UNIVERSITY OF TORONTO

Threat / Risk Assessment

Student E-Communications Outsourcing Project

Martin Loeffler — Information Security, I+TS

Creation Date:	Version	1.0	April 07, 2010
Last Updated:	Version	2.1	June 03, 2011

Table of Contents

Executive Summary

After an evaluation of available out-sourced email hosting options, the University of Toronto has chosen to pursue an email hosting agreement with Microsoft, via their Live@EDU service. As a result of this choice, the University has worked with Microsoft to ensure, via a combination of discussion, testing, and visitation, that the security of the Live@EDU service not only meets the level of protection provided by the current internally-hosted email service, but improves upon it, such that current and future threats to the privacy and security of student email are mitigated to the fullest extent possible.

Sensitivity of Data to Risk

To clearly articulate risk to information, and inform choices for risk mitigation, 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. This analysis also encompasses all of the above for supporting access, change, continuity, and accountability control systems.

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; and
4. Lack of accountability for use.

Service Environments, Asset Classes, Security Requirements, and Data Contexts

There are three service environments in which risks maybe expressed for the Live@EDU service: on a client (student-facing) computer, within the University of Toronto network, and within the Live@EDU computing environment. Within these environments, there are three classes of data assets that require protection: Email, Client credentials, and Administrative credentials.

Within these three environments, security requirements of: confidentiality, integrity, availability and accountability for use of data must be satisfied while the data is in the following contexts: storage, transport, use and under administrative or privileged access.

Practically speaking, these security requirements appear in this environment as follows:

Client computer systems

1. Storage on client computer (for example: temporary files, saved drafts, etc.)
2. In transport between client computer and Live@EDU (via public and University-hosted networks).
3. In use on client computer (such as when creating email).
4. Administrative access on a client computer (for example, during maintenance, or during home use, when most computer users typically log in with full privileges).

5. Storage of email on client computers, both private and shared.
6. Transport of email between client computers and Live@EDU.
7. Use of email (for example: reading, editing, re-directing).
8. Administrative access to email (for example: local anti-virus or anti-spam filtering programs).

9. Storage of administrative credentials (such as a separate user ID and password for making changes to a home or lab computers), prior to use.
10. Transport of administrative credentials (such as when logging in remotely to manage a computer).
11. Use of administrative credentials (such as to apply software patches or upgrades to client systems).
12. Administration of administrative credentials (such as forced password aging, or to apply password quality guidelines (password size, complexity, history, etc.)

University of Toronto computer systems

1. Storage of student login credentials, prior to login by student.
2. Transport of student login credentials from student computer to UT systems.
3. Use of student login credentials by UT to authenticate student.
4. Administration of student login credentials by UT staff (enrolment, modification, and revocation of access)

5. Storage of email, sent to / received from client computers, Live@EDU, and third-party email systems.
6. Transport of email, sent to / received from client computers, Live@EDU, and third-party email systems.
7. Use of email, sent to / received from client computers, Live@EDU, and third-party email systems.
8. Administrative access to email, sent to / received from client computers, Live@EDU, and third-party email systems.

9. Storage of administrative credentials, prior to administrative activity.
10. Transport of administrative credentials (such as when logging in remotely to manage a computer).
11. Use of administrative credentials (such as to apply software patches or upgrades to client systems).
12. Administration of administrative credentials (such as forced password aging, or to apply password quality guidelines (password size, complexity, history, etc.)

Live@EDU computer systems

1. Storage of student login credentials, prior to login by student.
2. Transport of student login credentials from student computer to UT systems.
3. Use of student login credentials by UT to authenticate student.
4. Administration of student login credentials by UT staff (enrolment, modification, and revocation of access)

5. Storage of email, sent to / received from client computers, Live@EDU, and third-party email systems.
6. Transport of email, sent to / received from client computers, Live@EDU, and third-party email systems.
7. Use of email, sent to / received from client computers, Live@EDU, and third-party email systems.
8. Administrative access to email, sent to / received from client computers, Live@EDU, and third-party email systems.

9. Storage of administrative credentials, prior to administrative activity.
10. Transport of administrative credentials (such as when logging in remotely to manage a computer).
11. Use of administrative credentials (such as to apply software patches or upgrades to client systems).
12. Administration of administrative credentials (such as forced password aging, or to apply password quality guidelines (password size, complexity, history, etc.)

