Research Ethics Board
Privacy and Data Security Workshop

Data Security Talk

Agenda

- Context
- Risk & Compliance – the drivers behind information security
- Data Protection
- Infrastructure
- Awareness
- Incident Response Plan

Context on Threats and Compromise

- Quarantine 25-50K external IP addresses/day
- Detect 10-30 suspicious internal devices/day
- Detect 5-10 suspicious UTORid accounts/day
- Highest risk services : web content managers, websites

- Marriott breach: 500 million over 4 years
- Amazon (customer names/email addresses)

Risk & Compliance

Definition of Risk:

"Risk is a function of the likelihood of a given threat-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organization[1]."

[1] National Institute of Standards and Technology SP 800-30

Risk & Compliance

Compliance implies adherence to published standards, controls and guidelines.

- Reduces (not eliminates) the effort needed to evaluate risk.

FIPPA

- Ontario government privacy regulation that covers data protection at the University.
- Specifics regarding the collection, use, protection and retention of data.
- Data used in research activities specifically addressed.

Risk & Compliance

PHIPA

Requirements for:

- breach notification capability to ‘custodian’ and periodic reporting of breach history, access management, logging, auditing and monitoring.

Recommendations:

- If you’re a custodian, develop practices and procedures. Be prepared to show them and they’re implemented.
- If you’re working with a custodian, ensure you’re aware of the practices and policies.
- If you’re not sure, get a risk assessment.

Risk & Compliance

NIH Genomic Data Sharing Requirements: checklist and sign-off

Compute Canada, Tri-Council are publishing data security standards and guidelines.

University of Toronto: Information Security Council, working groups for: Procedures, Standards, & Guidelines, Risk and Compliance, Incident Response, Education and Awareness, **Research!**

Final thought: Dealing with compliance is not new to research, biology and nuclear research and laboratory practices are heavily regulated. Infosec compliance efforts will only increase.

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 Isaac Straley, CISO
- Membership made up of faculty, staff, students
- Five WGs: Incident Response, Standards Guidelines Procedures, Education & Awareness, Risk & Compliance Metrics & Reporting, Research

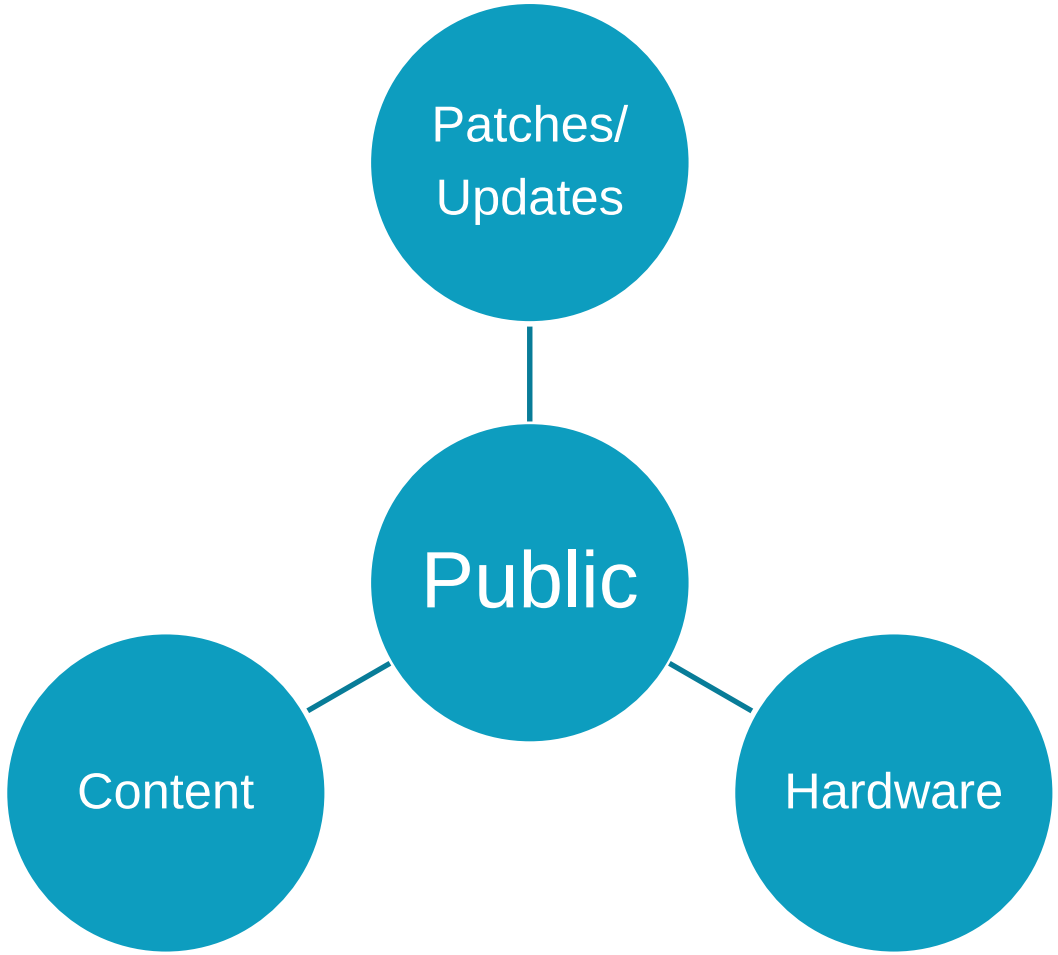
http://main.its.utoronto.ca/news/newly-formed-information-security-council/

