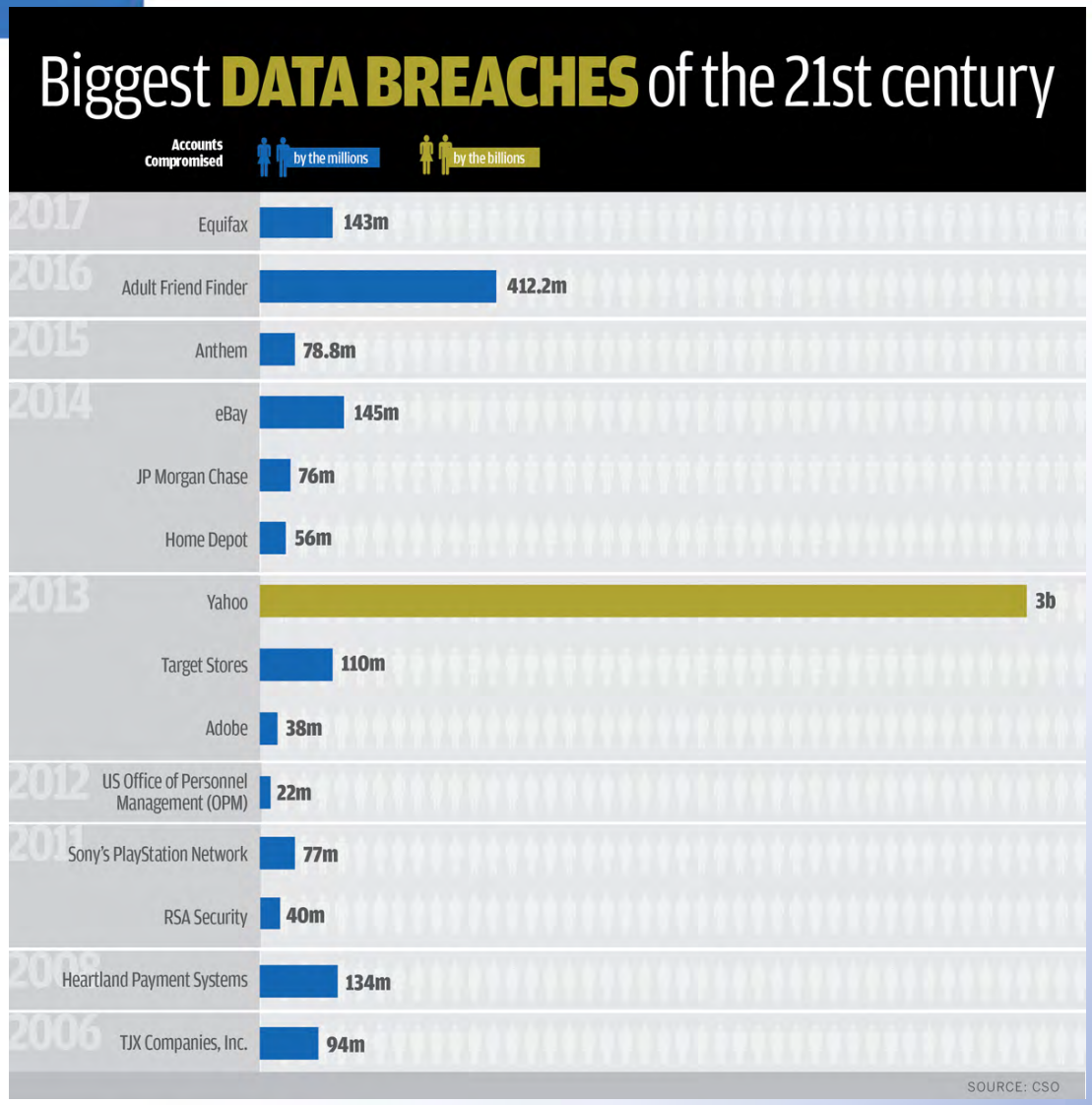
Cyber Security Threats - 2018

Presbyterian Church (U.S.A.)

Presbyterian Mission

David Dinkel
PC(USA) Information Technology

Can my company or organization be breached?



csoonline.com, 1/26/18

Presbyterian Church (U.S.A.)
Presbyterian Mission

What are the top cyber security threats today?

- Malware (esp. combined with social engineering)
- Phishing (for passwords and other sensitive info)
- Spearphishing
- Distributed Denial of Service (DDoS) Attacks
- Man in the Middle Attacks
- Credential Stealing and Reuse
- Pharming
- Spam
- Spoofing and Social Engineering attacks
- WiFi eavesdropping
- Viruses, Trojan Horses, Worms, Spyware, etc.