Security Requirements vs. Data Context Crosswalks

The Security Requirements vs. Data Context crosswalks match security requirements to data assets in all security contexts, for each service environment – one crosswalk per environment. Populating the crosswalk with security strategies, illustrates gaps in risk mitigation than need to be addressed; the fewer the gaps, the more robust the risk mitigation strategy.

This crosswalk assumes students are accessing the Live@EDU service via a web browser; due to the way in which Live@EDU handles client credentials, web-based connections offer the most options for protection of data and privacy, as opposed to the use of mobile phones and / or 'thick' (i.e. non-web browser based) clients.

Note: While the Live@EDU security policy is only available under NDA, Microsoft has publically announced that it follows, and is audited against, the ISO 27001:2005 standard.

<table>
<tr><th>Client Computing Systems Crosswalk</th><th></th><th>Storage</th><th>Transport</th><th>Use</th><th>Administration</th></tr>
<tr><td rowspan="3"></td><td>Confidentiality of Email</td><td rowspan="3">Students are advised to install an information security suite-type of application (including, at minimum: anti-virus, firewall, anti-spam and anti-phishing software components) to protect their data from unauthorized disclosure, alteration, or loss while stored on their personal computers.

Email should not be stored on shared computers (e.g. Lab or other public computers)</td><td colspan="2" rowspan="2">Communication between the web browser and the Live@EDU service is encrypted at all times.</td><td rowspan="3">Students and other personal computer users should take care not to use their computer with administrative privileges turned on, as that increases the potential for viruses and other hostile code to contaminate the user's computer.

While</td></tr>
<tr><td>Integrity of Email</td></tr>
<tr><td>Availability of Email</td><td colspan="2">The availability of the connection between a web browser and the Live@EDU service is limited by local Internet Service Provider reliability, and other technical issues outside of the control of the Live@EDU, or University of Toronto computing systems.

Users may download email to their computer; this is not recommended, as storing email locally introduces risks to confidentiality and integrity of the email.</td></tr>
<tr><td></td><td>Accountability for use of Email</td><td colspan="3">The University of Toronto Shibboleth authentication service keeps a record of the last time and date an account successfully authenticated.</td><td>Students and other personal computer users are advised to lock their personal computers when not in use, with a difficult to guess</td></tr>
</table>

				password.
	Confidentiality of User Credentials	Students are advised not to share the passwords for their personal computer accounts, or cache them in their web browser, especially in shared environments.	Communication between the web browser and user authentication services at the University of Toronto is encrypted at all times.	Students and other personal computer users should take care not to use their computer with administrative privileges turned on, as that increases the potential for viruses and other hostile code to contaminate the user's computer.
	Integrity of User Credentials	Students are advised to install an information security suite-type of application (including, at minimum: anti-virus, firewall, anti-spam and anti-phishing software components) to protect their data from unauthorized disclosure, alteration, or loss while stored on their personal computers.		
	Availability of User Credentials		The availability of the connection between a web browser and the Live@EDU service is limited by local Internet Service Provider reliability, and other technical issues outside of the control of the Live@EDU, or University of Toronto computing systems.	
	Accountability for use of User Credentials		Last times and dates of user logins are stored within the University of Toronto's Shibboleth service.	Students and other personal computer users are advised to lock their computers when not in use, with a difficult to guess password.
	Confidentiality of Administrative Credentials	Students are advised not to share the passwords for their personal computer administrative accounts, if such exist. Administrative accounts should have long, complex passwords, that are difficult to guess (pass-phrases are ideal for this purpose).	Students, and other personal computer users, are advised not to remotely connect to their computers using administrator-level credentials, and to use encryption at all times, if connecting remotely to their personal computers.	Students are advised not to share the passwords for their personal computer administrative accounts, if such exist. Administrative accounts should have long, complex passwords, that are difficult to guess (pass-phrases are ideal for this purpose). In addition, Students are advised to install an information security suite-type of application (including, at minimum: anti-virus, firewall, anti-spam and anti-phishing software components) to protect their data from unauthorized disclosure, alteration, or loss while stored on their personal computers.
	Integrity of Administrative Credentials			
	Availability of Administrative Credentials			
	Accountability for use of Administrative Credentials			

		In addition, Students are advised to install an information security suite-type of application (including, at minimum: anti-virus, firewall, anti-spam and anti-phishing software components) to protect their data from unauthorized disclosure, alteration, or loss while stored on their personal computers.		

