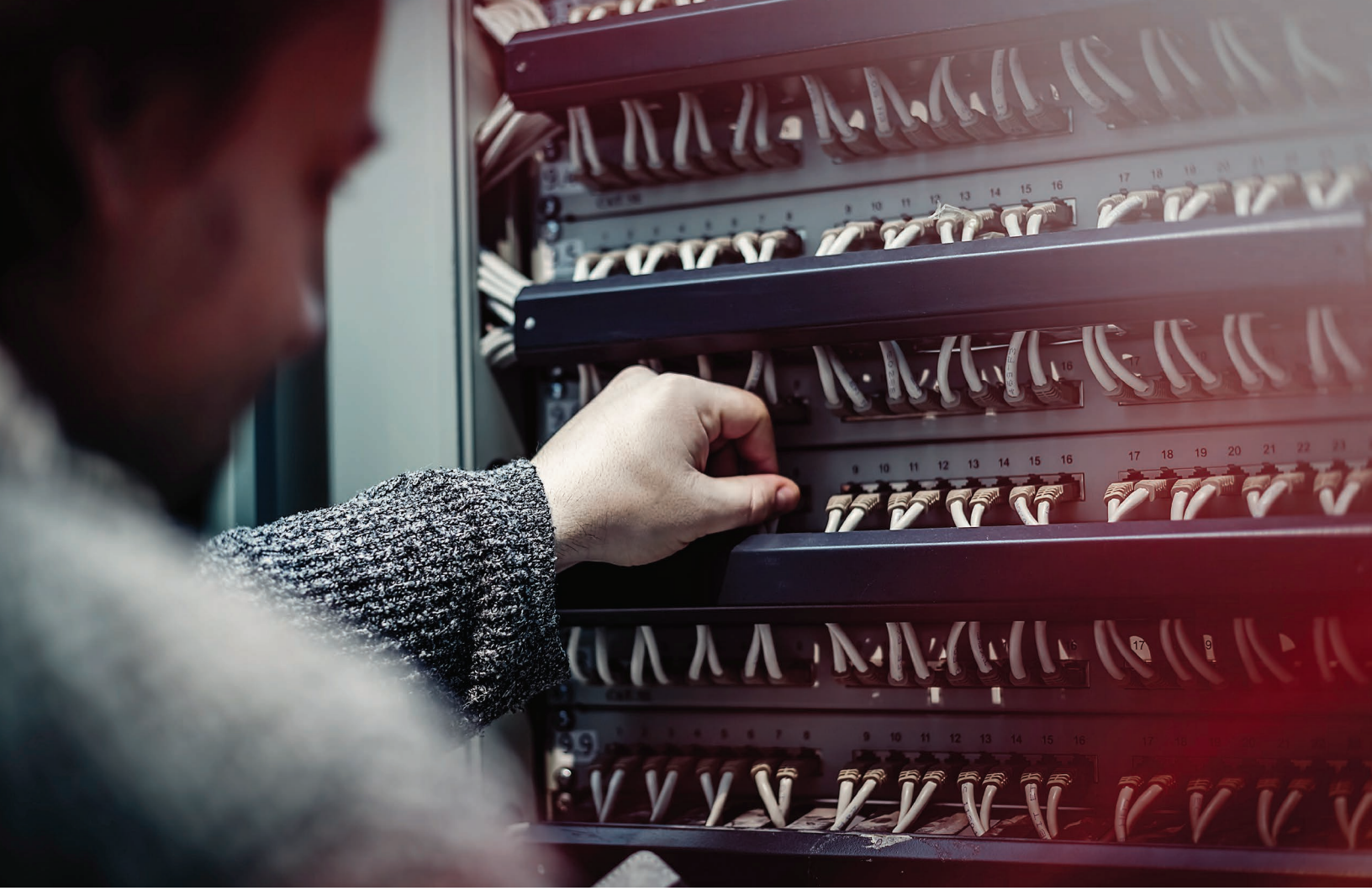
# DATA SECURITY IS A PEOPLE PROBLEM



## DATA SECURITY IS A PEOPLE PROBLEM

There are some things that only humans can fix. 95% of all security incidents involve human error. Ashley Schwartau of The Security Awareness Company says that the two biggest mistakes a company can make are “assuming their employees know internal security policies” and “assuming their employees care enough to follow policy.” There are many security risks to which your data is susceptible, but there is one method that remains a wonderfully effective hacking tool. That is the phishing scam. This scam is a legitimate looking email that asks the reader to click on a link. If clicked, the link can infect the user’s computer with malicious software that can steal passwords, logins, and other critical data. Alternatively, the email appears to be from a legitimate source, perhaps even duplicating a legitimate webpage. The distinction is that the phishing email asks the user to enter personal information, including passcodes. In either case, that is how hackers easily get into your systems.

What’s the best defense against this one? The single biggest defense is education. Training your people to be constantly wary of all the emails they receive. One way some firms are educating their people is by sending out their own “fake” phishing scams. Employees who click on the link inside are greeted with a notice that they've fallen for a phishing scam and then are offered tips how not to be fooled in the future. Think of it as the hi-tech version of Punk’d.

You  may not be ready to go that far, but it is important to provide ongoing training to all of your staff about phishing scams. Your staff are critical factors in your data security plans.

To avoid falling into these traps, you must: a) have a plan, b) educate users about your plan, c) make them care about procedures.

To give a quick summary, you need to have a defense plan for each of the layers that a hacker can attack: the physical  layer (i.e. you need policies to ensure that only authorized personnel can access your devices), the network layer (i.e. make sure that only authorised devices access your network, and your devices only access authorized networks), and the human layer (i.e. you should make your employees practice good password hygiene and are aware of security threats).

You should train employees on  your security and disaster recovery policies at least twice year, and your IT person should keep your employees up-to-date on security issues on a weekly basis. Make sure that they understand the risks of a breach.

Most importantly you need to create a “culture of security,” where employees go beyond the minimum guidelines laid down by your IT staff and always ask “is this good security sense” for every action they take.  You need to have clearly defined penalties for those who practice bad security, and reward those who display good security sense.

## CONTACT DETAILS

**Jack Harasimowicz**
Account Specialist
Email: Jack.Harasimowicz@iuvotech.com
Phone: 781-722-3221