Presbyterian Church (U.S.A.)
Presbyterian Mission

What are the cyber security threats you are likely to face?

From csoonline.com article by Roger A. Grimes, 8/21/2017

1. Socially engineered malware (Ransomware)
2. Password phishing attacks
3. Unpatched software
4. Social media threats
5. Advanced persistent threats

Presbyterian Church (U.S.A.)
Presbyterian Mission

1. Socially Engineered Malware

- User is tricked or coerced into running a malicious program
  - Could be clicking a malicious weblink, opening an infected file or installing compromised software

- Most common example of socially engineered malware is Ransomware
  - Ransomware encrypts key files on your PC—Word docs, Excel spreadsheets, photos, etc.
  - Impossible to recover your files in most cases

1. Socially Engineered Malware (cont.)

1. Socially Engineered Malware (cont.)

What can I do if I have been infected with Ransomware? Unfortunately not much.

- **Encryption keys are too complicated**
- **Cyber criminals have all of the control**

In cases of attacks which include large amounts of data (hospitals, government agencies, etc.) paying the ransom may be the only solution.

- **Take a chance and pay the ransom…usually in bitcoins and not easy to setup**
- **Keep your computer and wait…sometimes cyber criminals reach a point where they are no longer making money and release the decryption codes**

Presbyterian Church (U.S.A.)
Presbyterian Mission

2. Password Phishing Attacks

- Usually arrive in your e-mail inbox and appear to come from legitimate companies
  - They will incorporate real company logos and threatening verbiage (You have to change your password now!)
  - They will instruct you to change your password or provide other personally identifiable information
  - Spearphishing attacks where criminals study the company's employee organizational structure

- How to deal with this type of attack?
  - Be aware—sometimes if you hover your mouse pointer over a link in the e-mail, you will notice the link points to an illegitimate source
  - Some of these e-mails will include bad grammar or spelling errors
  - Deleting the e-mail is the best approach

Presbyterian Church (U.S.A.)
Presbyterian Mission

3. Unpatched Software

- All vendor operating systems Windows, Apple OSX, Linux, Apple IOS (iPhone and iPads), Android (phones and tablets), etc regularly release patches and new releases

- Many of these releases include operating system enhancements but they also often include security patches

- Upgrade your devices on a regular basis
  - Know how to update each of your devices
  - Pay attention to mainstream news stories that report a security related story because it often means you need to upgrade at least one of your devices

- Sometimes vendors will release a single patch to address a particularly serious issue—it is important that these types of patches are installed immediately

Presbyterian Church (U.S.A.)
Presbyterian Mission

4. Social Media Threats

- Usually arrive as a friend or application install request and sometimes can contain links to spread malware
- May be in the form of fake accounts (sometimes look like they are legitimate and usually famous people) and used to spread misinformation
- Unwitting release of information can be dangerous
  - "I will be on vacation…
  - Divulging too much personally identifiable information can be used by criminals
- Be careful of what you post, requests you receive and the information you consume

5. Advanced Persistent Threats

- **Usually sophisticated, extremely hard to detect and occur over a long period of time**
  - **Usually used to steal data and not to disable networks or computers**
  - **Example is Deep Panda in 2015 where it is believed that China hacked the US Government Office of Personnel Management and compromised 4 million employee records**

- **Can be started as part of a spearfishing attack**
  - **Spearfishing is throwing a threat at a particular target and hoping it sticks—an example is getting an employee to open an infected document or link**

5. Advanced Persistent Threats (cont.)

- Here is what an attacker can do once the initial attack is successful:
  - Install additional hacking tools to map out your network and applications
  - Extract data from key databases and move the data out of the network so that it can be used later (selling on the Dark Web)
  - Remove all evidence that you have been compromised but maintain network presence for future attacks

- What can you do to protect your organization against ATP attacks?
  - Be extremely careful when reviewing e-mail messages—don't open attachments or click on links unless you are completely confident of the source of the e-mail
  - Ensure that your AV software is installed, working and up to date
  - This type of attack most always requires advanced expertise—a dedicated security expert on staff or hiring a MSSP (Managed Security Service Provider)

Presbyterian Church (U.S.A.)
Presbyterian Mission

What can you do?

