treasurytoday
research | insight | analysis

Home | **Magazine** | **Handbooks** | **Benchmarking** | **Library** | **Community** | Search for…

Technology: best friend or Trojan horse?

Nov 2011   **Be the first to comment**

Related tags: risk management   technology   security

Print this page   Add to magazine

Send to a friend   Add to project

                        Ask an expert

Advances in technology and IT infrastructure are often seen as a treasurer's best friend. But beneath this rising tide of technology lies a darker undercurrent - the danger posed by hacking and other threats such as viruses and network outages.

According to a recent study conducted by the Ponemon Institute, the cost of cybercrime jumped 56% in the year leading up to July 2011. The median cost of cybercrime was $5.9m per year, according to the research, with a range of $1.5m to $36.5m each year per organisation. And no size of company is exempt from the crime – in fact large companies have become prize 'targets' for cyber attack.

Sony, for example, was hit by scandal earlier this year when it emerged that personal data of 77 million customers were stolen by an unknown hacker. Not only were customer names, dates of birth and email addresses exposed, but also the details of 10 million credit cards. The hacking scandal has left the multinational's reputation damaged and, alarmingly, revealed a company culture that treated information security as a secondary concern.

In April 2011 two large American banks were also forced to admit that customer lists were stolen from a third-party firm that they had both used for marketing campaigns, suggesting that IT security, even among the largest businesses, is not being taken seriously enough.

The weakest link

The past two years have seen a discernible shift in the nature of hacking attacks. Before, attempts to infiltrate a company's IT infrastructure centred on malware and automated tools developed to identify weak links in the system. Recently, however, there has been a steady rise in targeted attacks striking at specific areas of the business. Mobile technology nears the top of the list.

My dashboard

Indeed, according to a report released this week by M86 Security Labs, attacks on mobile devices are set to escalate dramatically in 2012. The report argues that mobile users are particularly vulnerable given that effective security solutions are still in their infancy. And with an increasing number of employees hooking up their personal devices to corporate networks, steps need to be taken to ensure the company's data is protected.

"I do think emerging technologies create new opportunities, but I also think companies need to take a security-minded focus to deploying new technologies," says Phil Pettinato, Chief Operating Officer of Reval, an enterprise treasury and risk management SaaS solution provider. "It is best practice to make sure that there are security reviews and related analysis done before you deploy a new technology."

Where does your organisation fit into all this? "Different companies are treating information security with different priorities," says Stephen Roger, Executive Director of the BKR International Asia Pacific Region, an independent business advisory firm which carried out a recent global survey on IT security in co-operation with MWR InfoSecurity, a British security consultancy business. "Our survey found that the majority of a company's information security approach is often related to their understanding of the threats."

"If a senior person in the company understands these threats, they are more than likely to drive information security in the organisation. Conversely, however, if there is a lack of understanding, there is then a lower priority and certainly a lower budget," Roger adds.

This is not to suggest, however, that businesses are unaware of the security threats they face. But there arguably exists an "overconfidence in the ability to deal with an incident and manage the repercussions of it," says Ian Shaw, Managing Director at MWR InfoSecurity.

"Today's environment is a lot riskier than it was before. There is so much valuable information stored on computers – credit card details, tax file numbers," notes Roger. "Treasurers control the money and oversee the funds of corporates; they should therefore be taking measures to ensure that security is in place to safeguard this information at all times." Client data protection, he says, should be at the top of the treasurer's priority list.

With the quantity of data to store only getting bigger – and their contents getting ever more sensitive – it is imperative that treasurers keep on top of information security trends; for, while technology might be a treasurer's best friend, it may also be a Trojan horse.

● ask a treasury expert

Forum discussions

Related articles

Peer recommendations

Reader Comments

You

Post Comment

Back to top

Recent content

Switching to eBAM

Mobile technology: friend or foe

BlackBerry leaves a bitter aftertaste

Jan-Martin Nufer, Transforming Treasury

Asian financial crisis

and much more...