Cybersecurity for Businesses and Municipalities

Jason White

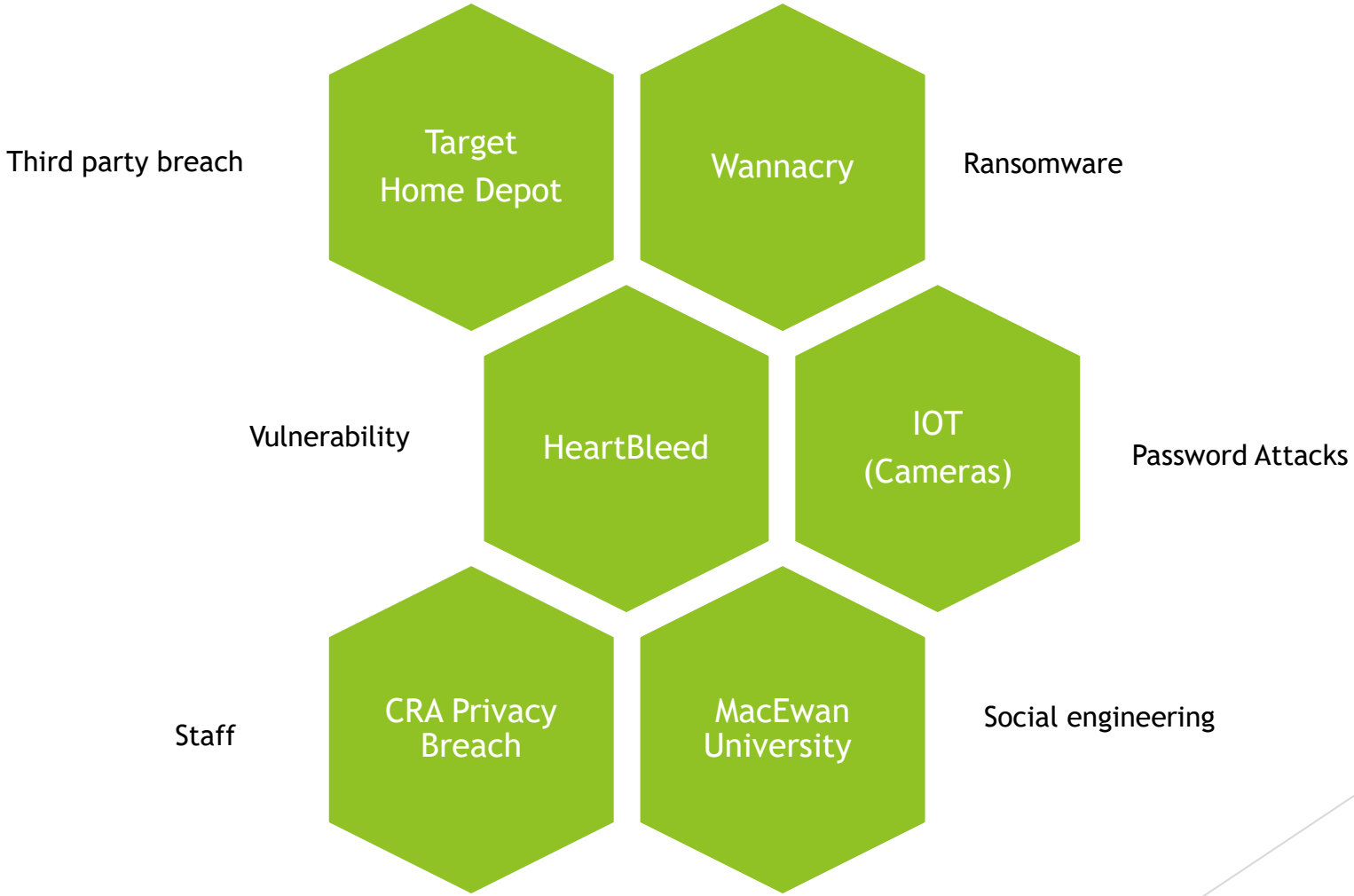
Information Technology Services Manager

County of Lennox and Addington

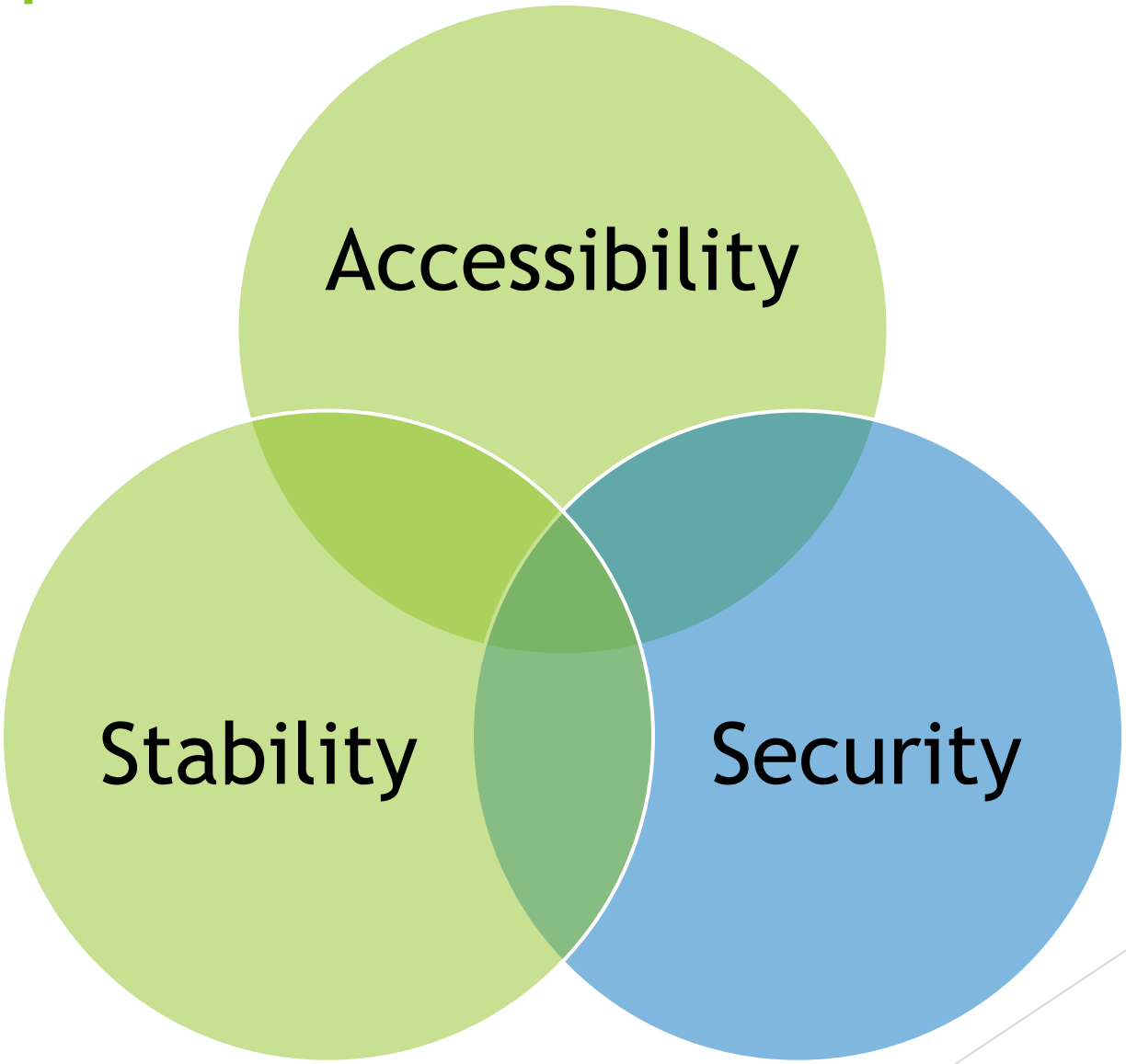
Cybersecurity today

- State:
  - More devices and services being introduced every day
  - More type of threats than ever and there is no indication of a slow down
- Concern:
  - We are at more risk than ever
- Effect:
  - A breach could result in
    - services not being delivered
    - a loss of trust in the organization
    - significant costs
    - severe impact on lives of those we serve
- We all have a role to play…

