Cyber-Attack: Surviving an incident

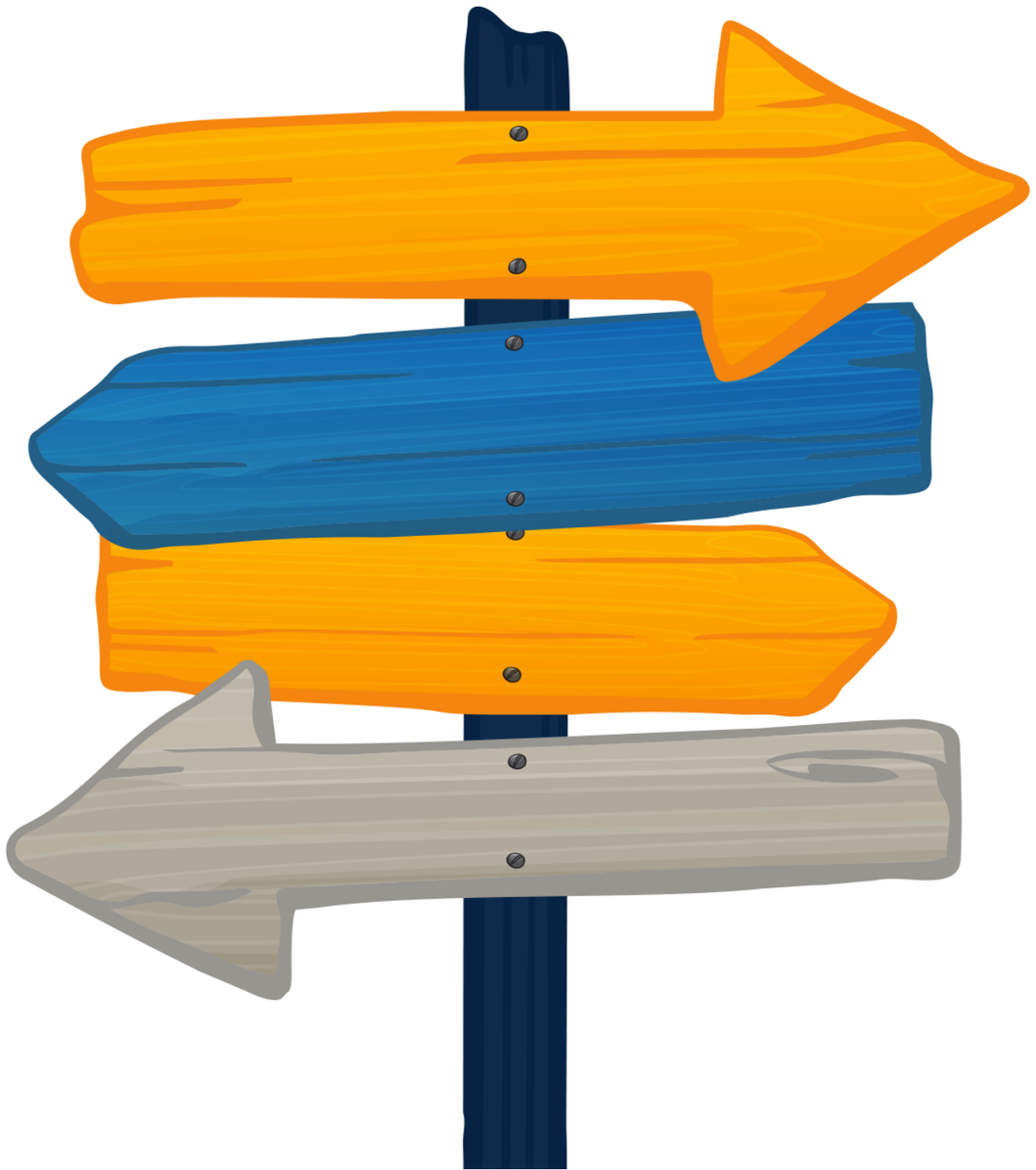
Bob White

Youth Services Bureau

Land Acknowledgement

We would like to acknowledge that we are joining from across Ontario from Aboriginal land that has been inhabited by Indigenous peoples from the beginning. As settlers, we're grateful for the opportunity to meet here, and we thank all the generations of people who have taken care of this land for thousands of years. We recognize that Indigenous practices of health and well-being have been in place in this territory for over 10,000 years and are maintained to this day. As healthcare leaders, we have much work to do ourselves to do our part and support the de-colonization of children's healthcare systems.

CMHO
Children's Mental Health Ontario
Santé mentale pour enfants Ontario



CROSSROADS

Re-imagining better mental health care for kids and families

2021 CMHO Virtual Conference

November 22 to December 3

Sponsored by

Knowledge Institute on Child and Youth Mental Health and Addictions

Institut du savoir sur la santé mentale et les dépendances chez les enfants et les jeunes

cymha.ca cymhaon CYMHAOntario @CYMHA_ON

Thank you to our Sponsor

Cyber Attack:

Surviving an Incident…

Description: the pandemic has shifted a large majority of our work into the online space leaving us more vulnerable to cyber attacks like phishing. This presentation will review a real-life cyber attack incident and cover the steps taken to ensure a smooth operational recovery. Discussion will focus on steps taken in the immediate aftermath, as well as preventative measures we can consider to prevent future attacks.

