Preparing for Cyber Attacks

What healthcare organizations need to do to stay secure

By Egor Kobelev, vice president, Healthcare & Life Sciences, DataArt

Posted on: May 9, 2016

According to Ponemon Institute, nine out of 10 healthcare organizations have been breached during the past two years.[1] Cyber attacks on healthcare organizations are up 125% compared to five years ago. The fifth largest industry in the United States (7.1% GDP) is losing around $6 billion annually because of cyberattacks. For the first time, criminal attacks constitute the number one cause of data breaches in healthcare.

Interestingly enough, while healthcare providers admit criminals are increasingly targeting healthcare companies, the vast majority are convinced their organization has not experienced a breach.[2] Therefore, they are not changing their behavior in a significant way because they do not see themselves as actual cyber attack targets. Perhaps it explains why security budgets in healthcare have not increased since 2014.[3] It remained at an average of 5% of the total IT budget, compared to 8% for government and 11% for financial services.Is it finally time to invest more into security measures?

Healthcare's Biggest Challenge

Even though spending more money on security might not be a bad idea by itself, it does not sound like the best approach for an industry that is notoriously inefficient. The United States currently spends more per person on healthcare than any other developed country. However, health outcomes in the United States are among the worst. The biggest challenge for the industry is lowering the cost of services while rising the quality of the outcomes. If only there was a way to achieve better security without a significant budget increase!

Let's consider the recent case with Anthem. Names, social security numbers, medical IDs, birth dates, street addresses, employment information (including income data) of 78 million people enrolled into the plan since 2004 were accessed by the hackers. The data was stolen over a period of weeks before the data breach was discovered. It looked like a sophisticated attack by a group of super-talented hackers, maybe even math geniuses, working day and night to decrypt the secure protocol, find and exploit the brand new vulnerability and create a state-of-the-art script to attack remote hosts. While this could have actually happened somewhere, sometime, the reality with Anthem was by far less impressive and not even close to a movie plot. An employee received a (socially engineered) email that looked like an internal message. He did not pay enough attention to it and let the hackers know everything they needed to get into the system, probably by just returning the email with domain credentials or submitting them on a phishing website following the link from the email. This terrible breach could have been prevented if this employee noticed either sender's address was somehow strange, the message did not look exactly like an internal message, or that the URL of the link he opened was unusual.

This case is a perfect illustration of one simple fact: you can get a significant boost in security without a comparable boost in spending. Security, while tightly coupled with information technologies, is not entirely an IT issue. Watchful, alert employees are one of the most important components of cybersecurity. Because criminals know most workers are responsive and trusting, they often use attacks that exploit human vulnerabilities rather than IT. The focus is usually on uninformed users who are targeted and fall victims to phishing emails that deploy malicious software into the company's network or are giving out sensitive information over the phone when exposed to social engineering. The best way to address such vulnerabilities is to establish company-wide security awareness training initiatives that may include classroom style training sessions, security awareness websites, hints, posters and flyers. Such initiatives usually cost only a fraction of spending for what is known as IT security, but could contribute to security in a meaningful and significant way.

SEE ALSO: Prevent, Mitigate and Transfer Cyber Attack Risks

Compliant Yet Insecure

A common argument one hears from healthcare security professionals is, "We're HIPAA-compliant, so we already have all required security measures in place." Indeed, in recent years compliance with standards and regulatory requirements, specifically HIPAA, became the number one driver for security efforts in healthcare organizations. Though change in security landscape is exponential, legislation is only incremental. Compliance-oriented mindset leads to the security strategy which addresses some past reality leaving patients' data unprotected from new challenges that arose after the legislation was passed.

Here is a good example to illustrate a compliant yet insecure measure. According to Trustwave Global Security Report 2015, "Password1" remains the top business password.[2] There might be nothing special about it at the first glance, but if you look thoroughly you may notice a few things. First, the password contains a mix of lower and upper case letters with a number. Second, it is longer than eight characters. If you think about a typical password policy in the organization, such a password perfectly complies with it. The popularity of "Password1" is primarily an attribute of network administrators setting up accounts for new employee,s but, as we all know, those passwords often don't change. Needless to say, the password is compliant but insecure. In fact, it doesn't even matter that there is only one digit, no special characters and the word is too simple. What matters is that there is such a thing as a "top business password" that gives attackers an easy tool. That is exactly the result of a narrow-minded, compliance oriented, "checkbox" approach to security.

To keep data secure, health organizations must build and manage a holistic security program that goes beyond a specific requirement of a governing law in terms of risk, confidentiality, integrity and availability. Healthcare security leaders need to plan ahead and establish a risk management plan consisting of best practices. It is a comprehensive multilayered approach to security that makes the company secure; compliance only makes it compliant.

Egor Kobelev is a vice president of Healthcare and Life Sciences at DataArt. With over 15 years in the IT industry, 10 of them in the healthcare sector, Egor brings a wealth of industry expertise to the company, advising major U.S. clients on technology approaches in research, regulation and security. Prior to DataArt, Egor worked as a software developer and software architect for a number of technology firms. He holds MS in Statistical Radiophysics from Voronezh State University.

References

1. Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data. Ponemon Institute. Available at: https://www2.idexpertscorp.com/fifth-annual-ponemon-study-on-privacy-security-incidents-of-healthcare-data
2. 2015 Security Health Check Report. Trustwave. Available at https://www.trustwave.com/Resources/Library/Documents/2015-Security-Health-Check-Report/
3. IT Security Spending Trends. SANS Institute. Available at https://www.sans.org/reading-room/whitepapers/leadership/security-spending-trends-36697

Original article — http://healthcare-executive-insight.advanceweb.com/Features/Articles/Preparing-for-Cyber-Attacks.aspx