



CYBER SECURITY: Trends and Tips to Manage, Respond to, and Mitigate Risk

PRESENTED BY:

- Andrea Eklund, VP/Chief Compliance Officer
• Unity Point Clinic
- Mac McMillan, President & CEO
• CynergisTek, Inc.

WHAT'S NEW? Current and Future Security Threats

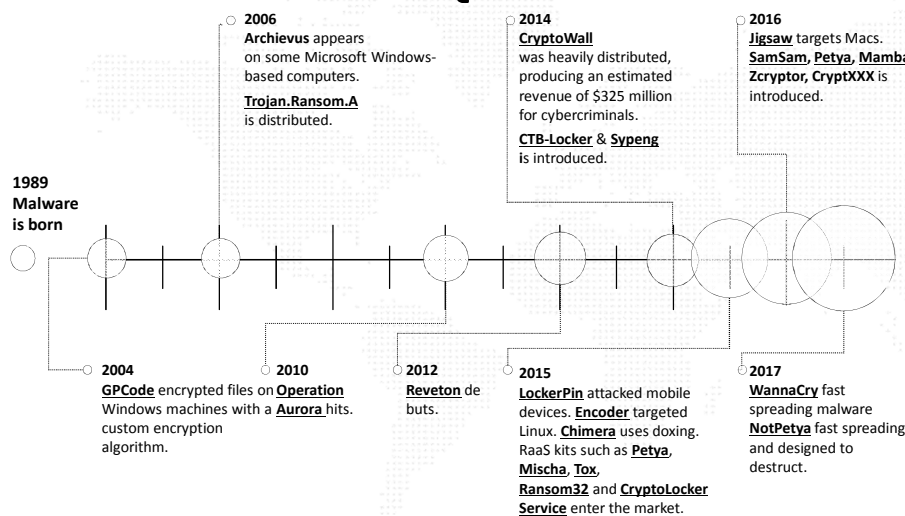
THE NEW REALITY OF HEALTHCARE



- Ransomware
- Phishing
- Hacked Workstation
- FTP Server Misconfigured
- Website Breach
- Database Misconfigured
- Email Breach
- Malware Attack
- Stolen Laptop

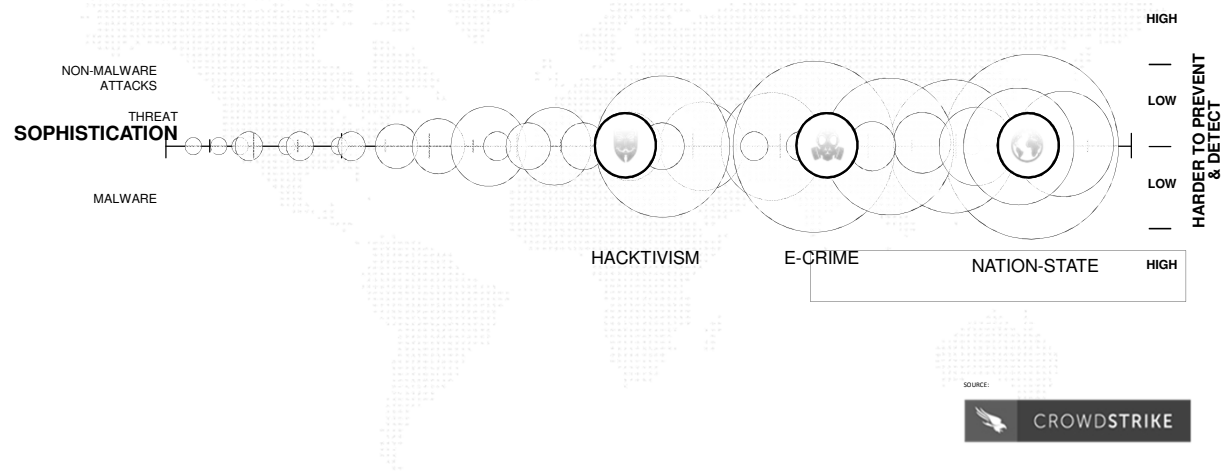
3

ATTACKS ARE GROWING IN FREQUENCY



- Every time a new smartphone is turned on, the digital attack surface grows. Every time a new device is connected to the Internet of Things (IoT), the cyber landscape becomes less secure.
– McKinsey & Company
- Industry experts estimates healthcare cyberattacks rose 320% between 2015 and 2016.
- Healthcare has emerged as the most frequently targeted industry, with 164 threats detected per 1,000 host devices.
– Vectra Networks Industry Report 2017
- Accordingly, health care cybersecurity spending is expected to reach nearly \$65 billion by 2021.
– Cybersecurity Ventures 2017

ATTACKS ARE GROWING IN SOPHISTICATION



IMAGINE.....



Your CEO Getting
Ready for an
Evening Out.....

AN AFTER HOURS CALL....NEVER GOOD NEWS

- Did you prepare?
- Do you know what impact looks like?
- Do you know how to respond?



