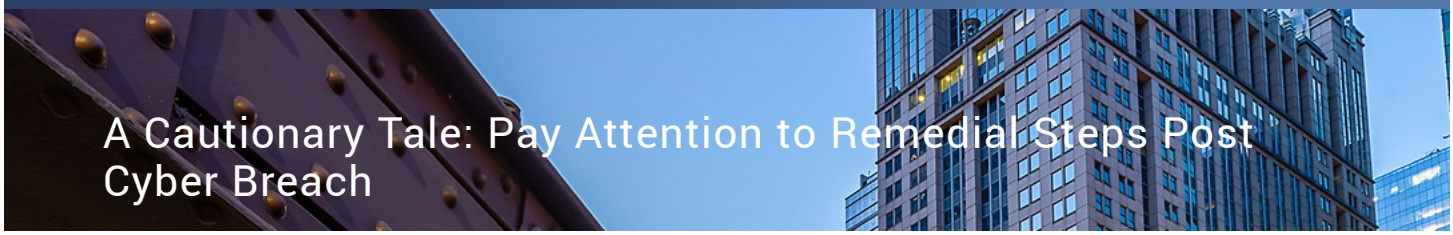
HEPLER BROOM LLC



A Cautionary Tale: Pay Attention to Remedial Steps Post Cyber Breach

By Glenn Davis on March 22, 2017
Posted in Civil Litigation

I remember in drivers' education class being shown the obligatory scary movie on railroad crossing accidents. After the wreck, one salty old train engineer says to another, looking at the demolished car, "Why don't they learn, Slim?" "I don't know, Jim," the other fellow says, scratching his furrowed brow.

In the information security world, we are past the need for scare tactics. Only an ostrich might be oblivious to the heightened cyber risks these days and their increasing frequency. Nevertheless, periodically you see cautionary reminders of mistakes that are made pre-, during, and post-security incidents.

Take one HIPPAA situation for example. The U.S. Department of Health and Human Services' Office for Civil Rights just announced a $3.2 million fine paid by The Children's Medical Center of Dallas. Why? In 2009 a BlackBerry device was lost, and in 2013 a laptop was stolen. Both devices contained unencrypted data which together revealed personal health information (PHI) for over 6,000 people.

In January 2010, Children's dutifully self-reported a breach on the loss of the BlackBerry device at the Dallas/Fort Worth International Airport in November 2009. The Blackberry lacked password protection and contained unencrypted electronic PHI and personal identifiable information (PII) on about 3,800 individuals.

When the laptop was stolen at the Hospital in April 2013, Children's filed a breach report the following July. It seems the laptop, too, contained unencrypted PHI and PII on nearly 2,500 individuals.

Hindsight is so crystal clear. How could Children's allow continued use of devices without encryption to protect PHI and PII, many of the devices dating back to the mid-2000s? And after the Blackberry was lost, how could it be that unencrypted laptops were still around, and the Hospital allowed its nurses and workforce to continue using unencrypted laptops and other mobile devices until 2013?

Children's decided to pay the fine and avoid a long and costly (and uncertain) fight to defend itself, a distraction from their care mission. In a familiar refrain, the Hospital reported there was no evidence, despite the two incidents, that any patients or their families were affected. It also reported that it now had new, enhanced levels of protection across the variety of devices in use and had beefed up training on the importance of protecting patient information, plus the security methods to do so.

In the healthcare sector, incorporation of mobile technology, virtual imagery over network infrastructures with remote access, and faster communication of medical data is vital to improved quality of care. Data breaches (whether by external attack or internal mistakes), or ransomware

(dedicated denial of service) are likewise threats to continuity of care and the physical and financial well-being of patients.

While these breathtaking changes in technology occur, headlines of healthcare organizations' information management lapses continue. The lessons of each incident must be carefully analyzed and applied to thwart future attack vectors and to protect patient information.

"Why don't they learn, Slim?" Regardless of the merits of Children's legal defenses, it is clear that the predictable events involving lost or stolen devices known to hold sensitive patient information did not inspire a hard look at both the devices used and the system protections in place in the days following those security incidents. The takeaway: don't get hit by that train. And that advice holds true for all organizations, not just healthcare institutions. Implement systems and protocols—in this case multi-factor authentication, end-point security, and encryption tools—to follow up on cyber incidents or loss of devices to ensure reasonable and effective precautions are in place to mitigate known or predictable risks.

Tags: Cyber Risk, Data Breach, Encryption, Healthcare, HIPPAA, Personal Health Information, Personal Identifiable Information