SPECIAL REPORT

Building the human firewall

People are more important than technology when it comes to cyber security

Thu, Apr 26, 2018, 00:00

Barry McCall

Just about everyone has been caught out by a cyber attack or knows someone who has – the person who opens an attachment on a seemingly innocent email only to find a pernicious virus and a ransom demand contained within it or th individual who responds to a request and unwittingly gives sensitive personal or company information away to cyber criminals.

The stories are legion. But they all tend to have one thing in common – technology wouldn't have saved the people involved.

All the firewalls in the world won't stop a hacker getting in the front if an employee opens up the back door. Technology i only ever going to be part of the solution. Cyber security needs to be about rapid response, isolating attacks, acting quickly and sharing information.

Vigilance, therefore, has to be embedded into the culture of all organisations. "You need to turn your staff into centurions in the cyber battle," says Tony Hughes, associate director, risk consulting, with KPMG. "Cyber security is about people, process, governance and technology. Everyone goes to work in the same way, to do the job as best we can. People don't consider themselves to be at the front line in cyber security. There needs to be a lot more training to develop awareness o what nasty things look like. Companies also need to create an open culture. If you do something wrong it is much better to report it early. A cover-up only makes matters worse."

Peter Oakes of Fintech Ireland agrees. "Very often it's not the original issue that arose from the breach that's the problem it's the cover-up," he says. And the consequences for companies which are perceived to have been less than forthcoming can be very serious.

"The markets are very unforgiving," he notes. "Just look at the downward spiral in tech stocks following the Facebook/ Cambridge Analytica disclosures. Organisations need to have the right protocols in place for what people do following a breach."

'Breach-ready'

Hughes agrees. "All organisations have to be breach-ready. Companies and their employees need to understand what to do in the minutes and hours after a breach," he says. "They need to have a business-continuity plan. They need to know how to respond to customers who might come after them for a GDPR breach."

People can also be first line of defence, Hughes adds. "It's very important that people are made aware of threats, including bad actors, out there."

Three Ireland head of business products, marketing and operations Nicola Mortimer says organisations need to create a "human firewall" to protect them against cyber attacks. "They need to build that and ensure that it is sufficiently strong t protect the company and the individuals who work there," she says. "It is known that most issues that arise are the result of human interaction and culture is critical in combatting that. You can apply all the technology you like but if someone opens the doors it is worthless. You have to make people aware of the risks and how attacks might arise."

One source she refers to is what has become known as social engineering. This is where the cyber criminals track someone on Facebook, make friends with them, and slowly but surely gather information which either facilitates blackmail or offers them a back door into their employer's networks.

Another avenue Mortimer points to comes in the form of the various free online storage apps available to people now. If organisations put an arbitrary cap on employees' storage capacity, they will quickly turn to these apps which are not protected by the employers' security systems.

"There are also physical aspects,"she notes. "How people get into a building is important. People should be vigilant in relation to who is coming and going."

Training on cyber security technology is important as well, she says. "What is the point in deploying new firewalls and security technology if you don't teach people how to use it? You would never dream of doing that with something like a new CRM system. You have to do it with security as well."

Training has to be continuous. "It's not static," Mortimer adds. "This is moving towards e-learning, where people can get the training in their own time, whenever they want. This is better than classroom-based sessions as it allows people to keep up with the latest developments and threats."

Think before you click

According to Tony Hughes, the message has to be: think before you click. "In the old days, you could identify the fraudulent emails pretty easily through the bad spelling and so on," he points out. "But the internet has allowed the bad actors to collaborate and become organised and pool knowledge so their activities are becoming much more sophisticated. People need to be aware of that so they are not caught out."

The other issue he points to is people's demand to conduct almost every aspect of their lives online. "The current generation of millennials has grown up with digital services and they want everything online and they want it to happen instantly. They want to be able to open bank accounts, buy tickets, do shopping and so on, all instantly. That presents challenges. How do you make these things secure when they happen in the blink of an eye? We have to look at new forms of biometric security like fingerprint-, iris- and face-recognition that mobile phone makers are looking at.

"The human has to be first port of call though. Organisations have to work to make the human the strongest link in the cyber security chain. You can't rely on a black box for security – you have to link it back to people and support them with governance, processes and technology."

MORE IN SPECIAL REPORTS

D-day for data protection as penalties to be introduced for breaches of new laws

Ireland difficult to topple as global aviation leader

Chinese firms continue on acquisition trail

Ireland can offer Brexit solutions