Why Hospitals Should Be Scared Of Cyberattacks

Joe Flower

If you are a CEO or COO of a health care organization, and your IT people have been trying to get your attention, it’s time to have a serious sit-down with them.

If they haven’t been trying to get your attention, it’s time to have a more serious sit-down with them, complete with charts and graphs and arrows on flip charts.

Here’s why.

Remember in November it was revealed that the Target retail chain’s computer systems were compromised? Some 70 million names, home addresses and phone numbers were stolen (pretty good raw material for identity theft) and 40 million credit card numbers.

It has turned out since then that some two dozen other companies, including Neiman Marcus, the Michael’s arts-and-crafts chain and the White Lodging Services hotel management firm, have been hacked in similar ways, with the attackers software sitting in the companies’ servers, credit card machines and cash registers often for months before they were detected, sucking down every transaction, every bit of data moved about.

Hey wait, you say, I have every confidence in our computer security. Why we passed a security audit just recently.

Heh. So did Target — just before they discovered the break-in. They got a clean bill of health, and the auditors failed to find the malware installed on every server, every credit card terminal, every cash register.

Why? Because the attackers have gotten way more sophisticated, and they used new techniques and methods of entry. You can now buy ready-made hacking software designed to do this on the Internet for less than $1000.

Here's the kicker.

Target has security guards at the doors, it has those beeper tags on small high-value items so you can't sneak them out without paying for them, it has burglar alarms — but the perps in the biggest heist in the company's history entered through the thermostat.

Got that? The thermostat.

Big-box stores have pretty sophisticated HVAC. Hospitals have much more sophisticated HVAC systems. Big-box stores typically outsource the management of such systems to outside firms. Most hospitals do the same. The outside contractor monitors and controls the HVAC over the Internet.

Continue reading... [1]

Source URL (retrieved on *09/20/2014 - 2:19am*):
http://www.surgicalproductsmag.com/blogs/2014/02/why-hospitals-should-be-scared-cyberattacks

Links:
[1] http://www.kevinmd.com/blog/2014/02/hospitals-scared-cyberattacks.html