Data Protection

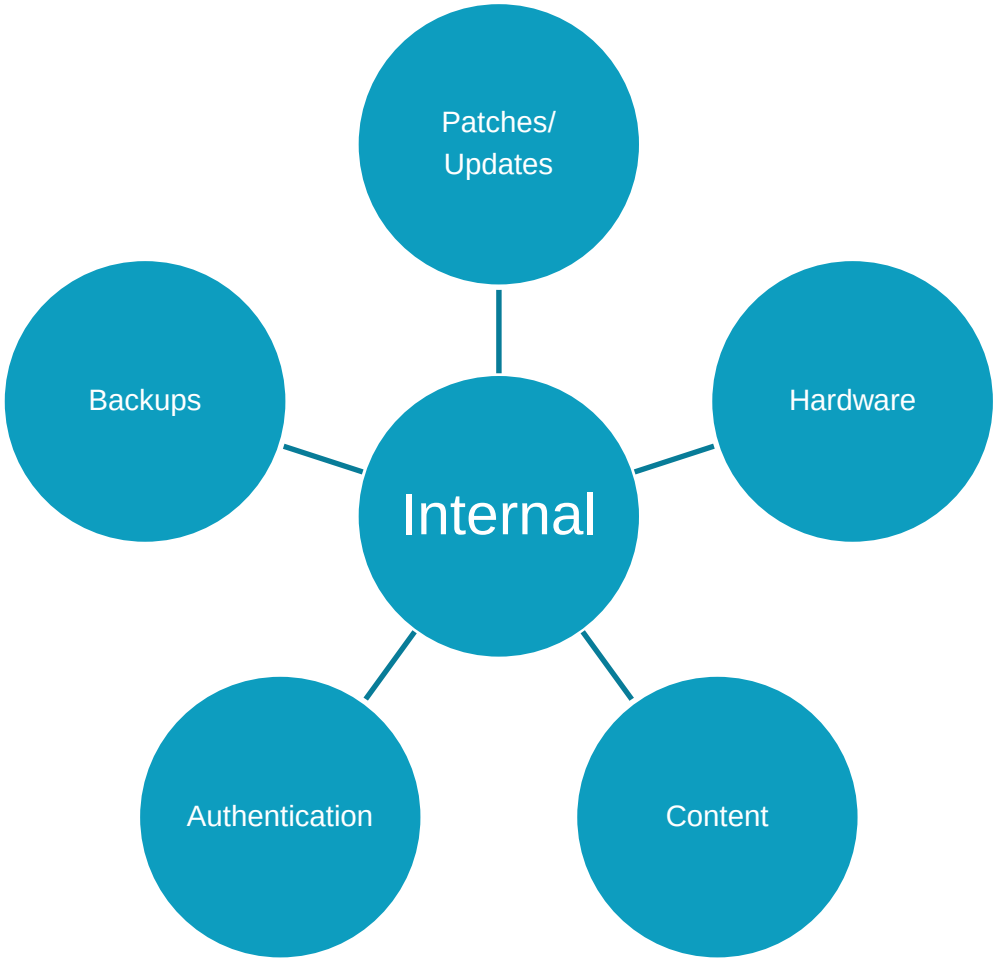
Data Security plans consist of:

- Data Classification (“public”, “internal”, “protected”)
- Standards and guidelines with controls that are proportional in strength to the classification.

