Beyond Security Awareness

TALKING ABOUT SECURITY IS NOT ENOUGH. WE ALL NEED TO ACT ON SECURITY PRACTICES.

RAJ GOEL, CISSP, is CTO of Brainlink International, Inc. and an IT and infosecurity expert who develops security solutions for various industries. Senior Managing Editor Joyce Chutchian spoke with Raj about the state of IT security.

Q: You've written and spoken a lot about social media threats and risks. What are your biggest concerns?

First of all, there is the myth that cybercrime and financial fraud is a recent concept, when in fact, the problems started in the 1934 to 1936 era, when the IRS issued Social Security cards. Your Social Security number became your de facto ID number, and it's still used today, despite all the corruption and identity fraud.

I give a popular talk at conferences, on how social media and the cloud are over-collecting worldwide, especially for the under-18 population. Kids who were born in 1983 and beyond have grown up with computers. They do everything online like SMSing and chatting. As teenagers, they are not wired to think of 34-year-old threats. We have built a surveillance engine; everything a 12-year-old says online will never be forgotten. And what they say and what their friends do and say, whether it be on a game website, retail or Facebook, will follow them and haunt them for the rest of their lives. It's all stored in the cloud, and they don't even know what the cloud really is.

Q: What are your biggest concerns about the cloud right now?

From a technical perspective, there is no clear definition of what the cloud is. Some people are relabeling it as private hosting, and private data centers are relabeling it as the cloud. From a legal perspective—under current U.S. federal law—what the cloud gives you technically, it takes from you legally. Take HIPAA for example: You are a doctor. If your records go missing, you are personally liable for that data loss. The customer records are lost, and the organization is held accountable for any breached data.

In the cloud, if your vendor loses data, the vendor is not liable. You are liable. I'm working with nonprofit, underprivileged healthcare organizations, and they want to be compliant. They don't have the budget, so they are moving to Google Apps. Google says not to use Google Apps for HIPAA or PCI. Vendors have been carefully insulating themselves from any liability without telling the customer. There is no lemon law for cloud computing. If Google loses your data…oops! The liability is yours.

Q: What can we do about this?

We need to educate everyone aged 18 to 60. This means educate ourselves, management, families, and other members of our society who help enforce the laws, design and pass them. Don't just collect a paycheck. Be involved as citizens of our society and in politics. As security professionals, we are all citizens, and we are all consumers. It is our charter that we have to be in the front lines of protecting fellow citizens, whether it be attorneys, accountants, teachers, parents, medical professionals, etc. Go talk to your local parent/teacher school groups. Talk to the Boy Scouts and Girl Scouts; local attorneys and bar associations.

I have spent more than fifteen years reading the law on security—and it's not how you can configure a firewall, it's how you can create a security policy. Encrypt your laptop. Don't be lazy. It's not enough to be educated—you need to enforce awareness. Just because a security question asks you for your mother's maiden name, doesn't mean you have to use her real name. Change your passwords frequently. Don't just talk about security, act on it. (ISC)²