The Cyber Security Crisis in HEALTHCARE

by Tom Skoog, Blue & Co., LLC

CPAs / ADVISORS
blue

The Cyber Security Crisis in HEALTHCARE

Although the global ransomware attack known as WannaCry? is all but old news, it hit the healthcare industry particularly hard and left many wondering how secure their organizations really are against similar attacks. Cyber security is one of the hottest topics in healthcare today and is creating a global crisis costing billions of dollars.

The Problem.

2016 was the worst year on record for cyber security breaches affecting the healthcare provider sector, and 2017 is quickly trending in the same direction. In fact, the provider sector is being attacked with more frequency, velocity and malice than any other sector in the U.S. economy, including financial services. The Ponemon Institute, an independent privacy, data protection and information security policy research organization, estimates that 88% of RansomWare attacks in the U.S. were directed at the healthcare provider sector. Furthermore, 89% of healthcare companies experienced a breach involving the theft or loss of patient data. Nationally, Ponemon estimates the number of cyber-attacks directed at the sector have increased 125% since 2010.

In 2016, the sector accounted for:

- The greatest number of Social Security numbers breached
- The most records exposed by employees due to errors or negligence
- More hacking and phishing attacks than any other industry

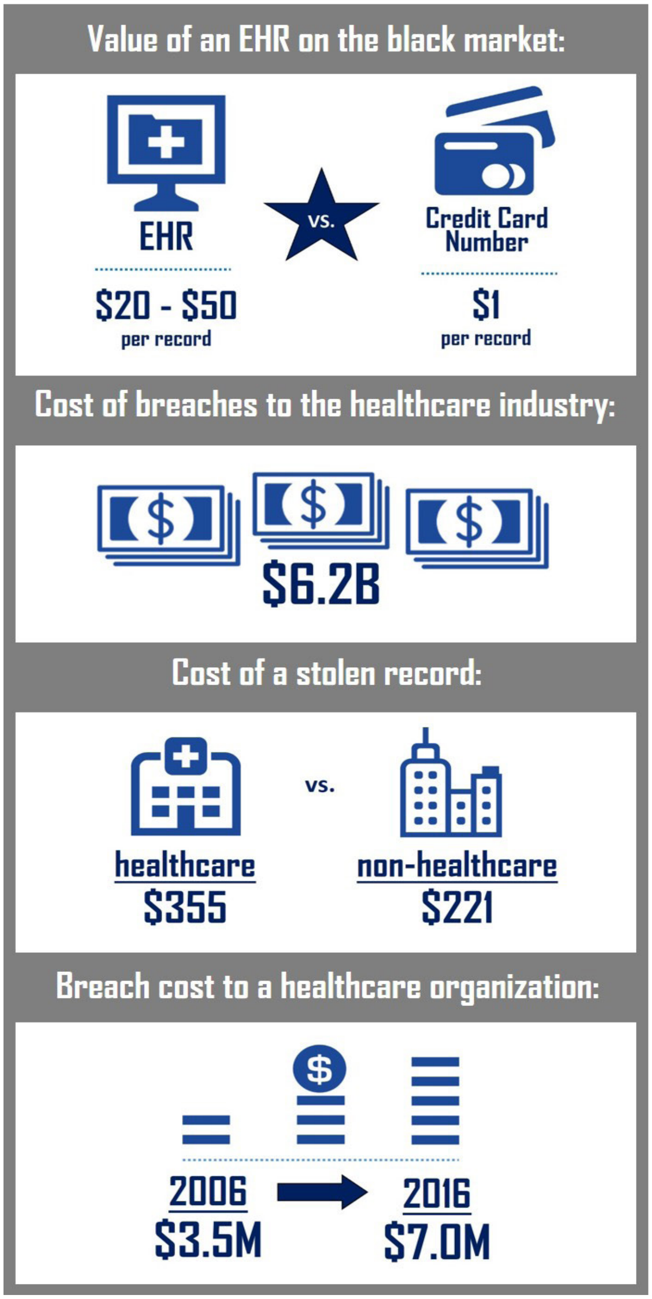
Finally, the provider sector accounted for 72% of breaches within the entire healthcare supply chain including payers, clearinghouses, pharma, etc.

CPAs / ADVISORS
blue

> No industry is **spending less on cyber security** than the healthcare provider sector, and yet no industry is **paying more per breach** and has more assets that are easily monetized.

Why Healthcare?

Whether you're the CIO/IT Director, CRO, CFO or CEO, you're probably asking "Why us?" The truth is, no industry is spending less on cyber security than the healthcare provider sector, and yet no industry is paying more per breach and has more assets that are easily monetized. Ponemon and Symantec (a security technology company) cite these statistics:



Additional Factors – The Internet of Things

If things weren't tough enough, changes in the delivery method of healthcare are exponentially adding to the cyber security challenge. These changes are extending (or eliminating) the borders that previously protected information. In the U.S., healthcare is experiencing one of the fastest adoption rates of Internet-enabled devices (Internet of Things or IoT) of any industry. While adoption enables more cost effective and efficient delivery of care, it also exposes the network to an endless number of "endpoints" that, if not controlled, dramatically increase the opportunity for not only data breaches, but worse, the potential malicious attack against these devices, which could end in life or death outcomes.

