Research

Cybersecurity Executive Brief

Research Data

The headlines are clear

Cyberattacks are sophisticated and constant. When massive, multi-billion dollar companies like Equifax are breached, leaving millions of customers at risk; it brings worldwide consumer attention to something healthcare IT leaders have quietly managed for years—cybersecurity.

Healthcare organizations have become a prime target for cyber threats and attacks. In 2016, 16.1 million individual healthcare records were impacted by 325 cyberattacks[1] — that's almost one attack per day. Consumer reporting agency Experian predicted 2017 as the "year of the healthcare cyberattack.[2] And it took a Hollywood, California hospital a week to decide to pay $17,000 to unlock its patient data[3]. What would you do if your systems were locked due to ransomware, blocking patients from being admitted or receiving care due to offline computers?

If cybersecurity threats are continuing to rise, is it possible that we are over-confident in how comprehensive our cybersecurity plans really are?

Trusted partner for your **Digital Journey**

Atos

We asked the market

In August, Atos surveyed almost 40 healthcare leaders, from executives to operational leaders, to identify their own confidence levels in their organizations' abilities to detect and recover from a cyberattack.

We found three common themes, let's look at these themes one at a time:

1. Cybersecurity plans were not comprehensive,
2. Uncertainty surrounds detection and recovery time and processes, and
3. Employee training continues to be a concern.

55% low confidence
protected from attacks similar to WannaCry

44% low confidence
cybersecurity plan accounted for entry points like medical devices and robotic systems

25% expressed concern
not adequately securing information collected from patient devices

Cybersecurity plans are not comprehensive

When asked how confident these leaders were that their operations were protected from attacks similar to WannaCry, *55 percent* expressed low confidence. Likewise, *44 percent* of respondents had low confidence or were unsure if their cybersecurity plan accounted for entry points like medical devices and robotic systems in labs and pharmacies. A full *25 percent* of respondents expressed concern that they were not adequately securing information collected from patient devices.

The takeaway

At a time when patient care is expanding from a hospital environment to a home environment, a data breach could bring physical harm to patients. In regards to IoT, are your devices tested for malware? Do you know what the risks are to patients and your operations from wireless devices? Imagine the reputational harm and likely litigation or lawsuits that could happen if malware impacted a hospital's surgical operations.

Uncertainty surrounds detection and recovery times

When asked how confident leaders were in their ability to fully recover from a cyberattack using their disaster recovery (DR) backup, *19 percent* had little confidence in their organizations' abilities to do so. Similarly, when asked how long it would take to detect and recover from an attack, *50 percent* said they were unsure. According to industry expert, IT Authorities, it takes 205 days to detect an attack[4], while Gartner decreases that prediction to "just" 99 days.[5] These statistics paint a bleak picture.

The takeaway

What does this mean for healthcare organizations? It shows that while there is growing awareness that medical facilities and hospitals are vulnerable, there is a lot of uncertainty about how to detect and recover from cyberattacks. To protect effectively against emerging threats, it is critical to combine prevention, detection and correction capabilities with reliable disaster recovery procedures that leverage redundant backup systems. Cybersecurity technologies working in silos are no longer effective against cyberattacks that morph continuously.

"50% of healthcare IT leaders were unsure how long it would take to detect and recover from an attack."

Are employees the biggest cybersecurity threat?

In rounding out the survey results, Atos asked the leaders if they were confident that their employees were well trained on cybersecurity and followed security policies. The results contradicted each other. Two-thirds of the respondents had a medium-to-high level of confidence that their employees were well trained. At the same time, *40 percent* had low confidence, or were unsure if their employees were transmitting confidential data and information out of the facility.

The takeaway

Employees provide the first line of defense against cyberattacks. Anthem Inc. recently paid $115 million to settle litigation over a 2015 breach that compromised 79 million individual records. This is the largest settlement to date, and it started when unsuspecting employees clicked on a simple email phishing scam.

The push for better and ongoing cybersecurity policy development and staff training can be overwhelming. As healthcare privacy concerns continue to be top of mind, are you confident in your current training approach?

Are you ready?

Healthcare organizations are all susceptible to potential cyberattacks, regardless of size or span of network. A lack of resources and expertise can hinder an organization's ability to detect and recover from an attack. Every healthcare organization has a cybersecurity strategy: Is it complete and comprehensive? Does it include regular testing, ongoing training and visible awareness reminders? Are you investing continuously? Do you view your cybersecurity strategy as an investment or it is just another check-the-box policy? If the latter, do you know your vulnerabilities?

It's often been said that it isn't a matter of if a healthcare organization will be the victim of a cyberattack, but when. Are you confident that you are protected?

Be prepared; attacks can come anywhere, anytime. As a global leader in cybersecurity, experts at Atos recommend a 4-step approach to cybersecurity:

1. Ensure all systems have the latest patches

2. Test and rehearse incident response and backup procedures regularly

3. Ensure employees are properly informed and trained on cybersecurity— employees are often the 'weakest link'

4. Use threat intelligence and behavioral analytics; antivirus software alone is not enough

"It isn't a matter of if a healthcare organization will be the victim of a cyberattack, but when."

Ensure all systems have the latest patches

Test and rehearse incident response and backup procedures

Ensure employees are properly informed and trained on cybersecurity

Use threat intelligence and behavior analytics

About Atos

Atos SE (Societas Europaea) is a leader in digital services with pro forma annual revenue of circa € 12 billion and circa 100,000 employees in 72 countries. Serving a global client base, the Group provides Consulting & Systems Integration services, Managed Services & BPO, Cloud operations, Big Data & Cyber-security solutions, as well as transactional services through Worldline, the European leader in the payments and transactional services industry. With its deep technology expertise and industry knowledge, the Group works with clients across different business sectors: Defense, Financial Services, Health, Manufacturing, Media, Utilities, Public sector, Retail, Telecommunications, and Transportation.

Atos is focused on business technology that powers progress and helps organizations to create their firm of the future. The Group is the Worldwide Information Technology Partner for the Olympic & Paralympic Games and is listed on the Euronext Paris market. Atos operates under the brands Atos, Atos Consulting, Atos Worldgrid, Bull, Canopy, Unify and Worldline.

Find out more about us
atos.net
ascent.atos.net

Let's start a discussion together

For more information: **info.na@atos.net**