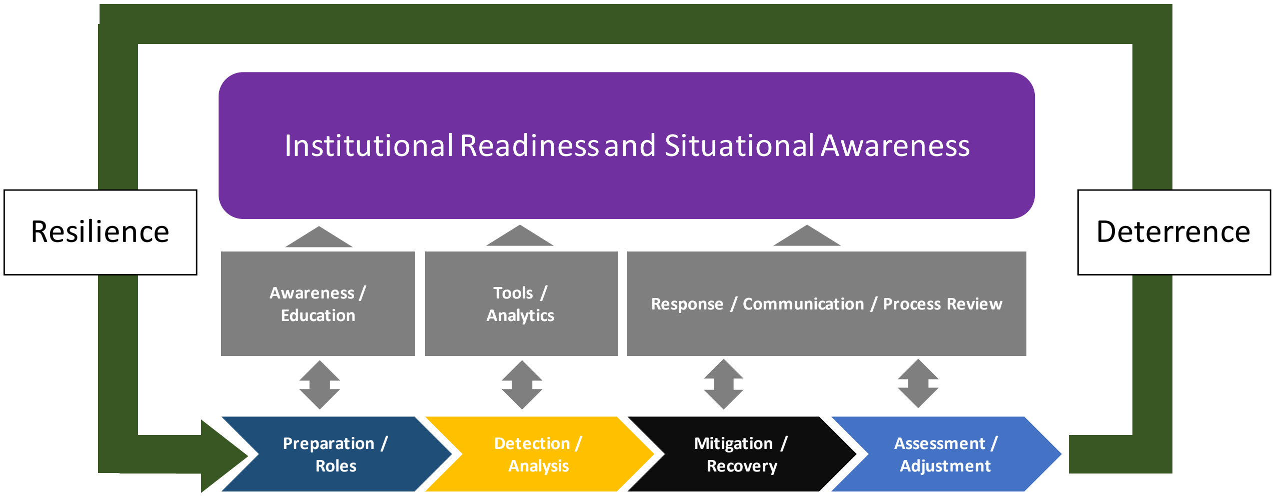


Figure 1: Western University Cyber Security Strategy

This strategic approach equips the Western community with the tools and thinking required to be resilient against occurrences. Further, the approach is built on an enabling mindset, allowing each of the institution's members to be responsible, responsive, and vigilant.

The NIST 800-53 standard allows for an iterative model whereby the constituent elements reinforce each other throughout a given sequence. Adapted for use within Western University, this framework is represented through the following diagram and is particularly apt for the CSIRP

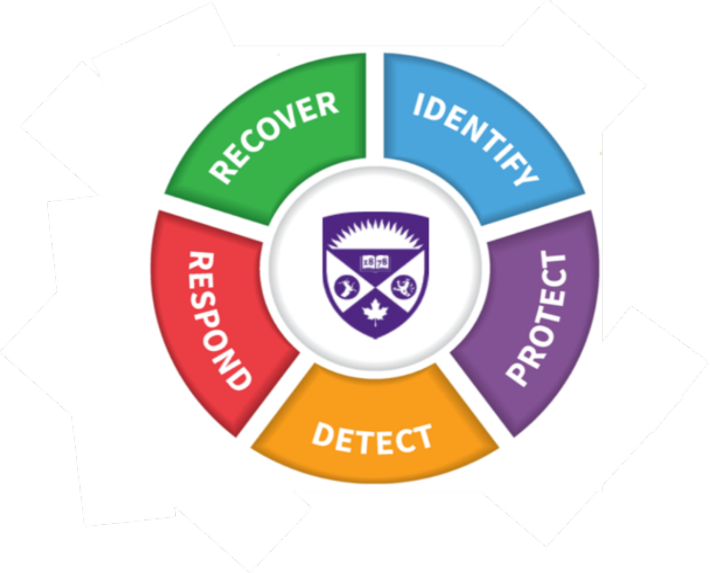


Figure 2: Western Cyber Security Strategy Methodology

The CSIRP brings these elements together and coalesces the tasks found within. Recently, the University Council of Chief Information Officers (CUSSIO) Security Special Interest Group (SSIG) produced a document entitled "Information Security Incident Response Guide" which was accepted and endorsed by the overall organization as a set of guidelines to be used to create institutional response frameworks. The Western University CSIRP document is based on many of the ideas and components of the CUCCIO SSIG effort.

The purpose of the Western University CSIRP document is to bring together a collated and coordinated response to cyber incidents as they might affect the institution. This plan will allow the disparate functions within the organization to become aware of and react to incidents more quickly and in a manner that would minimize potential effects.

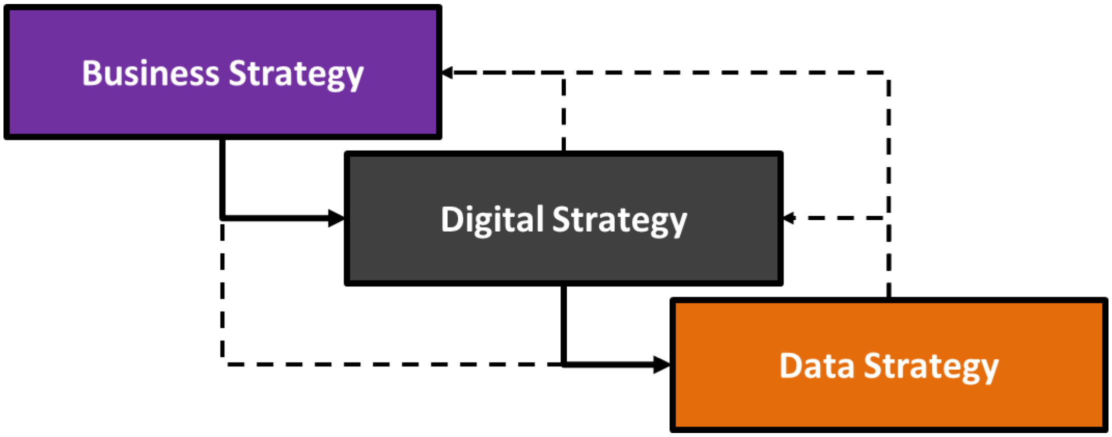
A cybersecurity event is anything anomalous that happens within the digital realm that is of specific or general security interest. This document is concerned with events that are categorized as Cyber Security Incidents, which rise to the level of representing harm or risk to the organization beyond day-to-day operations.

