Defending the Telehealth Ecosystem

Ronnie Daldos, CISSP
Lead Cyber Engineer
Cyber Physical and Mobile Technologies
The Power of Perspective

Common problems have common solutions

Systems thinking approach enables effective solutions

Integrating best practices across the public and private sector to resolve barriers to care to improve health outcomes within our communities

Our mission is to solve problems for a safer world.
Agenda

- Telehealth Ecosystem—A Complex “System of Systems”
- Cybersecurity and Privacy Risks
- Threat-Informed Defense
- Home Telehealth Use Case
- Key Takeaways
Enabling Healthcare Delivery and Outcomes

Innovative Concepts (e.g., AI with Wearables)

Remote/On Demand Staffing (e.g., Surge)

Store and Forward

Home Telehealth

Clinical & Web-Based Video

Rural Health Access

Disaster Response

©2018, The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited. Case number 18-0665.
The Telehealth Ecosystem
A Complex “System of Systems”

A highly distributed infrastructure with multiple access methods under independent management often utilizing multi-tenant environments.

*PGD=Patient Generated Data, BAA = Business Associate Agreement
Examples of Telehealth Cybersecurity and Privacy Risks

Unsecured Networks Present New Attack Vectors

Impersonation/Spoofing

Unsecured Endpoints (e.g., Medical, Consumer Devices)

Data Exfiltration
# Existing Defenses Inadequate to Protect Against the Growing Cyber Threat

<table>
<thead>
<tr>
<th>Changing Healthcare Environment</th>
<th>Existing Healthcare Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Growth in telehealth services</td>
<td>- Increased level of interconnectedness</td>
</tr>
<tr>
<td>- Emphasis on value based care, meaningful use and changes in reimbursement models</td>
<td>- Expanded attack surface</td>
</tr>
<tr>
<td>- Electronic information sharing for coordinated care (e.g., EHR)</td>
<td>- Distributed ownership &amp; management</td>
</tr>
<tr>
<td>- Mobility &amp; interconnected medical devices</td>
<td>- Cloud hosting in multi-tenant environment</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Existing Healthcare Defenses</th>
<th>Critical Needs</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Focus on perimeter/defense in depth</td>
<td>- Ensure the confidentiality, integrity, availability, and safety of the healthcare services providing patient care.</td>
</tr>
<tr>
<td>- HIPAA Compliance vs threat focus</td>
<td>- Improve existing defenses which are a soft target for the advanced persistent threat and criminal actors</td>
</tr>
<tr>
<td>- Lack of cyber situational awareness</td>
<td>- Identity and Access Management (IDAM)</td>
</tr>
<tr>
<td>- Limited technology funding</td>
<td>- Improve cyber situational awareness</td>
</tr>
<tr>
<td>- Limited qualified cyber workforce</td>
<td></td>
</tr>
</tbody>
</table>

A threat-informed defense will improve upon existing defenses by providing healthcare organizations a structured approach to identify, prioritize, and mitigate cyber risk.
Why Use a Threat-Informed Approach?

- Taking a threat-informed approach to cyber risk management allows:
  - Prioritizing limited cyber resources & funds on threats most relevant to your environment.
  - Assessing based on risk rather than compliance.
  - Understanding cyber adversary tactics, techniques and procedures (TTPs).
    - Identify gaps in defense & detection capabilities
    - Strategic tool acquisition
What is a Threat-Informed Defense?

- Knowledge of the adversary’s goals and motivations
- Identification of relevant threats
  - Sources of Threat Intelligence - Internal sources, NH-ISAC/ISAO’s, MITRE CAPEC™ & ATT&CK™
- An asset inventory with identification of their vulnerabilities
  - NIST National Vulnerability Database (NVD) – CVE®, CWE™, US/ICS-CERT
- Ranking system to prioritize threats (e.g., likelihood, impact)
- Security controls that mitigate risk
- Test cases that are exercised to evaluate the effectiveness of security controls
- Reevaluate your environment against new threats
Who is Targeting Healthcare?

**Insider Threat**

Anthem: Insider theft exposes data of 18,000 Medicare members

Anthem’s Medicare insurance coordination services vendor discovered in April that an employee was stealing and misusing Medicaid member data from as early as July 2016.

**Criminals**

Allscripts Ransomware Attack a Reminder of Cloud Risks

Points to heed for clients to view business continuity plans.

**Hacktivist**

‘Anonymous’ Targets Children’s Hospital

Supporters of the hackers collect the known as Anonymous have taken up the cause of a young girl after the State of Massachusetts removed her from her parents earlier this year. However, the method used to draw attention may have unintended consequences, which could impact patient care.

**Nation State**

NHS cyber-attack was ‘launched from North Korea’

By Christian Cueva

Security researcher, BBC News

10 June 2017
## Understanding Your Adversaries

<table>
<thead>
<tr>
<th>Adversary</th>
<th>Targeted (Specific Victims)</th>
<th>Untargeted (Indiscriminate)</th>
<th>Targeted (Specific Victims)</th>
<th>Untargeted (Indiscriminate)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individual / Small Group</td>
<td>YES</td>
<td></td>
<td></td>
<td>YES</td>
</tr>
<tr>
<td>Political Groups / Hacktivists</td>
<td>YES</td>
<td></td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Organized Crime</td>
<td>YES</td>
<td></td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Terrorism / Terrorist Org.</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
<tr>
<td>Nation States</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
<td>YES</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Threats addressed by existing defensive capabilities</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Threats not addressed by existing defensive capabilities</strong></td>
</tr>
</tbody>
</table>
Use Case: Home Telehealth

**Threat:** Modify or disable ICD

**Vulnerability:** Weak or non-existent access controls

**Mitigation:** IDAM

---

**Threat:** Gain access to the monitor

**Vulnerability:** Hard Coded Passwords

**Mitigation:** Code Security Review, Patch, IDAM

---

**Threat:** Intercept data or credentials

**Vulnerability:** Endpoint communications not verified.

**Mitigation:** Encryption, IDAM

---

**Threat:** Compromise integrity & availability of patient data

**Vulnerability:** Insecure Application Program Interface (API)

**Mitigation:** Encryption, Code review, Continuous Monitoring of API

---

**Threat:** Gain access to clinicians credentials

**Vulnerability:** Targeted Users

**Mitigation:** User Education, 2FA, Least Privilege

---

**NOTE** – Requires solution aligned with clinical constraints

©2018, The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited. Case number 18-0665.
Key Takeaways

- Telehealth is transforming the delivery of healthcare
- The telehealth ecosystem is a complex system of systems
- Taking a threat-informed approach to risk management helps you identify & prioritize threats that are relevant to the telehealth ecosystem.
- Prioritizing threats helps to focus cyber resources and funds on threats that are most likely to have the highest impact on the telehealth ecosystem.
- Reevaluate for threats and vulnerabilities anytime changes are made within the telehealth ecosystem.
Thank You!

Questions?

Interested in learning more about MITRE ATT&CK?
Julie Connolly from MITRE and Denise Anderson from NH-ISAC will be presenting:

“Detecting Cyber Threats with ATT&CK™ Analytics”

Tomorrow (3/7) @ 10am Session #123 - Marcello 4401
Follow up

To download a copy of this presentation, visit:

https://health.mitre.org/himss18

Improving the Patient Experience  Protecting Data & Devices

Follow us on social media: @MITREhealth

©2018, The MITRE Corporation. All rights reserved. Approved for public release. Distribution unlimited. Case number 18-0665.