labusinessjournal.com

LOS ANGELES BUSINESS JOURNAL

COMMENTARY | THE COMMUNITY OF BUSINESS℠ | Electronically reprinted from July 18, 2016

Still Only Human

Well-prepared employees remain middle-market companies' best defense against attacks by hackers.

No technology will be sufficient if employees practice poor cyberhygiene. Any employee with access to a company's computer system represents a threat.

By MICHAEL A. GOLD

CYBERCRIME cost the world economy about $500 billion in 2015 and this year's numbers will be even higher. The cost of data breaches is projected to reach $2.1 trillion globally by 2019. Worldwide spending on information security is estimated to have been $77 billion last year. In the midst of these astounding numbers, the role of the "human factor" gets lost. This is a frightening fact.

Why? Because a breach is just one click away – a single person can and often will overcome any technological safeguard. This is an unassailable reality, but it gets mostly ignored.

Los Angeles County is home to thousands of middle-market companies and is a repository of tremendous wealth in these businesses and their owners. While the bulk of media attention has been given to breaches at major companies, more than 60 percent of all breaches hit middle-market companies, many of them located in Los Angeles. And while large organizations spend lavishly on their cyberdefenses, middle-market companies are often daunted by the cost of cyberdefense technology, and faced with what appears to be an insurmountable challenge, frequently go without anything more than minimal protection. Combine this with the potential catastrophic impact that a breach can have on a middle-market company without the resources to weather a postbreach customer exodus and you have a recipe for disaster.

There is, however, one element of cybersecurity where a middle-market company might actually have an advantage over a much larger organization – the ability to deploy its employees – its human factor – as a key part of its cyberdefense. With a smaller head count and fewer layers between management and line personnel, a middle-market company has the ability to

raise cyberawareness in an effective way across its entire (and smaller) workforce and exercise better control over how its people use computers and the internet.

Major hacks have a common element – the "human factor." But we don't focus nearly enough on the defining role humans play at every step in the breach lifecycle. Viewing humans as a crucial element of cybersecurity conflicts with the common perception that cybersecurity is a "tech" problem that has a "tech" solution and the equally common and utterly false belief that "regular" people just can't be taught this stuff. Yet it is not remotely adequate to rely on even the best firewalls and antivirus software. No technology will be sufficient if employees practice poor cyberhygiene. Any employee with access to a company's computer system represents a threat.

External actors

IBM's 2014 Cyber Security Intelligence Index reported that 95 percent of all security incidents involve human error. Many of these are attacks by external actors who prey on human weakness to lure insiders to unwittingly give them access to sensitive information. Insiders – current and former employees, in particular – have become the most cited culprits of cybercrime.

Many attacks involve social engineering techniques, such as "malvertizing," to lure targeted individuals into making mistakes. Ninety-five percent of advanced and targeted attacks involved spear-phishing scams with emails containing malicious attachments that can cause malware to be downloaded to the user's computer or device.

Failure to account for the human factor fatally undermines cybersecurity technology. Richard Henderson, a security specialist for Fortinet's FortiGuard Security Lab, said in a Bloomberg report, "It doesn't matter how much money a company spends on infrastructure or technology, until you close the human gap in the equation, you are always vulnerable to attacks."

Cyber Edge Group's 2015 Cyberthreat Defense Report (North America and Europe) states that for the second year in a row, "low security awareness among employees" was cited as the top inhibitor to an organization's ability to defend itself against cyberthreats.

With statistics such as these, employee awareness and cyberhygiene should be at the forefront of corporate cybersecurity priorities. Effective cybersecurity must account for the "human factor." Flawed perceptions must give way to the reality that humans should be part of a company's cybersecurity strategy. Particularly in Los Angeles, with its vast number of mid-market companies, the objective of every one of these companies should be the creation of a "human firewall."

Michael A. Gold is co-chairman of the Cybersecurity and Privacy Group at Jeffer Mangels Butler & Mitchell LLP. Contact him at +1 (310) 201-3529 or MGold@jmbm.com.