Adaptive Threat and Risk Framework for Securing IoT in Healthcare

Building Elements for Next Generation Security Operations

AT&T Security Solutions
Introductions

<table>
<thead>
<tr>
<th>Carisa Brockman</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Governance, Risk, and Compliance Practice Director; AT&amp;T Security Consulting</td>
</tr>
<tr>
<td>• Over 16 years experience in information security</td>
</tr>
<tr>
<td>• Involved in HITRUST since inception</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Terry Hector</th>
</tr>
</thead>
<tbody>
<tr>
<td>Director and Chief Security Strategist, AT&amp;T Security Solutions</td>
</tr>
</tbody>
</table>
Agenda

• Growth of IoT
• Impact of IoT to the Healthcare Ecosystem
• Leading Practices for Securing IoT Healthcare Solutions
People are mobile, workloads are moving to the cloud, and IoT is exploding
Has IoT increased our exposure to cyber threats?

### IoT deployments are on the rise

How many connected devices do you have in your organization?

<table>
<thead>
<tr>
<th>Number of Devices</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>35%</td>
</tr>
<tr>
<td>Fewer than 100</td>
<td>32%</td>
</tr>
<tr>
<td>1,000-4,999</td>
<td>8%</td>
</tr>
<tr>
<td>5,000+</td>
<td>5%</td>
</tr>
<tr>
<td>100-999</td>
<td>1%</td>
</tr>
<tr>
<td>Don’t know</td>
<td>1%</td>
</tr>
</tbody>
</table>

Source: AT&T State of IoT Security, October 2015

---

### Key findings:

#### 50B

Connected devices estimated to secure by 2020

#### 458%

Increase in IoT vulnerability scans on the internet

#### #1

Barrier to customer adoption of IoT is security concerns

#### 90%

Of businesses lack full confidence that their IoT devices are secure

#### 14%

Of companies have a formal audit process for connected devices

---

1. Cisco, Inc.
2. AT&T Network Operations Center
3. IDC, 2015
IoT Benefits and Threat Landscape in the Healthcare Ecosystem

Benefits

- Allows physicians to efficiently monitor patient health
- Improves communication between physicians and patients
- Enables efficient and effective healthcare to patients

Risks

- Lives are involved!
- IoT increases complexity in protecting ePHI
- IoT-enabled devices were not built with Internet connectivity — or the requisite security — in mind
- Fundamentals of cybersecurity are not implemented and / or managed
- The IoT ecosystem has become a digital petri dish for hackers and other cybercriminals
- The IoT attack surface is magnified by scale, distribution, and the broad spectrum of IoT endpoints
A strategic framework for securing the IoT in healthcare
Today’s threat landscape requires a multi-layered approach to security

- **Device layer**
  - Mobile, IoT, Office/Fixed
- **Connectivity layer**
  - Securing the network
- **Data & application layer**
  - Securing workloads/applications

**Threat management**
- Detection & response
IoT Security
Control operational and service support costs with full management and support for your IoT environment

Application Security
- Web Application
- Mobile Application
- Code Analysis
- Data Privacy

Device Security
- End-point configuration
- Server configuration
- Gateway/Router configuration
- Penetration Testing
- IAM / Authentication & Access Control

Network Security
- Segmentation / Isolation
- Architecture Analysis
- Defense in Depth
- Secure communications

Cloud Security
- Service layer
- Data Residency & Protection
- WAN/Cloud Integration
- Segmentation

Security Operations
- Threat / Anomaly Detection
- Incident Response
- Event Mon. / Tamper Detection
- Behavior Analysis

*Requires an Interface Agreement (IA) to work with a third party or a Letter of Agency (LOA) to act on a customer’s behalf.
Fundamental practices and core security principles to keep potential risks in check

1. Adopt a risk-driven approach
2. Assess device security characteristics
3. Consider the entire healthcare ecosystem
4. Utilize existing security solutions
5. Automate security, where possible
Adopt a Risk-Based Framework and Approach

- Consider your organization’s legal and regulatory requirements and exposures
- Track your IoT solutions
- Assess the security vulnerabilities of each IoT element
- Map out worst-case scenarios
- Determine whether IoT devices and data can be isolated
- Gauge the value of the data from individual IoT devices
Assess Device Security Characteristics

- Consider information security concerns and operational security threats
- Employ existing controls, such as data encryption, network monitors, firewalls, and other familiar tools
- Inventory medical devices
- Are they network enabled?
- Is security built in? Is an MDS2 form available?

