UNIVERSITY OF TORONTO

Interim Threat / Risk Assessment

Student E-Communications Outsourcing Project

Martin Loeffler — Information Security, I+TS

Creation Date:	Version	1.0	June 24, 2010
Last Updated:	Version	2.0	July 6, 2010
	Version	2.1	July 6, 2010
	Version	3.0	July 12, 2010
	Version	4.0	Sept 22, 2010
	Version	4.1	Sept 22, 2010

Table of Contents

Executive Summary

The University of Toronto is exploring out-source options to replace its currently internally hosted and maintained student email system. As part of this exercise, an understanding of risks is required. These risks are not only to student email data, but potentially also to the reputation of the University itself.

The two vendors being considered to provide this out-sources service are Microsoft (via their Live@EDU product) and Google (via their Google Apps suite of web services). Both vendors are large, mature firms that are heavily invested in providing secure web-based services, and are unlikely to leave the marketplace.

On consideration of questions asked of both vendors, and an understanding of threats arising from legal, technical, and procedural sources, it is likely that out-sourcing email and associated services to either Google or Microsoft will result in reduced risk to student email data.

Sensitivity of Data to Risk

To clearly articulate risk to information, a Threat / Risk Analysis (TRA) is performed, identifying: data within the scope of the TRA; data sensitivity to risk of disclosure, loss, alteration, and unrecorded use or repudiation of receipt; agents or events that could cause such undesired outcomes to be realized; vulnerabilities that would enable threats to have an impact; and risk mitigation strategies that would address specific vulnerabilities.

The TRA regards 'security' as the effective and reliable mitigation of risk to confidentiality, integrity, availability and accountability for use of data, in the context of solution-specific vulnerabilities, and the sensitivity of data to risk.

Students have stated, via consultation, that they are prepared to accept known risks to the security of their data. This feedback has been confirmed through the University's observation of students' current practice of forwarding email out of the University of Toronto email system, to less secure systems such as Google mail, Hotmail, etc. As the practice of transferring email to an out-sourced solution already exists within the student population, the requirement for risk mitigation will be driven primarily by the data and usage requirements of official communications by the University of Toronto.

University of Toronto Data Usage

The University of Toronto currently uses email to communicate with students to achieve a variety of purposes: Communication in regards to accommodation of disabilities; academic censure, standing, and marks; financial matters; updates of personal / contact information; course requirements; and response to general queries. Given that these communications all take place via email, and that email between students is not separated from email between students and the University, all email must be regarded as being as sensitive as the most confidential of these communications. The sensitivities are as follows:

1. Communication in regards to accommodation of disabilities: Personally identifiable and health-related information - PHIPPA protected.

2. Academic censure, standing and marks; and, personal/contact information: Personally identifiable information - FIPPA protected.

Aggregate Sensitivity

Unless alternative arrangements are made in the handling of PHIPPA/FIPPA protected data, all email must be considered confidential and must be encrypted outside of the University of Toronto network. If PHIPPA/FIPPA protected data is removed from email sent by the University to students, while potentially private in nature from a student's point of view, the content of email is no longer classified by the University as confidential; while still requiring adequate access controls, non-confidential data does not require encryption outside of the University network.

Threat Scenarios

Threats in an email environment are many and varied, but are primarily the following:

1. Inappropriate access (disclosure / duplication / modification / deletion) to / of individual accounts
2. Loss of data in bulk
3. Loss of service
4. Lack of accountability for use

Given that each system under consideration provides the same basic functionality, using the same information (and absent system-specific architectural information), the threats to information are the same across all solutions.

Vulnerability Scenarios

System-specific vulnerabilities will be detailed after technology-level vendor discussions. Broadly speaking, vulnerabilities can be characterized as residing in the following areas:

Identification

In email, access identification is often the same as, or a portion of, a user's email address, which is communicated in clear text as part of the body of an email message; as such, access identifiers are low-sensitivity data, and the risk due to disclosure of access identifiers is low.

Authentication

Access credentials can be observed in transit, recovered from storage / memory, captured when input, or retrieved by administrators. As access credentials (i.e. passwords) are typically re-used many times before refresh, and provide full access to users' data when used in combination with easily-guessed access identifiers, access credentials are considered high-sensitivity data. As such, they must be protected from disclosure while in storage, transmission, use and administration.

Authorization

Account permissions are typically stored and administered by the service - vulnerabilities to account permissions are associated with vulnerabilities to system administrator access (Identification, Authentication and Monitoring). Management of system administrator-level vulnerabilities are tied to the reputational risk to the service vendor (discussed below, under 'Recommendations').

Isolation

In the absence of having unauthorized access to Identification and Authentication credentials, attempts may be made to circumvent access controls (typically through software vulnerabilities and / or social engineering attacks), so that possession of such credentials is not required to achieve unauthorized access to data. Management of access control-circumvention vulnerabilities are tied to the reputational risk to the service vendor (discussed below, under 'Recommendations').

Continuity

Loss of access to data may be temporary or permanent, depending on the vulnerability exploited. Management of continuity-level vulnerabilities are tied to the reputational risk to the service vendor (discussed below, under 'Recommendations').

Monitoring

Failure to monitor system and user activity severely limits the ability to trace / detect unauthorized service use, or attempts to circumvent access controls. Both Microsoft's and Google's solutions offer the University of Toronto the ability to provide its own activity monitoring, which is a requirement of the completed service architecture.

Risk Management Options

The Privacy Commissioner for Ontario has mandated that FIPPA and PHIPPA - protected data must be encrypted, when subject to risk of disclosure. Unless such information can be communicated to students other than via an outsourced email solution, that data must be encrypted - such an approach introduces issues of a technical nature, that are not currently fully resolved by currently available technical solutions. One possible alternative is to send notification of sensitive communications to students in an open email system, with the actual communication itself residing on a secure, University of Toronto - hosted and maintained system (such as Blackboard).

Exit Options

At the time of this writing, neither Microsoft nor Google explicitly support users exiting their service, they both do support account access via open standards such as POP and IMAP - conceivably an exit strategy could be built upon those protocols, allowing automated downloading of email data.

Residual Risks

All software has undiscovered weaknesses, and all procedures are subject to incomplete or non-observance; as such, risk is never completely eliminated. As well, the security of end-point devices is beyond the control of the on-line service provider; as such, unauthorized access to user accounts, singly or in bulk, should be anticipated.

Recommendations

Both vendors are subject to the provisions of the US PATRIOT act, however it is not clear, given reciprocal law-enforcement agreements between the United States and Canada, that hosting student email outside of Canada exposes that data to greater risk from governmental inquiry than at present. As the provision of web-based services is a large part of the business model for both firms, both firms are able to dedicate considerably more staff to the provision of a secure web-based service than any University or other educational institution; as such, the risk of unauthorized access due to technical or procedural vulnerabilities is likely to be less than at present.

Each platform offers sufficient functionality to satisfy the core requirements of the University of Toronto's intention to provide secure, reliable email to its students. As no security-level concerns invalidate either vendor, the decision between vendors will depend on additional functionality offerings, and, most importantly - as incident response depends on a vendor's willingness to engage - on the anticipated business relationship between the University of Toronto and the chosen vendor.