Toronto Public Library: Being hacked
Strategies for Regaining Confidence Post-Cyber Attack

Vickery Bowles, City Librarian
Steve Till-Rogers, Director Digital Strategy & CIO

July 10, 2024

tpl : toronto public library

basic facts

- Cybersecurity attack on the Toronto Public Library
- Identified by security monitoring email alerts
- Enterprise technology services proactively shutdown
- Impact reach is 100 branch locations across Toronto
- Business Continuity Response was immediate

cyber response governance model

Cyber Response Leadership Team (CRLT)

- Executive Leadership
- Senior decision body
- Engage with Breach Counsel
- Develop organizational communications
- Coordinate response process

Library Operations Centre

- Business Continuity Response Team
- Coordinate and distribute internal communications
- Liaison between business operations and technical recovery
- Lead orchestration of service recovery
- Coordination of Service Owners and various organizational teams

Management Response Team

- Library Management and Key Stakeholders
- Receive and distribute internal communications to staff
- Direct engagement with staff collectively
- Maintain standard operations as much as possible

business continuity response

Proactive plan for operational continuity

Library Operations Centre instantiated

- Business liaison team collaborates with technical teams

Focus on

- Internal corporate communications distribution
- Priority of service recovery and system restoration
- Coordination of service orchestration across business teams

breach counsel (legal counsel)

Ensure contact details are readily available for immediate engagement

Consulting on

- Communications (External)
- Legal obligations (e.g. Privacy, Identity Theft)
- Engagement with technical consultants
- Legal privilege

cybersecurity specialists

Ensure contact details are readily available for immediate engagement

Consulting on

- Containment
- Forensic Assessment
- Service Recovery (technology)
- Appropriate Security Assessment and Consulting

ongoing services

- **all 100 branches remained open**

- **borrowing, returning, registrations with workarounds**

- **wifi, programs & study space**

- **e-resources for most circulating & reference products** (authentication removed)

service recovery

Data Centre

- Complete rebuild of network within Data Centre and extending to branch (campus) edge
- Restoration of encrypted data from backup
- Implemented enhanced log management
- Increased security controls on accounts (user & service accounts)
- Prioritized all enterprise applications for service restoration

service recovery

Across 100 Branch Locations

- Secured and prepared endpoints at all locations (~5,000 endpoints)
- Passwords cycled on all IT services accounts
- Deployment of enhanced endpoint security tools (Microsoft Sentinel)
- Rebuild (restore) of Enterprise Applications into new network segments

lessons learned

2023 Cyber Security Tabletop exercise

Limited participation from some teams (everyone is busy)

Communications acknowledged informed their response

Credit Monitoring

2 years credit monitoring for staff

Evaluation ongoing to determine if any impact on customer data

Stakeholder communications

Library Board

- Regular closed session updates with participation from breach counsel, cyber experts and City CISO staff
- Final public report with confidential attachment

Staff

- Timely, transparent, regular and empathetic communications with Union and all staff: virtual town halls, FAQ's, emails, staff meetings
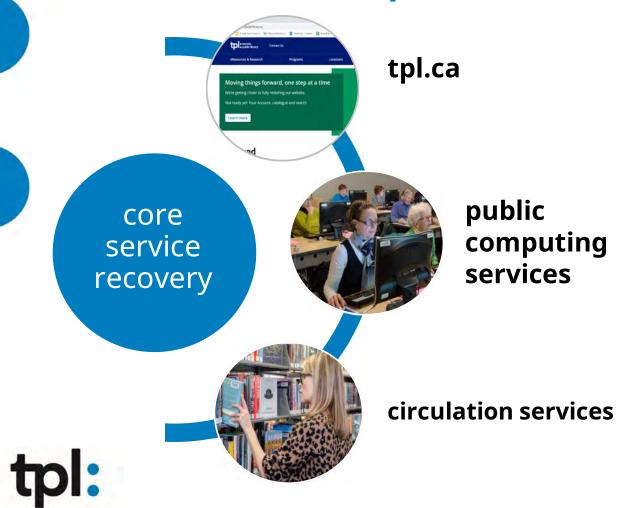- Email set up for staff to send questions; over 2,000 answered

Public

- Landing page established for regular cyber and service updates
- Email set up for public to send questions; over 3,00 answered
- Earned media, social media, and media requests were leveraged