Data Protection



Data Protection



Data Protection

Data Protection - Tips

- Encrypt USB drives on Microsoft Windows:

https://isea.utoronto.ca/infotip-encrypting-usb-drives-using-bitlocker/

- Encrypt USB drives on MacOS:

https://isea.utoronto.ca/infotip-encrypting-usb-drives-on-macos/

- Encrypt files on MacOS:

https://isea.utoronto.ca/infotip-encrypting-files-on-macos/

Data and Media Destruction

- File deletion on a device is not enough to guarantee inaccessibility, media must be considered.
- Magnetic devices: degausser + physical destruction OR full disk encryption
- Solid state drive: write random data pattern
- USB device: encryption
- Paper: cross cut shredder
- Cloud storage: don't use for 'protected' classification, O365 AIP, other tools for user-managed encryption of local/cloud storage, eg. Cryptomator, Boxcryptor.
- Encryption consideration: key management

Travelling and Data Protection

- Devices should not contain valuable or private data, access desired information remotely over the network at your destination.
- Be careful using wifi – all client software should use encrypted network communication.
- Disable Bluetooth if not in use

Data Sharing – O365

Office 365 can be used to share public and internal data. ‘protected’ data as covered by PHIPA or risk assessment should not be used until additional controls are available – eg. multi-factor authentication.

Data Classification	Infosec Controls	Examples
Public	Service*	Course info., research publications
Internal	Service, access control**	Research data
Protected	Service, access control***	PHIPA, PCI-DSS, data aggregate

* Service: security controls concerned with system hardware, operating systems, middleware.
** Access Control: one/two factor authentication, user authorization
*** Access Control: two factor authentication, user authorization

Data Sharing – O365 Tips

Office 365 for email, sharing files internally/externally, group collaboration

is more secure than

other cloud providers. Why? :

- Integration with internal authentication
- Logging, auditing, troubleshooting, recovery
- Internal support

Data Sharing – O365 Tips

- Share email attachments and OneDrive files internally: add or delete recipients to share with,
- Share email attachments and OneDrive files externally: remove or delete OneDrive file to stop sharing
- OneDrive files can be shared internally and externally.
- Access details (who and when) of local files is available.

Coming Soon:

- better controls for sharing externally: password assignment and auto time-limits for access
- Advanced Information Protection (AIP): ability to classify data on the Microsoft tools. ‘public’, ‘confidential’, ‘protected’.

Data Sharing – Email

Using email for exchange of sensitive or valuable information:

- Build trust with the recipient – have ‘starter’ email conversations, make a telephone call, encourage people to check with you to validate your email
- Use your University account for research communications
- Use a separate account or mailbox for your social or private email

Infrastructure

- Servers, storage: availability – backups, test restore.
- Network: firewall, remote access, intrusion detection
- Operating Systems and middleware: manageability, patching, updating, web servers,
- Application development: software coding practice, maintenance
- Tips:
  - Use services that are recommended and compliant with University recommendations.
  - Get professional assistance.