NOTE: The intended audiences for this document are internal stakeholders.

A cybersecurity incident may involve the introduction of malware or viruses (ransomware, cryptoware, propagating programs, etc.), distributed denial of service attacks, technological (platform) assets being compromised, or any sort of exploitation of cyber-vulnerabilities.

As a cybersecurity incident begins to take shape, it is critical that Western University implements a strong response mechanism with clear accountabilities and communications.

This document articulates the relationship between the Cybersecurity Incident Response Team (CSIRT) and key stakeholders across the organization. There are differentiations amongst key stakeholders in terms of entities that need to be notified quickly and those that need to be engaged as needed. Please consult the Stakeholders section below.



FURTHER NOTES RELATED TO CSIRP:

The Central Information Security Officer (CISO) is the primary Western Technology Service (WTS) leadership role with responsibility and accountability to assert initial judgment on cyber incidents. In the case of an absence of Director Cyber Security and Business Services (Brent Fowles) role, an appropriate designate will be named and communicated appropriately. The appropriate designate will be one of the following roles within the WTS leadership team:

- Director Application Services (Rob Brennan)
- Director Client Services (Sergio Rodriguez)
- Director Infrastructure Services (Dave Ghantous)
- Manager Information Security (Matthew Feeney)

Section 2: Basic Principles of Incident Management

1. There is no simple one-size-fits-all solution and things change:

Always keep in mind that every institution is different and Western University contains several autonomous entities within. The Cybersecurity Incident Response Plan (CSIRP) should be circulated and socialized throughout the organization for process commitment, while allowing for the model to be iterative and reviewed on an annual basis.

2. Commitment from executive management and governance structures:

Executive management should be actively involved in defining the university's incident response process. Western University executives should be aware of the risks of cyber incidents and of their own role in facilitating all members of the organization to assume their responsibility.

3. Involve key stakeholders:

Effective management of an incident will require input from a broad group of stakeholders on both the Western University's administrative and academic units. With respect to staff and faculty, ensure the information security reporting procedures are known, how to find the incident response plan, and of their own role within it, even if this just means informing the right person about anomalies.

4. Keep offline copies of response plan and playbooks that will be needed during an incident:

When an information cyber security incident occurs, teams may not have access to the files on their systems. Keep hard copies/offline copies of forms/logbooks/documents likely to be needed during a cyber security incident or crisis.

5. Essential backups should be separated from the rest of main systems:

It is important to have backup copies that are not linked in any way to Western University's active (or compromised) systems. This risk can be mitigated with network policy and logical separation.

6. Create and implement a strategy that recognizes the importance of logging and log retention:

Security Incident Event Management (SIEM) tools help trace back the origin of a cybersecurity incident. In developing data retention consider 60-, 180-day and 1yr log retention requirements.

7. Keep information security incident response playbooks and all related information or documentation up to date:

Annual review of Western University CSIRP and accompanying Playbooks is recommended.

8. Document every step of an information security incident:

Evidence will only be admissible in court if it has been collected respecting applicable laws and regulations dealing with Chain of Evidence

Section 3: Incident Preparedness Checklists

Before Incident

- Create a prioritized list of critical information assets to the functioning of Wester University whether managed by a central WTS group or not.
- Identify the stakeholders responsible for each critical asset.
- Create a Cybersecurity Incident Response Team or CSIRT (include individuals from Legal or Privacy, Communications, WTS, that will be responsible for all incidents.
- Develop and maintain communications lists and channels
- Develop and maintain the list of external cyber security resources
- Ensure proper monitoring and tracking technologies are in place to protect Western University’s information assets.
- Provide media training to the proper individual(s).
- Provide a university-wide process for faculty, staff, or third parties to report incidents or suspicious or suspected breach activities.
- Provide university-wide training on breach awareness, staff responsibility, and reporting processes.

During Incident

- Open an incident report and document the issue, detection, and response.
- Convene the Cybersecurity Incident Response Team (CSIRT).
- Convene a meeting with the appropriate internal stakeholders to discuss what must be done to restore operations.
- Convene a management meeting with the appropriate internal stakeholders to provide situational awareness to executive management.
- Triage the current issues and communicate to executive management.
- Identify the initial or root cause of the incident and activate the specialists to respond to the current issues to restore operations.
- Retain any evidence and follow a strict chain of evidence to support any needed or anticipated legal action.
- Communicate to affected third parties, regulators, and media (if appropriate).

Post Incident

- Update the incident report and review exactly what happened and at what times; also record what the decision points were.
- Review how well the staff and management performed during the incident.
- Determine whether the standing procedures were followed and if documentation matched procedures.
- Discuss any changes in process or technology required to mitigate future incidents.
- Determine what information was needed sooner.
- Discuss whether any steps or actions taken might have inhibited the recovery.
- Determine which additional tools or resources are needed to detect, triage, analyze, and mitigate future incidents.
- Discuss what reporting requirements are needed (such as regulatory, or public).
- If possible, quantify the financial loss caused by the incident.

