Basic Cybersecurity Measures to Protect Your Firm

September 11, 2015

We have seen numerous companies and individuals that were ignoring the use of the same password on multiple sites (by the lack of a clear policy and procedure) until they were finally compromised. Then the stuff hits the fan.

Like long-term care insurance and straight-through processing capabilities, people too often don't realize the need for strict cybersecurity measures until they're personally affected. Sure, lip service is routinely paid, but it too often takes a catastrophic situation to get someone's attention.

There are specific elements to be addressed on certain risks and their appropriate responses in three key areas; behavior, procedures and auditing.

 <u>Major areas of concern</u>

In calling the attempt to change dangerous cybersecurity behavior the "Achilles heel of hardware and software," Unitel Risk Management noted several major areas of concern:

- The aforementioned use of one password for multiple accounts
- Free Wi-Fi over unsecured networks
- Sharing devices on a network
- Being "too social" on social media
- Broadcasting data

Three simple recommendations to implement

"Simple things, like using a password manager, go a long way," explained the risk management team at Unitel. "Wi-Fi encryption, also known as a personal VPN, is also a basic step to take. Lastly, it is strongly recommended that you use two-factor authentication to secure online accounts."

For those not in the know, a password manager saves user credentials after logging into a secure site. It then automatically fills in those credentials when the user returns to the site. It also periodically offers to change passwords, often including what seem like Egyptian hieroglyphics to prevent an easy compromise from hackers.

Wi-Fi encryption is just as it sounds; it encrypts communication and data during transmission. It also prevents unauthorized "leeches" from making use of a network.

Two-factor authentication requires the user to provide two means of identification from separate credentials, one being physical like a keycard and the other from memory like a password.

While many steps might seem simple and obvious, the Unitel risk management team claims adoption at the enterprise level into a formal procedure is not as ubiquitous as one might think.

"The business world has to start with having more transparency around security issues," Unitel argued. "It's a hard conversation to have because firms might not be doing all they should and don't want to reveal that fact, but vendors, especially, need to start thinking about how they certify that each other are secure, properly integrated and protect against leaks."

Be constantly on guard

No matter how secure, sophisticated or far along someone is in their career, the Unitel risk management team noted that today it still "boils down to being at a Starbucks trying to get some work done."

We're our own worst enemies, and human nature dictates that we too often take the path of least resistance and do it as simply as possible, which includes logging on to a computer. For this reason, everyone in business these days must be constantly on guard.

What's really important for the business world specifically is testing. Auditing of the security measures should be consistent but not predictable. Think of it like the military, where they practice the same drills for weeks and then change it up to see how they'll respond in the wild. That should happen with every business; they should be absolutely sick of testing because they do it so much."

www.unitelinsurance.com
4435 O Street, Lincoln, NE 68510
800-755-0048 • Fax: 402-434-7272