What to Do?

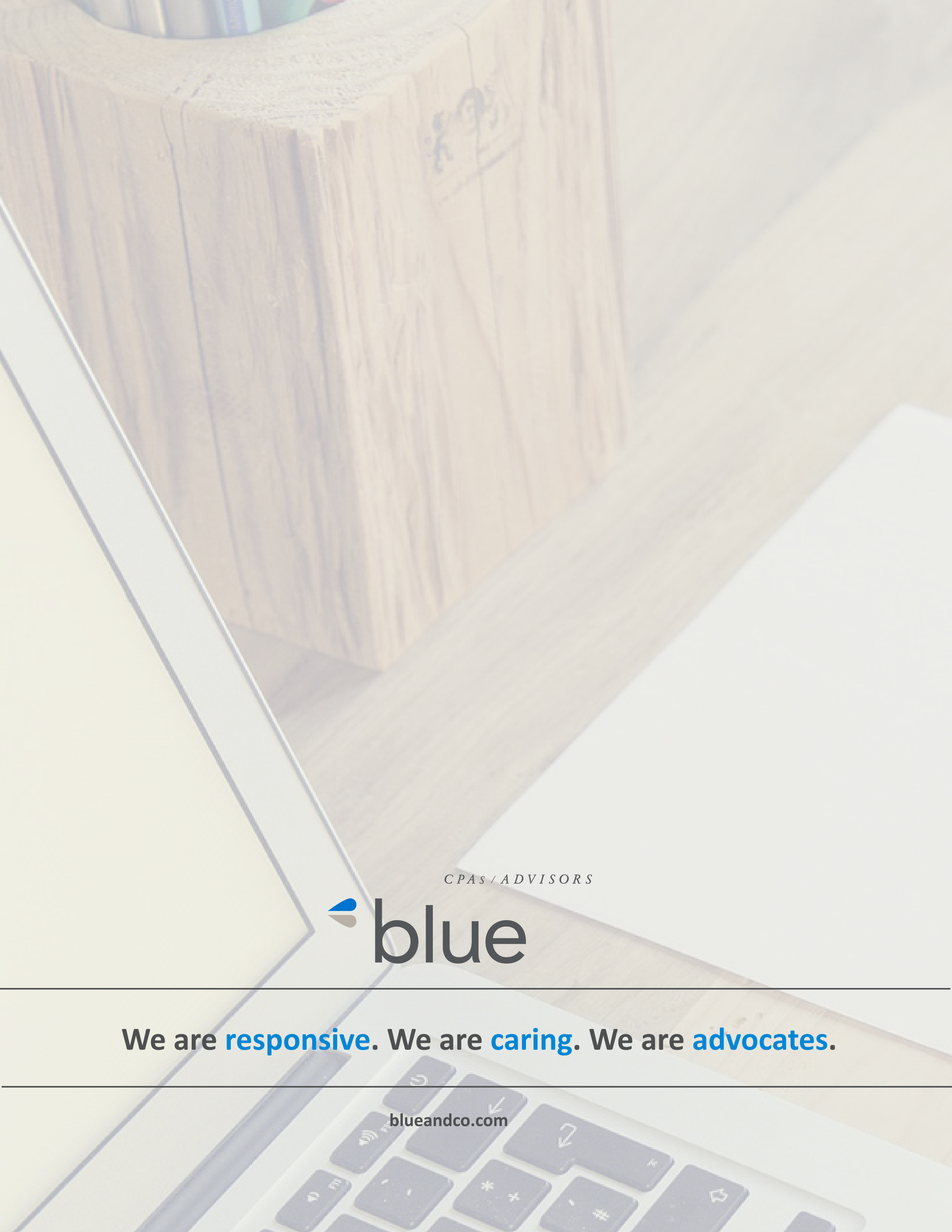
Organizations should stop chasing this problem solely with technology solutions. Conducting penetration tests or vulnerability assessments along with better firewalls is no longer enough. This traditional approach of securing the information from the outside and then working inward is wholly ineffective. A robust cyber security program must be in place to adequately protect your confidential patient information.

Blue & Co. has developed a tested methodology that considers cyber security from multiple perspectives. This "layered" approach begins with the identification of information and works outward. It helps companies prioritize information security efforts in the most cost-effective way available, while holistically addressing the multitude of risks and vulnerabilities to health information.

This approach allows Blue & Co. to make pragmatic and practical recommendations, which are implemented over time to reasonably address the cyber challenges facing your organization.

Tom Skoog, Blue & Co.'s cyber security leader, has over 27 years of experience helping clients address the issue of cyber security across a variety of industries, including healthcare. Our team of experts is available to meet with you to discuss ways in which your IT risk management procedures can improve within your organization.

Please contact Tom at 614-220-4131 or tskoog@blueandco.com.



CPAs / ADVISORS

blue

We are **responsive**. We are **caring**. We are **advocates**.

blueandco.com