Section 4: Stakeholder Groups

QUICK RESPONSE TEAM (QRT)

- Central Information Security Officer (CISO)
- Manager Information Security
- Security Operations (SEC/OPS)
- WTS Client Services
- SME(s) Subject Matter Experts (as required)
- Local Resources/Initiator (variable)

EMERGENCY TIER I (CSIRT.E1)

- **Director WTS Cyber Security and Business Services (or designated <u>CISO</u>)**
- **Director WTS Infrastructure Services**
- **Director WTS Application Services**
- **Legal Counsel**
- **Privacy Officer**
- Director Internal Audit
- Director Western Safety & Emergency Services
- Manager Emergency Management & Continuity of Operations
- Director WTS Client Services
- Associate Director OOR Information Technology
- Director HR Total Compensation
- Media Relations Officer (or designate from Communications & Public Affairs
- Supervisor General Accounting (Bankcard Committee)

Primary Triage Leads

EMERGENCY TIER II (CSIRT.E2)

- Associate Director WTS Data Centre, Network & Data Centre Operations
- Associate Director WTS Central Systems & Server Administration
- Manager Information Security
- WTS Infrastructure Leads & Helpdesk
- Distributed Information Technology Departments

EXECUTIVE TIER I (EXEC.E1)

- Provost and Vice-President (Academic)
- Vice-President (Operations and Finance) (**<u>Chair EOCG</u>**)
- Associate Vice-President (Human Resources) (**Vice Chair EOCG**)
- Associate Vice-President (Planning, Budgeting, and IT)

Primary EOCG Leads

EXECUTIVE TIER II (EXEC.E2)

- Vice-President (External)
- Vice President (Research)
- Vice-Provost (Academic Programs)
- Vice-Provost (Academic Planning, Policy and Faculty)
- Vice-Provost (Graduate & Postdoctoral Studies)
- Vice-Provost & Associate Vice-President (International Education)
- Vice-Provost & Chief Librarian
- University Registrar
- Associate Vice-President (Student Experience)

DECANAL TIER

- Arts & Humanities
- Don Wright Faculty of Music
- Education
- Engineering
- Health Sciences
- Information and Media Studies
- Ivey Business School
- Law
- Schulich School of Medicine and Dentistry
- Science
- Social Science

EMERGENCY OPERATIONS CONTROL GROUP (EOCG) MEMBERSHIP – EXTERNAL REF

- Vice-President Operations and Finance (**Chair**) (or designate)
- Associate Vice-President Human Resources (**Vice-Chair**) (or designate)
- Associate Vice-President Facilities Management (or designate)
- Associate Vice-President Institutional Planning and Budgeting & IT (or designate)
- Vice-Provost Academic Programs (or designate)
- Associate Vice-President Student Experience (or designate)
- Registrar (or designate)
- Associate Vice-President Housing and Ancillary Services (or designate)
- Associate Vice-President Research (or designate)
- Associate Vice-President Financial Services (or designate)
- Associate Vice-President Communications & Public Affairs (or designate)
- Director Campus Safety & Emergency Services
- Manager Emergency Management & Continuity of Operations
- Director WTS Applications Services
- Director WTS Cyber Security and Business Services (CISO)

EMERGENCY RESPONSE TEAM (ERT) – EXTERNAL REF

ERT Members – Command

- **Operations Leader**, Campus Community Police Service
- Manager, Fire Safety
- Director, Occupational Health & Safety
- Executive Director, Facilities Operations
- Fire Safety Technician, Fire Safety
- HazMat Team Leader

ERT Members - Support

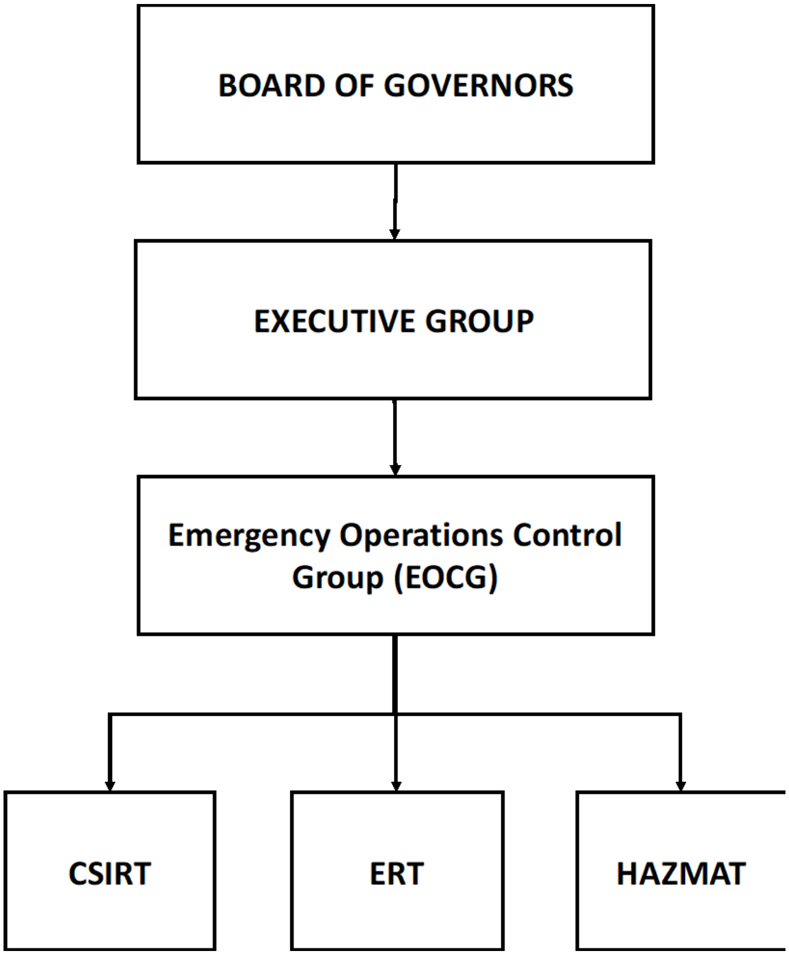
- Director, Media, and Community Relations
- Media Relations Officer
- WTS Telecommunications Team Leader
- WTS Technical Support Team Leader

