Adventist Health

"Your reputation is your business. A confidentiality breach means lost business."

— Bruce Chitester, Security Analyst, Adventist Health

INDUSTRY
Healthcare

COUNTRY
United States

PRODUCT TYPE
Forcepoint Web Security

SIZE
16,500 Users

SECURITY ISSUE
Embracing New Technology

OVERVIEW

Adventist Health is a not-for-profit health care organization which operates facilities throughout the western U.S. states of California, Hawaii, Oregon, and Washington. It is run by the Seventh-day Adventist Church. Its heritage dates back to 1866 when the first Seventh-day Adventist health care facility opened in Battle Creek, Michigan. Currently, Adventist Health contains 20 hospitals, more than 275 clinics, 15 home care agencies and a workforce of 31,000 employees, physicians, and volunteers.

CHALLENGE

For Bruce Chitester, Security Analyst at Adventist Health, the top security dilemma is how to safely embrace new technology without putting the hospital chain's patient database at risk. Although the healthcare sector faces some very specific regulatory and legal requirements, as well as medical technology obstacles to maintaining its data integrity, neither Adventist Health nor the healthcare sector at large are alone in having to meet this challenge. The reality is that ALL organizations face the difficulty and necessity of embracing new technology without putting their entire enterprise at risk. But as Adventist Health shows us, with the right Data Theft Prevention processes and tools in place, it can be done. The more powerful and sophisticated digital technology (and digitally-connected medical technology) becomes, the easier it is to use and save lives. Unfortunately, technological advances also make it easier for cybercriminals to access and exploit critical data. This mixed blessing of technological advancement and more sophisticated cybercrime is the new reality going forward.

Understandably, this new reality poses formidable challenges to IT security teams. From the perspective of saving lives, technological advance is obviously a good thing. The downside of that dynamic is the rising number and complexities of threat vectors. It is not a situation where the cyber defense responses become simpler over time, but rather just the opposite. The growth curve of the cyber threat landscape is both steep and evolutionary; thus the growth curve of cyber defense solutions that effectively address those threats must be so as well.

At the same time, organizations and businesses have no option but to operate in this rapidly evolving threat environment. It is, in every sense of the word, the cyber world that we have created for ourselves. Given that understanding, the following are threats that Adventist Health faces as they adopt new technology safely and effectively:

5 DATA THEFT CHALLENGES

Staying current with privacy regulations (HIPAA and Omnibus). Strict privacy laws require Adventist Health to meet a higher standard of client-privacy than most organizations outside the healthcare sector will need to meet. Healthcare providers have a federally-imposed legal obligation to protect the privacy of patient data in addition to standard consumer data, such as Social Security and credit card numbers. This vulnerability is much worse today than only a few years ago because, as Bruce Chitester observes, "medical records are all electronic now."

Staying current and secure with new communication technology. The explosion of communication tools such as iPads, smartphones, handhelds and even wearable connected devices such as smartwatches and other innovations have greatly increased the risks of a data breach occurring. Those risks become even greater as new communication gadgets come into use among medical personnel. Elevated threat levels can result from something as common as doctors using iPads to communicate medical information, test results or issuing prescriptions, for example.

Staying current and secure with new medical technology. As with wearable connected and other smart devices, medical gadgets also present an elevated risk factor to Adventist Health and other organizations in the healthcare sector.

> "One of the things I see very much as a threat factor is medical devices. I.V. pumps now have built-in wireless capabilities and a stripped down Linux or Windows OS. It is the same with heart monitors, and other medical devices. But the manufacturers are not particularly security-aware. The devices are built with connectivity, so they can connect with a pharmacy, but they lack any kind of firmware updates or security hole checks, and that is going to be a big (risk) factor."
>
> — Bruce Chitester, Security Analyst, Adventist Health

Those gadgets are just a small portion of what the medical industry has to deal with. Insulin pumps, I.V. pumps, and even wireless pacemakers and other medical care devices are all subject exploitation by cybercriminals. Chitester predicts that there will be a huge influx of attacks using devices like these as backdoor access to networks. Device vendors will have to scramble to put security measures in place.

Protecting patient data. In addition to standard consumer data, such as Social Security and credit card numbers, healthcare providers must take a holistic approach to protecting their clients' medical records as well. This is not only due to more stringent HIPAA and Omnibus requirements, but also because medical records are a prime target of data theft activity: A stolen driver's license is worth about $120 on the street. Stolen medical records, however, are worth almost 10 times that. There is no mystery why medical records are a major target of cybercriminals.

> **"That is why we have to build a Fort Knox around them."**
>
> **— Chitester**

He is absolutely correct.

The need for comprehensive, end-to-end identification of every threat vector. This need applies to all industries in general. In addition to medical records, Chitester notes that another serious challenge is with financial data. New federal regulations require separate networks for certain types of financial transactions, such as credit cards. To address this, Adventist Health uses multiple LATA (local access and transport area) networks:

> "All of (these vectors) combine to make security a very high priority and a cutting edge environment to work in, where we have to protect patient data, very specifically, and... we have to protect privacy of patient data in addition to standard consumer data, such as Social Security and credit card numbers. When someone swipes a credit card, the transaction is carried by a secure tunnel to the credit card processor."
>
> — Chitester

Adventist Health's data security challenge is an ongoing one, but one that is also instructive to all enterprises. As noted above, just as the threat level curve of the digital environment is steep and evolving, so are the costs involved with successful data breaches.

