DTO Doctors Technology Office
A GPSC initiative

WHAT MAKES AN EMR SECURE?

OSCARCON 2022

Doctors of BC - Doctors Technology Office

June 25th 2022

BRITISH COLUMBIA
GPSC General Practice Services Committee
doctors of bc

Join at

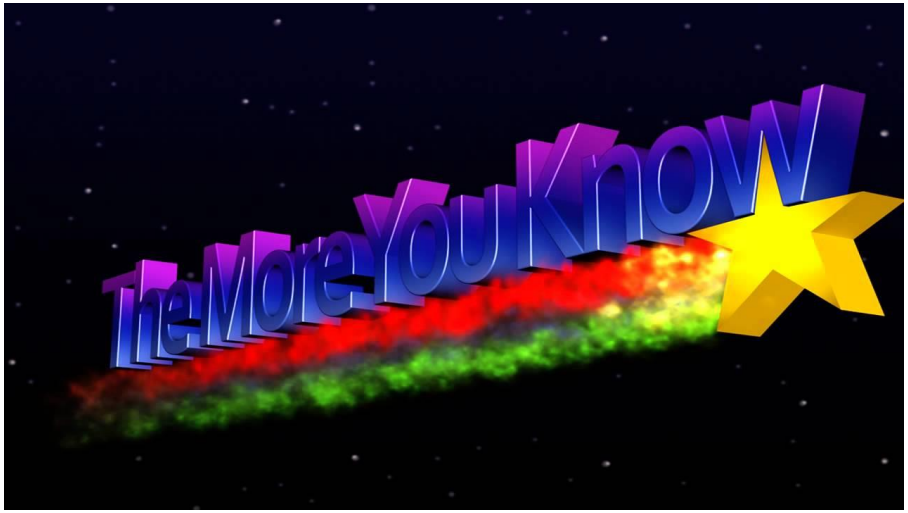
slido.com

#1889 434

DTO Doctors Technology Office
A GPSC initiative

TODAY'S AGENDA

- What are the main cybersecurity threats out there right now?
- How does it relate to EMRs?
- **What can you do to make a difference?**



WHO AM I?

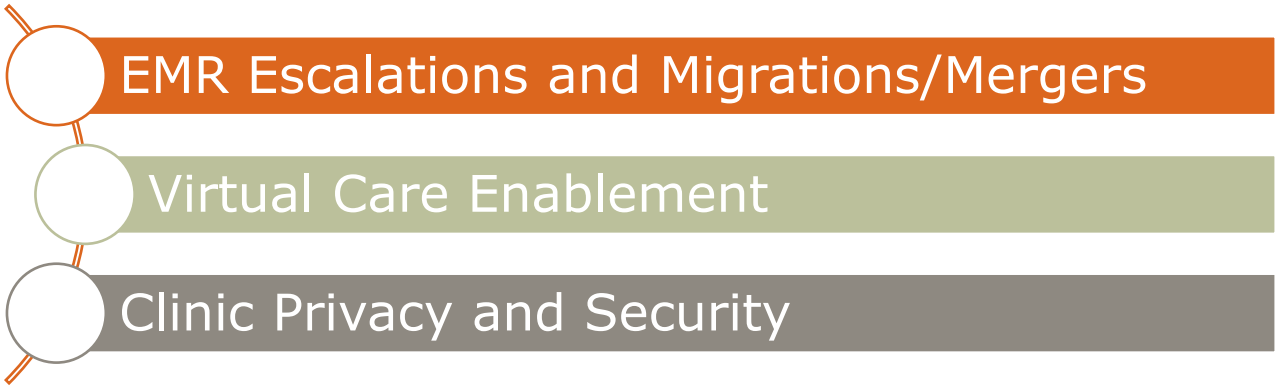
Chris Morse

Health Technology Partner - P&S Portfolio Lead

DTOInfo@doctorsofbc.ca

DOCTORS TECHNOLOGY OFFICE (DTO)

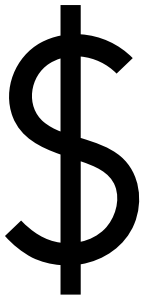
DTO provides tailored advisory support and resources to help physicians navigate the health IT landscape



HOW DOES OUR PROGRAM HELP?

1. Raise your defenses against cyber criminals
2. Have peace of mind that you are meeting the College and OIPCs “reasonability” standards
3. Know how to spot the signs of an issue and how to act before it becomes a more serious problem

WHY DOES THIS MATTER?



Cybercrime is on the rise

Attacks are more sophisticated

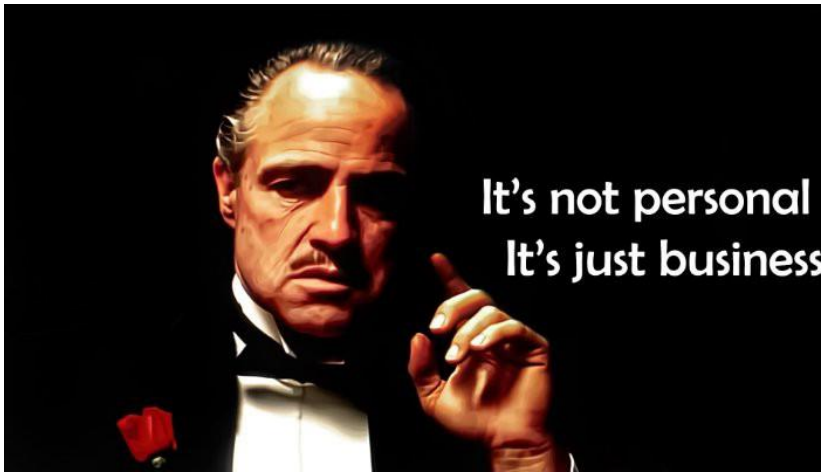
Attack Surface is increasing

WHAT'S YOUR COMFORT LEVEL WITH THE CYBERSECURITY THREAT LANDSCAPE?

- Super comfortable - I know the threats and many of best ways to mitigate them
- Fairly comfortable - I know more than basics and enough to not be the low hanging fruit
- Not too comfortable - I know passwords are important but that's about it
- Highly uncomfortable - I lay awake at night and worry

WHAT EXACTLY ARE THE THREATS?

- Social engineering
  - Credential theft
- Software and network vulnerabilities
  - Zero days
  - RDP and open ports
- Ransomware
  - Full network encryption
  - Data exfiltration



Most threats are to facilitate one of two things:

