

Cyber Security Threats - 2018



Presbyterian Church (U.S.A.)

Presbyterian Mission

David Dinkel

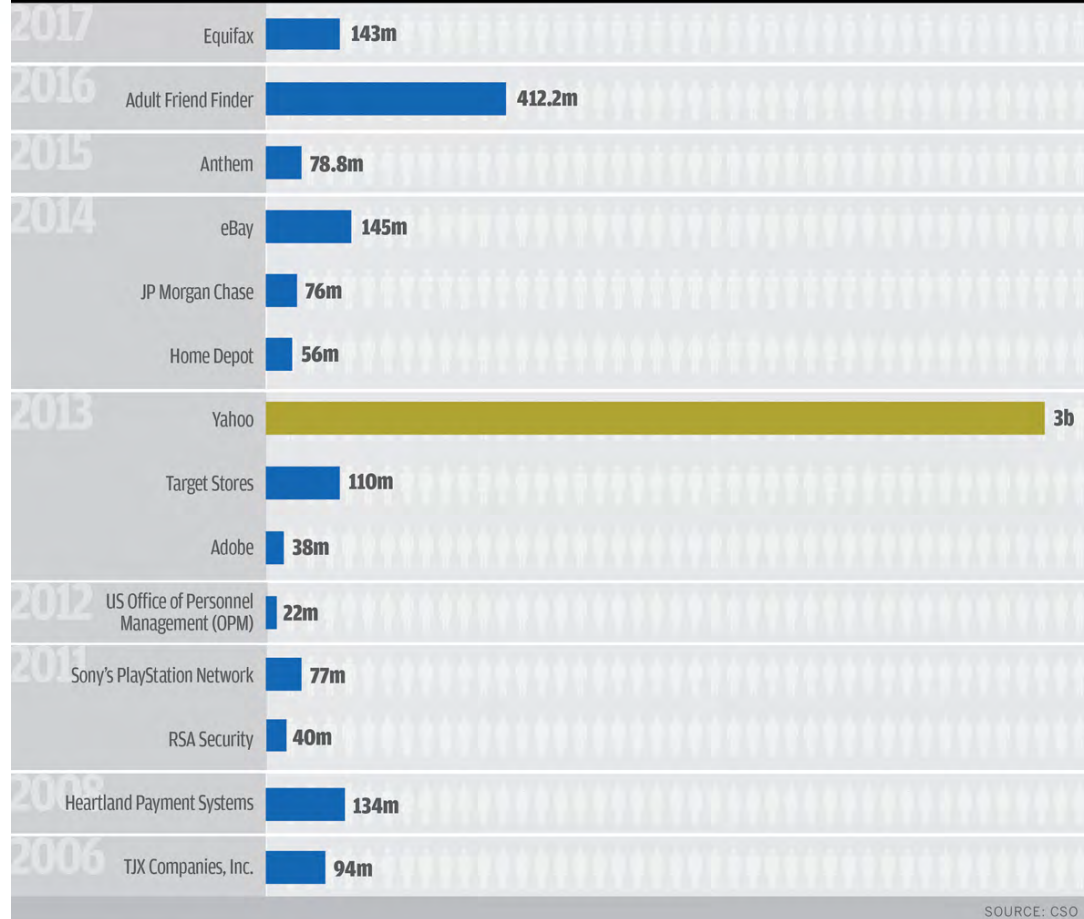
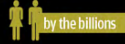
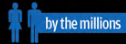
PC(USA) Information Technology



Can my company or organization be breached?

Biggest **DATA BREACHES** of the 21st century

Accounts
Compromised



SOURCE: CSO



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.





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

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

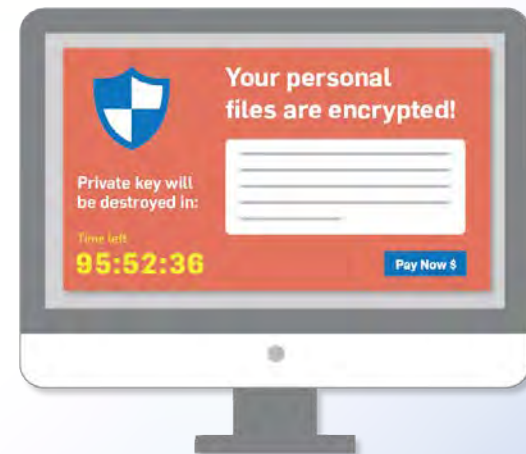
1. Socially engineered malware (Ransomware)
2. Password phishing attacks
3. Unpatched software
4. Social media threats
5. Advanced persistent threats





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.)

