Your security technology configuration could expose your clients private data

A data breach is estimated to cost your company $3.9 million dollars and by 2021, Cybercrime damages are estimated to reach $6 Trillion globally. In response, companies are spending an estimated $90 Billion in security products in 2018 alone to attempt to minimize the multitude of attacks.

But is purchasing new technology enough?

- Anthem pays OCR $16 Million in record HIPAA settlement following largest health data breach in history (https://www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html)
- Due to an incorrectly configured server, BJC Healthcare exposes 33,000+ patient records on the web for 8 months breach (https://www.hipaajournal.com/phi-of-33420-bjc-healthcare-patients-exposed-on-internet-for-8-months/)
- Phising scam results in 35,000 patient records exposed for ATI Physical Therapy (https://www.healthcareitnews.com/news/email-hack-ati-physical-therapy-breaches-data-35000-patients)
- Phishing attack exposes 1.4 million PHI records at UnityPoint (https://healthitsecurity.com/news/phishing-attack-exposes-phi-of-1.4m-unitypoint-health-patients)
- Phishing attack on Acadiana Computer Systems exposed the PHI of 31,000+ individuals (https://www.hipaajournal.com/phishing-attack-on-acadiana-computer-systems-exposed-the-phi-of-31000-individuals/)

If your company's data are compromised due to improperly configured security devices and software, then you are still on the hook for the damages. Plus, the public will hold you responsible for not taking the necessary actions to protect their data, regardless of who configured and maintains the equipment.

Choosing to invest the time necessary to utilize the security features of your existing and new security products, along with on-going end-user training, greatly ***decreases*** your chances for breach.

It's one thing for a company to invest in security products to protect both its data and its customers' information; yet, it's an entirely different thing to have the security products correctly configured to take advantage of the security features. We all see articles about "Best Practices" to help prevent cyber-crimes and these articles are there for a reason. However, these "Best Practices" are frequently ignored, which can result in a data breach. Something as simple as not properly configuring and enabling multi-factor authentication greatly increases your risk for a data breach through a phishing attempt.

Almost all the security products on the market provide very limited protection straight out of the box. This is by design as the manufacturer does not understand your business or what applications you use and therefore does not want to disrupt business operations. The result leaves the implementation and maintenance of the security products to resellers and service providers who claim their "recommended" security products, on which they receive a margin, will "prevent" ransomware, viruses and other malicious attacks; all the while giving you a false sense of confidence that your data is protected.

However, the integrators will rarely turn on many of the security features available because it takes time to evaluate and phase those security features into production to help avoid disruption to your business operations. That additional time to implement the additional security features also comes at a cost and the integrators fear they may lose a sales opportunity because the cost is higher than their competitors'.

Cyber-criminals are banking on poorly configured security, password settings, social engineering, among others, to gain access to your information as almost half of the targeted attacks are directed at small companies because many choose not to invest in security.

Another factor to consider is whether your cyber-insurance carrier would cover your claim in the event of a breach. Several insurance carriers have denied claims for "failure to maintain" their computer systems with reasonable security practices.[1]

If there is a breach and your cyber-insurance carrier does not cover the claim, your company may be out of business.

When considering whether your company's current security technologies are enough to help protect your business and customers' data, consider the following:

- There are zero guarantees that the security products you implement will "***prevent***" a data breach, regardless of security device configurations. Be wary of integrators who guarantee or claim to prevent ransomware, viruses, malware and / or data breaches.
- There are no shortcuts to securing your data because security is complicated. Short-term engagements often fail to identify and mitigate potential breach points to your data and are merely a band-aid to mitigate one or two of the vulnerabilities. Long-term engagements allow for a comprehensive review of the vulnerabilities with your environment, mitigation of the vulnerabilities, and then ***another comprehensive review*** to see what may have been missed or has become a vulnerability, allowing you to mitigate those as well.
- Understand that the more security features you implement, the more IT administrative overhead is required to manage it, requiring you to invest in training for your IT staff or to ensure that your IT vendor is capable and properly trained in how the technology functions.

Here at NextStep Technology Solutions, LLC, we partner with your company and integrate our team with yours to understand your business, which allows us to help create a security plan to help protect your company's data within your budgetary constraints. We are not a reseller but your partner in business.

Our team of experienced professionals are available for consultation for companies looking to ensure that they are making the best use of their technology to support their business while protecting their customers' data.

To learn more, please contact us at info@nextstepts.com

NextStep
TECHNOLOGY SOLUTIONS
Creating Business Efficiencies By Leveraging Technology

[1] https://www.hpe.com/us/en/insights/articles/cyber-insurance-what-companies-look-for-and-why-claims-get-rejected-1808.html