



If this page does not print out automatically, select **Print** from the **File** menu.

---

## Experts warn of data security 'police state'

Arresting times ahead

Robert Jaques at NetEvents in Evian, vnunet.com 26 Feb 2007

Ill-conceived or poorly implemented IT security regimes could leave enterprises struggling to survive within the restrictive confines of an information "police state", experts have warned.

Andy Buss, a senior analyst at [Canalys](#), said at the recent NetEvent symposium in Evian that IT security should be an enabler, not a hindrance.

"What we are really not looking for is a police state where no-one can actually do anything," he told delegates.

"What we want is the ability to get the job done, flexible business processes and being able to work where and when you want, but in a way that guarantees the security and integrity of the people and the data using that network.

"Remember that companies are all different; from large to small they have different requirements, skills and needs, internally of their budget, their infrastructure, and crucially of the partners that deliver those solutions."

James Collinge, director of product management at security firm [TippingPoint](#), maintained that viable corporate security policies must address potential dangers posed by staff and the multiplicity of access devices connecting to corporate networks including PCs, laptops, PDAs and smartphones.

"From our point of view, we see not only the user, but the device as being the true threats. As you all know the network security perimeter is collapsing down around the critical assets of the enterprise network," he said.

"It is no longer at the firewall, it is no longer at the VPN concentrator. It has now collapsed down right in front of the data centre.

"So, although the user can be malicious, in most cases they are good users. They might take their laptops to Starbucks, which can infect their PCs. They did not do it maliciously, it just happened that way.

"Once they come back into a network our approach is to do very strong classification of information flows, the end-user and the device itself, and then perform some kind of enforcement on that."

This view was endorsed by Bruno Hareng, EMEA product manager at HP's ProCurve Networking division.

"It is not only the user that can be malicious. If you want to build a secure network you have to be sure that network devices, switches, routers and security devices are also trusted," he said.

"So the trick is to build a trusted access for the user, and a trusted network by itself at the perimeter and the infrastructure itself.

"That is also one of the challenges for IT administrators to start from the basis of making sure that their infrastructure is trusted and securely managed. "

Karl Driesen, EMEA vice president of sales at [Infoblox](#), argued that firms must concentrate on keeping a close eye on data to identify malicious activity, be it intentional or not.

"What people never did in the past was to make the connection between the problems and the users having initiated the problems. That is why it is not only the data but the source which needs to be checked," he said.

"It is not one or the other. New technology is giving much more insight into what the source is initiating, but it is definitely not replacing the in-depth analysis of the data.

"Lots of problems in IP environments are not intentional problems initiated by users. Many problematic events are being initiated without the users knowing it."

[Permalink to this story](#)

[www.vnunet.com/2184194](http://www.vnunet.com/2184194)

---

This article was printed from the **VNU Network**  
**VNU Business Publications**  
© 2006 All rights reserved

---

**Close** this window to return to the website

---

Vendor  
Video **Q&A**

**Q.** No clear document  
output strategy?

In .  
**X**