Understanding Hacking Threats in a Complex Environment

Presented by:
Mac McMillan
Co-Founder & CEO, CynergisTek

CYNERGISTEK

CynergisTek, Inc.

Founded in 2004
CynergisTek has been providing services to our clients since 2004, but many of our clients have been with one or both of the founders since well before the company was founded.

Consulting Services
CynergisTek provides consulting services and solutions around information security, privacy, IT architecture, and audit with specific focus on regulatory compliance in healthcare.

Synergistic
The name "CynergisTek" came from the synergy realized by combining the expertise of the two co-founders – building scalable, mature information security programs and architecting enterprise technical solutions.

Securing the Mission of Care
CynergisTek Services are specifically geared to address the needs of the healthcare community including providers, payers, and their business associates who provide services into those entities.

Today's Presenter

- Co-founder & CEO CynergisTek, Inc.
- Chair, HIMSS P&S Policy Task Force
- CHIME, AEHIS Advisory Board
- Healthcare Most Wired Advisory Board
- HCPro Editorial Advisory Board
- HealthInfoSecurity.com Editorial Advisory Board
- Top 10 Influencers in Health IT 2013
- Top 50 Leaders in Health IT 2015
- Director of Security, DoD
- Excellence in Government Fellow
- US Marine Intelligence Officer, Retired

Mac McMillan
FHIMSS, CISM
CEO, CynergisTek, Inc.

Today's Topic

Agenda

- The Changing Nature of Threat
- The Future of Information Security
- Questions

Why Information Security is Challenging in Healthcare

- **The prime directive**. First priority is taking care of patients, and we need quick and easy access to information to do that.
- **Innovation**. A never-ending stream of new IT products and services are promising to improve the delivery of care.
- **Complexity**. Hundreds to thousands of applications must work together seamlessly, but also must be secured.
- **Costs**. Healthcare organizations are under pressure to reduce costs, making more spending to address security a tough sell.
- **Convergence**. Healthcare aggregates all forms of sensitive information: PHI, PII, PCI, etc.

Why Healthcare Workers Should Care About Information Security

- Protecting the personal data that we are entrusted with is the right thing to do, and in fact it's even part of the Hippocratic Oath!
  - *I will respect the privacy of my patients, for their problems are not disclosed to me that the world may know.*
- It's the law. In fact, there are multiple laws that affect healthcare organizations: HIPAA, HITECH, Meaningful Use, FISMA, FERPA, State Laws, etc…
- ***But Most Important*: Information security risks are now undermining healthcare's intellectual property, brand, and mission, and threatening patient care and safety in the process.**

Cybersecurity Risk

Strategic	Goals of the Organization
Operational	Processes that Achieve Goals
Financial	Safeguarding Assets
Compliance	Laws and Regulations
Reputational	Public Image

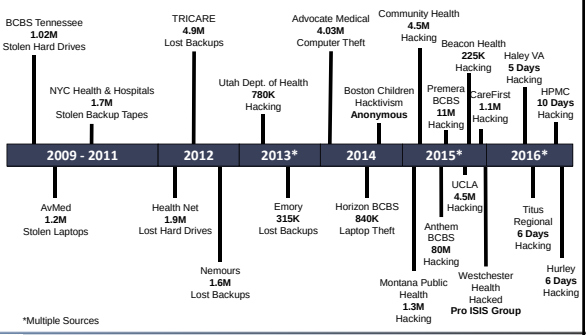
The Threat Changes

The Cyber Threat Spectrum

Hacktivism → Crime → Insiders → Espionage → Terrorism → Warfare

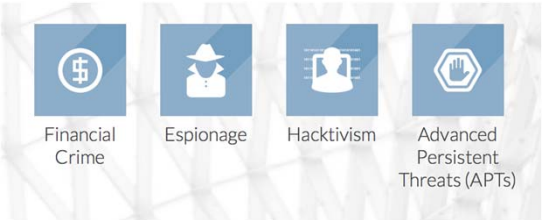
Evolving Healthcare Threat Landscape

From lost/stolen devices to hacking



*Multiple Sources

The Many Faces of Threat

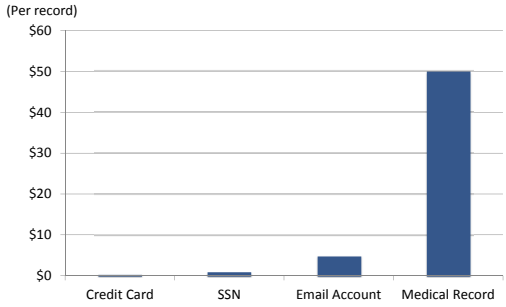


*Source: Understanding Cyber Attackers and their Motives. FireEye.