- Manager, Power Plant Operations

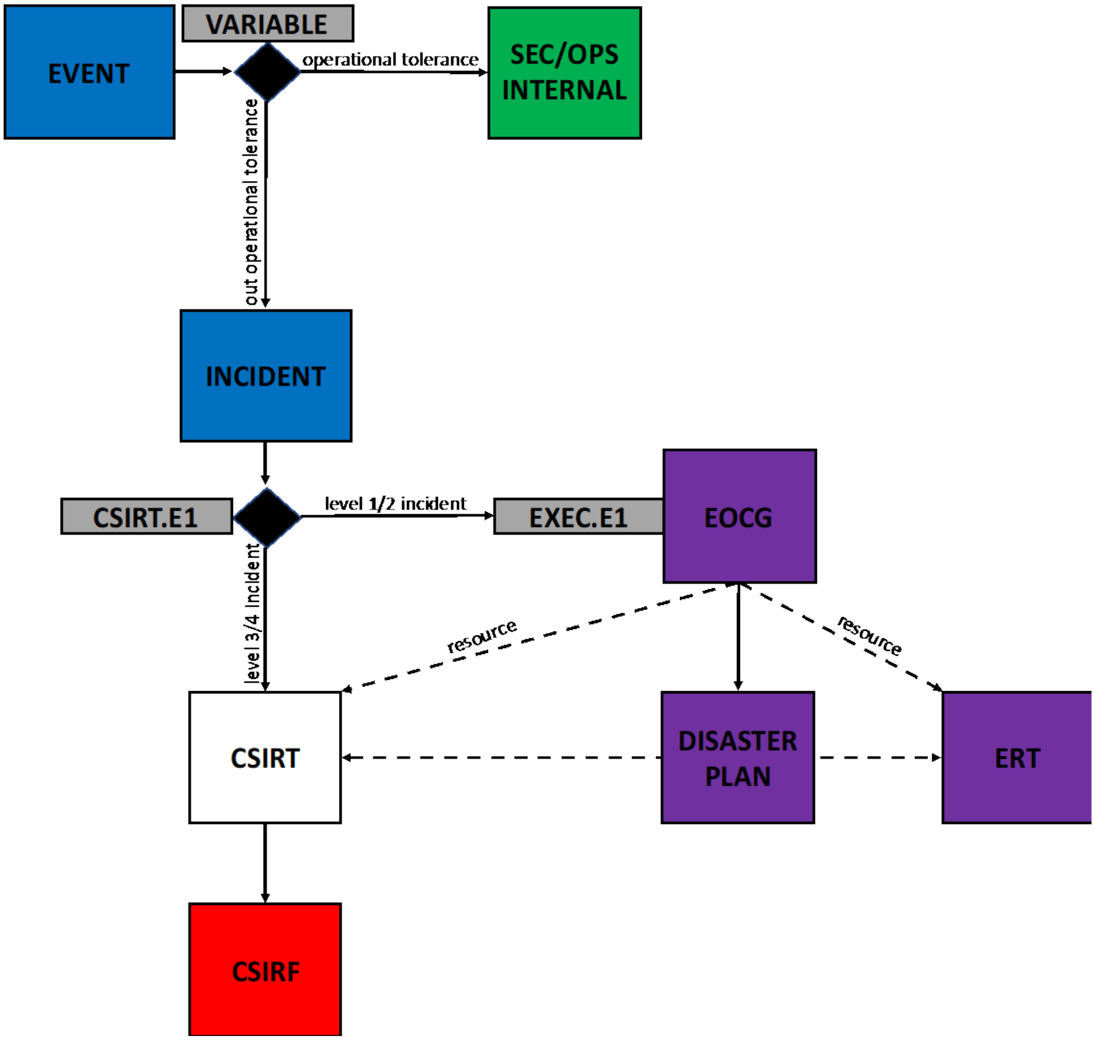
BANKCARD COMMITTEE MEMBERSHIP – EXTERNAL REF

- Supervisor General Accounting (**Chair**)
- Director Internal Audit
- Director WTS Cyber Security and Business Services
- Director WTS Application Services
- Compliance Auditor Financial Services
- Director Procurement Services
- Manager Information Security
- Director Fin&Adm Research Parks
- Associate Director Ops Bookstore
- Accounting Analyst Financial Services

