iNTERBiT DATA

white paper

Confronting a growing threat: A pragmatic approach for healthcare cybersecurity leaders

By Arthur Young, Founder and President, Interbit Data

When it comes to healthcare, 2020 will go down as the year of the pandemic, when COVID-19 swept across the globe and swamped health systems with gravely ill patients and red ink. But it will also be remembered as the year when cyberattacks against hospitals went mainstream.

With organizations shifted to remote workforces, the coronavirus pandemic has opened the door to cybercriminals, who are shamelessly exploiting for financial gain new IT security vulnerabilities exposed by the pandemic.

Sadly, healthcare is now the No. 1 most targeted industry in the U.S. for ransomware, a strain of malware that encrypts computers and networks and demands payment to unlock them, with monthly attacks up 71% in October, Check Point Research reports. Cybercriminals have even targeted at least seven companies involved in researching vaccines or treatments for COVID-19. The spike in attacks prompted a joint alert from federal authorities in October outlining ransomware threats, and Microsoft followed up with a plea to world leaders "to affirm that international law protects health care facilities and to take action to enforce the law."

And yet among all industries, healthcare appears uniquely vulnerable to crippling cyberattacks. In this white paper, we'll outline the distinct cost pressures and vulnerabilities confronting hospitals, lay out some of the financial implications of a cyberattack, and offer pragmatic suggestions for approaches you should take not only to strengthen your IT environment, but to win over leaders in your C-suite.

© 2020 Interbit Data Inc. All rights reserved.

Uniquely vulnerable

Healthcare is unique among industries for its urgency: It requires confidential patient health information to be readily accessible to staff 24/7, both onsite and remotely, across multiple care settings and on multiple devices, to enable collaboration and continuity of care.

Unfortunately, when it comes to cybersecurity preparedness, hospitals were already in a bad position when the pandemic hit. Just 4 to 7% of a health system's IT budget is devoted to cybersecurity, compared to about 15% for other sectors such as the financial industry, according to Lisa Rivera, a former federal prosecutor who is now focused on advising healthcare providers and medical device companies. In 2019, just 44% of healthcare providers met NIST Cybersecurity Framework standards.

According to a 2020 CHIME Survey of Health System CIO Priorities, which polled respondents shortly before the COVID-19 outbreak:

70% reported operating cost pressure

61% said they had limited IT bandwidth

> Just 4 to 7% of a health system's IT budget is devoted to cybersecurity, compared to about 15% for other sectors such as the financial industry, according to Lisa Rivera, a former federal prosecutor who is now focused on advising healthcare providers and medical device companies.

Of course, the pandemic has only compounded those cost pressures, filling ICUs with sick, highly contagious patients and forcing hospitals to discontinue high-margin elective surgical procedures. Meanwhile, the twin distractions of COVID and supporting the IT needs of remote workers opened new doors to cybercriminals to steal healthcare data. Patient records, which contain date of birth, credit card information, Social Security number, address and email, command as much as $1,000 on the dark web, according to Experian.

Meanwhile, healthcare technology is proliferating, with examples including diagnostic technology, medical devices, EMR-based workflow support, digital consumerism, telemedicine, revenue cycle management applications, plus diverse data lakes, repositories and cloud platforms for privacy, security and data management. Driven by the promise of increased clinical efficacy and operational efficiencies, venture capital investment in HIT innovation has soared to an all-time high.

© 2020 Interbit Data Inc. All rights reserved.

That's led to more fragmentation and complexity, which has increased the number of security vulnerabilities. All those medical devices, which lack the IT security features found in other network devices like laptops and tablets, are easy targets, with an average of 6.2 vulnerabilities each and roughly 60% of medical devices at end-of-life stage, with no patches or upgrades available, according to the Open Source Cybersecurity Intelligence Network and Resource. IT research firm Gartner predicted that in 2020, more than 25% of cyberattacks in healthcare delivery organizations would involve the Internet of Things — wirelessly connected and digitally monitored implantable medical devices (IMDs) — such as cardioverter defibrillators (ICD), pacemakers, deep brain neurostimulators, insulin pumps, ear tubes and more.

The most common point of attack continues to be the Remote Desktop Protocol, or RDP, which often operates on vulnerable platforms, and which has proliferated in use with so many people working remotely during the pandemic. RDP enterprise credentials can be purchased on the dark web for as little as $20. Coveware explained that when "combined with cheap ransomware kits, the costs to carry out attacks on machines with open RDP were too economically lucrative for criminals to resist."

With limited budgets and a hesitancy to learn new systems, medical technology at many facilities quickly becomes outdated. A 2019 Forrester Study found that:

- 40% of server hardware in data centers is three or more years old
- Legacy maintenance often exceeds industry-standard refresh cycles and, in some cases, extends beyond the five-year mark
- IT departments are falling short of meeting business needs and spending more time and resources on legacy systems ill-suited to support innovative technologies such as artificial intelligence and advanced security measures

Yet it is human error, not technology, that remains the biggest weakness, with nine in 10 breaches initiated when someone opens up an email or clicks on a link that opens the door to malware. Despite this, nearly a quarter of all healthcare employees in the U.S. report never having received training on cybersecurity awareness aimed at helping users detect and properly react to phishing scams, according to a report analyzed by Health IT Security.

© 2020 Interbit Data Inc. All rights reserved.

Compounding financial pressure

Between ransomware payments and financial penalties for data breaches and other factors, porous cybersecurity can create acute financial pain for healthcare organizations.

According to a study from IBM Security and the Ponemon Institute, the cost of a data breach for health care organizations rose from $380 per breached record in 2017 to $408 in 2018. Across all industries, health care has the highest cost for data breaches.

One in 10 healthcare organizations has paid a ransom, according to a survey by cybersecurity technology firm Imperva. The average ransomware attack causes 15 days of downtime, with the average demand paid by organizations having risen to an astonishing $233,817 in the third quarter of 2020, reports Coveware.

Costs for a cyberattack don't end when system restoration is complete. Following a cyberattack, hospitals face higher advertising costs, according to a Dec. 2018 report from the American Journal of Managed Care. Insurance premiums also typically rise, while the damage to a hospital's brand is real but hard to quantify.

A cyberattack in October against the University of Vermont Medical Center that crippled all 5,000 computers on its network was costing an estimated $1.5 million per day in lost revenue and recovery costs, the health system's CEO said nearly a month and a half after the attack occurred and weeks after systems were restored.

Beyond financial costs, there are massive risks to patient safety.

One doctor at a hospital in Oregon that was hit with ransomware and had to resort to paper records told Insurance Journal, "The increased workload is astronomical for all hospital employees and will inevitably have an impact on patient care."

Hospitals need to think about how they can maintain access to critical patient information during a downtime in order to minimize operational costs, assure business continuity and safeguard high-quality patient care.

1 in 10

HEALTHCARE ORGANIZATIONS
has paid a ransom

> The increased workload is astronomical for all hospital employees and will inevitably have an impact on patient care.

© 2020 Interbit Data Inc. All rights reserved.

The pragmatic HIT executive

Caught in the middle of all this is the HIT leader, who is faced with a near-impossible task list (especially considering the cost constraints outlined above):

- ☑ Align, integrate and securely maintain an increasingly complex IT ecosystem
- ☑ Manage massive amounts of patient data, plus a growing network of connected medical devices
- ☑ Meet all HIPAA requirements
- ☑ Work within dwindling budgetary resources
- ☑ Diagnose vulnerabilities and secure PHI with every innovation, update and upgrade that occurs across the HIT ecosystem

It's worth noting that there is no silver bullet cybersecurity solution capable of 100% impenetrable defenses. Instead, it's prudent to employ a number of different approaches in order to bolster your IT systems and reduce your risk. We list them in a continuum, from less secure options that lead to more system downtime to higher security with less downtime.

- Vulnerability Management Utilities, such as operating system and application patching, endpoint protection technology, and Risk Based Authentication
- Multi-factor authentication, which Microsoft has found blocks 99.9% of all automated cyberattacks
- Ongoing training on cybersecurity best practices, which is critical given staff turnover and the outsize role your users play in cybersecurity
- Self-service portals for healthcare professionals to be able to manage updates and password re-sets on their own devices and free up IT staff
- Next-generation antivirus (NGAV), especially those using artificial intelligence to proactively detect and identify threats, including never-before-seen malware and exploits
- Payload-based signatures, which can detect patterns in the content of files, rather than a simple attribute such as hash. One signature can block tens of thousands of variants from the same family of malware.
- Offline backup storage and restoration, including disaster recovery and cloud-based platforms. The problem with this is that, given the long gestation periods of many kinds of malware, which take time to spread throughout a network before being triggered, backups may be simply duplicating the malware, and may require a deep dive by IT staff to ensure that backups don't contain it.
- Storage as a Service, or STaaS, with auto-refresh services, which many small organizations find a convenient and less expensive way to manage backups and refresh applications and middleware tools that manage data
- Simulations and recovery preparedness training, which is critical for getting clinicians and physicians on board with cybersecurity best practices and knowing what to do in a downtime scenario
- Offline backup and restoration solutions, which reduce the risk to patient safety, the operating costs of maintaining downtime workflow and the threats to your brand and resulting increases in insurance premiums. This option can also minimize the threats of ransomware, while boosting leverage in negotiations
- Practice, simulations and recovery-preparedness training

© 2020 Interbit Data Inc. All rights reserved.

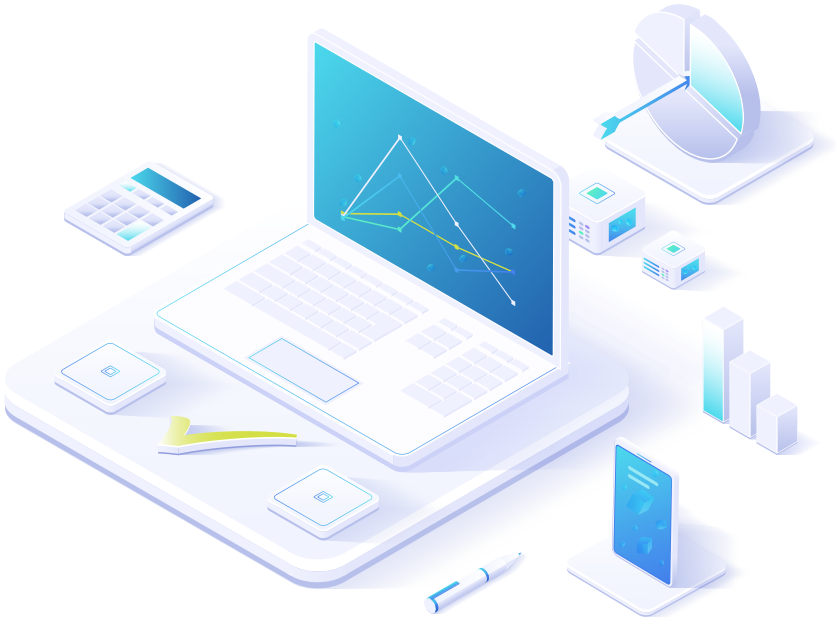
Getting buy-in

All of these tactics cost money and change all the time because cybercriminals constantly adjust their tactics. The question is, how do you convince the C-suite to pay attention and prioritize investments in cybersecurity?

The major challenge: There is no return on investment in cybersecurity. It's the wrong approach. Cybersecurity is not about increasing profitability, but rather about reducing loss. In order to determine a return on your security investment, you'll need to undertake four tasks:

1. **Assess your vulnerabilities.** You'll need to conduct an inventory of your vulnerabilities including system backup, anti-phishing capabilities, the homogeneity of medical devices in your organization, offline backup and restoration capabilities, and reliance on legacy infrastructure.
2. **Estimate your exposure.** You'll need to determine your cost of a single loss by weighing factors including, but not limited to, a typical ransomware demand, service disruption, costs for recovery, financial penalties, and concerns about patient care and safety.
3. **Determine proposed cost of countermeasures.** Think about expensive measures like cybersecurity technology or artificial intelligence to minimize the complexity of your IT and security environments, or beef up governance, risk management and compliance programs.
4. **Set an expected return on security investment.** You'll need to come to agreement on a level of reduced exposure, bearing in mind that certain countermeasures will do double-duty by helping with other needs, such as HIPAA compliance. Speed to recovery should always be a key goal.

> **The major challenge:** There is no return on investment in cybersecurity. It's the wrong approach.



© 2020 Interbit Data Inc. All rights reserved.

In conclusion

Health systems are poorly suited to fight a dynamic arms race with cybercriminals. There are limited funds to invest in countermeasures, with no silver bullets. Downtimes lead to heightened risks to patient safety and higher operating costs because of the workflow disruptions, and data breaches may disrupt the processes of care that rely on health IT, and the costs of repairing a breach may also divert financial resources away from patient care, necessitating the need for products like Interbit Data's NetSafe solution, which ensure uninterrupted access to patient information in any kind of downtime.

Many of your best moves are simply pragmatic ones that don't necessarily cost a lot of money but offer high returns on the time and effort invested:

- ☐ Hold HIT vendors, partners, suppliers accountable to higher cybersecurity standards
- ☐ Leverage professional associations, like the AHA or HIMSS, to advocate for greater federal investment in securing healthcare system from rogue attacks
- ☐ Where possible, improve automation of refresh services, detection and response
- ☐ Beef up training and effective self-service utilities where possible
- ☐ Prioritize offline backups and restoration solutions to:
  - Reduce patient safety risk
  - Reduce operating costs of maintaining downtime workflow
  - Minimize ransom threats and increase negotiation leverage
  - Minimize threats to brand and rising insurance premiums

Interbit Data provides software automation solutions that ensure your patient care teams have secure, uninterrupted and reliable access to clinical and administrative data when and where they need it.

INTERBIT DATA
Critical information. When & where you need it.

251 W. Central St. #36 ▪ Natick, MA 01760 ▪ 508.647.0013 ▪ interbitdata.com

© 2020 Interbit Data Inc. All rights reserved.