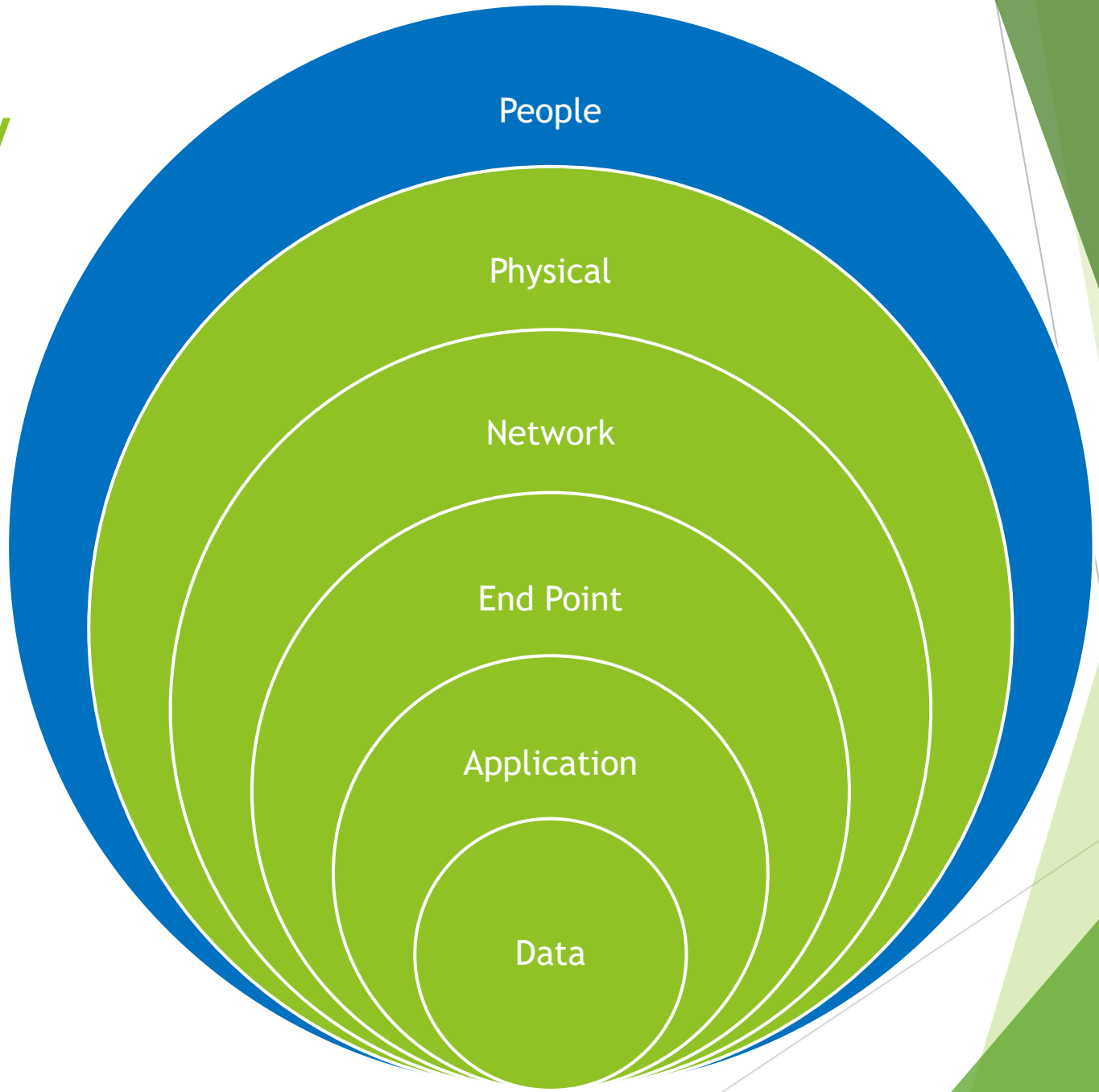
What is happening out there?



