By Clinton Henry

HACKING PEOPLE: Why Your Biggest Vulnerability Isn't In Your IT Department

Last week, Chris stopped off at his local coffee shop to have a chai before heading off to a trade show to deliver a keynote speech.

As he sat at his usual spot near the counter a heated discussion ensued next to him regarding the 3rd Quarter of 2017. In the middle of the morning's caffeinated hustle and bustle, a marketing meeting was in progress.

He knew it was a marketing meeting because the three employees left the screens on their computers open to "Marketing Plans." Much to his amazement, they "abandoned" the table and were apparently on line (as well as online). They left two smartphones and a couple of memory sticks out in the open, plain as a Pumpkin Spiced Latte.

While reasonable predictions aren't always correct, there's a strong possibility that sooner or later the company will experience a breach. Moreover, it's highly unlikely that anyone within the business or IT has taken a serious look at how its users operate to protect from this sort of vulnerability.

The Biggest Risk

The biggest risk for any organization getting hacked is neither the firewall nor the server. It is another problem altogether: Social Engineering. Social engineering is when employees inadvertently (or out of malice) give cyber thieves sensitive corporate or client information. The problem with most businesses and IT departments is while they may be eager to "invest" in cybersecurity measures for their organization, they often neglect investing in shielding the most common attack surface motivated hackers use to gain access: employees.

Let's review some of the socially engineered pitfalls that occur all too often:

Public Wi-Fi – Public Wi-Fi is to your computer network as Kryptonite is to Superman or garlic is to a vampire. Unless you are sending out information that is encrypted via a secured site, never conduct any business from an unsecured Wi-Fi hotspot.

Public Places – In the space of two seconds, it would have been possible for a thief to take screen shots of the 3rd Quarter plan with a smartphone, or to swipe the smartphones and stick drives or even one of the laptops. Any document, especially any document with links to your organization, is all a cyber thief needs to get going. Never leave documents unattended.

Ever hear of "Visual Trespass?" It is the practice of someone in any public space "looking over your shoulder" viewing your computer screen. Here's an apt example: Alison, the head of tax and audit for a publicly traded company was traveling and noticed a stranger was trying to observe her computer screen in an airport while she was working on her corporation's soon- to-be-public 10-k filing! While the stranger may have been rude (and not a cyber thief), the person working on those financials was misguided and careless.

Moreover, public conversations that should be held in private can undo a company quite easily. Recently, the same Chris from earlier was in O'Hare airport while a gentleman next to him was on the phone with a colleague who needed access to a file. The helpful companion, within earshot of Chris, decided it was a good idea to give his coworker his personal password so he could access the file. If Chris was an opportunist, he could have simply made conversation with the unsuspecting traveler later and traded business cards, giving Chris his username and company along with his password. The businessman would have been none the wiser.

Phishing – Remember those emails we once received from Nigeria, Lithuania or Romania that named us as the heirs to great fortunes? All they needed to secure the millions owed to us was a credit card number. People fell for it in droves. Then there were fake job postings that asked us for background information. The postings looked legitimate and we gave them what they asked for – and we fell for that too. Phishing has not gone away. It has become so sophisticated that we believe it comes from our bosses or a supplier or a nonprofit we might support. The links in the email are typically malware that can infect the entire network and grab important files. Don't fall for it. When in doubt, always verify. An interesting fact: Millennials are more prone to falling for phishing than older employees! Over-familiarity with and blind trust of technology can be a dangerous thing.

Vindictiveness – Remember the angry employee who was terminated? What precautions were taken to make sure that he or she was immediately shut out from the network? Terminated employees can sometimes be vindictive. Have a plan and protect your data so the recently fired sales executive can't walk to your competitor with your latest leads or biggest accounts.

Vendors – Your computer network is only as good as who has access to that network. Many cyber thieves have successfully snuck in through a back door by going through the networks of your vendors. This is a potentially huge problem for any organization having a continuous relationship with suppliers. If your network is "secure" but your vendors have cyber security that is more like Swiss cheese, it can potentially create a huge vulnerability in your network.

Remember: While most internal IT organizations often seek funding for the latest network security equipment or software to beef up cybersecurity, they often neglect to engage their users to harden the organization from social engineering attacks that are commonly used to compromise a company. Neglecting to offer sufficient training for their users leaves the organization vulnerable to a hacker using a company's own employees against it.

Clinton Henry is one of the world's leading cyber security and identify theft experts. Known for his engaging keynotes and insightful perspective on business and personal cyber security, Clinton has amassed a loyal following of business and IT executives who look to him for guidance on how to protect their corporate profits and reputation from attack or compromise.
For more information on hiring Clinton for your next event, please visit www.ClintonHenry.com.