Basic requirements for secure connected devices

- Is security built in?
- Software/firmware update capability
- System reset
- No default password
- No ancillary services
- No backdoors
- Device support
Consider the Entire Healthcare Ecosystem

The Internet of Things is NOT about “things” and technology
Industry lines are blurring in IoT

The future is integrated
Combined Approach to IoT
Transforming industries requires ecosystems and collaboration

Industrial Internet Consortium

To further development, adoption and widespread use of interconnected machines, intelligent analytics and people at work

2014 Founding Members

- AT&T
- Cisco
- IBM
- Intel
- GE

Now 201 members

More than 2X growth since 2014

IBM and AT&T collaborating on M2M solutions for cities, institutions and enterprises.

GE and AT&T collaborating to build solutions to help maintain and remotely control industrial machines.

© 2015 AT&T Intellectual Property. All rights reserved. AT&T, Globe logo, Mobilizing Your World and other marks are trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. All other marks contained herein are the property of their respective owners. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.
Use Existing Security Solutions

*AT&T security solutions help protect customer vulnerable points*

**Customer Assets**
- Public Web Sites
- Corporate Email
- Network Access
- Mobile Endpoints
- Cloud Applications
- All Assets

**Prevent**
- AT&T Cloud Web Security Service
- AT&T Secure
- AT&T VPN
- Enterprise Mobility Management
- AT&T NetBond

**Detect & Respond**
- Response Consulting
- AT&T DDoS Defense
- AT&T DDoS Defense with Kona Site Defender
- Managed Trusted IP Services (MTIPS)
- AT&T Enhanced Cybersecurity Service
- AT&T Security Event and Threat Analysis
- AT&T Threat Manager – Advanced Log Management

© 2016 AT&T Intellectual Property. All rights reserved. AT&T, the Globe logo and all other AT&T marks are trademarks and service marks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.
Monitor & Automate

Threat Detection & Analysis

Threat Analysis
Provides a broad view of the security in your network by efficiently correlating alerts from multiple devices and device types across the entire enterprise
Leverages AT&T proprietary data and Insights and 3rd party feeds
Distills billions of raw logs to a few cases
Implementation support can be provided by AT&T consulting for asset identification and implementation verification
Monitor & Automate
Threat Analysis

Network Discovery & Device analysis to identify applicable components

Output from multiple security devices normalized and correlated

Device management agnostic; AT&T management or MSS services encouraged

24x7x365 analyst support contact via telephone or email.

© 2016 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.
Monitor & Automate

**Threat Analysis**

- **Notification of prioritized events** based on their risk to the company and the ability to mitigate them.
- **Recommended mitigation plan** provided as part of AT&T determined critical and actionable alerts.
- **Custom weekly AT&T Threat Analysis Report** identifying threats that may effect your business.

© 2016 AT&T Intellectual Property. All rights reserved. AT&T, the AT&T logo and all other AT&T marks contained herein are trademarks of AT&T Intellectual Property and/or AT&T affiliated companies. The information contained herein is not an offer, commitment, representation or warranty by AT&T and is subject to change.
“Actionable” alerts are generated
• Suppression of duplicates and false positives
• Correlation of information from multiple sources
• Ongoing refinement of algorithms and thresholds

Alerts are surrounded with contextual “drill-down” information
• English language alert names
• Linkage of alerts to Methods and Procedures
• Linkage of alerts to protocol and port information
• Automatic initiation of queries for supplemental details

Flexible layered design for managing rule
• Engine performs short interval inspection and alarming
• Queries allow data mining over days, weeks and months

Threat Analysis
Innovative Approach to Alerting