The Pulse of Cyber Security
About Me

Clayton Darnell, CISSP

- In information security for 10+ years
- Experience from defense manufacturing, restaurant, security consulting and telecom industries
- BS in Information Security
- Two adorable dogs

My opinions are solely my own and not representative of my employer

These are not regulatory or legal recommendations. Should be considered best practices
Goals!

- Overview of current events
- Review risk and impact
- Homework
Agenda

- Definitions!
- What has changed?
- Worst case scenarios are real!
- Using history to look forward
- Security is incomplete without U!
- Questions?
Definitions!

**Ransomware**
- A type of malware that threatens to block access to user’s data unless a ransom is paid.

**Malware**
- Software that is intended to damage or disable computers and computer systems.

**Data Breach**
- Data has potentially been viewed, stolen or used by an individual unauthorized.

**Exploit**
- Software designed to take advantage of a flaw in a computer system, typically for malicious purposes such as installing malware.
What has changed?

- Malware grows more destructive
  - CryptoWall – 2015 - email delivered ransomware
  - Locky – Q1 2016 – email delivered ransomware
  - SamSam – Q1 2016 – spread through backdoors in web applications
  - WannaCry – Q2 2017 – spread over the internet
  - NotPetya – Q2 2017 – Targeted cyber-attack on Ukraine

- Cyber Attacks in healthcare are leading to full stop of operations.
Worst Case Scenarios Are Real

---

Our computer network was compromised as part of a global hacking of computer networks.

To meet patient needs, we need to ensure network continuity.

We believe we have the systems in place to recover.

As we address this, we will continue to communicate updates and protect patients, our employees, and our business.

---

**Urgent!**

This hospital is on a major incident.

If your condition is not life threatening, please visit your GP or an another health care facility.

---

**Attention DLA Employees**

All network services are down. Do not turn on your computers! Please remove all laptops from docking stations. Keep them turned off.

*No exceptions*

---

**Customer Update**

We are working through the incident impacting our systems. Everything is being done to recover as soon as possible.

Further updates will follow.
On Friday May 12, 2017, it infected more than 230,000 computers in over 150 countries

Required no human interaction and spread over the internet

Utilized an Exploit called EternalBlue
  - Microsoft released a patch March 14th, 2017
  - Released by hackers on April 14th, 2017

Healthcare impact included:
  - Dharmais Hospital, Indonesia
  - Harapan Kita Hospital, Indonesia
  - U.K. National Health Services

Multiple medical systems found vulnerable
NotPetya

- Began on June 27, 2017
- Targeted at Ukraine
- Spread like WannaCry but only on private networks
  - Can spread through vendor, business and VPN connections
- Healthcare impact included:
  - Heritage Valley Health System of Pittsburgh
  - Pharmaceutical company Merck & Co.
  - Software provider Nuance Communications
Using history to look forward

But wait, you just said all of this is a new concern!

- Attacker’s motives stay the same
  - Money, fame, disruption, etc...
- Attacker’s methods follow similar paths
  - They reuse what they know works
  - They use known exploits
  - Usually issues are patched prior to attacks
Security is incomplete without U!

- Watch for malicious or unsolicited emails
  - Take caution when opening attachments
  - Don't give out your password
- Patch!
  - Or ask about patching!
- Research past issues for your organization
- Tabletop incidents with your Security and IT teams
- Put pressures on vendors to uphold good security practices as well
Questions?
Resources

- https://www.privacyrights.org/data-breaches
- https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf