AVAYA

4 CYBERSECURITY TRENDS SHAPING HEALTHCARE IN 2017

Cybersecurity is a top concern for healthcare organizations — the frequency and associated economic impact of breaches has risen drastically since 2010. It remains a critical issue in 2017, bringing with it both new and familiar challenges

In the last 2 years, **89%** of healthcare organizations have **experienced a data breach** involving the loss or theft of patient data, **costing the industry $6.2 billion**[1]

45% of healthcare organizations say they were hit with **more than 5 breaches**[1]

The average cost of each hack was **$2.2 million**[1]

Possible effects of a data breach:

- Life threatening errors in records
- Identity theft and disclosure of private information
- Multi-million dollar fines, lawsuits
- Loss of customers

50% of consumers would **avoid or be wary of using a medical device** if a breach was reported[2]

40% of consumers would **abandon or hesitate using a health organization** if it was hacked[2]

HOSPITAL

52% of healthcare organizations **plan to upgrade security in 2017**[3]

Network security will be the #1 security focus for healthcare organizations in 2017[3]

WHAT WILL 2017 LOOK LIKE FOR HEALTHCARE?
WE'LL SEE 4 BIG TRENDS

1 Healthcare will remain the #1 attacked industry

...And is also one of the least prepared to deal with cybersecurity threats. Healthcare organizations have massive amounts of valuable data, but often lack a strong security infrastructure.

Healthcare is the #1 most cyberattacked industry[4]

46% say they **don't have the technology to effectively prevent or quickly detect** unauthorized patient data access, loss or theft[1]

47% had **unpatched vulnerabilities** in their network in 2016[5]

55% of healthcare organizations have a **Network Security score of a C or lower**[6]

2 Ransomware attacks will grow

Ransomware became the dominant security issue of 2016 as hackers proved they can just hold your files hostage if they can't steal them. Ransomware interrupts the ability of the organization to do business, and can even have a significantly greater financial impact than a simple data breach.

In just Q1 of 2016, there were about **4,000 ransomware attacks per day**[7]

The average cost of unplanned downtime: **$8,950 a minute, per incident**[8]

Less than ½ of ransomware victims fully recover their data[9]

88% of all ransomware detections in the U.S. **occurred at healthcare organizations**[5]

3 IoT will further strain security

There are thousands of IoT devices on healthcare networks, posing risks to any hospital, treatment center, or patients using devices. A hacked device can be used as an entryway into the network or even forced to malfunction.

The healthcare IoT market is predicted to be worth **$410B** by 2022[10]

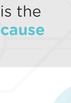
By 2020, more than **25% of identified attacks** in enterprises **will involve IoT**[11]

58% of healthcare organizations say **IoT devices are a high priority security issue** in 2017 — more than any other issue[12]

4 People continue to be the biggest liability

Security awareness and employee training among medical and administrative staff remains low. Employees are often the target of phishing and other social engineering attacks.

Social Engineering is the #1 detrimental security factor for healthcare organizations[5]



Social Engineering is the **3rd most common cause for breaches**[9]

69% of healthcare organizations say **employee negligence** is one of the top 2 security threats they worry about most

VS

45% say **cyber attackers** are one of the top 2 security threats they worry about most

WHAT CAN YOU DO?

As long as cyberattacks remain profitable, they will continue. All healthcare organizations can do is to improve their defenses and make it harder for hackers to succeed. We recommend:

1. **Start with a risk assessment,** which will help you identify what really needs to be protected, how to make a case for funding, and make the most of your security budget.
2. **Partner with a security expert** for resources and expertise in order to ensure the success of your cybersecurity strategy.

With Avaya, your network and patient records are more secure than ever, regardless of device or location. Our cutting-edge new hyper-segmentation technology renders intruders — no matter how they got in — effectively blind to the rest of the network. And Avaya Surge™ empowers you to take advantage of evolving IoT technology while protecting and safeguarding your network, devices and data.

Find out more at **Avaya.com/healthcare**

AVAYA

Sources:

1. Sixth Annual Benchmark Study on Privacy & Security of Healthcare Data, Ponemon Institute, May 2016
2. Top health industry issues of 2016: Thriving in the New Health Economy, PwC Health Research Institute
3. 2017: The Year Ahead in Health Information Technology, Healthcare IT News
4. 2016 IBM X-Force Cyber Security Intelligence Index
5. 2016 Annual Healthcare Industry Cybersecurity Report, SecurityScorecard
6. Security Engineering Research Team Quarterly Threat Report, NTTSecurity, Q2 2016
7. Symantec Security Response, 2016
8. Surviving Ransomware: IT Pros Share Their First-hand Experience & Tips, Barkly, 2016
9. 2016 Cost of Data Center Outages, Ponemon Institute and Emerson Network Power
10. Internet of Things (IoT) in Healthcare Market Analysis Report, Grand View Research Inc., May 2016
11. Top 10 Security Predictions Through 2020, Gartner, 2016
12. 2016 Data Breach Investigations Report, Verizon Enterprise Solutions