The screenshot shows the Wana Decrypt0r 2.0 ransomware interface. It features a dark red background with white and yellow text. On the left, there is a large white padlock icon. Below it, two boxes indicate payment deadlines: 'Payment will be raised on 5/15/2017 16:32:52' and 'Your files will be lost on 5/19/2017 16:32:52', each with a corresponding 'Time Left' counter. The main text area contains sections titled 'What Happened to My Computer?', 'Can I Recover My Files?', and 'How Do I Pay?'. At the bottom, there is a Bitcoin payment section with a QR code, a Bitcoin address, and a 'Copy' button. Two buttons, 'Check Payment' and 'Decrypt', are located at the bottom right.

Wana Decrypt0r 2.0 [English]



Payment will be raised on
5/15/2017 16:32:52
Time Left
02: 23: 59: 49

Your files will be lost on
5/19/2017 16:32:52
Time Left
06: 23: 59: 49

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send \$300 worth of bitcoin to this address:
 **bitcoin** ACCEPTED HERE
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw [Copy]

[About bitcoin](#)
[How to buy bitcoins?](#)
[Contact Us](#)



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**



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





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





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)**



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





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)



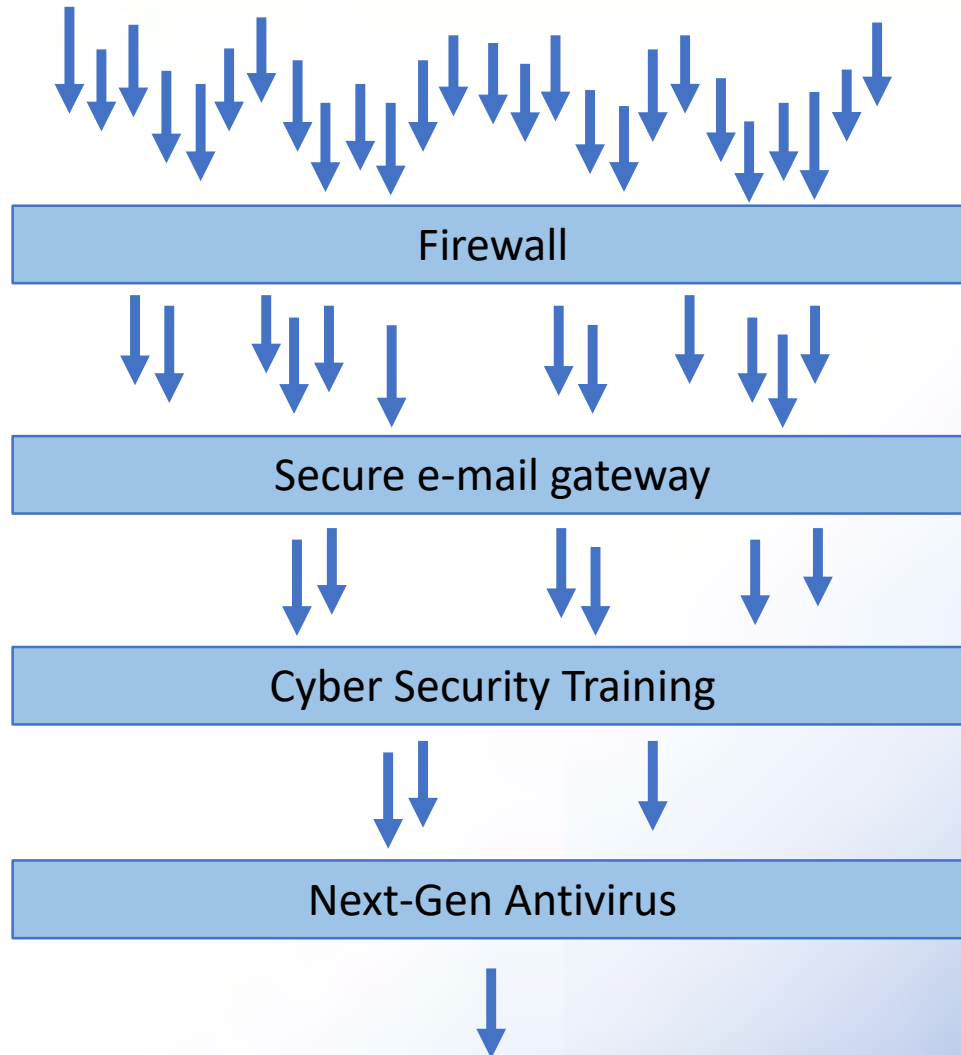
Carbon Black.





Layered approach to security

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

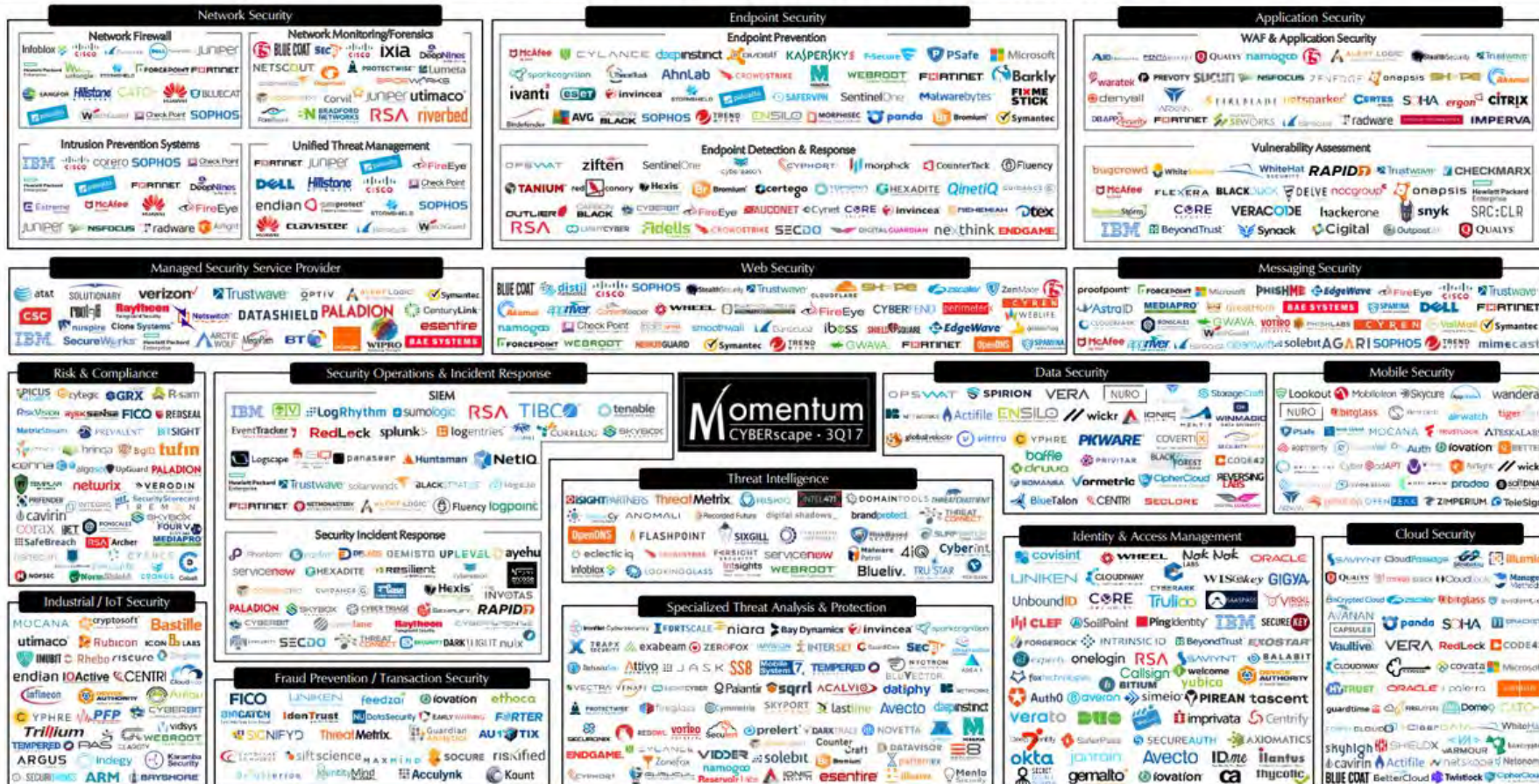


Attacks



Cyber Security Vendor Landscape

CYBERscape: The Cybersecurity Landscape





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!



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

Questions?

