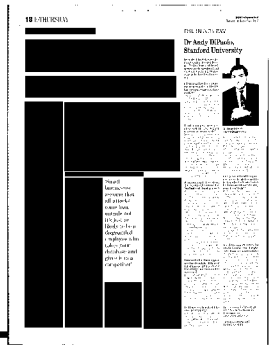
Publication: Irish Independent Business
Date: Thursday, November 11, 2004
Page: 18
Extract: 1 of 2
Circulation: 181.080
Author:
Headline: Small businesses present a big target



DATA & SECURITY PART II

Small businesses present a big target

In the second of his three-part series, JOHN COLLINS examines how small businesses tend to ignore the obvious risks presented by poor security rather than seeing the rewards of tighter controls

SPENDING money on IT security is similar to investing in an insurance policy — it's a monthly cost that you can't afford not to have but at the same time you hope you'll never have to draw down. Given that many small and medium-sized enterprises (SMEs) have limited IT resources, and in many cases don't have dedicated in-house staff, it's not surprising that security slips down the list of priorities and is often viewed as a cost rather than an investment.

Microsoft is currently engaged in a major campaign to make small business owners aware of the importance of security, both through its involvement with the Government and industry-sponsored Make IT Secure initiative (**www.makeitsecure.ie**) and through organising free security training sessions for businesses around the country.

"For small businesses, the challenge is making them aware that security is as big an issue as it is," says Mike Hughes, Microsoft Ireland's security and compete manager. "They wouldn't leave their office door open overnight with the PCs sitting on the desks. We have to make them aware that they need to take PC and internet security equally seriously."

"Resources are the key difference for smaller companies; large companies will inevitably have more resources," says Emmet O'Rafferty, group chairman of security firm Topsec. "Further down the chain, the ability of management to address and take ownership of security is more of a problem. Compared to other parts of the business they won't have a handle on what they are spending on security and why they are spending it. They don't have the measurement tools, and policies are either poor or not properly administered."

Without a clear understanding of the potential costs of a security breach, it is very difficult to know how much an organisation needs to be investing. Certainly the impact and increased frequency of major viruses and internet worms such as Blaster over the past 18 months has put security further up the agenda but, as O'Rafferty points out, people forget very quickly about these threats if they don't happen to hit their firm.

"Problems start with people so you have to have policies in place that cater for the needs of the organisation," he says. "You need to specify on what basis people have email and internet access — it's no different to having restricted access in a building. Enforcing policies creates the right culture and sets the tone. If you don't do that, why are you putting defences in place? There's no point just putting technology in place without policies."

In fact, for most SMEs the bulk of what is required in terms of security will cost them nothing but is actually a case of good housekeeping and taking the time to implement security in the products they already have.

"It's very easy for SMEs to see security as a big complex thing but there are some easy things to do to get them 90pc down the road and they cost next to nothing," says Hughes. As a bare minimum, businesses should have a firewall on all PCs; regularly update their antivirus software and install new patches for operating systems and applications as they are released by vendors — a task that the software can increasingly do on an automated basis.

Policies need to be in place to cover what activities are acceptable on the company network and at what times. Policies also need to cover the use of passwords; these need to be strong (eg to be at least eight characters long with a mix of numbers and letters) and should be changed on a monthly basis. "It's a pain for employees but the security it brings is worth it," says Hughes.

Physical security also needs to work in tandem with IT security to cover things such as a 'clean desk' policy (so written passwords aren't just left lying around) and to ensure servers are securely locked away.

Hughes also points out that small business owners that think the size of their business will protect it from attack are guilty of wishful thinking.

"If there's a major virus or worm released, small businesses will be swept along with it and can potentially lose access to their applications and data," says Hughes. "They also assume that all attacks come from outside but it's just as likely to be a disgruntled employee who takes your database and gives it to a competitor. And as larger businesses become more aware and tighten up their procedures, potentially hackers will target SMEs as they will be more attractive targets."

While security of the core network and office PCs is something SMEs need to tackle themselves, many are also turning to managed services to handle the management of email and other tasks that have important security implications.

Specialist security companies and internet service providers alike are finding that SMEs are happy to hand over their email servers if they can be guaranteed a service that is virus and spam free. Netsource has almost 700 customers for its Virtual Mail Server service, which provides server-side content and virus filtering.

"Our focus groups have shown that there is a lack of in-house understanding of what is needed," says Louise McKeown, sales and marketing manager with Netsource. "They are all reading about spam and viruses but they don't know what to do to tackle it themselves."

Publication: Irish Independent Business
Date: Thursday, November 11, 2004
Page: 18
Extract: 2 of 2
Circulation: 181.080
Author:
Headline: Small businesses present a big target

Next week: security issues facing big business

Mike Hughes, Microsoft Ireland's security and compete manager