The recent and very public data thefts involving Home Depot, Target Stores, Nordstrom's and Michael's were just a few of the casualties in a year of unprecedented levels of cybercrime. Each of those breached businesses lost multiple millions of dollars in sales and market share. Much of those losses can be directly traced to the damaged reputations caused by the breaches themselves.

Going forward, the frequency and costs of cybercrime are only going one direction, and that direction is up. Your organization's approach to cybersecurity needs to be able to successfully meet these challenges each and every day and every minute of every day. Data Theft Prevention is that approach.

SOLUTION

Chitester has moved Adventist Health into the SEIM (security event and incident management) environment with strategic partners that specifically include Forcepoint™, and going forward will involve consolidation of services and solutions as their defense strategies evolve. A foundational part of Bruce's threat defense strategy has been to build a comprehensive infrastructure that mitigates threats:

> "If an end-user pulls an obfuscated Java script down via a browser because they randomly hit the wrong website and the script exploits the browser to create a back door into the network, Forcepoint— Adventist's threat management system —catches the script in a sandbox."
>
> — Chitester

Forcepoint now handles threat intelligence for Adventist Health's web and blocks dangerous sites. Chitester has put triggers around these types of events, so that if a script or another type of threat is identified and trapped, Forcepoint issues an alert.

This appears on a portal, identifying the threat, the user and the forensics. Forcepoint will also handle this through the Cloud, heading off hundreds of threats of different types, such as obfuscated Java scripts, bot networks and unauthorized data postings. Chitester estimates that they catch at least 5 to 10 a week:

> "With Forcepoint, everything that Adventist sees, other Forcepoint customers also see and vice versa. (The Forcepoint network has close to 1 billion end points.) It is updated more frequently than other, similar networked offerings...and the amount of data that we see is enormous...The number of threats that have been identified is enormous. In this way, the database of known threats is continually expanded. It is getting to the point that the number of threats should diminish because the database we are checking them against continues to get larger."
>
> — Chitester

With the Drop Box services, Forcepoint monitors usage and issues alerts if someone is using an unauthorized service provider. The service issues reports listing users who are not in compliance. Chitester talks about Forcepoint as a key security partner:

> "The protection is very good. End users are not happy when they get blocked from going anywhere, but the fact is they are getting blocked. They are not able to visit a site that is on a bot network, or a site that has been hacked with obfuscation code. We very much enjoy that protection."
>
> — Chitester

RESULTS

Forcepoint continues to play a vital role in Adventist Health's security plans when it comes to sandboxing potential threats:

> "If the device goes off our net, then it is a problem. We take this very seriously...these devices have to go through the same protocols as anything else in our environment to get off the net and onto the public network. If a device is given access to the public network from the private Adventist Health network, then it has to pass through the Forcepoint devices, and we know for sure where it is phoning home to and that nothing is coming back in on it."
>
> — Chitester

Bruce also appreciates the efficiencies and Data Theft Prevention policies that Forcepoint delivers:

> "The cloud detonation is the right way to do it. Other security providers detonate locally, and they do not always have enough time to do the detonations. Forcepoint has enough time. Adventist has to pay the subscription costs, but it does not have to purchase larger servers or more machines to provide adequate resources for its security software to operate optimally. Forcepoint handles all of that, and Adventist Health likes that business model. Forcepoint is getting closer to 'end-to-end' than I have seen anybody do it."
>
> — Chitester

In today's world of advanced and targeted cyber-attacks, the need for comprehensive, end-to-end identification of every threat vector must be met fully; there is no other alternative. Furthermore, HIPAA and Omnibus privacy rules require an added level of privacy for medical data. At the same time, the menu of medical devices with connectivity is constantly expanding. As Chitester accurately points out, the threat of a data breach via unprotected devices is formidable:

> “Your reputation is your business. A confidentiality breach means lost business.”
>
> — Chitester

When it comes to innovation, organizations of all sizes and types have no choice in the matter: they must be able to continuously adopt new technology and adapt to the expansive communications revolution in order to compete in today’s market. Unfortunately, the evolving digital technological revolution puts powerful and discrete connectivity in the hands of everyone, everywhere, including threat actors. That means an expanded threat surface for cybercriminals and greater challenges for cybersecurity professionals. The risk of exploitation by evermore sophisticated cyber threats rises with the ascent of the digital connectivity curve.

For the foreseeable future, the dilemma of safely adopting new technology while at the same time protecting your data against rising levels of cyber threats is here to stay. As digital technology continues to rapidly evolve and cyber-attack vectors multiply across all digital channels, the task of organizations being able to grow and adopt new technology with safety and confidence remains a challenge. However, these challenges can be met with the right holistic security posture that Data Theft Prevention provides so your company can enter a new era of cybersecurity.

Adventist Health has relied on Forcepoint security solutions since 2006.

CONTACT

www.forcepoint.com/contact

ABOUT FORCEPOINT

[CASESTUDY_ADVENTIST_HEALTH_EN] 300001.021317