Robert White

Director, IS&T

Youth Services Bureau of Ottawa

What just happened?

- INITIAL ATTACK VECTOR: slow network, encrypted files, AD compromised
- SECOND ATTACK (@48hrs): AD

INITIAL OPERATIONAL STATE ?

- SERVER FILES UNAVAILABLE ✘
- CURRENT BACKUPS UNAVAILABLE ✘
- STAFF ACCESS TO NETWORK RESOURCES, DISABLED. ✘
- CLIENT MANAGEMENT SYSTEM – UNAFFECTED ✓
- MESSAGING SYSTEMS – UNAFFECTED ✓

SURVIVABILITY MEASURES…

- IMPLEMENT SECURITY CHANGES
- RESTORE/RECOVERY OF ACTIVE DIRECTORY
- ZERO TRUST COMPUTING
- TEMPORARY MOVE TO CLOUD
- CMS REVIEW
- REVAMP OF DATA STORAGE POLICIES/PROCEDURES
- DATA RECOVERY
- USER AWARENESS

WHAT WE DO DIFFERENTLY…

IMPLEMENT A SECURITY GOVERNANCE AND MANAGEMENT PROGRAM THAT IS ALIGNED WITH BUSINESS GOALS:

- RISK TOLERANCE ASSESSMENT THAT TAKES INTO ACCOUNT SECURITY OBJECTIVES AND BUSINESS GOALS; MUST BE BOTH OTHERWISE THEY WILL CONFLICT.
- SECURITY PRACTICES FRAMEWORK; WORK TOWARDS EFFECTIVE RISK MITIGATION STRATEGY, IMPROVEMENT OF SECURITY POSTURE (E.G. CREDENTIAL MGMT PRACTICES, MFA FOR ADMIN ACCOUNTS, AND CULTURE/AWARENESS)
- AUDIT (METRICS, KPI, ACCOUNTABILITY MODEL) AND CONTINUOUS IMPROVEMENT

ACHIEVEMENTS…

- SECURE BACKUP SOLUTION
- SEPARATED GUEST TRAFFIC FROM NETWORK
- NEW SECURITY FABRIC TO ADDRESS MALWARE ACTIVITY
- INTEGRATED CYBER-SECURITY WITH BUSINESS ACTIVITY
- EARLY STAGES OF CYBER-SECURITY GOVERNANCE PROGRAM
- MOVING TO THE **IDEAL STATE**: SECURITY PRIORITIZED OVER CONVENIENCE

