Where to start with risk?

1. Phishing & Social Engineering

2. User Awareness, Education, Training

Ref: https://er.educause.edu/articles/2017/1/information-security-risky-business
Infosec Awareness & Education Program

• Faculty, students, admin and technical staff.
• Phishing test campaigns
• Social media, website communications, Managing Digital Footprint presentation
• Initiate and participate in the October cyber-security events.
• securitymatters.utoronto.ca
securitymatters.utoronto.ca

Devices: software maintenance, loss of device

Data Protection & Hygiene: sharing data, working off-site

Password Management: strength, UTORid management
Info, self serve password reset:

https://www.utorid.utoronto.ca/cgi-bin/utorid/acctrecovery.pl
U of T Phish Testing Stats

Initial Tests
• Staff (with pre-awareness) fail rate: 10 - 15%
• Staff (w/o pre-awareness) fail rate: 30%

Subsequent Tests
• Staff fail rate: 3 - 7%

Testing measures include checking for opening, link clicking and data entry.
Security Planner

• Advice for users delivered using a point-and-click app.
• From Citizen Lab
• Help with devices, email, social media, online shopping.
• https://securityplanner.org
Privacy and Information Security Compliance

FIPPA: www.fippa.utoronto.ca
PHIPA: www.ipc.on.ca/health/collection-use-and-disclosure-personal-health-information
CASL: fightspam.gc.ca
PCI-DSS: www.pcisecuritystandards.org/pci_security

Influencers: PIPEDA, GDPR
Aside: General Data Protection Regulation (GDPR)

• Affects data usage for EU residents outside of EU
• Stricter consent requirements
• Short timeline for breach reporting (72 hours)
• Right to be forgotten
• U of T implications

• More information: https://nyti.ms/2Lq0rAC
Information Security Governance at U of T

- Policy on Information Security and the Protection of Digital Assets
- Creation of Information Security Council (CIO Bo Wandschneider)
  - Co-chairs: Ron Deibert (Citizen Lab) and CISO
  - Membership made up of faculty, staff, student
- Five WGs: Incident Response, Standards Guidelines Procedures, Education & Awareness, Risk & Compliance Metrics & Reporting, Research

http://main.its.utoronto.ca/news/newly-formed-information-security-council/
What It Means

- Clear guidance (mandated in some cases) on the design, deployment and operation of online services.
- Classification of data into categories that dictate handling.
- Increasing tendency to using services that ‘comply’ rather than build from scratch.
- Wider awareness about what to do in the event of a compromise, malware attack, or breach.
What It Doesn’t Mean

• Loss of ability to innovate.
• There will be no malware or phishing attacks or data loss.
Awareness and Education – Part 2
Faculty/Staff/Student Info

• USB storage device encryption for Windows, file/folder for MacOS
• Password Managers
• Trusted source for popular tools, utilities
• Separate browsers for banking and recreational use
• Stand-alone desktop/laptop configuration
• backups
• Collaborative effort?
Office 365

Email Attachment Sharing:
• Share with U of T faculty/staff/students, external, non-O365 users
• Don’t want to share, remove permissions or rename the file.

One Drive Sharing:
• User configuration of access to docs, view ‘who and when’ contents accessed.
• Convenient as Dropbox with more control and protection
# Office 365 - Data Storage and Sharing

What data can I store/share on OneDrive/SharePoint/Teams?

<table>
<thead>
<tr>
<th>Data Classification (provisional)</th>
<th>Infosec Controls</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Service*</td>
<td>Course info., research publications</td>
</tr>
<tr>
<td>Confidential</td>
<td>Service, access control**</td>
<td>PII, single person account info.</td>
</tr>
<tr>
<td>Restricted</td>
<td>Service, access control***</td>
<td>PHIPA, PCI-DSS, data aggregate</td>
</tr>
</tbody>
</table>

* Service: security controls concerned with system hardware, operating systems, middleware and logging/audit.

** Access Control: one/two factor authentication, user authorization

*** Access Control: two factor authentication, user authorization
Awareness and Education – Part 2

Service Architecture

- Data security management applies to both on-prem & cloud.
- Logs and audit capability
- Browsers or rich clients?
- Integration with UTORid authentication and authorization.