Other stakeholders

- Proactively engaged
  - City of Toronto
  - Mayor's Office
  - Information and Privacy Commissioner

phased reinstatement of services

tpl.ca

public computing services

core service recovery

circulation services

tpl web site

tpl.ca

core service recovery
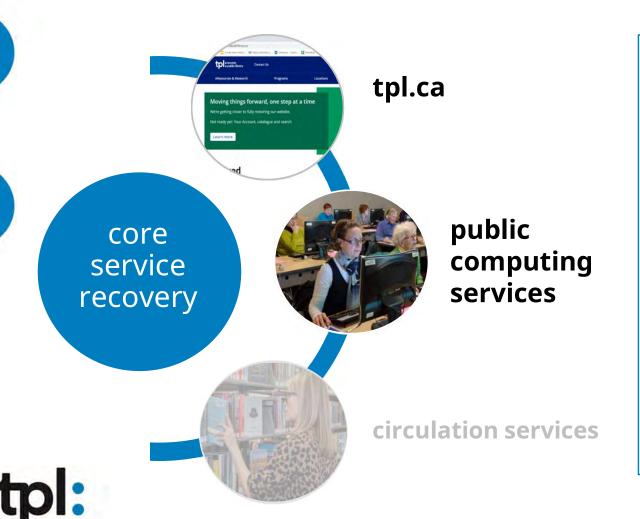
public computing services

circulation services

phase 1 (after 3 months)
- ✓ familiar version of website
- ✓ more information about library services & programs
- ✓ easy-to-access digital resources
- ✓ friendlier navigation
- ✓ key electronic resources restored (incl. LinkedIn Learning, eLearning pages)

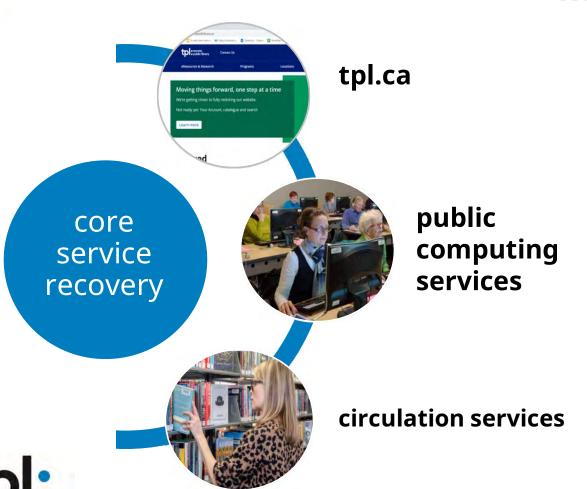phase 2 (after 4 months)
- ✓ Your Account
- ✓ Catalogue
- ✓ Search

public computing

tpl.ca

public computing services

core service recovery

circulation services

restored (after 3 months)

✓ reserve and access PC computers in all branches

✓ Digital Innovation Hub PCs available

✓ Learning Centre computers available and classes resume

✗ No printing service available

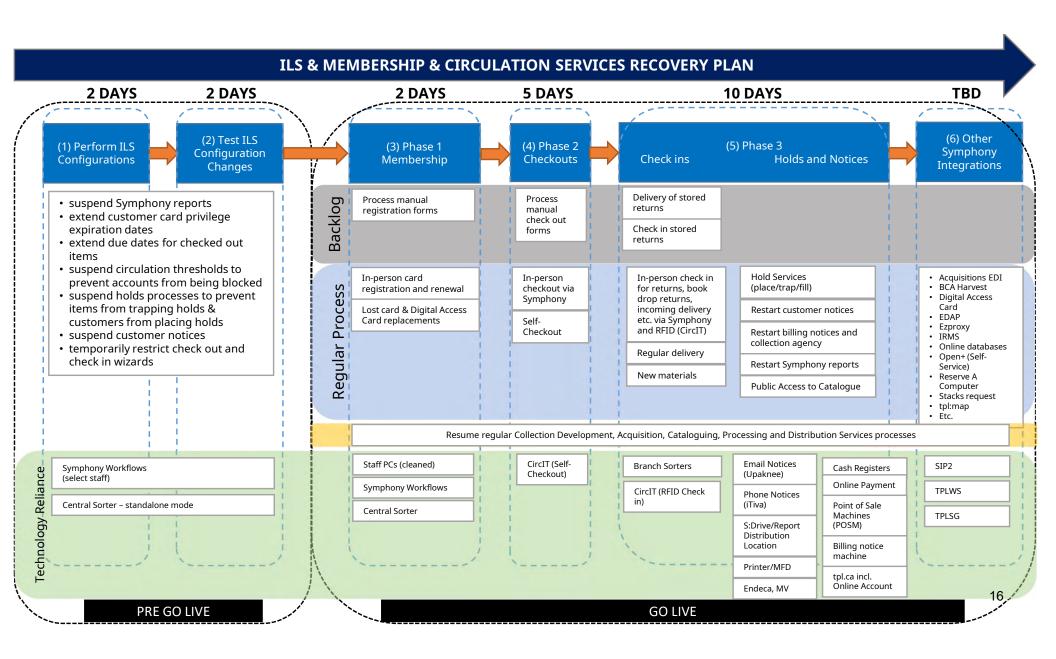**9,000+ sessions booked in first week**

materials circulation

core service recovery

tpl.ca

public computing services

circulation services

phase 1 & 2 (after 3 months)
- ✓ backlog of registrations and checkouts uploaded
- ✓ preparation for large scale material processing begun

phase 3 (after 3.5 months)
- ✓ checking in stored returns and new items
- ✓ holds notifications sent out and customers receiving holds
- ✓ customers can place and manage holds with staff assistance.
- ✓ self-checkout terminals available for use in branches

