ROETZEL
FOCUSED ON WHAT MATTERS TO YOU

CORPORATE COMPLIANCE ALERT

9/14/15

Five Things You Can Do Today to Increase Information Security

Small healthcare organizations have very valuable data. In 2013, medical-related identify theft accounted for 43 percent of all identity thefts reported in the United States. And, according to some reports, healthcare data is up to 50 times more valuable than credit card data on the black market. Indeed, the FBI has released a private industry notification, stating that: "The health care industry is not technically prepared to combat cyber criminals' basic cyber intrusion tactics, techniques and procedures, much less against more advanced persistent threats. The health care industry is not as resilient to cyber intrusions compared to the financial and retail sectors, therefore, the possibility of increased cyber intrusions is likely."[1]

Yet, given the array of threats, and their relative sophistication, implementing a comprehensive cybersecurity, detection, and response plan can seem daunting, especially to smaller enterprises. While it is important to have a comprehensive, auditable approach to data security, below are five things you can do today to move toward a more secure environment:

1. **Implement Physical Security Protocols**: The physical security of devices containing protected health information is paramount. No matter how strong your software protections (i.e. firewalls) may be, if an attacker is able to physically access the computer containing the information in an unencrypted format, the value of these protections is lost. Make sure you have a documented policy in place regarding the use of computers and mobile devices, and an inventory of all devices. Develop minimum password requirements for each user that require unique features and characteristics. Make sure computers and other devices cannot be seen or reached by the public. And disable local vulnerabilities, such as USB drives, unless you really need them.

2. **Train your employees**: The biggest security threat to most enterprises is its own employees. Train your employees to be aware of attempts to achieve unauthorized access to your network. Train them in areas such as spear-phishing, shoulder surfing, password protection, physical hardware security, and basic encryption.

3. **Have coffee with the "security guy/gal"**: Do you know who is in charge of network security at your organization? If not, find out. If so, invite them out for a cup of coffee. Ask them what they are concerned about. Ask them what they would do, and if you get a bunch of acronyms, have them break it down for you in simple terms. Very often, security gaps arise from misunderstandings or even the complete absence of communication between business decision-makers and security personnel.

4. **Change your public wi-fi password, today!**: Does your organization support a public or "guest" wi-fi network? If so, it is likely the password has not been changed for quite some time. You freely give this password to all sorts of visitors for temporary use and it may be a vulnerability. So change it frequently in case an old password slips into the wrong hands.

5. **Start small, but have a plan**: Information security can be daunting. Don't rush out and purchase the latest and greatest threat detection system without carefully considering your needs. Not all businesses need, or can afford, A+ security. The key is focused, risk-based analysis of the company's security needs, and a plan to address these needs that has buy-in from the business leaders and the IT experts.

[1] http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf (last visited 7-6-15).

If you have questions or concerns related to cybersecurity or data breach readiness, please contact any of the following Roetzel attorneys for additional information.

Christian M. Auty
312.582.1684 | cauty@ralaw.com

James L. Ervin, Jr.
614.723.2081 | jervin@ralaw.com

Amanda M. Knapp
216.615.7416 | aknapp@ralaw.com

This Alert is informational only and should not be construed as legal advice. ©2015 Roetzel & Andress LPA. All rights reserved. For more information, please contact Roetzel's Marketing Department at 330.849.6636.