HOW TO USE THIS TEMPLATE

Who should complete this template: to be completed by the unit IT leader.

Timeline: The leadership update should be issued within four hours from the time of incident discovery.

Additional notes: This template provides an example of what information should be shared with decision makers (CAO, Dean, Unit head). All information should be accurate, factual, validated and preferable vetted by the CISO.

Additional considerations for the group to consider: should we identify key contacts, what are the timelines to have an NDA, engage forensic, etc. …

This issue is under solicitor-client privilege. Please mark communications as such and limit the amount of electronic communication in all formats to essential messages to response activities.

Description: Basic timeline and description of key facts, including dates

Incident Classification: High. A little more description on impact

Incident Manager:
Incident Management Team:
Division
- <Name> Director, Information Technology
- <Name>, <role>

ITS
- CISO
- <name>, InfoSec Architect
- <name>, role

Unit
- <name>, <role>

Incident Management
- <name>, Counsel
- <name>, FIPPA

Priorities
- Determine attribution of attack
- Determine potential and scope for data exfiltration
- Confirmation of impact and containment
- Communicating impact to clients (if necessary)

Noteworthy updates
- Forensics company engagement <date>. Bi-weekly calls scheduled with written updates.
- On-boarding of the forensic investigation.
- Establish/create master timeline documents.
- Establish a data sharing agreement and NDA.

Impact Assessment

Task	Description
The information that was exposed and approximate number of individuals and records concerned	
To who it was exposed;	
For how long it was exposed;	
Likely consequences of the breach;	
Operational impact to the unit; Workarounds to be put in place;	

Next Steps, including measures taken or proposed to contain the breach

Task	Owner	Target Date	Status
Complete initial external forensic review and receive timelines	…	TBD	In Progress
Determine root cause and impact	…	TBD	In Progress
Draft notification to clients (if necessary)	..	TBD	In Progress
Draft notification to IPC (if applicable)	…	TBD	In Progress
Create an NDA between U of T and the forensic investigation company	TBD	TBD	Not Started

Risks and Issues, including reason for delay for any report not made within 72 hours

Type	Description	Mitigation / Strategy
Issue	Increased complexity due to international connection	Work closely with our International partners
Issue	Limited internal expertise in analysis nation state attribution	Engage qualified external forensic firm
Issue	Forensic services are high cost.	Clearly scope work, regular meetings to review, and perform work with local resources when possible.
Risk	Uncertainty and confusion in roles and tasks.	Identified a clear Incident Manager, meeting schedule, and task list.
Risk	Data sharing between investigations	Review data that is being shared

Frequently Asked Questions (for internal use only)

Q: Is this a data breach? Has data been exposed to hackers?
A: Evidence exists that an attacker was in the environment, either in an automated fashion but more likely under human control. A suspicious data transfer happened to one of the suspected bad IP addresses strongly suggesting some kind of data were transferred out of the environment.

Q: Which data are involved?
A: The exact data impacted is still being investigated. The impacted systems include **<description of systems>** and/or **<users>**. Description on the nature of data and its classification level. Use the following levels for reference: https://isea.utoronto.ca/policies-procedures/standards/data-classification/

Q: Were the data encrypted?
A: Initial triage indicates there was **<encryption/no encryption>** in place. Provide additional explanation.

Q: Are there external companies available to help?
A: There are no companies on retainer for information security forensics or data recovery. Information Security has engaged Mandiant to provide additional forensic support.

Q: Do we have obligations to notify?
A: Initial triage notices went out to individuals indicating they needed to change their passwords. A review is being conducted to determine if a follow-up to email users to indicate that they should review their email communications for any concerns. A FIPP Office review is pending the information security forensics investigation, but initial analysis is there will need to be a notification to the Privacy Commissioner.

Additional Resources:

Privacy Breaches Guidelines for Public Sector Organizations
https://www.ipc.on.ca/wp-content/uploads/2019/09/privacy-breach-protocol-e.pdf

Stakeholders

Role	Name	Active and/or Informed
IT Manager		A
IT Director		A
HR		I
CIO		A
Legal		A, I
FIPPA		
Law Enforcement		NI
Provost's Office		
President's Office		