Ack: Chart from Microsoft
Architecture

• A broad topic and a key aspect in addressing information security (infosec: built in not bolted on).
• At U of T today:
  • Design or procure services with lifecycle in mind - hardware, operating system, networking, security services, middleware. EIS private cloud/systems services.
  • Sharing of enterprise data with units
  • Application software – custom or purchased?
  • Interface with authentication/authorization – UTORauth
Architecture – Getting Complex...

- Production Zone
- Quality Assurance Zone
- Development Zone

- Presentation Tier
- Application Tier
- Database Tier
- UTORauth Authentication & Authorization
Web Services

• High rate of compromise: content managers (WordPress, Drupal), web development platforms (PHP, Java-Struts).
• Cause: software versions not up-to-date, not patched, plugins obtained from questionable sources.
• Solution: Manage professionally, use web application firewall, use deep packet inspection firewall or intrusion prevention system.
Application Development

- review security documentation for platforms.
- Follow secure coding practices eg. input validation
- Use code analysis tools eg. HP Fortify
- For web programming, OWASP Top 10.
- Check web apps on deployment and periodically using a web vulnerability scanner.

- security.admin@utoronto.ca
A little humour...

https://www.youtube.com/watch?v=Usq3SO_Fvjg

Acknowledgement to Cisco
Information Security Operations
Information Security Risk Assessment

• New or existing project/service, procurement, unit assessment

• Process: gather information via questionnaires/interviews, assess and document risks and mitigations

• Deliverables: identify risks and mitigations for project owners, business managers, enhance awareness

• U of T questionnaire, HECVAT docs – have a look!
• ISEA staff can provide training

isea.utoronto.ca
Detection, Analysis, Response

Suspicious Devices

• U of T devices detected via threat intel from outbound traffic
• Top causes: phishing, URL analysis, remote access, dynamic DNS
• Response: daily dept. IT notification
• Risk: BYOD represents majority of compromised devices.
• Mitigation: endpoint protection, network segmentation

Data: 6 months of daily measurements Mar-Sept 2017
Detection, Analysis, Response

Suspicious UTORid Accounts

- Suspicious location and geo-diverse logins
- One characteristic: compromised password
- Response: ISEA prioritizes events, resets password
- Risk: Individual impact
- Mitigation: awareness/education, UTORid self-serve password reset

Data: 6 months of daily measurements Mar-Sept 2017
Detection, Analysis, Response

Vulnerability Detection

- Monthly network scan.
- Highest Risk Score
- Response: Tenanted reporting to depts.
- Risk: Substantial
- Mitigation: month-to-month reporting, enforcement.
- Contact: security.admin@utoronto.ca

Data: May 7, 2018 scan
Detection, Analysis, Response

Automated Response

- High confidence access attempts 10K–50K/day.
- Response: Automatic quarantine 1hr–14 days.

Data: 6 months of daily measurements Mar-Sept 2017

isea.utoronto.ca
Detection, Analysis, Response

• Security Information and Events Monitor (SIEM) is the central hub for gathering data, normalization, analytics, and reporting.
• Automation is a huge aid, expertise is needed to identify areas ripe for automation.

Priorities:
• Move from point-service to integrated analysis
• Add services, enhance analysis capability
• Add tenanting
Identity and Access Management

- UTORauth is a key source of data for infosec operations – authentication and authorization.
- Services:
  - UTORid account creation/lifecycle
  - UTORid standard and high assurance authentication (password and eToken)
  - webSSO, UTORauth attribute directory, Grouper
Identity and Access Management

Priorities:

• Improve UTORid password status: detect/update ‘old’ passwords.
• Expand use of multifactor authentication
• Add support for OAuth2, OpenID Connect

Self Serve Password Reset Enrolment:

https://www.utorid.utoronto.ca/cgi-bin/utorid/acctrecovery.pl
Enterprise Active Directory

• Primary role in UTORauth identity and access management and account synchronization with Office 365.
• Departments use the one-way-trust feature to get access to UTORid accounts and password login.
• Uptake on ‘single forest, single domain, multiple OU’ is slow.
• New technologies on the scene: InTune

Priorities:
• Review Active Directory usage/risks, impact of InTune

isea.utoronto.ca
Thanks.

mike.wiseman@utoronto.ca

Image acknowledgement:

www.shutterstock.com
sdhrconsulting.com