Priorities a little off the mark?

Michael Barwise

As I write this, the UK Cyber Security Challenge is under way. It seems timely to consider its emphasis, and that of an interesting report - "A Human Capital Crisis in Cybersecurity" published earlier this month by the US Center for Strategic & International Studies.

Both ventures seem grounded in the premise that the proximate cause of our abysmal level of security on the Internet is a shortage of brilliant hackers wearing white hats. It's a fashionable position - indeed hacking and vulnerability research has for ages been the sexiest part of the business, with its own clique of celebrities. But is it really the most important part, and will expanding the echelon of the radiant-titfered sexy really prove to be the panacea we long for? To quote a famous lady, "No, no, no!"

Let's look at some more or less randomly selected facts.

Every vulnerability discovered by the researchers - and don't get me wrong, we do need them and they do a good job - has first been created by someone else.

The most common password currently in use seems from recent breach records to be "password", but for every password obtained via a brute force breach, thousands - maybe vastly more - are given away every day by unwitting - read "unobservant" - users via phishing attacks. And often much more than mere passwords is given away.

A substantial proportion of malware infections occur because some web designer failed to protect a legitimate - even mainstream - web site's backend database from injection of malicious JavaScript via a public page. That's just sloppy programming.

Directed hacking attacks on government and corporate systems most often make use of glaring omissions or errors in configuration, obvious design flaws or failure to keep systems up to date in the face of known vulnerabilities. The intricate and cunning does feature in attacks, but nothing like so often.

So, disappointingly to some, most of the time we are not operating at the "bleeding edge" - neither is the proximate cause of our state of insecurity in general the extreme cleverness of a special breed of superheroes in black hats, nor is our greatest potential protection the extreme cleverness of a special breed of superheroes in white hats.

I accept that sometimes a very new, cunning attack vector gets exploited widely, such as the current Windows .lnk bug that has gone wild since the middle of July. But our greatest weakness and the root cause of most of our problems is failure to pay proper attention to detail or apply forethought at all points on the supply chain from designer through developer, implementer and maintainer to user. It's a human problem first and foremost, not a technical one.

Perhaps not surprisingly, the word "psychology" occurs nowhere in the 53-page Human Capital Crisis report, and the word "human" occurs only in its title. The report concentrates exclusively on technical capacities and how the population of those with them can be dramatically increased in size via programmes and initiatives. To be fair, it does in passing note and deprecate the prevalence and inadequacy of paper compliance, but it pays no attention to the "human equation" - the rock on which the best of technical intentions often founder.

The Cyber Security Challenge consists of three competitions - one in robust network design, one in digital forensics, and one in finding security flaws in a web site from the client side. All good stuff and necessary, but a very small part of the overall security problem we face.

I would like to see competitions in the design and review of robust business processes, the creation and implementation of workable policies that don't end up as shelfware, and the design and creation of bug-free software and protocols. In short - testing people in thinking before they act, thinking while they are acting and anticipating the outcomes of their actions. That's really what is missing.

The bottom line is that every vulnerability is either a piece of flawed design or a piece of flawed programming - a mistake - and there are so many mistakes being made it's a miracle anything works at all. But mistakes by implementers and users of these already flawed systems are at least as common. Training up an echelon of experts in finding and countering the symptoms of the purely technical subset of mistakes may be needed as a short-term expedient, but it's not a valid long term solution to

the whole problem. We must learn to make fewer mistakes in the first place. Otherwise the bad guys will always be ahead of us and we'll ultimately lose the fight.

Originally appeared on the Infosecurity Network, July 2010