Cybercrime as a Business

- Trends in cybercrime all make cyber-criminals more effective
  - Cybercrime-as-a-service model* gives less technically-savvy criminals access
  - Dark web marketplaces make "monetizing" stolen data as easy as buying on Amazon
  - Cybercriminals are adopting tactics previously only used by nation-state attackers

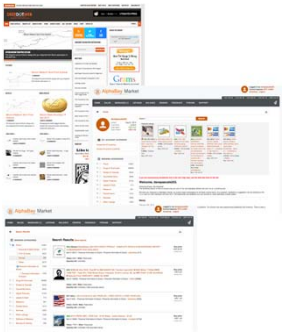
Black Market Value of Stolen Data



Sources: http://histalkmobile.com/2014-a-perfect-storm-for-data-breaches/
http://krebsonsecurity.com/2013/06/the-value-of-a-hacked-email-account/

Dark Web Marketplace

- A Bitcoin wallet, PGP for encrypted communication, and a TOR browser and you are in business…



Cyber Extortion is Rampant

- First appeared around 2005
- Two forms: Crypto ransomware (data) and Locker ransomware (system)
- Sophisticated attacks use:
  - New asymmetric keys for each infection
  - Industrial strength & private/public key encryption
  - Privacy enabling services like TOR and bitcoins for payments
- Indifferent to target, everyone is a target (home/business)
- Malvertising, spam email, downloaders/botnets & social engineering

The United States is the largest target worldwide by a huge margin. SOCs worldwide report as much as a 10X increase in ransomware attacks from December to January with no abatement.

Cyber Espionage is Growing

Cyber espionage is being carried out by nation-state actors for political purposes

- Large breaches such as Anthem, Premera, Community Health Systems, UCLA are suspected cases of espionage
- A case example is the OPM intrusion presumed by a Chinese group that captured security clearance documents
- But…they are also targeting industrial control systems that control and manage critical infrastructure

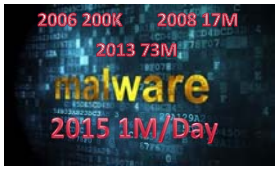
Hacktivism

- Attacking for a cause
  - Anonymous hacked Boston Children's in 2014 over a child parental rights case
  - GhostShell attacked several U.S. universities in 2015 leaking sensitive information
  - Anonymous hacked Hurley Medical Center in 2016 over the Flint Michigan water issue
  - Pro ISIS groups have hacked hospital websites

Targeted (APT) Attacks

Typically nation-state attack groups

- "APTs are known for being highly sophisticated, using multiple vectors to attack a target network, and having unrelenting tenacity"
- Many attacks go undetected for considerable periods of time, estimated 280 days on average
- Phishing, zero day attacks, ransomware have increased dramatically in 2016



"There is widespread agreement that advanced attacks are bypassing our traditional signature-based security controls and persisting undetected on our systems for extended periods of time. The threat is real. You are compromised; you just don't know it." – Gartner Inc., 2012

* Source: Understanding Cyber Attackers and their Motives. FireEye, 2015.

What Are Vendors Doing With PHI?

May 2014

UBER

"There you are, I was tracking you."

- The taxi-hailing commuter platform Uber had two breaches in 2014 that weren't reported until 2015 gaining the ire of the New York SAG.
- What they did:
  - First they allowed internal users access to riders PII and displayed it through a tracking system called "God View".
  - Second they had a breach of their riders data base that permitted a third party access to 50,000 riders PII on GitHub.
- The settlement requires Uber to employ encryption, better access controls and multi-factor authentication.
- Health Systems are partnering with Uber to help patients not miss appointments.

How Secure Are Vendor Solutions?

December 2015

JUNIPER NETWORKS

- Juniper admits Netscreen firewalls have been vulnerable for 8+ years.
- Juniper continued to use compromised Duel_EC encryption even after NIST and others recommended discontinuance.
- Juniper added Dual_EC to its firmware in 2008.
- Investigators are trying to determine if this was random, but do not believe it was.
- Regardless Juniper did not move to fix until outed by researcher.

The Insider Threat

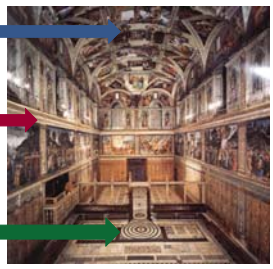
- *93% feel vulnerable to insider threats*
- *59% worry about privileged users most*
- *Contractors/service providers next biggest concern*
- *2010-2015 20% increase in ID/Med ID theft*
- *37% feel user awareness training is failing*
- *Traditional audit methods are failing right and left*

Closing the Gap

Security is the ceiling.

Leadership are the walls that bring security and compliance together.

Compliance is the floor.