Section 5: Accountability Tree

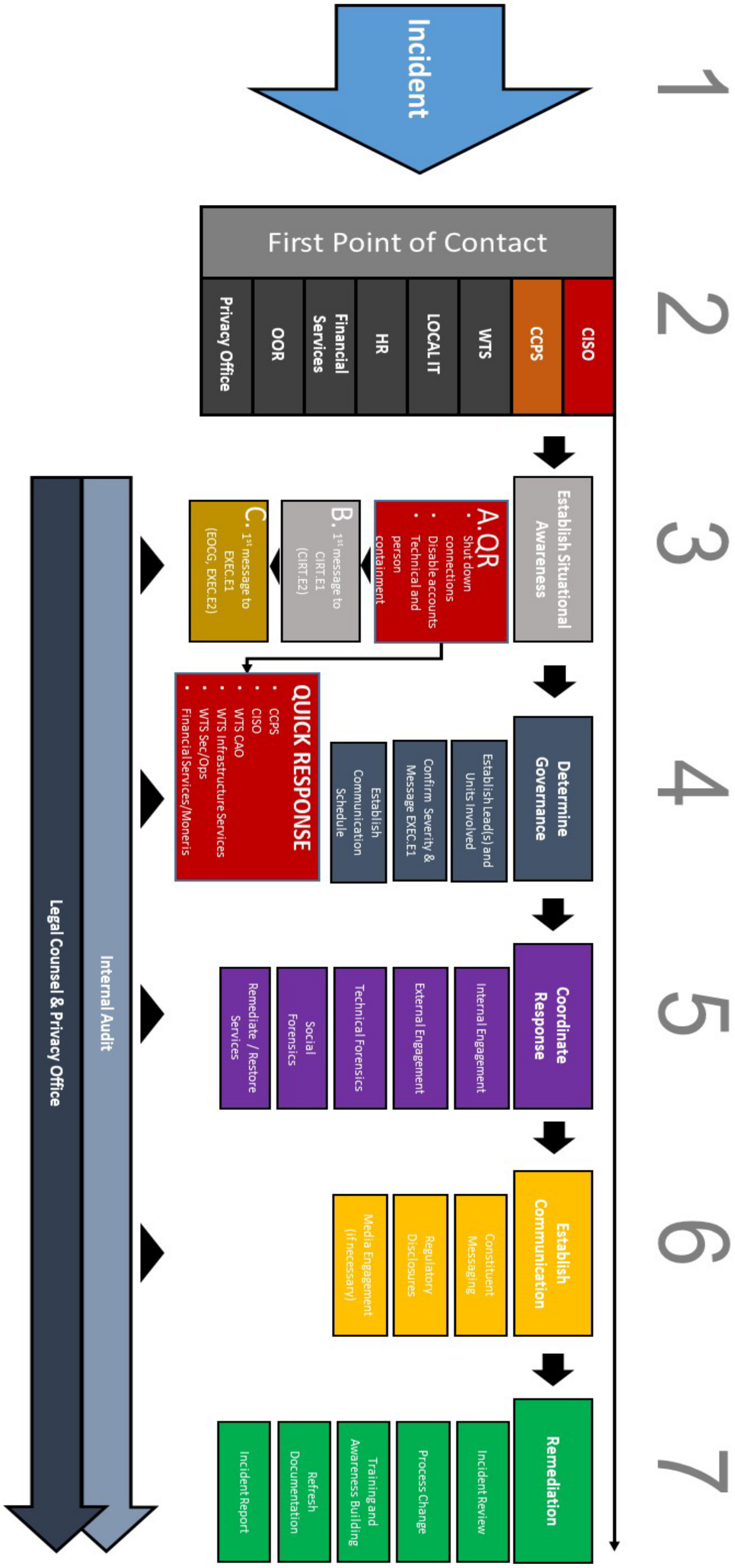


Section 6: Initial Decision Tree (CSIRT or EOCG)



VARIABLE	multiple actors involved in understanding event vs incident
CSIRT.E1	decision to escalate to EOCG based on best information available
EXEC.E1	decision, based on recommendation from CSIRT.E1 to pass to EOCG

Section 7: Cyber Incident Response Process



Section 8: Cyber Security Incident Response Protocol

Bolded items indicate key defined group
<u>Bolded/Underlined items</u> indicate accountable entity

Step 1 – Incident Discovered

- Incident is discovered via:
  - Notification from partner organizations or agency
  - Active or passive monitoring of systems
  - Direct contact by observer, impacted unit, or individual
  - Physical event has occurred or is in process
- End Users have understanding of what an incident means and what rises to the test of that description that would invoke this framework
- End Users can contact any of the likely escalation groups
- Escalation groups have understanding of responsibilities and accountabilities
- To be cyber-resilient, everyone is involved

Step 2 – Incident Reported

- Incident is reported to an escalation group (collection of units established as likely contact points for initial reporting)
  - Note: a breach process is defined for (e)commerce-related activities (through Western's **Bankcard Committee**) and that plan aligns well with the CSIRP (difference includes contacting payment providers with any fraud information, see **Appendix A: Bankcard Breach Plan**)
- Incident reporting will be encouraged to funnel to **CISO** or **Western Special Constable Service (WSCS)**, but constituents may contact other departments directly and variably
  - Contacted departments should involve **CISO** as soon as incident is made apparent (even if in preliminary stages)

Step 3 – Situational Awareness and Quick Response

- **<u>CISO</u>** or **SEC/OPs** establishes and executes **Quick Response** (QR) process if a person, account, computer, or other technology requires immediate action:
- **<u>CISO</u>** messages **CSIRT.E1** about incident to engage in preliminary and coordinated action strategy (message establishes incident as such, but can be spare on details)
- **<u>CISO</u>** (coordinates with **CSIRT.E1**) messages **EXEC.E1** for situational awareness
- **CSIRT.E1** confirms severity (see rubric below); **(<u>CISO</u>)** recommends to **Chair/Vice-Chair EOCG** to pass incident response to **EOCG** and/or to engage 3rd party **Cyber Insurance agency**

INFLECTION POINT – **<u>EOCG</u>** (through Chair and Vice-Chair leadership) takes over Incident Response (see **WESTERN UNIVERSITY DISASTER PLAN**); AND/OR **Cyber Insurance** agency allocates 3rd party firm to oversee response (initiated by **CISO** and then coordinated through **<u>EOCG</u>**); **CSIRP** process ends

OR

Incident Response remains with **<u>CSIRT</u>** and continues through plan below

Step 4 – Confirmation and Governance

- **CSIRT.E1** establishes **Incident Lead** (**CISO**, by default)
- **Incident Lead** establishes next steps, meeting schedule, notifications, mitigation tactics, recovery options, and integrates appropriate stakeholder groups and departments for action(s)
- **Incident Lead** informs **EXEC.E1**, **CSIRT.E1** of plans and emergent information (if necessary)

Step 5 – Coordinated Response

- **Incident Lead** to coordinate **CSIRT.E2** processes and steps to resolve immediate concern(s)
    - Technical, social, and process-level forensics completed
    - External discoveries, notifications as required, vendor discussions with technical team and Legal (if applicable)
- **Incident Lead** message regular updates to **CSIRT.E1** and **EXEC** teams (as necessary)

Step 6 - Communications

- **Incident Lead** engages communication to affected internal constituents (as necessary)
- Communications through regulatory channels by **Privacy Officer** (as necessary)
    - Communications with other affected parties by **Privacy Officer** (privacy disclosures, PIPEDA, GDPR, financial components) and **Communications and Public Affairs** (as necessary)
- **Incident Lead** engages communications with vendor(s) by **Procurement Services**, technical team(s) and **Legal Counsel** (as necessary)
- **CISO** engages communications to **CUCCIO**, Canadian Shared Security Operations (**CanSSOC**), Ontario Cybersecurity Higher Education Consortium, Canada Centre for Cyber Security (**CCCS**) (as deemed relevant, required, and/or permitted)

Step 7 – Review and Close

- **Incident Lead** reviews incident and makes appropriate recommendations for changes to processes, documentation, personnel, activities, and/or monitoring tools
- Remediate technology through internal technical channels or with vendor (various)
- **Incident Lead** Close-out report to be communicated to WGIS CSIRT.E1 and EXEC Teams (as necessary), WGIS and WTS-Management
- **Incident Lead** closes incident and issues report to stakeholders
- Engage in training and awareness-building exercises (various)

Section 9: Incident Levels

Levels are indicated by Severity Chart in Section 10 (with IMPACT as first factor and URGENCY as second)

Level 1
CRITICAL (P1) / **HIGH (P2)**

Level 2
MEDIUM (P3)

Level 3
LOW (P4)

Level 4
MINOR (P5)

Section 10: Incident Severity Rubric

		IMPACT Business criticality, number and type of people affected		
		SIGNIFICANT / LARGE • Large number staff affected and/or not able to do their job properly • Large number of customers are affected and/or acutely disadvantaged in some way • Damage to business reputation is high	**MODERATE / LIMITED** • A moderate number of staff are affected and/or not able to do their job properly • A moderate number of customers are affected and/or inconvenienced in some way • Damage to business reputation is moderate	**MINOR / LOCALIZED** • A minimal number of staff are affected and/or not able to do their job properly • A minimal number of customers are affected and/or inconvenienced but not significantly • Damage to business reputation is minimal
URGENCY How fast must the service be restored?	**HIGH** • Damage caused by incident increases rapidly (exponential) • Interrupted work is time-sensitive or at a critical time e.g. year end, exams, beginning of term • Prevent a minor incident from becoming a major incident • Several users with "VIP" status are affected.	**CRITICAL** **P1**	**HIGH** **P2**	**MEDIUM** **P3**
	MEDIUM • Damage caused by incident increases considerably over time (straight line) • A single user with VIP status is affected	**HIGH** **P2**	**MEDIUM** **P3**	**LOW** **P4**
	LOW • The damage caused by the Incident only marginally increases over time. • Work that cannot be completed by staff is not time sensitive.	**MEDIUM** **P3**	**LOW** **P4**	**MINOR** **P5**

	CRITICAL P1	HIGH P2	MEDIUM P3	LOW P4	MINOR P5
Response Target	Immediate	1 Hour	4 Hours	6 Hours	Next Business Day
Escalation Time	Immediate	Immediate	1 Hour	3 Hours	
Immediate Tasks	• Start Jira SOC Incident • Escalate Jira Incident • Notify Listed Systems Administrators/Owners • Act as Incident Commander Until Escalation Hand-Off	• Start Jira SOC Incident • Escalate Jira Incident • Notify Listed Systems Administrators/Owners • Act as Incident Commander Until Escalation Hand-Off	• Start Jira SOC Incident • Act as Incident Commander • Open a "War" Room	• Start Jira SOC Incident • Act as Incident Commander	• Start Jira SOC Incident • Act as Incident Commander
Escalation	Escalate Per Below • Provide Update, Seek Direction • Hand-Off Incident Commander Role		Escalate Per Below • Provide Update, Seek Direction	Email security@uwo.ca • Provide Update, Seek Direction	Email security@uwo.ca • Provide Update, Seek Direction
Escalation Path	+0:00 Call/Text Manager of Information Security, Then Send Email to security@uwo.ca				
Contact #'s **Manager of Information Security** C. 519-777-6267 H. 226-779-9665 **Director of Cyber Security** C. 519-857-3023	+0:05 If no response back from Manager of Information Security, call on alternate phone #'s (per staff directory). If no answer leave voice message and send SMS and email				
	+0:10 If no call back from Manager of Information Security, call/text Director of Cyber Security (CISO). If no answer leave voice message and send SMS and email.		+1:00 If no call from Manager of Information Security, call/text Director of Cyber Security. If no answer leave voice message		
	+0:15 If no call back from either Manager of Information Security or Director of Cyber Security (CISO), call both again on alternate phone #'s (per staff directory). If no answer, call alternate CISO Director.		+2:00 If no call from Manager of Information Security or Director of Cyber Security (CISO), call both again on alternate phone #'s (per staff directory). If no answer, call alternate CISO Director		