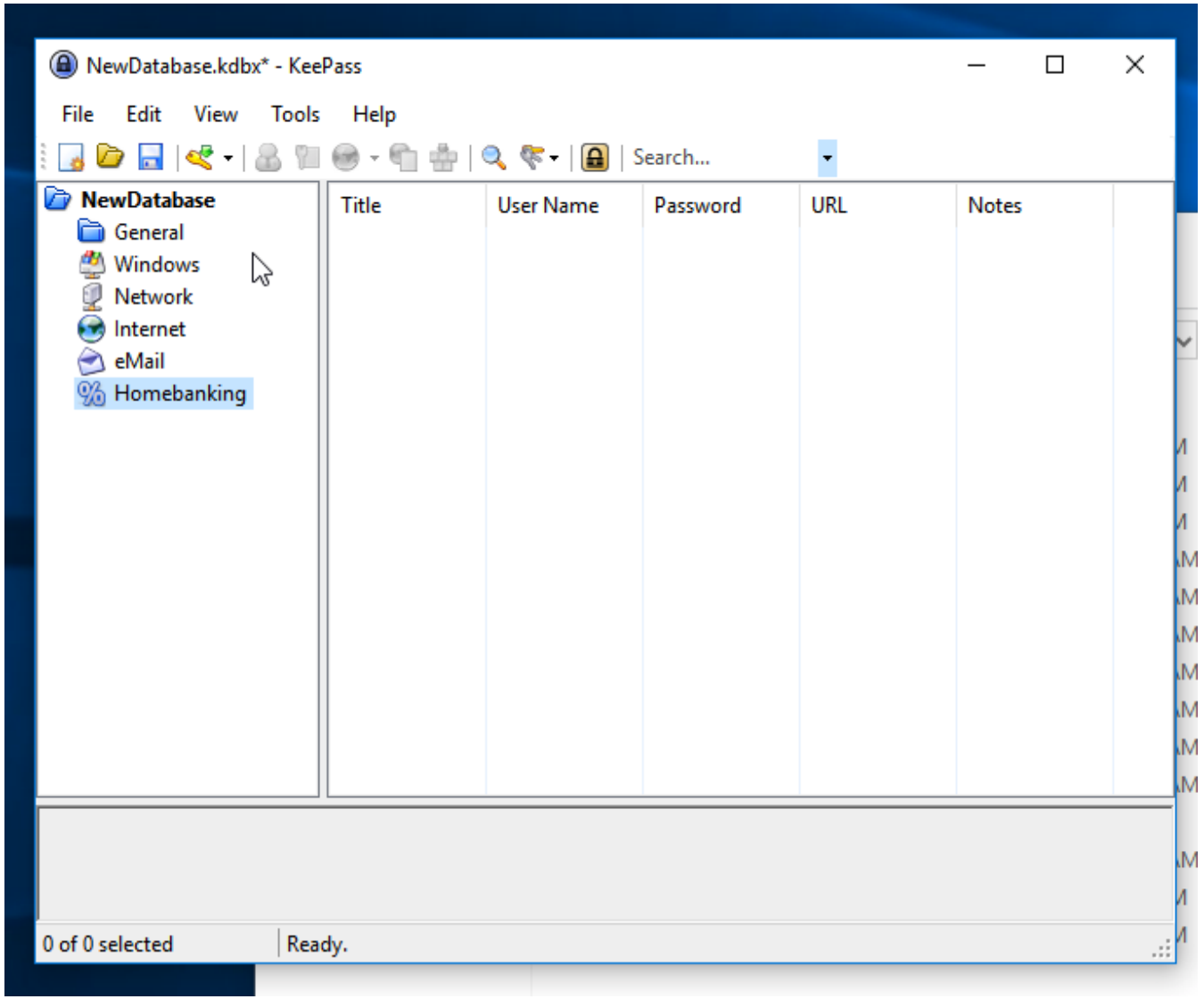
Personal Device Security

- Patching and updating device software.
- Verify the source of open-source or community-licensed software.
- Mobile devices: use a strong password, turn storage encryption on.
- Use separate work and leisure devices.
- Use separate browsers for work and leisure.
- Give each person a unique account on a device – don’t share accounts or passwords.

Passwords

- Use a password manager.

https://isea.utoronto.ca/infotip-using-a-password-manager/



Your UTORid Account

- Register for Self Serve Password Reset:

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

- Change your UTORid password:

https://www.utorid.utoronto.ca/cgi-bin/utorid/changepw.pl

Awareness to Prevent Compromise

Phishing/malware in email is a primary vector to obtain login credentials and compromise devices.

- Phishing is targeted. Validate received email – call the sender, send a separate message to obtain confirmation
- ‘mouse-over’ hyperlinks to examine hostnames – do they make sense?
- Investigate suspicious attachments or URLs using ‘virustotal.com’. **
- Don’t use untrusted portable storage.
- Have a backup of valuable data (suggestion: Acronis.com)
- Have a plan with steps to take if compromise occurs

Incident Response Plan – Keep Handy

- Don’t hesitate to seek assistance.
- Report the incident.
  - Call tech support.
  - Email to security.response@utoronto.ca to report and for compromise response help.
  - Contact FOIL for data breach assistance.
- Be prepared to restore devices from scratch – recover from backups.
- Avoid interacting with perpetrators, paying ransom.

Thanks.

mike.wiseman@utoronto.ca