Building an Information Security Program

Knowledge: Anatomy of a Cyber Attack

Frameworks: A Common Taxonomy For

- Describing an organization's **current** cybersecurity posture
- Describing its **target state** for cybersecurity
- Identifying and **prioritize** areas of improvement
- Employing a **repeatable** process for review
- Continuously **assessing** its cybersecurity posture
- **Communicating** cybersecurity risks to both internal and external stakeholders
- Conducting regular **measurements** of control effectiveness
- **Demonstrating** compliance

A *Holistic* Approach To Data Security

Reference: NIST Cybersecurity Framework

Adopt an *Offensive* Posture

- ***Educate and inform***, ensure users know how to identify and avoid common threats
- ***Remain current***, refresh, harden, patch and manage system configurations with diligence
- ***Employ layers***, protections at the endpoint, network, file layers, etc. can make it more difficult for hackers
- ***Deploy complimentary controls***, use both signature or rule based solutions with heuristic solutions
- ***Enhance detection***, deploy NGFWs, malware filters, A/V filters, IDS/IPS, etc.
- ***Prioritize contingency planning***, back up everything, offline as well, practice incident response
- ***Be ready***, establish relationships, acquire tools
- ***Be objective***, use independent third parties to perform readiness audits, tests and assessments

The United States is the largest target worldwide by a huge margin when it comes to advanced persistent threats.

Where Do We Start? *Risk Assessment*…

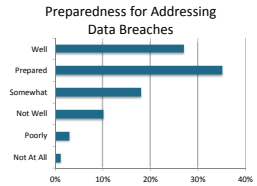
Expect A *Smart* Defense

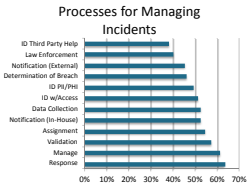
38% have had more than five incidents.

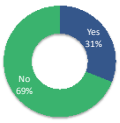
90% of healthcare organizations have experienced at least one data breach in the past two years.

Incidents in most cases can be prevented by following well known policies, procedures, standards and best practices.

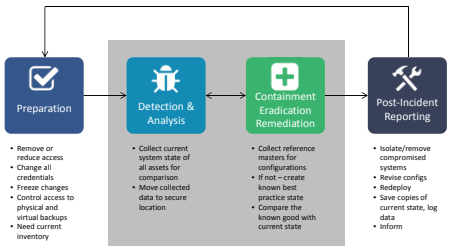
Make *Preparedness* A Priority







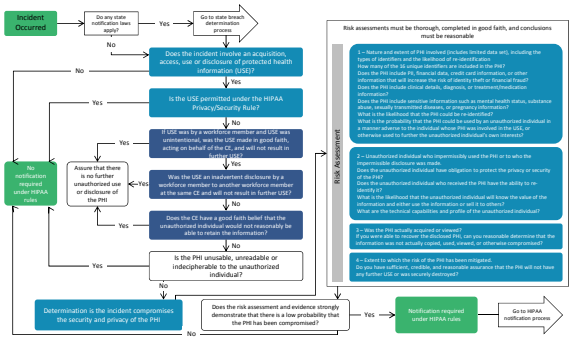
Organization & Practice Are Critical



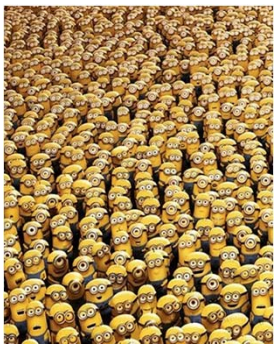
> Life is about timing. – Carl Lewis
>
> So is breach mitigation – Mac McMillan

Discipline Yields Better Results

HIPAA Breach Notification Decision Flowchart



Enlist *ALL* of Your Security Team



- Training & awareness at all levels:
  - Workforce
  - IT Staff
  - IRM Members
  - Executives
  - Board
- New approaches that focus on interaction.

Governance and Support Are Crucial

- Majority of boards report that they do not understand cyber threats
- Many executives report that they just expect its covered
- Boards/execs are becoming more involved and interested in security
- They still want to know how it ties into the business

It's Time For A Paradigm Shift

What Can We Expect

- Social engineering attacks targeting people will continue increase (phishing, water cooler, social media) as hackers first option
- IoT will provide basis for attacks on attached devices of all kinds
- Ransomware will continue to be successful in targeting healthcare
- Medical device and wearable hacks will surface soon
- Growth in cybercrime-as-a-service make attacks viable for less sophisticated actors

Resources for Getting Started

- HealthIT.gov Guide to Privacy and Security of Electronic Information (v2.0, April 2015)
  - http://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf
- FTC start with security program
  - https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business
- Critical security controls project
  - https://www.sans.org/critical-security-controls/
- NIST Cybersecurity Framework
  - http://www.nist.gov/cyberframework/
- Poster series
  - http://www.ncsc.gov/publications/pii/index.html
- Protecting your personal information awareness videos
  - http://www.dni.gov/index.php/resources/protecting-personal-information

Questions

Questions?

Mac McMillan
mac.mcmillan@cynergistek.com
512.405.8555
@mmcmillan07