Your IT Department's Goals



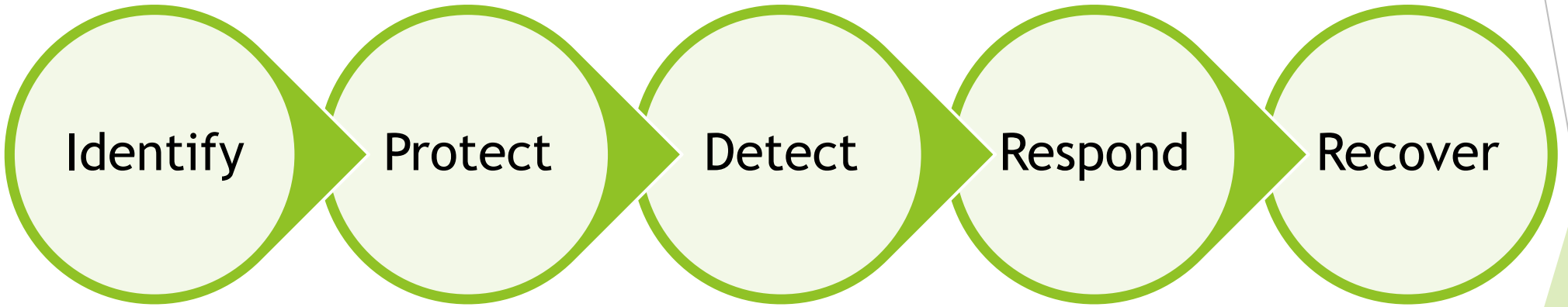
Cybersecurity The Onion



Phases of the Intrusion Kill Chain

Reconnaissance	Research, identification, and selection of targets
Weaponization	Pairing remote access malware with exploit into a deliverable payload (e.g. Adobe PDF and Microsoft Office files)
Delivery	Transmission of weapon to target (e.g. via email attachments, websites, or USB drives)
Exploitation	Once delivered, the weapon's code is triggered, exploiting vulnerable applications or systems
Installation	The weapon installs a backdoor on a target's system allowing persistent access
Command & Control	Outside server communicates with the weapons providing "hands on keyboard access" inside the target's network.
Actions on Objective	The attacker works to achieve the objective of the intrusion, which can include exfiltration or destruction of data, or intrusion of another target

NIST Cybersecurity Framework



We all a have a role to play.

Passwords… we all love passwords

- Use complex passwords
  - lowercase and capital letters, as well as a combination of letters, numbers and special characters.
- Use words or phrases that cannot be found in any dictionary of any language.
- Do not use passwords that are based on personal information that can be easily guessed
  - (birthdates, telephone number, or the name of your spouse, child or pet).
- Use different passwords on different systems or websites.
- Change your password on a regular basis.
- Do not share your password with anyone else.
- Do not write your password down and leave it in your desk or next to your computer.

Protect information

- Be sure to lock your computer when you walk away from it, even if you will only be gone for a short period of time.
- Do not leave your mobile devices unattended since having physical access to a device makes it easier for an attacker to break into it.

At the end of each day:

- Ensure that confidential or sensitive documents are removed from your desk and printers before leaving for the day.
- Remember to shred or properly destroy confidential documents when they are no longer needed.
- For both security and business resilience purposes, take your computer and mobile devices home each night.

Think before you click

- If it sounds too good to be true, it probably is. Don't click any suspicious links.
- Hover over links contained in messages and make sure they direct you to the correct website.
- Pay attention to the email address of a sender to ensure it is legitimate.
- Avoid downloading free software (especially those displayed in pop-up ads), which is a frequent source of viruses.
- Be suspicious of threatening or unnecessarily urgent emails.
- If you receive an email or instant message from a business contact that seems unusual or does not sound like something they would typically say, contact them through another means of communication and ask them if they actually sent the message before opening it.
- Avoid clicking on links, pictures and videos with catchy phrases such as "funniest ever" or "you have got to see this."
- Do not provide personal information unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information.

Social media

Exercise caution when posting personal information that may make you or your family vulnerable, such as your address or information about your schedule, routine or vacation plans.

- If your connections post information about you, make sure the combined information is not more than you would be comfortable with strangers knowing.
- Be wary of out-of-context connection requests. Since creating a social media account only requires a valid email address, it is easy for hackers to impersonate anyone online.
- Take advantage of social media site privacy settings to limit the information you make available to friends of friends or the public.

USB drives

- Do not connect personally-owned USB drives to company computers.
- If you find a USB drive on the floor, in an elevator or at a coffee shop nearby your facility, retrieve the device, deliver it to your local IT team and inform them of its suspicious origin.
- Always physically secure any USB drives containing confidential information.
- When possible, use passwords and encryption features.
- Disable Autorun

Working outside the office or traveling

- Do your best to avoid open, unsecured Wi-Fi networks (such as those in hotels, airports, airplanes and coffee shops) to conduct personal or professional business. If there is no alternative, use VPN to establish an encrypted connection.
- Use a privacy screen. Be aware of people nearby, who may be reading over your shoulder or shoulder surfing to gain access to your personal information.
- Refrain from using your work email or credentials personal account creation on e-commerce, media and blog sites.

