KANSAS CITY
BUSINESS JOURNAL

Optiv Security: Simple steps to make every business more secure

LESLIE COLLINS
Kansas City Business Journal

With October being National Security Awareness month, the Kansas City Business Journal turned to Overland Park's Optiv Security for tips on how businesses can better protect themselves.

John Turner, director of cloud security enablement for Optiv, shares four simple steps every business should take:

Identify your exposure to threats

You can't begin to adequately protect your business from cyber-security threats unless you "take stake of what your exposure is," which can include the company's online presence, local computers, security policies and email systems. Make sure that computers are updated on a regular basis and that antivirus software also is up to date. Even components, such as Adobe Flash Player, need to stay up to date, he said.

"All of the threats out there take advantage of flaws in the software and the companies that make all the little bits of software that run on your phone or your computer," he said. "I think many companies get lost in the business focus, and (keeping software and computers updated) is something that you can fall behind in pretty easily."

But hackers can exploit outdated software to take control of a computer, he said.

John Turner, director of cloud security enablement for Optiv Security

Change your passwords

"Many people haven't changed their passwords in five years, or ever," he said.

A number of people use the same password for their social media and other online accounts as they do for their business accounts, which makes businesses vulnerable, he said. It also could lead to phishing, where an employee reveals information that allows a hacker to access the workplace system. To lessen cyber threats, passwords for both personal and business accounts should be changed frequently, he said.

Encrypt your laptop and mobile device

With advances in operating systems, it's easy to encrypt a company laptop or other mobile device, he said. And unlike years ago, encrypting the hard drive doesn't eat up computing power. It ensures that if the mobile device is lost or stolen, the information on the hard drive is safe. Even if the hard drive is removed, the data remains scrambled and unreadable.

Host a security awareness training refresher

"Think about retraining these folks again, running them through a formalized cyber-security training or something that your team puts together internally," he said. "When we think about cyber-security training for employees, it's really about being aware of the threats that exist, that may come into our mailbox, that may come in through a fraudulent purchase order or a malicious link in an email."

Even taking 30 minutes of training time is beneficial, and every employee should participate, he said. Topics can include setting up passwords, explaining phishing emails and detailing how personal social media accounts can create a potential threat vector in the business.

"The value is pretty big," he said of training. "Employees really are the first lines of defense of any organization from the cyber-security perspective. They're the ones that are interacting all the time with outside organizations. They really are the front door in many ways of every organization. … The benefit is really improving your company's cyber-security posture by reducing its threat surface and by creating smarter employees."