7

WHAT IMPACT LOOKS LIKE

- Elective surgery and general appointments cancelled!
- Diversion
- A/R delays
- Payroll issues
- Two full weeks of downtime – enterprise-wide
- Opened Incident Command Center – 24/7
- Paper processing for nearly everything
- Younger staff were often clueless – “Thank God for older nurses!”
- Needed many “runners” to go everywhere (pick up lab orders, etc.)
- Confusion and inconsistency re: backloading of data/charges

8

WHAT IMPACT LOOKS LIKE

- **“Downtime Boxes”** were designed for 2-3 days
 - Ran out of forms and prescription pads
 - Used print shop for what they could
 - Old versions of paper order sets
- **Phones** initially impacted (on the same network)
 - Lost ACD/menu functionality for several days
- **OR schedule** reviewed for “elective” or “postpone-able” procedures
 - No PACS availability – access to images a challenge
- **Business Continuity Devices** – lost nearly all value after a couple of days
- **IT** directed to focus on payroll and materials mgmt.
 - You have to pay your staff and order your supplies
- **EMR** was never actually infected – but limited workstation access made it virtually unusable/inaccessible
 - Focused on a few workstations in order to maintain up to date census

9

IMPACT ON PEOPLE

- **Staff** burn-out, mistakes, stress, irritability
- **Forced** a few “stay home” days for some staff
- **Stress/worry** that any negative patient outcome would be “our” fault
- **Stress/worry** about missing something critical increases
 - Access to servers/databases with critical cancer regimen data
 - Access to old clinical data/images
 - Access to allergy data, etc.
- **“Remediation services”** not what was expected
 - Required obtaining extra staff from peer organizations and temp agencies

10



WHO'S JOB IS IT ANYWAY?

Overlapping roles of compliance and security in identifying and assessing security threats.

COMMON GOAL

- **Protect the organizational data**
- **Know current state by:**
 - **Proactively identifying risk;**
 - **Assessing business impact;**
 - **Documenting assumption or mitigation of risk; and**
 - **Monitoring controls put in place.**
- **Be prepared to respond**

ROLES AND RESPONSIBILITIES

- **Compliance**
 - Assess and manage the organization's compliance regarding applicable laws, regulations, and policies.
 - Monitor adherence to policies and procedures.
- **Information Security**
 - Defines, analyzes, and addresses security risks that threaten business activity.
 - Risk Assessment
 - Business Impact Analysis

13

ROLES AND RESPONSIBILITIES

- | | |
|---|--|
| <ul style="list-style-type: none">• Compliance<ul style="list-style-type: none">- Evaluate policies and procedures to ensure regulatory requirements are met.- Test procedures to determine if they are working as intended.- Address gaps by working with operational leadership to create a Corrective Action Plan ("CAP").- Monitor CAP progress.- Document resolution. | <ul style="list-style-type: none">• Information Security<ul style="list-style-type: none">- Identify controls to meet regulatory requirements.- Test procedures to determine controls are working as intended.- Conduct Risk Assessment<ul style="list-style-type: none">▪ Accept risk and document mitigating controls.▪ Identify mitigation measures and implement CAP.▪ Document resolution. |
|---|--|

14



HOW TO LINK THE COMPLIANCE AND SECURITY FUNCTION. Practical strategies

OVERSIGHT RESPONSIBILITY

- **Reporting Structure.**
 - Information Security report to Compliance, CEO, or Board.
 - Routine Board Reporting and Education.
- **Compliance Committee includes ISO.**
- **Enterprise Risk Management Committee includes Compliance and ISO.**

BOARD REPORTING

Theft & Loss

Nearly half of all breaches involve some form of theft or loss of a device not properly protected or paper.

Insider Abuse

Breaches in healthcare continue to be carried out by knowledgeable insiders for identity theft, tax fraud, and financial fraud.

Unintentional Action

Breaches caused by mistakes or unintentional actions such as improper mailings, errant emails, or facsimiles are still prevalent.

Cyber Attacks

Majority of large breaches reported in 2017 involved some form of hacking and represented nearly 99% of the records compromised.

17

BOARD REPORTING

- Cybercrime will cost businesses over \$2 trillion by 2019
- 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



BOARD REPORTING

- Financial impact/risk
- Financial support for prevention
 - 89% of respondents said their 2018 budgets were dedicated to business functions
 - “Only a small fraction” was being saved for cybersecurity

Q4 2017 Black Book survey (323 strategic decision makers in US HCOs – provider and payer)

- Financial support for response/resumption



19

CHANGING RISK PRIORITIES

From “Business Critical” to “Mission Critical” to “Life Critical”

Confidentiality	Availability	Integrity
<ul style="list-style-type: none"> • PHI (HIPAA) • But also PII & PCI • Account information • Billing & payment data • Intellectual property <ul style="list-style-type: none"> - Clinical trials - Research - Design & formularies • Legal & HR documents • Identities & credentials 	<ul style="list-style-type: none"> • Clinical systems <ul style="list-style-type: none"> - EHR & specialty - Ancillary (PACS, lab, pharma) - ePrescription/EPCS • Medical devices <ul style="list-style-type: none"> - Availability of clinical services and results • Business systems <ul style="list-style-type: none"> - Email - Billing, scheduling 	<ul style="list-style-type: none"> • Critical patient data <ul style="list-style-type: none"> - Prescriptions, medications - Dosages - Allergies - History - Diagnosis - Alarms • Critical technical data <ul style="list-style-type: none"> - Calibration - Safety limits
Patient Experience: “Patient Trust Zone”		
Patient Harm: “Patient Safety Zone”		

20

THANK YOU



Questions?

Mac McMillan, FHIMSS, CISM
President & CEO
mac.mcmillan@cynergistek.com
512.402.8555

Andrea Eklund
VP & CCP
andrea eklund@unitypoint.org
515.471.9304