Incident Commander Role	Team Member Role
• Remain at your post and continue forensic investigation • Assign team member to engage internal and external escalation resources as needed • Assign team member for a warm handoff if necessary • Keep the incident record up to date • Determine what/when/how to communicate to affected users • Communicate with management as prescribed in the playbook • Post Incident Review (next business day)	• Take direction from the Incident Manager • Assist the Incident Commander with further investigation

Section 11: Message Template

TO: [EXEC.E1 / CIRT.E1 / CIRT.E2 / EOCG / ERT]
FROM: [CISO / INCIDENT LEAD]
SUBJECT: [CONFIDENTIAL / SENSITIVE/OPEN] / [GREEN / YELLOW / ORANGE / RED] – CYBER SECURITY INCIDENT [“X”] *[UNDERWAY / UNDER INVESTIGATION / IN RECOVERY / COMMUNICATION / CLOSED] *
MESSAGE:
This message is a notification that a Cybersecurity Incident is emerging or has occurred.

This event is affecting ______.

[Known Details]

Update will be provided in/at [1 hour/30 minutes/time of day].

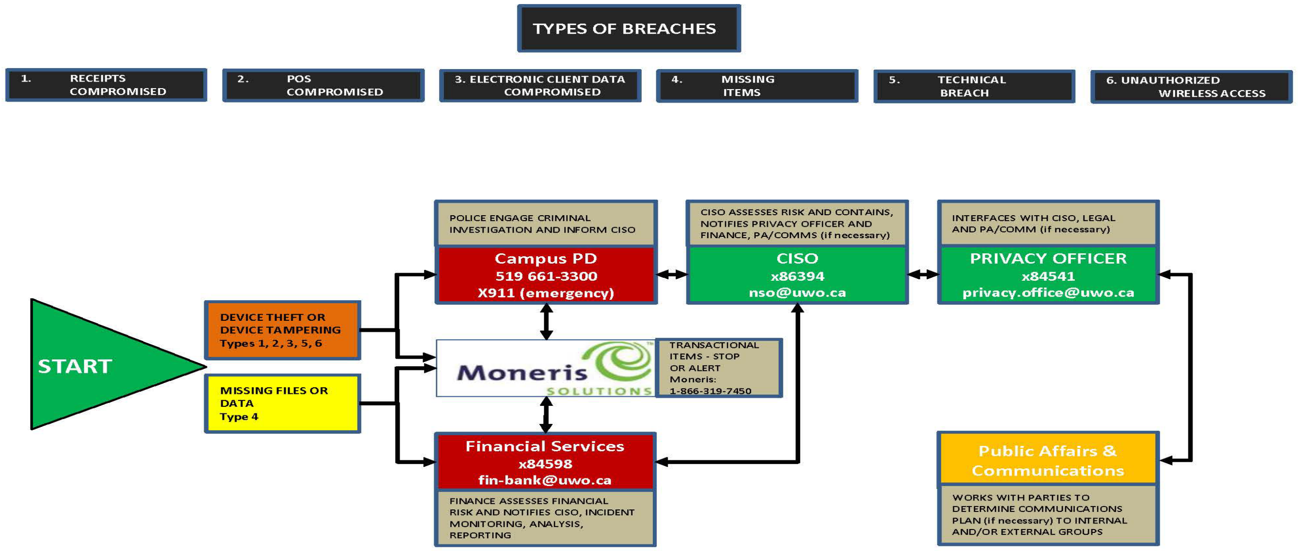
Mode of update will be [email / conference call / in person meeting]: [details]

[Actions Required of Recipient(s)]