1. **Immediate payment**
2. **Identity theft (to get paid later)**

ANATOMY OF AN ATTACK

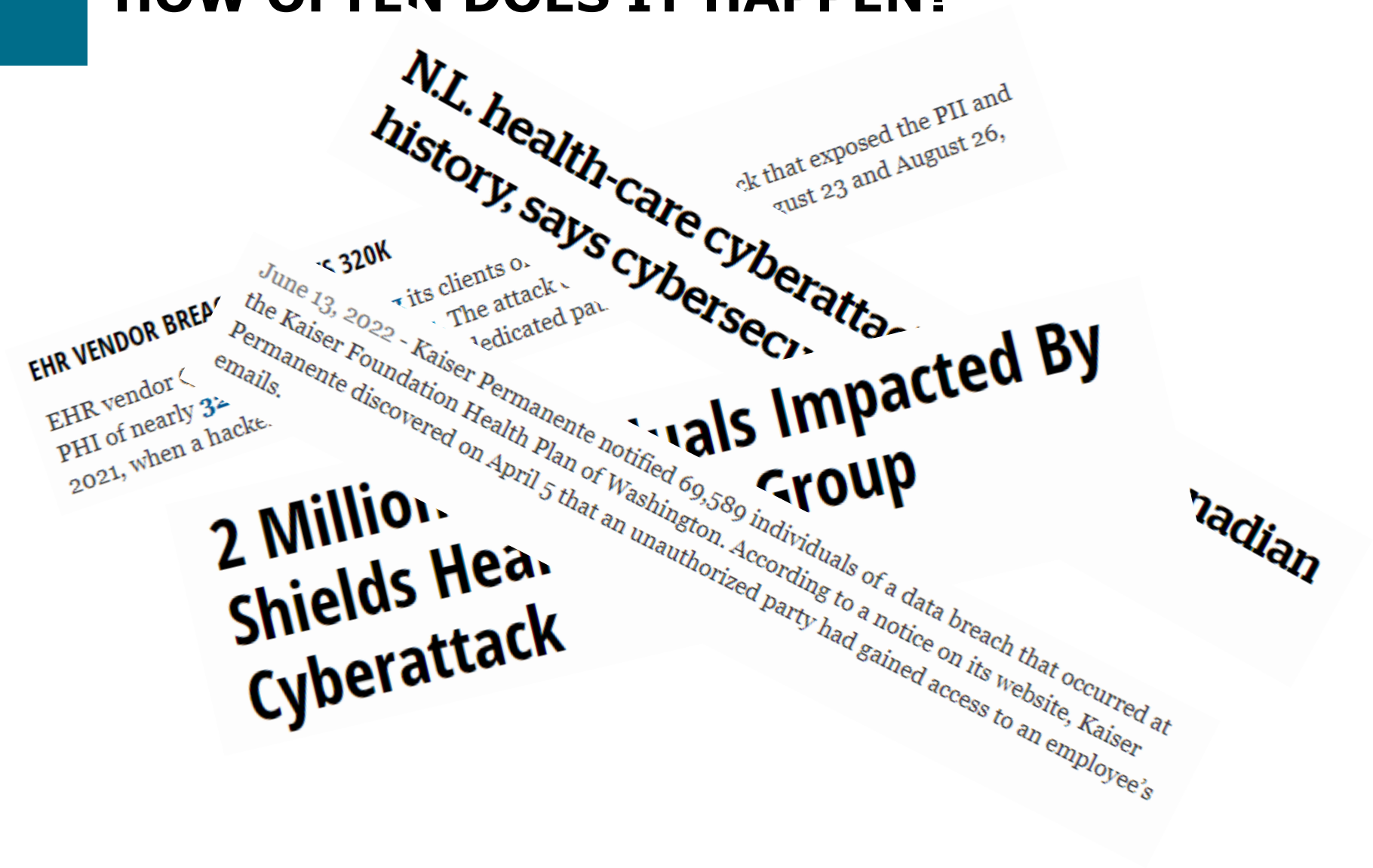
Recon
- Public information

Initial Access Brokerage
- Thread hijacking
- Use of common, legit services
- Office documents with macros
- Zero-day vulnerabilities

Lateral Movement and Privilege Escalation
- CobaltStrike
- Root Access

Payload Deployment
- Encryption
- Exfiltration

HOW OFTEN DOES IT HAPPEN?



WHAT ARE A CLINIC'S RESPONSIBILITIES?

- Legislative
  - Personal Information Protection Act (PIPA)
  - Freedom of Information and Protection of Privacy Act (FOIPPA)

- Professional
  - College of Physicians and Surgeons Guidelines (CPSBC)
  - Canadian Medical Protective Association (CMPA)

"…ensure that *appropriate* security provisions have been made"[1]

"..must consider what a *reasonable* person would consider appropriate under the circumstances"[2]

"…take *reasonable* steps to protect their patient's privacy"[3]

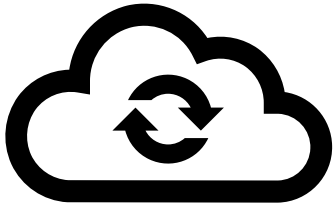
[1]*CPSBC – Medical Records, Data Stewardship and Confidentiality of Personal Health Information*
[2]*Personal Information Protection Act (PIPA)*
[3]*CMPA – Good Practices – Privacy and Confidentiality*

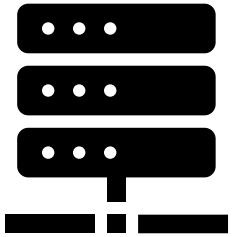
WHAT IS "REASONABLE" FOR AN EMR?

1. Data Storage
   - How is our server exposed to the internet? How would we know if there was an intrusion?
   - How could someone physically access EMR servers or data?
   - Is our EMR data backed up? Where? How?
   - What encryption techniques are in use?
2. Access Management
   - What authentication mechanisms are in use?
   - How is remote access managed? VPN? DaaS?
3. User Awareness and Training
   - Can your users spot threats?
   - Can your users identify high risk behaviours?

WHERE IS MY DATA?

