

What does 2011 hold in store for IT security managers?

This year is set to be a landmark one for British business, with a myriad of new technologies and communications tools changing the way we work, and e-government services finally coming of age as local and central bodies turn to IT to help them work within austerity budgets. However, with this increased reliance on IT comes increased risk



With an increasing number of new technologies finding their way into the workplace, either through company-sanctioned deployment or employee ownership, the risks to the workplace from data loss, theft, malware infection and hacking are on the rise. This, combined with pressures on IT departments to keep Identity and Access Management (IAM) in check, also means that companies are at risk from ex-employees using company IT accounts even after they have left, even if they went in less than positive circumstances.

To find out more, Risk UK spoke to Chris Boyd of GFI Software about the changing threat landscape and the challenges this will pose for IT managers and security specialists during the year ahead.

How has the threat landscape changed since 2010, and why?

Social networks have been an important aspect for a few years, but we're now posting sensitive company information to "behind closed doors" communities of business-centric portals, in addition to the more usual public facing sites such as Twitter and Facebook. I think it's fair to say these kinds of third party services hosting your company data will become a target in 2011, which will probably include everything from targeted phishing attacks to disgruntled ex-employees that have not had their network and application logins to these services revoked, logging in and obtaining potentially sensitive material that can then be used for financial gain or simply to create significant embarrassment or regulatory trouble.

Where and who are the new generation of security threats and challenges coming from? What are the motivating factors?

The old problem of strong passwords is as big an issue as ever, partially because of the recent Gawker hack which saw many users become compromised across many services due to shared passwords. The fact that so many of us use the same username and password across all our online data silos means that when one becomes compromised, everything can unravel like a house of cards - from a PayPal account to a Gmail mailbox. As many services look to strengthen their offerings (two factor authentication for Gmail and tougher, randomised logins for online banking are prime examples of this), so too will attacks become increasingly

sophisticated. We sometimes see attempts at man-in-the-middle attacks on banks using two factor authentication, and this will continue as the services we're offered have their security bolstered. In all cases, money seems to be the motivating factor and it's been that way for some time.

Will major events this year and next (Cricket World Cup, Olympics, Voting Referendum etc), pose additional security risk for companies?

Yes, particularly anything dealing with sensitive information. Right now there has been a big online push to recruit volunteers for next year's Olympics, and no doubt there will be more such drives to sign people up to help with individual events related to the games. Such things will likely become the target of either direct (hacking) or indirect (phishing) attack. It will be very interesting to see if the online submission form for the 2011 census becomes a target for hack attempts and data theft.

How important to brand and company reputation is a good approach to enterprise IT security?

It's very important. If a handful of staff all use a company Twitter feed, they probably have a very basic password for convenience - at that point, the corporate Twitter feed is only a few steps away from an embarrassing and potentially brand damaging incident. Companies should take ownership of the situation and see if they already have a presence on all the major and emerging social networks out there - in many cases, the presence has been set up by someone unrelated to the company, or a well meaning employee running an unofficial webpage. Location based services need locking down, too - anyone can potentially place you on the map and any unmonitored comments/discussions that turn nasty could reflect poorly on the company the page is associated with. As social media outreach is becoming part of the day-to-day communications process of a business, so to must it become part and parcel of day to day information security.

What about regulation - is it getting easier for companies to protect themselves from the fallout of external cyber attacks, or harder for them to meet new IT security compliance standards?

New forms of technology in the workplace are proving difficult for IT staff to manage - everything from mobile devices to videogame consoles in the workplace potentially offer users a way to post to Twitter and Facebook from inside the network, even if said websites are blocked or managed for compliance purposes. It's fair to say there's a bit of catch-up involved in learning about the types of services these convergent technologies offer. Having said that, there are tools available to regulate Facebook application use on a granular level and even Twitter can now be monitored / regulated on the corporate network so things are getting better.

"It will be very interesting to see if the online submission form for the 2011 census becomes a target for hack attempts and data theft"

GFI
www.gfi.com