ADMINISTRATIVE PROCEDURE

BYU OIT and CES SOC Data Requests

Procedure Contents

Effective Date: 1 Nov 2021
Last Updated: New

Responsible University Officer: VP Technology/CIO

Procedure Owner:
Chief Information Security Officer

Procedure Contacts:
John Payne (CISO)
801-422-9099
John_Payne@byu.edu

Paul Angerhofer (OGC)
801-422-6727
Paul_Angerhofer@byu.edu

RELATED POLICY: Information Use, Privacy, and Security Policy (https://policy.byu.edu/view/information-use-privacy-and-security-policy)

INTRODUCTION:

On occasion, the Office of IT (BYU OIT) and the CES Security Operations Center (CES SOC) receive requests to provide access to private data or perform atypical investigations that are unrelated to cybersecurity threats. Requests may come from offices with a business need to know information related to activity that violates university policies such as the Church Educational System Honor Code, the Personnel Conduct Policy, etc. These requests resemble the following questions:

- Did a user access another user's data or university account?
- Where on campus has an individual been and when were they there?
- Did an individual send a particular email to a specific group?
- What websites has an individual been visiting? Has inappropriate content been downloaded to an individual's university-owned device?
- Who made the vulgar post on an online message board?

While we appreciate the vigilant efforts of these groups, BYU OIT and the CES SOC have limited capacity to address these requests. In addition, there may be privacy or legal issues associated with how, when, or why this data is shared. This document outlines how to make data requests and addresses some of the challenges associated with fulfilling them.

This procedure is intended to reinforce legal protections for BYU OIT employees and CES SOC analysts as well as the privacy rights of individuals involved in investigations.

APPLICABILITY

BYU OIT and the CES SOC will honor data requests from campus units with a business need to know; requests from units that do not have a business need to know will not be honored.

Requests from individuals, those not associated with the university, and law enforcement will only be honored at the discretion of the Office of the General Counsel.

PROCEDURE

The following procedure should be followed for information requests such as those in the bulleted list above:

1. The requestor should email their request to the Chief Information Security Officer and should copy the procedure contact from Office of the General Counsel, both listed above.
2. The email request should include the scope of the problem, desired objectives, and the date(s) for which data is desired.

Requestors should be aware that BYU OIT and the CES SOC will not be able to provide answers in every case. (See the challenges section below.)

FORMS/INSTRUCTIONS

The key online forms related to this procedure are:

- None exist as of the date of this publication. Please reach out directly to the Procedure Contacts (listed above in header).

ADDITIONAL CONTACTS

If the primary contact is not available to assist with data requests, one of the following may be contacted:

- Joe Taylor – Assistant VP Information Technology – Joe_Taylor@byu.edu
- Scott Hunt – Assistant VP Information Technology – Scott_Hunt@byu.edu

APPENDICES

Challenges

We strive to prevent the exposure of our analysts to pornographic content. During an investigation, we will not require employees to view videos or images on a device or to document any adult or explicit content they may find. It is difficult to draw this line quantitatively. If our employees are uncomfortable with content they happen across, we will ask them to stop and immediately report back rather than explore further.

BYU OIT and the CES SOC do not have visibility to all electronic communication activity for the campus community. While our security systems provide protection and visibility, they do not provide comprehensive visibility and are only deployed in areas of highest value. Much of the traffic to and from the internet is encrypted, preventing inspection. Some examples of the challenges we face when trying to address the questions above include:

- ***Encryption of outbound internet traffic*** Most internet traffic is now encrypted. When traffic was not encrypted, we were able to provide details about what sites were visited, content accessed, interactions performed, and more. We do not have the ability to view the contents of an encrypted web session. (For example, we cannot see any details when you visit your bank website.) For encrypted traffic, web filtering tools rely on the reputation of the website you are visiting and only block sites that are known to be in categories of concern.

- ***Encryption of hard drives*** Operating System vendors are providing better drive encryption, making it harder to perform disk forensics. In the past, we were able to copy a hard drive and indicate what was on the device, what had been deleted, etc. Some drive encryption prevents that entirely. Administrative passwords, usually maintained by the departmental CSR, can allow an inspection of the current state of a drive but might not show what has been deleted. For example, the newest MacOS encryption blocks many of the traditional disk inspection tools.

- ***Visibility*** While BYU OIT and the CES SOC have visibility into network activities on campus, as well as to the much of the activity occurring on OIT managed systems, there is not a central repository of log data associated with university workstations or departmental computers. Additionally, we have no visibility to equipment or websites that the university does not own. For the most urgent requests, where activity has occurred on third-party systems, we must reach out to system owners or security teams to aid an investigation. This is also true of campus SaaS solutions.

- ***Remote work*** The CES SOC has several network traffic analysis and protection tools. None of those are activated when an individual is working remotely. Sophos may indicate it has blocked some concerning website browsing, but all it does is indicate a site that was hit along with a broad category that Sophos associated the site with. There is no other indication the type of browsing activity that was done before, during, or after the block activity. While we would have a record of that activity if it occurred on a campus network, we do not when the activity occurs remotely. This limits the context we can wrap around the overall activity. The difficulty of attribution is compounded when individuals share their device password(s), leave devices unlocked, or do not secure devices when not in use.

- ***Staffing*** A disk inspection is a multi-day effort. The larger the hard drive, the longer it takes to accomplish forensics work. The CES SOC has not scoped their workforce to accommodate regular disk inspections. Any requests for a forensics disk inspection impede our ability to conduct our standard operations.

RELATED INFORMATION

- ***None***