Mobile device and application security

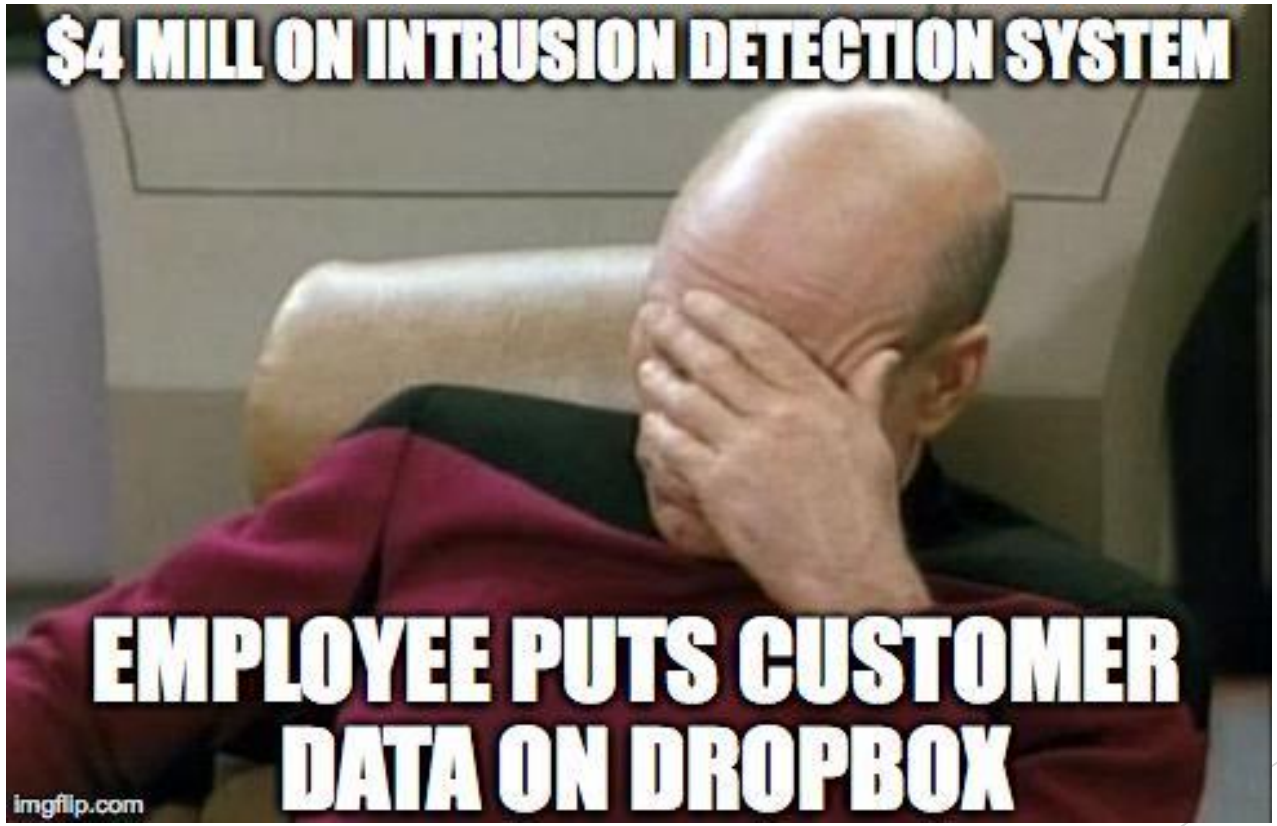
- Protect your portable devices such as your smartphone and tablet.
- Never leave these devices unattended in a public space such as in a coffee shop, hotel or airport.
- Enable password security on all of your devices, and select passwords that are difficult for others to guess. That way, if your mobile device is lost or stolen, it will be more difficult for an attacker to gain access to your information.
- Only purchase or download necessary applications from official app stores.
- Just like you would with your PC, keep your smartphone's software up to date. Mobile phone software and network services have vulnerabilities, just like their PC counterparts do.
- Only use electrical outlets to recharge your mobile devices. Avoid connecting your devices to a public charging station.

Some Resources

- The CIS Critical Security Controls for Effective Cyber Defense
  - https://www.sans.org/critical-security-controls
- Cyber Insurance
  - General liability will likely not cover damages related to Cyber Breaches anymore
  - New coverage will provided access to new resources
  - Mileage will vary by insurance provider and condition of your origination.
- Password Manager
  - Keepass
- File archive and encryption
  - 7-Zip


KEEP
CALM
AND
ASK
QUESTIONS

Thank you


$4 MILL ON INTRUSION DETECTION SYSTEM
EMPLOYEE PUTS CUSTOMER DATA ON DROPBOX
imgflip.com