University of Toronto Computing Systems Crosswalk		Storage	Transport	Use	Administration
	Confidentiality of Email	The University of Toronto will not be storing student email – staff and faculty email will continue to be stored on existing, legacy systems. Students should take care not to download and store email on common-use computers in the University environment.	All mail transported between the University of Toronto and Microsoft will be encrypted via Microsoft's FOPE ("Forefront Online Protection for Exchange") service.	Reading and composition of student email will be performed in direct connection with Live@EDU environment; Students should take care to only access Live@EDU from trusted (i.e. computers with the latest operating system patches and current anti-virus software installed and running) workstations or personal computers	The University of Toronto is working to establish permissions within the Live@EDU system that minimize access by UofT administrative staff to email stored within the Live@EDU environment.
	Integrity of Email	The University of Toronto will not be storing student email – staff and faculty email will continue to be stored on existing, legacy systems.			The University of Toronto will not be storing student email – staff and faculty email will continue to be stored on existing, legacy systems.
	Availability of Email		While the University of Toronto does not store student email, student email passes through UofT systems before	Reading and composition of student email will be performed in direct connection with Live@EDU environment, and is not stored on	

			reaching Live@EDU. The UofT is upgrading its core network to provide connection redundancy, however is still subject to external network service provider failures.	any UofT system.	
	Accountability for use of Email	The University of Toronto Shibboleth authentication service keeps a record of the last time and date an account successfully authenticated.	All access to email stored within the Live@EDU service is via encrypted connection	The University of Toronto Shibboleth authentication service keeps a record of the last time and date an account successfully authenticated.	
	Confidentiality of User Credentials Integrity of User Credentials	University of Toronto servers are managed to a security baseline to minimize risk of compromise (see Appendix A – Information Security Baseline)	Network communication between clients and UofT for the purpose of authentication is always encrypted.	Both the University of Toronto and Microsoft filter mail traffic for viruses and spam, which include phishing attacks – attempts to solicit user credentials through trickery and fraudulent emails.	University of Toronto servers are managed to a security baseline to minimize risk of compromise (see Appendix A – Information Security Baseline)
	Availability of User Credentials	User authentication is performed by the Shibboleth user authentication service. This service has been implemented in a logically redundant way, so that if one virtual server fails, a backup is ready behind a load balancer. Availability of this service is subject to potential failures in infrastructure and intervening networks.			
	Accountability for use of User Credentials	The University of Toronto Shibboleth authentication service keeps a record of the last time and date an account successfully authenticated.			
	Confidentiality of Administrative Credentials Integrity of Administrative Credentials	University of Toronto servers are managed to a security baseline to minimize risk of compromise (see Appendix A – Information	Traffic is encrypted at all times between client computers and the University of Toronto's authentication service.	University of Toronto servers are managed to a security baseline to minimize risk of compromise (see Appendix A – Information Security Baseline)	

		Security Baseline)		
	Availability of Administrative Credentials	Availability of this service is subject to potential failures in infrastructure and intervening networks, however a failure of administrative access is unlikely to affect client access to the Live@EDU service, unless un-remedied for a significant period of time.		
	Accountability for use of Administrative Credentials	The University of Toronto records successful administrative user authentications.		

Live@EDU Computing Systems Crosswalk		**Storage**	**Transport**	**Use**	**Administration**
	Confidentiality of Email	Live@EDU facilities and services are protected as detailed in Microsoft's internal security standard, which meet or surpass the University of Toronto's security standards. Compliance with these internal standards are verified by annual SAS70-II audit, however the standard itself is protected by NDA ("Non-Disclosure Agreement") and cannot be published but the University. Attestations made in Microsoft's internal security standard were verified by a physical inspection of the Microsoft Chicago data centre.	All mail transported between the University of Toronto and Microsoft will be encrypted via Microsoft's FOPE ("Forefront Online Protection for Exchange") service.	Live@EDU facilities and services are protected as detailed in Microsoft's internal security standard, which meet or surpass the University of Toronto's security standards. Compliance with these internal standards are verified by annual SAS70-II audit, however the standard itself is protected by NDA ("Non-Disclosure Agreement") and cannot be published but the University. Attestations made in Microsoft's internal security standard were verified by a physical inspection of the Microsoft Chicago data centre.	
	Integrity of Email				
	Availability of Email		Microsoft's network, while robust and redundant, is still subject to outages due to external network service provider failures.		
	Accountability for use of Email	Microsoft provides an interface where their "PowerScript"	All mail transported between the University of Toronto and	Microsoft provides an interface where their "PowerScript" scripting language can generate reports of when a Microsoft administrator accesses an email box other than their own.	

