Relevance is the key to users' security understanding

François Amigorena

François Amigorena, IS Decisions

A recent piece of research found that a shocking seven out of 10 office workers admitted that, should they become aware of a security breach at work, they wouldn't know who to report it to.

This survey was across a sample of 2,000 people in the UK and the US, and to most security professionals will probably not be that surprising. We all know that user education on security is lacking in most organisations. But this really is the most basic of knowledge requirements. Surely if you are going to teach your users anything at all with regards to security, the first thing you tell them is who to report to in the event of discovering a breach?

This suggests that this statistic doesn't just show that user understanding about security is lacking – it means that the majority of the time there is no understanding whatsoever. User education is woefully inadequate.

No 'one size fits all'

Although that is very likely the case, there is something else worth saying about the revelation, and that is that it will not be a standard answer to 'who do you report a breach to?' across all organisations.

In some cases the right person to report to might be an IT manager, another the MD, perhaps a chief security officer or even human resources. The person you report to may be dependent on the nature of the brief. On closer inspection, it's not that straightforward a question to answer. And this is why we need to start looking at the issue of relevance and relativity. Who does have responsibility for security in the organisation and how is that communicated to employees?

Real consequences

These are the basic elements of security training, yet any security professional who has embarked on training employees will be familiar with the lack of engagement that can occur. If security does not impact employees directly, their career goals or day-to-day work, then (perhaps understandably) it is unlikely to be a priority. Naturally, the priority is getting their work done, and in some cases that might involve circumventing security policy – sharing a password so a colleague can access a specific file, sharing something off the network without the correct administration rights.

If we start relating security back to the things that do matter to employees – namely their career goals and everyday work – then we start to see more positive behaviour. If sharing a login with a colleague results in your own restricted access, then you are much less likely to do that. If the consequences for bad security behaviour are as severe as impact on promotion, or even potential for dismissal, then suddenly it becomes very much in your best interest to pay attention in that training session.

Training *in situ*

Many of us have experienced training at work that has been inspiring at the time but mostly forgotten by the time we're back at the coalface the next day. The key to successful work training is to create practical ways of employing what you have been trained to do in actual situations. Most trainers will tell you that successful training is a combination of theoretical and 'on the job', and the same is the case for training users on security issues.

"Explaining to your users what the potential risks are in directly relatable terms will ensure that they comprehend them more fully"

It is not enough to tell users what they should and should not be doing, then just dismiss them to go about their daily working lives. Instead, use training in conjunction with telling users what is good and bad behaviour *in situ*. For example, they could be served an alert when logging in from a new device or location, when attempting to access a file they don't have rights for, or otherwise engaging in suspicious behaviour.

By explaining that what they are doing is wrong and why when they actually engage in taking a particular action, users are far more likely to comprehend more fully.

Know your audience

We know that any approach to internal security is not a case of 'one size fits all', and so it is important to know your audience and how to relate it in their terms.

In the recent '*Insider Threat Peer Report*', which contains the views of several IT and security professionals, Joseph Reyes, IT manager at Bellicum Pharmaceuticals, said: "In the biotech industry, executives tend to listen when the conversation is the theft of intellectual property. They understand the need for forensics and the ability to find out who did what and when they did it. I think when you can show that an idea can be stolen and that you can get the tools to either watch when that is occurring or identify who did it after it occurred, you become a hero."

> ***"In the biotech industry, executives tend to listen when the conversation is the theft of intellectual property. They understand the need for forensics and the ability to find out who did what and when they did it"***

This principle is adaptable for any industry. In finance it may be fraud that employees are most wary of; in law, perhaps client-sensitive information. In education, students may not immediately understand the risks of sharing a password with a friend until you explain that, while lending front-door keys to a friend is relatively safe if you get those keys back, once you give a password to a colleague they can access your files whenever they like until you effectively change the locks by changing your password. Explaining to your users what the potential risks are in directly relatable terms will ensure that they comprehend them more fully.

How technology can help

We've talked a lot about the use of language and how to interpret security issues and rules. These are cultural factors, but technology can help deploy them. It can be the vehicle through which you deploy these cultural tactics, if you have technology that allows for real-time monitoring, risk indicators and a complete view of network activity. This will be a solution that allows you to:

Detect suspicious access, and alert users and administrators automatically to anomalies so that they understand what 'suspicious' looks like *in situ.*

Manage mobile users, with users working across smartphones, tablets, laptops and desktops.

Restrict access to sensitive files so employees can only access the files and systems they need.

Restrict concurrent logins, eliminating the possible windows in which unauthorised users can access sensitive information.

One thing you might want to set up is alerts that let users know exactly who to report to if they detect any suspicious behaviour. That way you should find that your users are not part of the 70% that are in the dark about the most basic of security training principles.

About the author

François Amigorena is founder and CEO of IS Decisions, a provider of infrastructure and security management software solutions for Microsoft Windows and Active Directory. IS Decisions offers solutions for user access control, file auditing, server and desktop reporting and remote installations. Its customers, including the FBI, the United Nations and Barclay's, rely on IS Decisions to prevent security breaches, ensure compliance with major regulations, such as SOX, FISMA and HIPAA, quickly respond to IT emergencies and gain time and cost-savings for IT.

Reference

1. 'The Insider Threat Peer Report'. IS Decisions. Accessed Mar 2015. www.isdecisions.com/insider-threat-peer-report/.