WHY HOSPITALS ARE A HACKER'S DREAM COME TRUE:

A REVIEW OF THE 2018 UNISYS SECURITY INDEX™

UNISYS | Securing Your Tomorrow®

Security Concerns Are High Among Consumers Worldwide

Security issues are rampant within the healthcare industry. Hospitals must defend themselves against an ever-changing threat landscape – often with limited budgets. Patient information is spread throughout the organization, presenting appetizing opportunities for cyber criminals. Medical devices are often used as open backdoors into healthcare networks.

Today's consumer is highly aware of and concerned about these risks. The Unisys Security Index™, the only recurring snapshot of security concerns conducted globally, gauges the attitudes of consumers on a wide range of security-related issues. In 2018, Unisys surveyed more than 13,000 consumers in 13 countries to generate the data for this report. Results show that security concerns globally among individuals continue to hold at the highest level ever since 2007, as measured by the Unisys Security Index.

To provide the type of customer experience that healthcare consumers expect and demand, providers must understand where and why security concerns exist and take steps to proactively address and alleviate these concerns.

Identity Theft and Bankcard Fraud Top the List of Consumer Fears

Among consumers, the highest security concerns are those where people feel they may have the least amount of personal control: Identity Theft and Bankcard Fraud. Globally, people surveyed are more concerned about Identity Theft (68 percent seriously concerned) or Bankcard Fraud (66 percent seriously concerned) than they are about possible physical harm related to Disasters/Epidemics (53 percent seriously concerned) or Personal Safety (50 percent seriously concerned).

Consumers have a right to be concerned. There has been a steady drumbeat of news around data breaches involving the personal and financial data of millions of consumers. Hospitals and healthcare institutions have featured prominently in many of these headlines.

Healthcare records are attractive to hackers because they can command up to 40 times the value of credit card data. Whereas the market price on the dark web for stolen credit card numbers ranges from $.50 to $5.00 per number, personal health information (PHI) can bring in $10 to $50 per record.[1] When consumer data is stolen from a healthcare organization, it can be used to build fake identities for the purpose of defrauding healthcare payers, channeling rebates meant for healthcare providers, and supporting forged visa applications.

There are two reasons hackers have a good track record attacking hospitals and healthcare systems. First, healthcare is a "laggard" industry from a technology adoption standpoint. Consequently, the robust security stance one finds in other industries (e.g., Finance or Retail) is typically lacking in healthcare. Gaps and vulnerabilities abound and hackers are swift to take advantage of them.

Second, there is a great deal of latency in healthcare processes. Healthcare billing systems are often fragmented with no single bill, and billing is often not complete for up to a month post-discharge. Therefore, if a hacker steals that person's data, a month or more can go by before anyone even realizes that the data has been stolen. During that month, the hacker can use the data to build an independent persona with which he/she can make financial transactions and purchases. This is in contrast to the retail space where, if a credit card is stolen, the breach can be identified nearly immediately, leading to rapid account closure.

Data Privacy Impacts Value-Based Care

Data privacy is another area of concern for consumers. For example, nearly two-thirds (64 percent) of Argentinians surveyed reported they do not trust the organizations that store their data in the cloud to protect it. In Brazil, only nine percent of respondents say they are highly confident that the country's new General Data Protection law will be effective. In the Netherlands, only a third (34 percent) believe their privacy is sufficiently protected within the covenants of the new 'De Sleepwet' law.

[1] "Cybersecurity, Cybercrime and Data Breaches: Healthcare Under Attack," eFax Corporate, 2018.

Healthcare organizations have a special reason to strengthen data privacy: namely, the movement to value-based (rather than fee-based) care. In value-based care, providers receive payment based on patient health outcomes. In order to make value-based care a reality, a tremendous amount of collaboration and information sharing must take place regarding specific diseases, disease states, medical observations, treatment results, etc. This sharing relies in large part on mining thousands upon thousands of patient records to compare data, create composite profiles, identify trends, and so on.

However, all that patient information is currently regarded as private. To meet the information-sharing demands of value-based care while simultaneously guaranteeing patient privacy, healthcare organizations must significantly strengthen the measures they take to protect data privacy. Healthcare institutions will need to work together – ideally on a global scale – to establish a specific set of privacy guidelines, protocols, and processes that everyone agrees to follow. By agreeing to and practicing such standards, healthcare institutions will be able to contribute their own, secure information to the pool of patient data and subsequently access the total pool to further the demands of value-based care.

Connectivity Is on the Rise

Connected devices are multiplying exponentially within the healthcare industry, bringing opportunity and risk in equal measure. The Unisys Security Index notes that consumers largely support the use of connected devices globally. However, in contrast, data security continues to be a rising concern, forcing many to rethink the wisdom of openly sharing information among these devices. Additionally, a significant proportion of consumers may not want organizations to have access to certain types of personal data because they do not feel that there is a compelling reason for the organization to have such information.

These trends are well-illustrated in two questions posed by the Unisys Security Index. The first question asked respondents if they would support medical devices such as pace makers or blood sugar sensors that would immediately transmit any significant changes to their doctor. An overwhelming majority (79 percent) of respondents indicate support for this type of connection.

In contrast, the second question asked if respondents support health insurance providers tracking their fitness activity via wearable monitors to determine premiums or reward safe behavior. Only 38 percent of respondents support such connections, whereas almost half (48 percent) state they would not support this. The top reason respondents gave for not supporting such an application was the absence of a compelling enough reason for health insurance providers to have this information.