		scripting language can generate reports of when a Microsoft administrator accesses an email box other than their own.	Microsoft will be encrypted via Microsoft's FOPE ("Forefront Online Protection for Exchange") service.		
	Confidentiality of User Credentials	In the case of web-only access, Microsoft does not receive user credentials. When using a non-web client (such as Outlook), credentials are protected by Microsoft's internal security standards. Users are strongly advised to connect to Live@EDU via web-browser only, as rich-client based authentication requires that user credentials be divulged to the Live@EDU service.			
	Integrity of User Credentials				
	Availability of User Credentials				
	Accountability for use of User Credentials	For all instances of user authentication, a record is kept at the University of Toronto.			
	Confidentiality of Administrative Credentials	Administrative access to the Live@EDU facilities and services are protected as detailed in Microsoft's internal security standard, which meet or surpass the University of Toronto's security standards. Compliance with these internal standards are verified by annual SAS70-II audit, however the standard itself is protected by NDA ("Non-Disclosure Agreement") and cannot be published but the University. Attestations made in Microsoft's internal security standard were verified by a physical inspection of the Microsoft Chicago data centre			
	Integrity of Administrative Credentials				
	Availability of Administrative Credentials				
	Accountability for use of Administrative Credentials				

Risk Management Options

In summary, the following technologies will be used to achieve each of the above functional requirements:

Identification and Authentication

1. Web clients are identified and authenticated via Shibboleth, which does not require divulging user credentials to the Live@EDU service.

2. Rich clients, while needing to divulge their credentials to Live@EDU, are forced to use encrypted versions of their authentication protocols

3. Administrators of both the Live@EDU and UofT services are required to authenticate securely, and their credentials are protected by their respective institutions' security standards

Authorization

1. Individual account permissions are managed by the Live@EDU authorization system.

2. Administrative roles and responsibilities are managed through the same authorization system – the University of Toronto is working to define administrative roles that provide administrators with a minimum of access to users' email.

3. Live@EDU users are strongly encouraged to protect their own computers by use of strong passwords.

Isolation

1. Data – whether email or authentication traffic – is encrypted at all times between the University of Toronto and the Live@EDU service.

2. Physical media does not leave the Microsoft environment; systems are physically protected through a robust and redundant variety of standard physical barriers.

3. Both UofT and Live@EDU systems are protected from hostile Internet traffic through industry-standard technologies, such as firewalls, intrusion-prevention systems, and system hardening procedures.

4. Live@EDU users are strongly encouraged to protect their own computers with security software that includes, but is not limited to a personal software firewall and anti-virus software. Users are further encouraged to apply vendor-supplied patches as soon as they are available.

Continuity

1. Both Live@EDU and University of Toronto services are robust and redundant in design.

2. Both Live@EDU and University of Toronto services, however, are subject to potential service outages from intervening network service providers – this is an exposure that all users of the Internet are vulnerable to, given the shared nature of the Internet.

Monitoring

1. The University of Toronto keeps a log of all successful authentications against its Shibboleth service.

2. The University of Toronto keeps a log of all successful authentications by administrative users.

3. Activity within the Live@EDU service may be monitored through PowerShell scripts.

Privacy Impact Assessment

1. Please refer to the document: "**Privacy Impact Assessment** Student E-Communications Outsourcing Project" for a full discussion of privacy in the context of the Live@EDU service.

Exit Options

1. The University of Toronto has exit options available to it, should the Live@EDU service prove unsatisfactory for whatever reason, such that user data can be fully recovered and migrated to another service provider, or back under the direct administration of the University if so desired.