- Stay focused – this is the most important!
  - Review every e-mail carefully before opening attachments or clicking on links
  - If you are even a bit suspicious, delete and empty your email trash
- Protect yourself with the best of breed anti-virus and anti-malware solutions
- Back up your data – preferably to two different locations (local and cloud)
- Find a free (and paid) cyber security course and take it (and take it seriously)
  - ESET.com and Cybrary.it both offer free courses. Wombat and Knowbe4 are the top subscription-based security training vendors.
- Stay up to date on your patches!
  - PC's, phones, tablets and iOT devices (stoves, thermostats, light bulbs, refrigerators, etc).
- Be cautious when surfing the web
  - Freeware and rogue websites can cause big issues

Presbyterian Church (U.S.A.)
Presbyterian Mission

Advances in fighting cyber crime

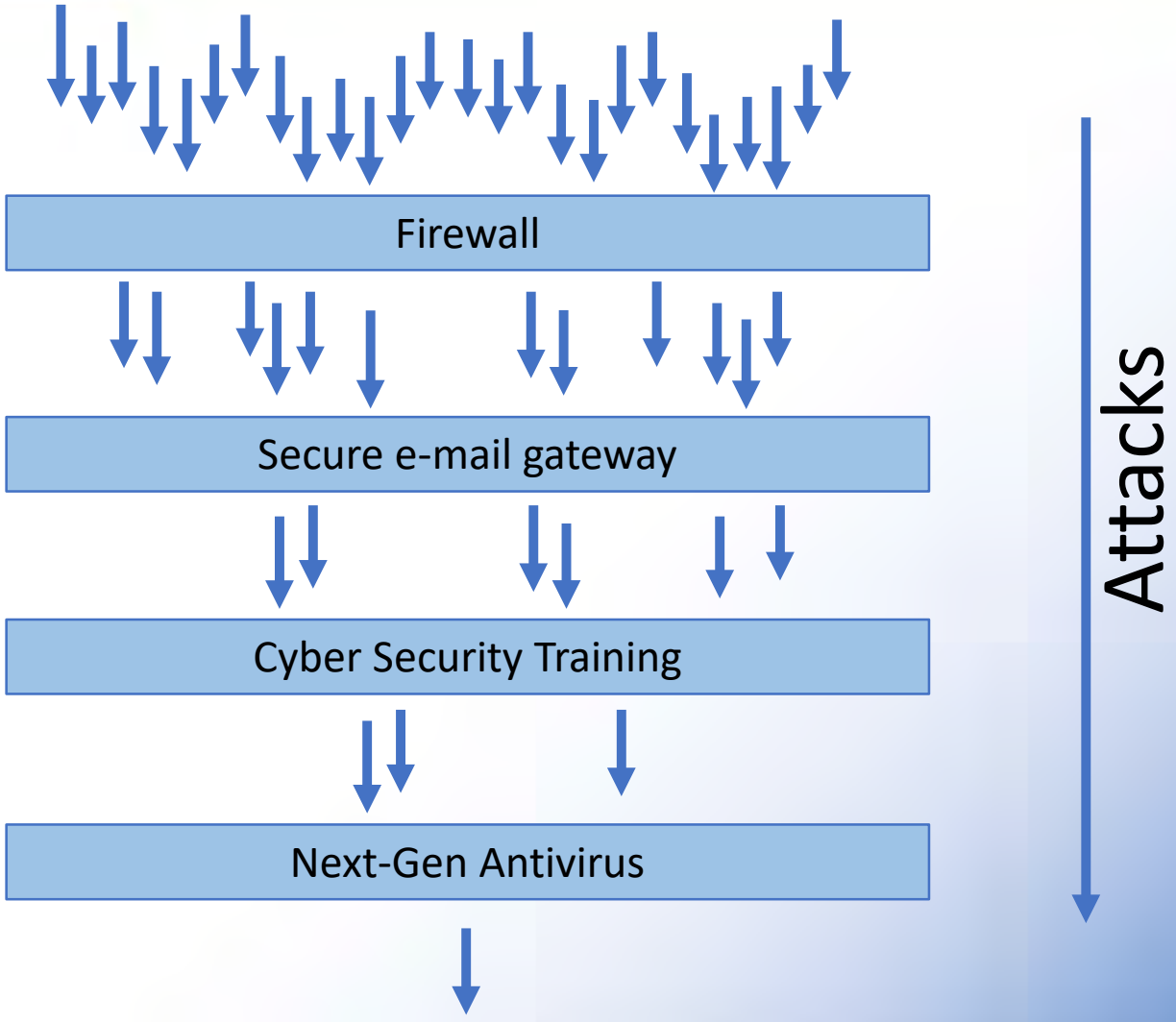
- **Better anti-virus/anti-malware solutions based on sophisticated predictive mathematical algorithms that can detect malware patterns (Cylance, Carbon Black and others)**
  - **Some actually try to keep track of infected URL links and will block them if you accidentally click on them**
- **More emphasis on security by subscription services like Office 365 (Advanced Threat Protection)**
- **Focus on cyber security awareness and education (staysafeonline.org, wombat.com, knowbe4.com)**