Oscar is one of the only EMRs that continues to have a strong locally hosted userbase in BC





- Encryption in transit and at rest
- Server management or outsourced
- Managed backups
- Physically secure facilities

- Self-host (local or web)
- Pay for infrastructure and upkeep
- Extra work to harden and configure server
- Extra work to configure remote access

DO YOU KNOW WHERE YOUR DATA IS?

1. Yes – Our service provider hosts in a private cloud
2. Yes – Our service provider outsources it to another infrastructure/platform provider
3. Yes – We host it locally or on our own web server
4. No idea!

WHO HAS ACCESS?

- Identity and Access Management (IAM) and Roles Based Access (RBA) continue to be cornerstones of data security
- Robustness of these systems varies widely across EMRs
- Common high-risk behaviours are:
  - Sharing account credentials
  - Lack of password management policies
  - Using admin accounts for daily tasks
  - Weak authentication mechanisms
  - Poor training surrounding phishing and social engineering

HOW IS EMR ACCESS MANAGED AT YOUR CLINIC?

- Our EMR has multi factor authentication enabled
- We use a VPN and directory service
- We have a variety of different roles assigned under the “least privilege” model
- We can only log in when we’re physically at the clinic
- We use passwords ONLY and none of the other options
- I’m not sure

FEATURES IN OSCAR

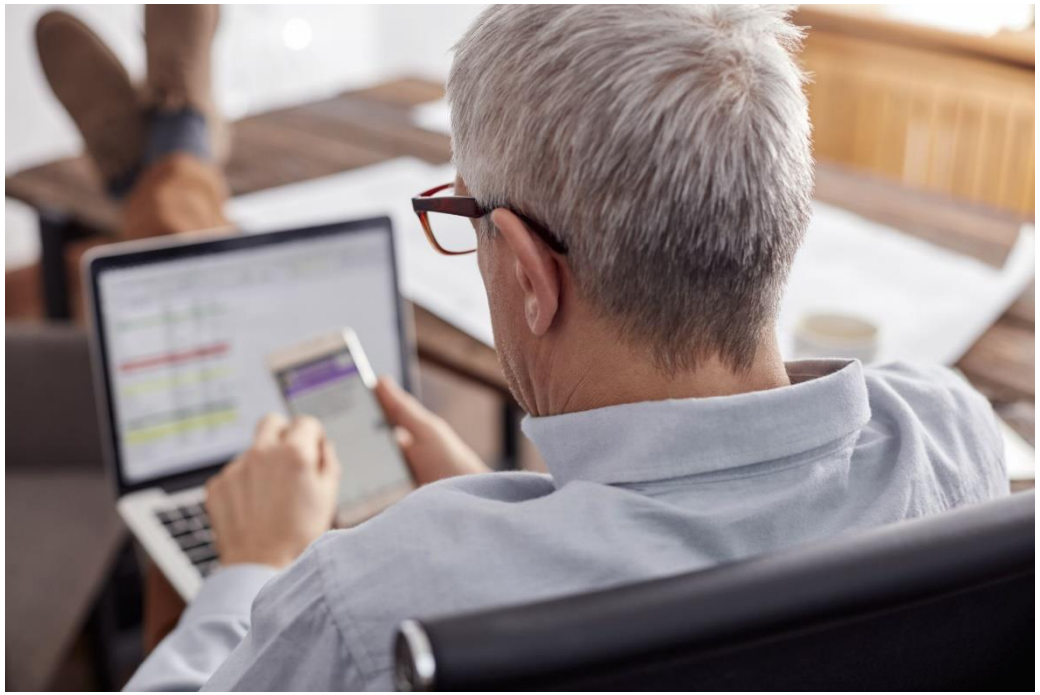
- Selection of default roles and ability to customize
  - World Oscar User Management Guide
- New Multi-factor authentication (MFA) using Timed One Time Password (TOTP)

And you can supplement with other tools to streamline if you're motivated

- VPN with AD
- DaaS (e.g. JumpCloud or Cloudflare)