Residual Risks

1. All software has undiscovered weaknesses, and all procedures are subject to incomplete or non-observance; as such, risk is never completely eliminated. External testing of security measures is essential to minimize growing risk exposure, but a risk of service compromise will always exist.
2. The security of end-point devices is beyond the control of the University or any external service provider; as such, unauthorized access to user accounts, singly or in bulk, should be anticipated (potentially due to phishing attacks, viruses, or other anti-social online activity yet to be developed), and remediation exercises planed / practiced.
3. Microsoft's Live@EDU service is subject to the provisions of the US PATRIOT act. However, given reciprocal law-enforcement agreements between the United States and Canada, hosting student email outside of Canada does not expose that data to any greater risk from governmental inquiry than were it to reside entirely in Canada.
4. IT staff are as human as the users of an IT service, and as such the possibility remains of mis-use of the authority and access afforded to such staff to enable them to perform the job duties. All IT systems are subject to this exposure, which is best dealt with through sound hiring, security, and service monitoring practices.
5. The business relationship between the University and Microsoft may change such that continuing to participate in an out-sourced email service may become unappealing to either or both of the parties. The University should be prepared to examine alternatives in such an eventuality, including the re-insourcing of email services, should that be the best alternative.

Recommendations

The security – both physical and logical – applied by Microsoft provides risk mitigation every bit as good as, and in many ways better, than what currently is provided by the University of Toronto to any of the University's many email systems. As such, a decision to proceed to out-source the provision of email services to Live@EDU (and any service that may succeed Live@EDU, provided it maintain the same high level of security preparedness of Live@EDU), will accrue a net security benefit to the University, with an investment of time and effort considerably less than that required for the University to provide the same benefit in-house. That said, there are a number of observations that came out of the process of pursuing the Live@EDU service:

1. It would have been desirable to have been able to publically discuss Microsoft's security policies and practices – nothing is gained by obscuring the broad principles and efforts an organization makes towards risk management, and in fact may impart a false sense of security in the mistaken belief that such action genuinely keeps information from being leaked. The advantage, had we been free to openly discuss Microsoft's security posture, would have led to a broader security discussion, and a more informed decision on behalf of our constituents.

2. It was clear during all discussions with Microsoft that the business relationship was key, and that near-constant contact was required to ensure that matters of service implementation were successfully resolved to the University's satisfaction – the University must be prepared to sustain this level of collaborative effort, as the greater part of the potential of the Live@EDU (and subsequently the Office 365) service is yet to be realized, and will not be realized without such effort.
3. In comparison to the near-universal practice of commercial IT service providers, the University of Toronto does not engage external security vulnerability testing. While the University does not have any reason to believe its information systems are insufficiently protected, it is recommended that the University develop a regular, formalized, network and IT service vulnerability scanning practice in support of our obligations as customers of Live@EDU. This practice may be more economical to develop internally than to source externally, while providing the same value.
4. The University should consider maintaining a core of knowledge about the management and provision of email services, should the University ever decide that re-insourcing emails services is an attractive option.

Appendix A – Security Baseline

University of Toronto servers are compliant with the following Information Security Baseline practices:

http://www.its.utoronto.ca/rules-and-regulations/regulations_guidelines/informationsecurity/Security_Baseline.htm

Certain practices have become de facto requirements for the protection of data. These practices constitute what is considered to be a managed security baseline:

1. *Prompt installation of vendors' software updates to correct known vulnerabilities.*
2. *Installation and regular update of anti-virus software.*
3. *Encryption of confidential information on devices that are physically insecure, or not under the University of Toronto's control [see the I+TS Full Disk Encryption website]*
4. *Encryption of network communications, such that user credentials and other confidential information are not visible in transit over insecure networks.*
5. *Protection of networked devices via firewalls.*
6. *Education of administrators and users as to best practices for protecting data while in storage, use and communication.*
7. *Physical protection of resources that restricts removal by unauthorized persons.*
8. *Back up of critical data, with backups tested for readability and protected to the same level as data that is in use.*
9. *Effective and practiced incident response procedures, including (but not limited to): monitoring of, and response to unauthorized access to systems and data.*
10. *Disabling un-needed network services.*
11. *Deletion of 'guest' or non-password protected accounts.*
12. *Choosing security settings that are more strict than typically insecure default values, and changing default passwords.*

For a system to be considered secure, it must have applied the above security practices with a timeliness and effectiveness that reflects the sensitivity of information stored / communicated by the system.

This list of specific practices will be updated as technologies and risk management practices mature; these updates will be communicated to the University of Toronto Information Technology support community.

For guidance on what uses of information and communication technology are considered appropriate, please refer to the policy: "Appropriate use of Information and Communication Technology"

Where specific technologies, exposure, or assets mandate additional protections be followed (for example, two-factor authentication), those protections are followed in addition to the above practices.