15

ILS & MEMBERSHIP & CIRCULATION SERVICES RECOVERY PLAN

2 DAYS	2 DAYS	2 DAYS	5 DAYS	10 DAYS	TBD
(1) Perform ILS Configurations	(2) Test ILS Configuration Changes	(3) Phase 1 Membership	(4) Phase 2 Checkouts	(5) Phase 3 — Check ins — Holds and Notices	(6) Other Symphony Integrations

(1)/(2):
- suspend Symphony reports
- extend customer card privilege expiration dates
- extend due dates for checked out items
- suspend circulation thresholds to prevent accounts from being blocked
- suspend holds processes to prevent items from trapping holds & customers from placing holds
- suspend customer notices
- temporarily restrict check out and check in wizards

Backlog

(3) Phase 1 Membership	(4) Phase 2 Checkouts	(5) Check ins
Process manual registration forms	Process manual check out forms	Delivery of stored returns
		Check in stored returns

Regular Process

(3) Phase 1 Membership	(4) Phase 2 Checkouts	(5) Check ins	(5) Holds and Notices	(6) Other Symphony Integrations
In-person card registration and renewal	In-person checkout via Symphony	In-person check in for returns, book drop returns, incoming delivery etc. via Symphony and RFID (CircIT)	Hold Services (place/trap/fill)	• Acquisitions EDI
Lost card & Digital Access Card replacements	Self-Checkout	Regular delivery	Restart customer notices	• BCA Harvest
		New materials	Restart billing notices and collection agency	• Digital Access Card
			Restart Symphony reports	• EDAP
			Public Access to Catalogue	• Ezproxy
				• IRMS
				• Online databases
				• Open+ (Self-Service)
				• Reserve A Computer
				• Stacks request
				• tpl:map
				• Etc.

Resume regular Collection Development, Acquisition, Cataloguing, Processing and Distribution Services processes

Technology Reliance

Pre Go Live (1)/(2)	(3) Phase 1 Membership	(4) Phase 2 Checkouts	(5) Check ins	(5) Holds and Notices	(6) Other
Symphony Workflows (select staff)	Staff PCs (cleaned)	CircIT (Self-Checkout)	Branch Sorters	Email Notices (Upaknee)	Cash Registers	SIP2
Central Sorter – standalone mode	Symphony Workflows		CircIT (RFID Check in)	Phone Notices (iTiva)	Online Payment	TPLWS
	Central Sorter			S:Drive/Report Distribution Location	Point of Sale Machines (POSM)	TPLSG
				Printer/MFD	Billing notice machine	
				Endeca, MV	tpl.ca incl. Online Account	

PRE GO LIVE | **GO LIVE**

16

materials Check-in

23,000
boxes stored in branch
locations processed

15

trailers processed

phased reinstatement of services
check-ins, holds (over 3 week period)

1.41+ million
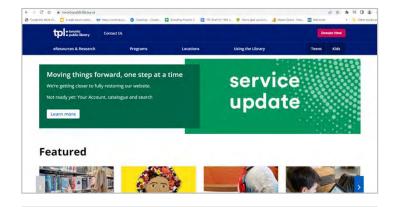items **checked in**

620,000
items **sorted**

117,000
holds **placed**

94,200
holds **placed** from Feb 29-Mar 3

110,000
holds **available for pick-up**

tpl:

communications: website, email

communications: social media

communications: earned media

THE GLOBE AND MAIL

Toronto Public Library gradually recovering from hack, more services back in February

TORONTO
THE CANADIAN PRESS
PUBLISHED JANUARY 19, 2024

CityNews Everywhere

Toronto Public Library's website partially restored months after cyberattack

CBC

Toronto Public Library reinstates circulation, hold services following ransomware attack

Toronto Public Library storing returned books at 12 trailers off site in wake of cyberattack

CP24 WATCH LIVE | NEWS WEATHER TRAFFIC VIDEO CP24 BREAKFAST LIFESTYLE CONTESTS MORE

Service partially restored on Toronto Public Library's website but catalogue, personal accounts still down

Global NEWS Toronto Public Library systems to remain down until 2024 following cyberattack

customer feedback

"**You have all done an incredible job** through these horrible circumstances and we are all so very happy to see things returning to normal."

"Yesss. I got so hyped seeing a TPL truck yesterday."

"We appreciated you before this happened... **now we appreciate you more.**"

"So excited for you to be up and running again!"

I'm a volunteer with Leading to Reading and yesterday **when my kid saw that the computers were working again, his face absolutely lit up** and he rushed over to the kids' section to see if the shelves had been restocked. They had! **He said to his mom, "I'm going to take out all the books!"**

@torontolibrary you are the best! **Waiting patiently for library life to return to normal** and supportive of whatever you have to do.

thank you
questions?