But…

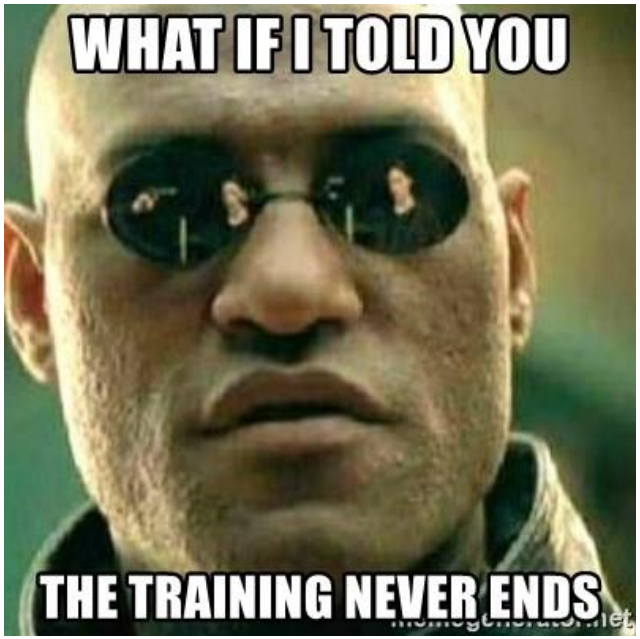
WHAT'S THE WEAKEST LINK IN DIGITAL SECURITY?



Us, the technology *users*

USER TRAINING AND AWARENESS

- Setting up a system that is security by design, not an add-on
- Encourage a culture of sharing problems and learning from them
- Do a phishing challenge together
- Keep apprised of news headlines and the latest vulnerabilities, particularly if you self-host
- Understand the importance of credential management.



PASSWORDS – WHAT'S THE PROBLEM?

Password strength:

- oscar – instant
- Il0veosc4r – 1 day
- oscaristhebestemr – 800,000 years

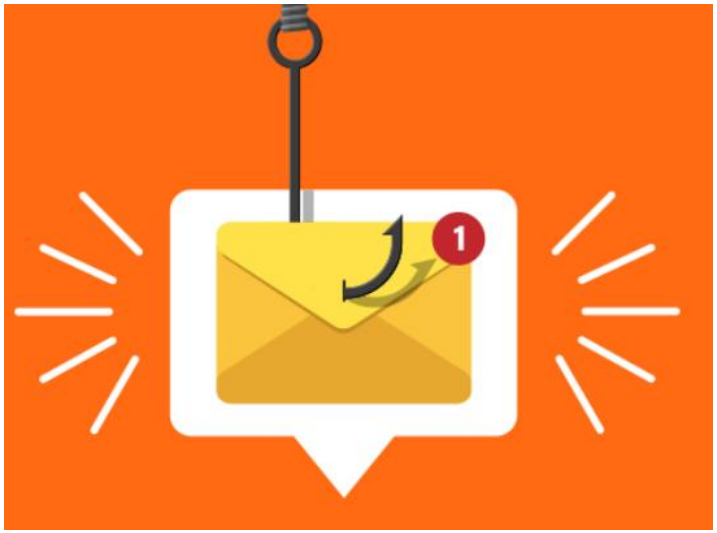
Password re-use:

- 13% use same password across all accounts[4]
- 52% use same password for multiple accounts[4]

[4]Harris Poll survey, December 2018

PHISHING AND SOCIAL ENGINEERING

- **Be suspicious** of unsolicited emails
- **Hover** over links and email addresses, without clicking, to verify
- **Manually confirm** website address
- If its someone you know, **verify** through another channel



Phishing Quiz

THE MOST IMPACTFUL THINGS YOU CAN DO THIS WEEK…

Formalize the building blocks of your P&S program

1. Nominate a Privacy Officer – we can support you!
2. Perform a self-assessment and call us to review
3. Train and skill up on P&S
   - Security in Low Doses Course – Free and 1 CME for Physicians
   - SAEGIS Shield

ADDITIONAL RESOURCES

- Physician Office IT Security Guide
- Clinic Security Toolkit
  - Guide for Privacy Officer and Security Lead
  - Password Management Guide
  - Multi-Factor Authentication
- DTO Virtual Care Resources
  - Virtual Care Quick Start Guide & Toolkit
  - Getting Patients Back to Practice Guide
  - Guide to eFaxing from Home
- Contact us at DTOinfo@doctorsofbc.ca or 604-638-5841