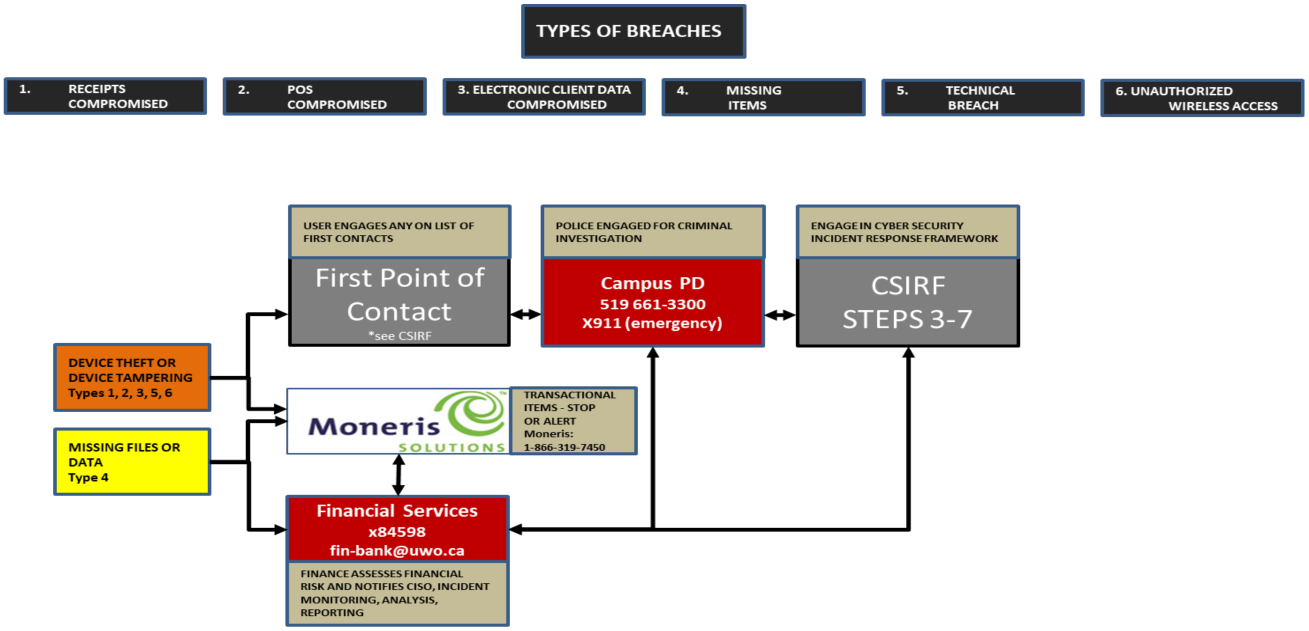
Appendix A: Terms and Acronyms

BANKCARD	Western Standing Committee for PCI DSS Compliance
CCCS	Canada Centre for Cyber Security
CanSSOC	Canadian Shared Security Operations
CSIRF	Cybersecurity Incident Response Framework
CSIRT	Cybersecurity Incident Response Team
CIRT.E1	Emergency I Tier
CIRT.E2	Emergency II Tier
CIRT.E3	Emergency III Tier
CISO	Central Information Security Officer
CUCCIO	Canadian University Council of Chief Information Officers
CUCCIO SSIG	CUCCIO Security Special Interest Group
EOCG	Emergency OPERATIONS CONTROL GROUP
ERT	Emergency Response Team
EXEC.E1	Executive I Tier
EXEC.E2	Executive II Tier
EXEC.E3	Executive III Tier
HR	Human Resources
IT	Information Technology
ITSC	Information Technology Steering Committee
OOR	Office of the Registrar
PCI DSS	Payment Card Industry Data Security Standard
PVP	President/Vice-Presidents
QRT	Quick Response Team
SEC/OPS	Security Operations Group (WTS)
SME	Subject Matter Experts
WGIS	Working Group on Information Security
WSCS	Western Special Constable Service
WTS	Western Technology Services

Appendix B: Bankcard Breach Plan


TYPES OF BREACHES
1. RECEIPTS COMPROMISED
2. POS COMPROMISED
3. ELECTRONIC CLIENT DATA COMPROMISED
4. MISSING ITEMS
5. TECHNICAL BREACH
6. UNAUTHORIZED WIRELESS ACCESS
START
DEVICE THEFT OR DEVICE TAMPERING Types 1, 2, 3, 5, 6
MISSING FILES OR DATA Type 4
POLICE ENGAGE CRIMINAL INVESTIGATION AND INFORM CISO
Campus PD 519 661-3300 X911 (emergency)
CISO ASSESSES RISK AND CONTAINS, NOTIFIES PRIVACY OFFICER AND FINANCE, PA/COMMS (if necessary)
CISO x86394 nso@uwo.ca
INTERFACES WITH CISO, LEGAL AND PA/COMM (if necessary)
PRIVACY OFFICER x84541 privacy.office@uwo.ca
Moneris SOLUTIONS
TRANSACTIONAL ITEMS - STOP OR ALERT Moneris: 1-866-319-7450
Financial Services x84598 fin-bank@uwo.ca
FINANCE ASSESSES FINANCIAL RISK AND NOTIFIES CISO, INCIDENT MONITORING, ANALYSIS, REPORTING
Public Affairs & Communications
WORKS WITH PARTIES TO DETERMINE COMMUNICATIONS PLAN (if necessary) TO INTERNAL AND/OR EXTERNAL GROUPS

🟥 Primary Contact Points and Lead Response
🟩 Response Team
🟨 Communications


TYPES OF BREACHES
1. RECEIPTS COMPROMISED
2. POS COMPROMISED
3. ELECTRONIC CLIENT DATA COMPROMISED
4. MISSING ITEMS
5. TECHNICAL BREACH
6. UNAUTHORIZED WIRELESS ACCESS
USER ENGAGES ANY ON LIST OF FIRST CONTACTS
First Point of Contact *see CSIRF
POLICE ENGAGED FOR CRIMINAL INVESTIGATION
Campus PD 519 661-3300 X911 (emergency)
ENGAGE IN CYBER SECURITY INCIDENT RESPONSE FRAMEWORK
CSIRF STEPS 3-7
DEVICE THEFT OR DEVICE TAMPERING Types 1, 2, 3, 5, 6
MISSING FILES OR DATA Type 4
Moneris SOLUTIONS
TRANSACTIONAL ITEMS - STOP OR ALERT Moneris: 1-866-319-7450
Financial Services x84598 fin-bank@uwo.ca
FINANCE ASSESSES FINANCIAL RISK AND NOTIFIES CISO, INCIDENT MONITORING, ANALYSIS, REPORTING

🟥 Primary Contact Points and Lead Response
🟩 Response Team
🟨 Communications

Appendix C (Document Revisions)

Revision Number	Date of Issue	Author(s)	Brief Description of Change
1.0		Colin Couchman	Original Document
2.0	April 4th, 2022	Dominique Perreault	Formatting changes to bring the Playbook and CSIRP into alignment
2.1	April 26th, 2022	Dominique Perreault	Replaced instances of CSIRF with the more accurate CSIRP. Clarified membership of the QRT. Updated external links.
2.2	June 22, 2022	Scott Davis – Manager, Emergency Management & Continuity of Operations	1. Replace Campus Police w/Special Constables (Individual) where appropriate. 2. Replace Campus Police w/Campus Safety & Emergency Services (Department) where appropriate. 3. Add new position of Manager, Emergency Management & Continuity of Operations where appropriate.
2.3	July 12th, 2023	Brent Fowles – Director Cyber Security	1.Update named roles