LESSONS LEARNED…

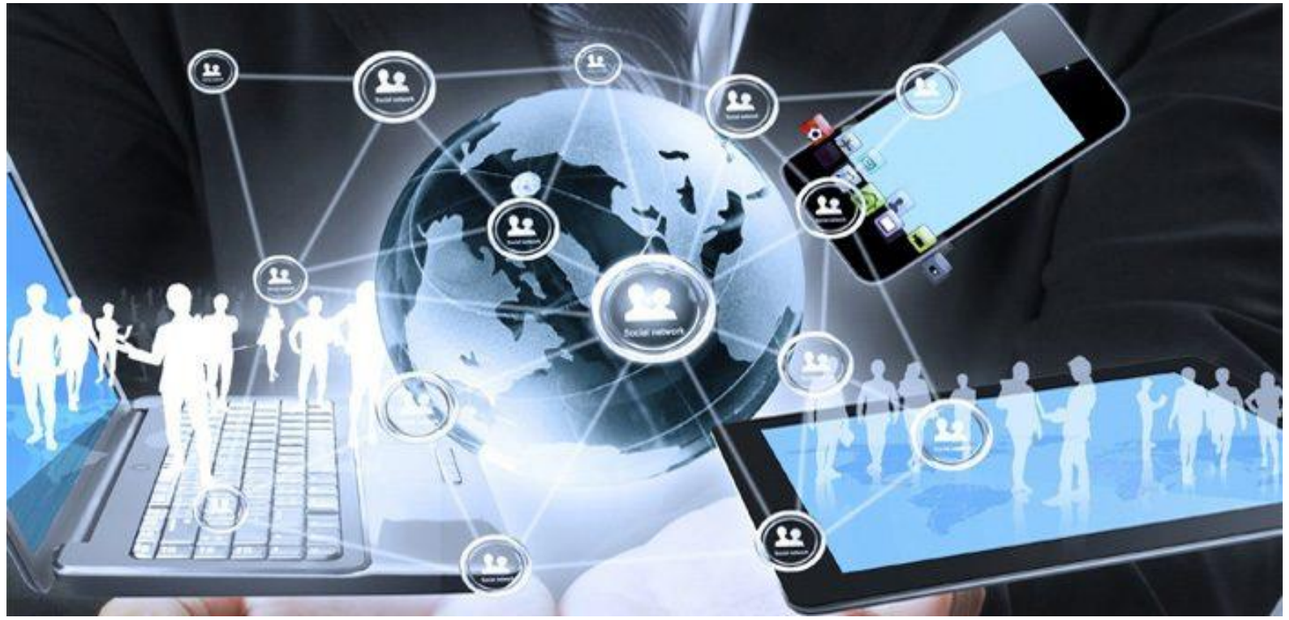
TODAY, A CYBER-SECURITY PROGRAM IS A NON-NEGOTIABLE REQUIREMENT FOR ORGANIZATIONS TO OPERATE IN TODAY'S THREAT LANDSCAPE.

- Requires a huge investment;
- We already have technology for this, right? (EPP – endpoint protection platform)

MOST IF NOT ALL ORGANIZATIONS (IT) ARE ALREADY DOING IT IN SOME FORM; THE KEY IS TO ADD A FRAMEWORK AND STRUCTURE SO THAT ALL STAKEHOLDERS AND COMPONENTS (PEOPLE, PRACTICES/PROCESSES, AND POLICIES) ARE INCLUDED IN A STRUCTURED GOVERNANCE PROGRAM.

SOME TIME INVESTMENT REQUIRED AT THE FRONT-END BUT THE PAY-OFF IS PRICELESS IN TERMS OF THE VALUE TO THE ORGANIZATION.

MUST BE AT MINIMUM THE SAME PRIORITY AS SERVICE DELIVERY.



Thank You

Robert White

Youth Services Bureau of Ottawa