Security Incident Response and Breach Notification Procedure

Security Incident and Breach Response Procedures

The purpose of this document is to outline ITS's general approach to dealing with security incidents relating to, or affecting, Carleton's network and computing environment. It is not intended as a comprehensive framework along the lines of ISO/IEC 27035, but rather as 1) a framework for helping clients understand what is happening, and 2) a template we can look to internally for guidance, in the heat of the moment, in case of a security incident.

This document also outlines our specific response steps where personally identifiable or otherwise very sensitive information has been disclosed.

[ ] [Motivation] [Detection] [Risk Assessment] [Mitigation]

Motivation

Maintaining Carleton's network and overall computing environment has become, increasingly, a cybersecurity challenge. 2017, in particular, was a bad year for for cybersecurity. 2017 saw a number of highly publicized breaches, like the Equifax hack, as well as new vulnerabilities on computer processors (Spectre and Meltdown), and the rise of ransomware. In response to these security challenges, ITS has taken steps to improve our ability to monitor our network, detect anomalies, and mitigate vulnerabilities (or outright compromises) when discovered.

This document is concerned, in particular, with mitigation, that is, with ITS's response when a vulnerability or compromise has been discovered. There is also a detailed section outlining what actions we will take if we determine that personally identifiable or otherwise very sensitive information has been disclosed.

By "vulnerability" we mean an operating state that could allow malicious parties to perform unauthorized actions, for example, an unpatched/un-updated Windows desktop that could be subverted and used as platform for bitcoin mining, spamming, or monitoring of other network traffic to facilitate additional unauthorized actions. By "compromise" we mean an actual breach, that is, a circumvention of our normal operations by a malicious party that presents an immediate reputational and/or financial risk to the college.

A breach could be something as minor as, for example, the theft of user credentials, allowing unauthorized parties to assume the identity of a Carleton user. A breach could also be something as significant as exfiltration of a large amount of sensitive data, or outright theft/ransom of an entire administrative database.

Detection

Detection of anomalous or unauthorized activity in Carleton's computing environment that presents either a reputational or financial risk to the college may come to ITS through a variety of channels, including

- User reports
- Automated alerts
- Semi-automated scanning (for example, when we have reason to suspect a problem exists)
- Analysis of log data by security staff

Risk Assessment

Once a problem has been identified, we assess. In complex cases, we may engage third parties, for example, cybersecurity firms with expertise in the area where we've experienced a compromise.

Investigation and assessment can be difficult and it is sometimes intrusive. It may require careful examination of things like activity logs and email. In general, ITS takes the privacy of the Carleton community very seriously and will only examine and analyze what is strictly needed in order to assess the full extent of a threat that's been identified. Furthermore, the smallest possible group of people will conduct such investigations. And they will not communicate any findings relating to individual user actions other than those strictly relevant to the investigation they are performing. Our goal is to to limit risk and damage, and to protect the campus from the normal threats that all networked computing environments are subject to.

Ultimately, in any given case, we want to reach a point where we understand our risk.

- How immediate is the threat?
    - Is the threat potential (a "vulnerability"), or are we looking at an actual breach?
    - If the threat is potential, what is its CVS score? How are other schools/businesses addressing the risk? What actions do our software vendors recommend?
    - What is the actual (and potential) financial risk to the college?
- Who is affected?
    - A single person or device?
    - A few people (like a small department) or small number of devices?
    - A large number of people or devices, possibly the entire college?
    - Internal or external users?

Mitigation

Once affected people and systems have been assessed, ITS will assign appropriate resources, which may include

- Helpdesk staff
- Desktop experts
- Systems or application administrators
- ITS leadership
- Campus leadership
- External parties (law enforcement, forensics experts, auditors); see below on PII disclosure response

Action we may take to mitigate vulnerabilities and breaches may take a variety of forms, such as

- Temporarily locking a user's account, to limit damage to their personal information and resources
- Locking multiple accounts to prevent damage from spreading to new accounts or devices
- Taking one or more devices physically (or virtually, via software) off the network, to prevent intrusion
- Removing unauthorized software ("malware")
- Reimaging/rebuilding affected machines, resetting them to a "known good" state
- Requesting that a user, or set of similar users, update software, in order to secure a device they are responsible for
- See also PII disclosure response procedure below

(PII response plan temporarily deleted while being worked on and edited; must be re-included from Personally Identifiable Information (PII) Disclosure Notification Procedure)

Richard Goerwitz
January 2018

- Security Incident Response and Breach Notification Procedure
- What All Is ITS Logging/Monitoring?
- When and why does my password expire?
- Internet Explorer Security Zones
- McAfee VirusScan Mac