WHAT’S NEW? Current and Future Security Threats

- Ransomware
- Phishing
- Hacked Workstation
- FTP Server Misconfigured
- Website Breach
- Database Misconfigured
- Email Breach
- Malware Attack
- Stolen Laptop
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 estimate 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, healthcare cybersecurity spending is expected to reach nearly $65 billion by 2021.
- Cybersecurity Ventures 2017

1989 Malware is born
2004 GPCode
encrypted files on Windows machines with a custom encryption algorithm.
2010 Operation Aurora hits.
2006 Archievus appears on some Microsoft Windows-based computers.
Trojan.Ransom.A is distributed.
2014 CryptoWall was heavily distributed, producing an estimated revenue of $325 million for cybercriminals.
CTB-Locker & Sypeng introduced.
2015 LockerPin attacked mobile devices.
Encoder targeted Linux.
Chimera uses doxing.
RaaS kits such as Petya, Mischa, Tox, Ransom32 and CryptoLocker Service enter the market.
2016 Jigsaw targets Macs.
SamSam, Petya, Mamba, Zcryptor, CryptXXX is introduced.
2012 Reveton deuts.
2017 WannaCry fast spreading malware NotPetya fast spreading and designed to destruct.

ATTACKS ARE GROWING IN SOPHISTICATION

THREATS

MALWARE NON-MALWARE

NATION-STATE HACKTIVISM E-CRIME

HARDER TO PREVENT & DETECT

LOW HIGH HIGH LOW

SOURCE: IMAGINE…………… IMAGINE…………… IMAGINE…………… IMAGINE……………

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?

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

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
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

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

**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 19% of the records compromised.

• 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
  - 80% 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 (CEO change, medium in US HCOs - provider and payer)
- Financial support for response/resumption

CHANGING RISK PRIORITIES

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

<table>
<thead>
<tr>
<th>Confidentiality</th>
<th>Availability</th>
<th>Integrity</th>
</tr>
</thead>
<tbody>
<tr>
<td>PHI</td>
<td>Clinical systems</td>
<td>Critical patient data</td>
</tr>
<tr>
<td>PII</td>
<td>HR &amp; specialties</td>
<td>Prescriptions, medications</td>
</tr>
<tr>
<td>PCI</td>
<td>Medical decisions</td>
<td>Designs</td>
</tr>
<tr>
<td>HIPAA</td>
<td>Availability of clinical services and results</td>
<td>Allergies</td>
</tr>
<tr>
<td>Technical</td>
<td>Business systems</td>
<td>History</td>
</tr>
<tr>
<td>Information</td>
<td>Email</td>
<td>Diagnosis</td>
</tr>
<tr>
<td>Intellectual</td>
<td>Billing, scheduling</td>
<td>Alarms</td>
</tr>
<tr>
<td>Property</td>
<td>Critical technical data</td>
<td>Critical operations</td>
</tr>
<tr>
<td>Legal</td>
<td>Clinical systems</td>
<td>Critical access</td>
</tr>
<tr>
<td>&amp;</td>
<td>Medical devices</td>
<td>Critical applications</td>
</tr>
<tr>
<td>Business</td>
<td>Availability &amp; overview</td>
<td>Critical compliance</td>
</tr>
<tr>
<td>Services</td>
<td>Billing &amp; payment</td>
<td>Critical informatics</td>
</tr>
<tr>
<td>Clinical</td>
<td>Clinical systems</td>
<td>Critical maintenance</td>
</tr>
<tr>
<td>Services</td>
<td>Results</td>
<td>Critical infrastructure</td>
</tr>
<tr>
<td></td>
<td>Business systems</td>
<td>Critical business</td>
</tr>
<tr>
<td></td>
<td>Legal &amp; HR documents</td>
<td>Critical technical services</td>
</tr>
<tr>
<td></td>
<td>Policies &amp; procedures</td>
<td>Critical technical systems</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Critical physical security</td>
</tr>
</tbody>
</table>

Patient Experience: "Patient Trust Zone"
Patient Harm: "Patient Safety Zone"

THANK YOU

Questions?

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

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