Cybersecurity in Healthcare: Why It’s Not Enough, Why It Can’t Wait

While cyberattacks and data breaches are rising across industries, healthcare is lagging behind in cybersecurity investment:

**Worldwide spending on IT security is projected to increase 34% from 2015 spend.**

<table>
<thead>
<tr>
<th>Year</th>
<th>IT Security Spending (in billions)</th>
</tr>
</thead>
<tbody>
<tr>
<td>2015</td>
<td>$75.4B</td>
</tr>
<tr>
<td>2018</td>
<td>$101B</td>
</tr>
</tbody>
</table>

The U.S. financial market is the largest market investing in cybersecurity, with a cumulative spend forecasted to exceed $68 billion between 2016-2020.  

Cybersecurity is approximately 16% of the federal IT budget for 2016.  

In comparison, the healthcare industry averages are much lower, with less than 6% of their IT budget allocated to IT security.

Healthcare data is unique, which makes the privacy and security of it so critical: Criminal attacks, the number 1 root cause of healthcare data breaches, are rising.

**WHY?** Medical records contain most of the data hackers want, making them ideal for ONE-STOP STEALING. Weak cybersecurity makes electronic protected health information (ePHI) more vulnerable.

While credit cards can be canceled when lost or stolen, medical records can be compromised for years.

Electronic health records sell for $50 per chart on the black market, compared to $1 for a stolen social security number or credit card number.  

**Why is cybersecurity important?**

1. Medical records contain most of the data hackers want.
2. Weak cybersecurity makes ePHI more vulnerable.
3. Medical device manufacturers are not mandated to incorporate cybersecurity features in their design and development.

The 2016 HIMSS Analytics Healthcare IT Security and Risk Management Study reveals several gaps in the current state of healthcare cybersecurity:

- **Compliance is not assurance.**

  - 20% of respondents comply with key mandates only (HIPAA, HITECH).
  - Surveys don’t address significant changes in IT, including cloud and mobile, to properly secure ePHI.

- **Medical device manufacturers are not mandated to incorporate cybersecurity features in their design and development.**

- **Healthcare organizations are not filling the gaps in medical device security.**

  - 50% of survey respondents are only beginning to address medical device security.

Survey respondents ranked the importance of a cybersecurity strategy for their organization high, but only 23% have an ongoing, consistent risk-management program.

**These 5 steps** can help your organization move from a reactive to a sustainable, business-driven approach:

1. **COMPLY** with key mandates; base security controls
2. **STAY AHEAD** of threats
3. **LET RISK ASSESSMENT** drive priorities
4. **IMPLEMENT** a sustainable risk-management program
5. **LET BUSINESS PRIORITIES** advance the security strategy

Find out how you can build a proactive cybersecurity strategy at www.symantec.com/healthcare

References:

3. https://www.whitehouse.gov/omb/budget/
4. The HIMSS Analytic Healthcare IT Security and Risk Management Study
8, 9, 11, 12 The HIMSS Analytic Healthcare IT Security and Risk Management Study