OpenDNS
Carbon Black.
KnowBe4 Human error. Conquered.
CYLANCE
wombat security technologies
SentinelOne
Office 365

Presbyterian Church (U.S.A.)
Presbyterian Mission

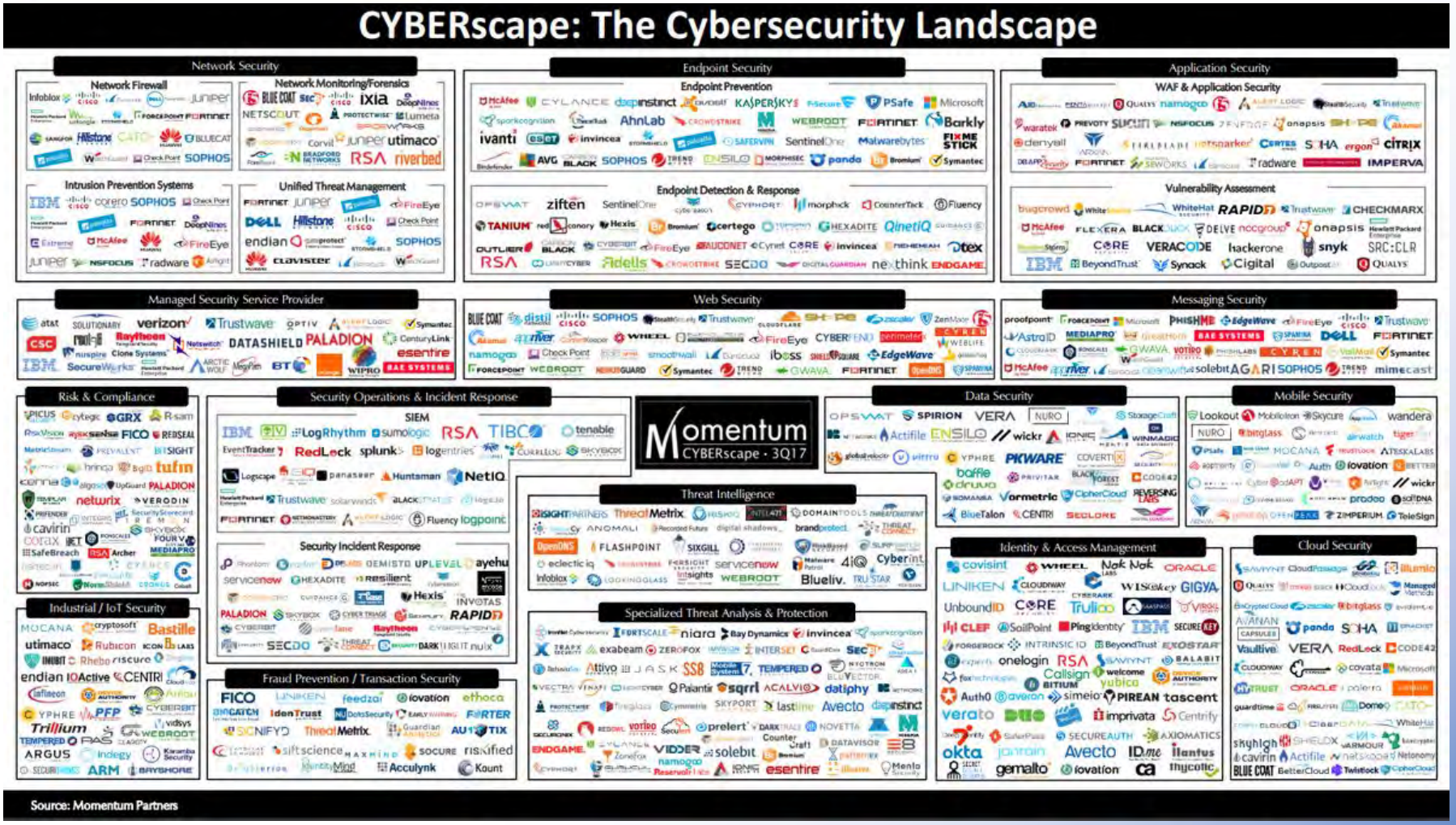
Layered approach to security

There is no cyber security "silver bullet"—you need a layered approach using multiple technologies



Presbyterian Church (U.S.A.)
Presbyterian Mission

Cyber Security Vendor Landscape



Source: Momentum Cyber Security Group, LLC

Presbyterian Church (U.S.A.)
Presbyterian Mission

Learn more about various threats

Government of Canada

https://www.getcybersafe.gc.ca/cnt/rsks/cmmn-thrts-eng.aspx

Awareness is the key!

Questions?