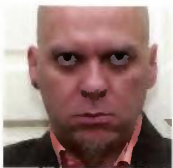




Insight



Securing your home office

Here's an interesting question for all you information security professionals out there: how secure is your home IT? No, seriously. There's no doubting that you have a handle on keeping data secure across the enterprise alright, but how clued up are you away from the office where things are actually rather different in terms of both risk and response? **Davey Winder** investigates

Although there is some weight to the argument that cybercrime is pretty much a high-tech scattergun these days, with no great regard being given to whether the target data is on a corporate network or within the home, the truth is that there are some important differences between the two in terms of the threat landscape. One key area of difference is the average user profile at home, an aspect that is easily overlooked by the infosec professional used to one-size-fits-all employees.



No one needs to become the CSO of their own house

Frank Kenney

Throw young and technologically naive children into the mix, together with inquisitive and rebellious teenagers, and the risk landscape becomes much harder to manage. "Children have grown up with technology and are adept at driving it", David Emm, senior security researcher at Kaspersky Lab reminds us. "The internet is a relatively new phenomenon and there's no 'online common sense' to match the guidelines we're able to pass on to children about how to cross the road safely".

This is why it's vital to look at the non-technical context in which family computers are used. "Not allowing a child to have a computer in their bedroom, but locating it in a family room; simply sharing childrens' online experience from a young age; or establishing guidelines about what's safe and isn't safe online", Emm suggests.

Teenage angst

That said, infosec professionals are also far less likely to underestimate the value of computer security software than your average Joe. This puts them in an ideal position to best protect the family.

"Certainly from anecdotal conversations I have had with infosec professionals at trade shows or conferences, they do transfer their best practices to their home environment", Rik Ferguson, senior security advisor at Trend Micro, told us. "Infosec professionals certainly know enough to restrict the user accounts of their kids from having administrator privileges", Ferguson adds.

Unfortunately, a lack of time rather than awareness is often the main problem when it comes to home security, and while one-size-fits-all solutions provide a quick fix, they might not provide the most secure one.

As Norton security expert Con Mallon says, "Teenagers use the internet in a different way and therefore parents need to tune their



It is near impossible to keep a logical separation of your home and office domains



[Infosec professionals] do tend to practice what they preach both at work, and at home



John Walker, ISACA

home security to address this. Many teenagers do not email – communicating over instant messaging and social networking sites is far more appealing to this audience”.

Then there are the multiple devices that connect to the internet to consider. “Cybercriminals can use that to their advantage and tempt your teenager into downloading that game or music in a format in which a virus, worm or malware can then enter the home network and infect and impact all of the family”, Mallon warns.

Indeed, recreational use is something that is simply dealt with in the corporate environment by generally blocking it, which is not an option at home if you have teenage kids or something called a life! “Perhaps professionals are in danger of becoming complacent and likely to fall over the bad things”, admits Nigel Hawthorn, VP EMEA marketing, Blue Coat Systems, who adds that conversely, “we’re more aware of the most obvious social engineering threats, so [we] can take preventative measures on these”.

Everything changes, everything stays the same

So those are the obvious differences between home and corporate information security, but what about the similarities? David Bennett, director EMEA consumer business development at Webroot, states the obvious when he says they are both about

the need to protect data and identity. So why not apply similar password management strategies at home as you do at work? Is it really that difficult to imagine getting your family to choose more secure passwords and change them on a defined basis?

“The solution is actually very close irrespective of business or home”, Bennett insists. “Both require a similar approach partly protected by applications such as standalone AV, defined password and access management, or security suites that drive out the natural human laziness with password management by creating alphanumeric encrypted passwords with simple association to sites where log on details are required”.

The very basics of keeping applications patched and security software up to date will be second nature to every infosec professional and best practice applied wherever they are, surely? Not according to Sean Sullivan, security advisor at F-Secure, who reckons that sadly best practice does not always get transferred to the home network.

“Best business security practices include items such as password lock screensavers”, he says by way of example, adding “most home users don’t lock their computers when they are ‘away’. Also, most people do not yet screen lock their smart phones, most of which can easily provide access to the same websites and email accounts that people attempt to protect at home”.

Doing your homework

Not only are there similarities in protecting home and business networks, but often the boundaries between the two become blurred. If you are bringing work home, should your employer secure the home network as well? Steve Furnell, IEEE member and professor of information systems security and head of the Network Research Group at the University of Plymouth, is convinced that it would help if businesses were able to take a holistic view and appreciate more that a security culture shouldn’t simply stop at the office door.



Are infosec professionals practising what they preach and eating their own dog food in their homes?



“Staff may be more receptive if they can see that they’re getting wider support to their personal benefit rather than just the employer’s”, he told *Infosecurity*, adding, “anything that businesses can do to affect their users’ security mindset will be likely to help them regardless of whether they are at home or at work”.

Indeed, his research at the University of Plymouth has indicated that security practices at home can be tangibly affected by whether the user has been exposed to related training at work. “Based upon a survey of 333 users, we found that if they’d been trained at work then 12% more of them were likely to shred confidential documents before disposing of them”, Furnell revealed, “and 17% more of them were likely to change the default password on their home router”.



Staff may be more receptive if they can see that they’re getting wider support, to their personal benefit rather than just the employer’s

Steve Furnell

So where does the real responsibility for security fall? Kevin Bocek, a director at IronKey, is also keen to point out that enterprise responsibility for data protection doesn’t depend on distance from the enterprise. “Work data must be protected wherever it goes and private data must be regulated under the UK Data Protection Act, by law”, he reminds us. “Information security professionals should assume the worse”, Bocek insists, “to ensure they provide systems that protect data wherever it goes”.



Sean Sullivan, F-Secure

CONFESSIONS OF AN INFOSEC PROFESSIONAL

Frank Kenney, Ipswitch File Transfer’s VP of global strategy, works from a home office and has a confession to make: as much as he tries to keep a logical separation of domains, there are times when he finds himself checking email or opening up spreadsheets on the wrong machine. “The problem is, I sometimes check corporate email with my personal machines and devices”, Kenney told us “allowing potential malware to have access to sensitive and proprietary corporate information”.

Because availability and usage of prosumer devices such as the iPhone and iPad continue to rise, and these devices are targetted at younger audiences yet require a greater amount of security and overall risk mitigation (make sure you put a passcode on your iPhone and install remote wiping applications), companies should offer simple reminders and incentives to home users to implement common-sense security mechanisms. For example, set up reminders to change emails and passcodes, as well as recommendations for offline backup and subscriptions to anti-viral tools.

“No one needs to become the CSO of their own house”, Kenney says, “but incorporating information security best practices into overall house security processes (alarm system, house keys, smoke detectors, anti-virus) will mitigate the majority of the risks to home users and thus their home away from home, corporate environments”.



Infosec professionals certainly know enough to restrict the user accounts of their kids from having administrator privileges

Rik Ferguson

Hawthorn of Blue Coat Systems suggests that “if an acceptable usage policy is flexible enough to allow for non work activities, it should cover home usage also”, and argues that while there is a degree of joint responsibility involved, ultimately it’s the organisation’s data and reputation that could be compromised otherwise.

Paranoia

At the end of the day, information security professionals tend to suffer from a high level of paranoia according to Professor John Walker, a member of the ISACA Security Advisory Group and CTO of Secure-Bastion. “When it comes to their home, and family use, they are the group who understand the risks and what they mean in real terms, so they do tend to practice what they preach both at work, and at home” Walker says. He concludes: “If they do not, they could just be in the wrong job!” ■