BCNET CONNECT

HIGHER ED & RESEARCH TECH SUMMIT

Risk Assessment for SaaS and Cloud Services

March 9, 2022

We are…

BCIT :	Nthusi Kaisara, Cyber Security
Langara:	Joanne Rajotte, Privacy
	Isabel Wong, Infrastructure
UBC:	Robert Tremonti, Privacy and Information Security Risks

BCNET CONNECT

Introduction

Why should we care?

Langara Cloud Story

- 2010 : Microsoft BPOS ….. US
  - 2012 : Desire2Learn (now BrightSpace) ….Student LMS… Canada
    - 2013: Global Relay hosted Zimbra…Email… Canada
      - 2017: O365 for Employees….Email… US (in Canada now)
        - 2018: Workday …. ERP….Canada
          - 2019: O365 for Students….Email
            - …….

- 2022: 30+ Cloud software
  - Misconception…SaaS/Cloud = no work for institution?

BCNET CONNECT

Risk Assessment of SaaS and Cloud Services

ON THE ROAD…		IN THE CLOUDS…
• Highways, roads, bridges, tunnels • Street lighting, traffic signs, traffic signals • Road construction, repair, maintenance	**INFRASTRUCTURE**	• IaaS, PaaS, SaaS, XaaS • Public cloud, private cloud • Vendor hosted
• Sedans, sports cars, SUVs, motorcycles • Pickups, delivery vans, transport trucks • Buses, passenger vans, • Emergency vehicles, service vehicles	**APPLICATIONS**	• Collaborative tools, e-mail & messaging, video conferencing • Health and wellness, clinic management • HR, Finance, recruitment, CRM • Learning Management Systems, course development • Facilities management, equipment management

• Manufacturers
  • Mercedes, Ford, Honda, Hyundai, Tata, Volvo
  • Harley Davidson, Kenworth, Lamborghini
• Dealerships, rental and fleet agencies
• Support Services
  • Service stations
  • Mechanics & repair shops
	VENDORS	• PeopleSoft, SAP, Salesforce, Oracle, Workday
		• AWS, IBM, Microsoft, GOOGLE
		• Slack, ZOOM
		• Consultants, contractors, integrators
		• Imbedded services, add-ons
		• Analytics

• Individual drivers • Passengers	**CLIENTS & USERS**	• BC Educational Institutions • Instructors, Students, faculty, Staff • General public, business partners, donors, etc.

BCNET CONNECT

BCNET CONNECT

Data Management

..... Nthusi

Data Management

Data Access	• Authentication: MFA / 2FA • Authorization: User profiles provisioning / de-provisioning, any third party access to data
Encryption	• Cloud-Based Encryption • Bring Your Own Key (BYOK) • Hold Your Own Key (HYOK) • AES 256-bit encryption
Data Ownership	• Rights to use, disclose • Intellectual property rights • Data shared with fourth-party

BCNET CONNECT

Data Management cont.

Data Transmission	• Security controls for data transmitted between the user and the provider • Security controls for when the provider transmits data from one location to another (if applicable) • Verify provider data leak prevention capabilities
Data Integration	• Process flow and a detailed data flow diagram • Integration requirements with other solutions • Data format(s) used (e.g. files on secure FTP or service calls)
Data Storage	• Storage location and how will the data be stored • Data tenancy segregation / multi-tenancy • Controlled access to the data and storage media • Stored data protected / secured by the provider (e.g., encryption)

BCNET CONNECT

Data Management cont.

Data Backup	• Data back-ups stored on-site / off-site • Verify if there is any subcontractor involvement • Verify process to restore data from the provider’s back-up
Data Retention	• Cloud data retention policy, in alignment to FIPPA, PCI, who enforces it, and verify if any exceptions • Cloud data ownership, SaaS provider\user • Retention period for sensitive data (alignment to FIPPA) • Exit Strategy – recovery of data during termination • Data destruction certificates
Disaster Recovery	• Natural disaster (master service agreement force majeure clause) • DRP and BCP policy • Restoration procedures • Service-level: Recovery Time Objectives (RTO), Recovery Point Objective (RPO), Maximum Tolerable Outage (MTO) • Failover site location and certified to the same standards as the primary facility

BCNET CONNECT

Attestations

..... Robert

Attestations

SOURCES OF COMFORT	
ATTESTATIONS	• SOC 2 type II • ISO 27000 series certifications • PCI-DSS • Other audit reports
VENDOR DOCUMENTS	• Terms of Use • Privacy Policy • Penetration test and vulnerability reports • Vendor “trust centre” documentation and whitepapers
REPORTS	• BitSight • Industry news reports
TOOLS	• CAIQ – Consensus Assessment Initiative Questionnaire • HECVAT – Higher Education Common Vendor Assessment Tool
QUESTIONS	• Ask questions that matter to **your** organization

BCNET CONNECT

Privacy

..... Joanne

Why Assess Privacy Risks?

- Comply with *Freedom of Information and Privacy Act* requirement to protect personal privacy:
  - ***Prevent*** unauthorized collection, use, and disclosure of personal information stored inside or outside of Canada
  - ***Identify*** initiatives that involve personal information
  - ***Document*** controls put in place by institutions, service providers, and commercial data centres to protect privacy
  - ***Decide*** whether to proceed by using assessments to make informed, risk-based decisions

BCNET CONNECT

Why Assess Privacy Risks? cont.

- Organizations that protect and respect privacy:
  - ***Instill*** trust and confidence in our operations
  - ***Enhance*** our public reputation
  - ***Improve*** our competitiveness against others in our sector

BCNET CONNECT

When to Assess Privacy Risks

Use Privacy Impact Assessments for:

- **New** initiatives
- **Significant changes** to existing initiatives
- **Sensitive** personal information **stored outside of Canada**

BCNET CONNECT

How to Assess Privacy Risks

- No **one size** fits all
- Establish **thresholds** for the level of assessment to be completed
- Identify responses to risks that are in keeping with the **level of risks** assessed

BCNET CONNECT

Q&A

BCNET CONNECT

Risk Assessment of SaaS and Cloud Services

MYTHS and MISCONCEPTIONS
Removal of the FIPPA data residency restrictions means a privacy notification and obtaining consents are no longer required…
The SaaS vendor is now responsible for properly protecting our data….
The vendor is hosting its applications on AWS / AZURE / GOOGLE and using their security, so there's nothing to worry about…
The vendor follows "industry standards", so there's no need for concern
The vendor encrypts data at reset, so there's no need to further encrypt any of our sensitive data…
The vendor has breach notification processes, so we don't need to have our on processes or worry about this…
The vendor is smaller shop, so we shouldn't ask / expect them to protect our data as well as the big vendors...

BCNET CONNECT

Contacts and Resources

Nthusi Kaisara, Cyber Security, BCIT nthusi_kaisara@bcit.ca

Joanne Rajotte, Privacy, Langara College jrajotte@langara.ca

Isabel Wong, Infrastructure, Langara College iwong@langara.ca

Robert Tremonti, Privacy and Information Security Risks, UBC robert.tremonti@ubc.ca

- Sample Cloud Hosted SaaS Assessment Questionnaire, Brock University
- EDUCAUSE HECVAT
- CSA CAIQ
- Privacy Impact Assessment (PIA) Template

BCNET CONNECT