These two questions show that, in general, consumers are willing to share their personal data when they perceive that their health and safety will be protected by doing so. At the same time, they are less supportive of using payer-oriented tracking and monitoring applications. This is understandable, since there is a very different relationship between a patient and his or her doctor versus a subscriber and his or her insurance company. In a nutshell, the prevailing perception is that a doctor's top priority is the health of his or her patient. A health insurance company's top priority, in contrast, is the "health" of the business.

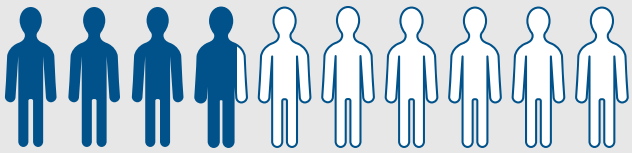
There are some early signs, however, that the benefits of tracking and monitoring applications in the health insurance area are beginning to be recognized. The question regarding tracking fitness activity via wearable monitors to determine premiums or reward safe behavior had a jump in support from 33 percent in 2017 to 38 percent in 2018 – the highest increase in support across connected devices issues covered in the survey.

Medical Devices Are Vulnerable To Cyberattacks

Internet attacks are specifically called out in the results of the Unisys Security Index. The threat of viruses and hacking is reported as the third greatest global security concern in 2018, with 62 percent of respondents reporting that they are seriously concerned. Indeed, seven out of thirteen countries have increased levels of concern about Viruses/Hacking since the 2017 index.

In the healthcare industry, one of the greatest vulnerabilities present is in the area of medical device security. Some 10 percent to 20 percent of medical devices in hospitals are Internet-connected; this number is growing rapidly. Unfortunately, many connected devices older than two or three years possess little to no inherent device security. For example, even if there are passwords, they are typically something weak such as "12345" or "Admin." In addition, devices that do contain security protections are often not configured appropriately within the hospital network to actually be secure. In fact, only about 25 percent of hospitals have explicit security protocols in place for medical devices.

The result is that medical devices are very often the weak link in securing today's hospital networks. Hackers continue to exploit this vulnerability mercilessly. For example, ransomware is costing hospitals millions each year and stolen data continues to impact hospital reputations and patient trust worldwide.



Only **38 percent** of respondents support such connections

whereas almost half **(48 percent)** state they would not support this

Take Action Today

Hospitals and healthcare systems are facing a dynamic threat landscape that calls for risk-relevant security solutions. These solutions must be robust yet cannot interfere with efficient business operations or negatively impact patient care. As a leader in security for the healthcare industry, Unisys recommends the following actions to strengthen security systems and promote customer trust:

1. **Pay attention to security basics.**
   With cyber threats growing around the world, healthcare organizations may be tempted to immediately adopt the latest and greatest technology without first covering the basic precautions foundational to any successful cyber-strategy. While the latest security innovations can be important tools for addressing cyber challenges, they will not help if hospitals fail to address commonsense security practices such as password protection.

2. **Get a professional cybersecurity assessment.**
   Before security can be strengthened, it is necessary to know exactly where risks and vulnerabilities lie. Detailed risk assessments enable healthcare organizations to determine the probabilistic likelihood and success of different attacks against existing infrastructure and data assets. For example, an assessment will show whether medical devices connected to the network or doctors who review patient data on personal phones represent significant vulnerabilities. These insights then can be used to prioritize security spend based on potential impact, maximizing return on investments and ensuring protection of the most vital systems and assets.

3. **Adopt a zero-trust security model.**
   A zero-trust approach to security means that internal network traffic is *a priori* not trusted as legitimate, nor are employees and partners trusted to always be well-meaning with systems and data. Unisys-sponsored research conducted by Forrester Consulting in 2018 shows that 58 percent of respondents agree that network perimeters are indefensible in today's technology ecosystem – a mosaic of distributed cloud workloads and mobile/remote users. Consequently, Unisys strongly recommends embracing a zero-trust approach that is identity- and data-centric, based on network segmentation, data obfuscation, security analytics, and automation.

4. **Implement a medical device management system.**
   A medical device management system that incorporates both microsegmentation and data encryption addresses security by supporting and enhancing the inherent security within each medical device. It also protects connected devices lacking any security features of their own. Such a system allows the creation of communities of interest (CoI) within the hospital so that only those groups of individuals who need to see data from a device can actually access that data. For example, a nurse may be able to see only the data generated by a patient monitor, whereas a clinical engineer could only be able to view the device data and information about the condition of the device itself. Other personnel – and, most importantly, hackers – would be unable to gain any visibility into the device *or* its data.

5. **Approach security with the patient in mind.**
   To build trust among patients, healthcare systems must be completely transparent regarding the steps they are taking to safeguard patients' personal information. Further, it is important to educate patients on steps they themselves can take to bolster their own security.

About Unisys

Unisys is a global information technology company that builds high-performance, security-centric solutions for the most demanding businesses and governments on Earth. Unisys offerings include security software and services, digital transformation and workplace services, industry applications and services, and innovative software operating environments for high-intensity enterprise computing. For more information on how Unisys builds better outcomes securely for its clients across the Government, Financial Services and Commercial markets, visit www.unisys.com.

For more information on Unisys security offerings, visit: www.unisys.com/security

For more information on Unisys Healthcare solutions, visit: www.unisys.com/industries/commercial/life-sciences-and-healthcare

For more information visit www.unisys.com

Printed in the United States of America 02/19 19-0038