

## Industry News

- Security News
- Company News
- People Moves
- Jobs forum
- Knowledge base
- Request a quote
- Industry links
- Security events
- Directory **GET LISTED!**

## Product News

- Access Control
- CCTV
- Intruder Alarms
- IT Security
- Manned Guarding
- Perimeter Protection
- Physical Security
- Remote Monitoring
- Security Services
- Fire, Health & Safety
- Other Security Services

## Security links

### Advertise on Security Park

Reach Security Park's audience of 120,000 Security Professionals (well over the audience of printed Security magazines!), for a fraction of the cost of print advertising.

### RSS XML feed for this page

The latest Security news: CCTV, remote monitoring, access control, biometric, smart cards, IT and network security, intruder alarm, perimeter protection, manned guarding, physical security, fire, health and safety, available via an XML RSS feed.

[Secure](#)

### Free e-mail newsletter

Free subscription click [here](#)

Need a [reference book?](#)  
Find it on Amazon:

**NOW**  
on orders over **£19**  
[See details and conditions](#)

Posted in [Security News - IT Security](#) - on 13/10/2005

## Software developers should be held personally accountable for Security design flaws

Howard Schmidt - a former White House cyber security adviser, now CEO of R&H Security Consulting - led calls at the SecureLondon 2005 conference for software developers to be held personally accountable for the security of the code they write.

Schmidt insisted that better training for software developers would be critical to improving software quality. He feels that many developers lack the skills required to write secure code. He said: "In software development, we need to have personal quality assurances from developers that the code they write is secure."

Schmidt's comments follow the release of a Carnegie Mellon paper which studied the impact of security flaw announcements on software vendors' stock prices.

Schmidt referred to the example of a team of developers he recently met who had established a web application to talk to a back-end database using SSL: "They had strong authentication, strong passwords, an encrypted tunnel. The stored data was encrypted. But when that data was sent to the purchasing office, it was sent as a plain text file. This was not an end-to-end solution.

"We need individual accountability from developers for end-to-end solutions so we can go to them and say, 'Is this completely secure?'" He also pointed to the findings of a recent Microsoft survey which concluded that 64 per cent of software developers lacked confidence that they could write secure applications.

"Most university courses traditionally focused on usability, scalability and manageability - not security," he said. "Now a lot of universities are focusing on information assurance and security but, traditionally, web application development has been measured in mouse clicks - how to make users click through."

The British Computer Society (BCS) concurred that there should be accountability in software development but argued that software companies should be held responsible for the security of the code written by their employees, rather than by the employees themselves.

A security representative for the BCS said in an interview: "Howard has gone to an extreme by saying software developers should be held personally responsible for the security of the code they write but we broadly agree with the direction he's taking. I know a lot of developers who would be very uncomfortable with that level of accountability, especially if that were legal accountability. It is a company's responsibility to make sure the security features of its software are tested with rigor."

Yochi Slonim, CEO of Identify Software, a firm which provides application problem resolution technology, shed some light on the issue by emphasising the finer points of tackling software quality at the QA testing level. With firms under pressure to meet scheduled release dates, bugs can make their way into the final product, bringing operational faults as well as security vulnerabilities. This reinforces the BCS view that companies can do more to ensure software quality standards are consistently high. The focus should be on perfecting the QA process rather than apportioning blame.

Slonim maintains that a time or staff intensive approach to fixing and preventing software flaws is no longer necessary and that software vendors cannot afford to be held back by this misconception. "Application problem resolution technologies can both accelerate test cycles and improve quality levels by providing a log of user actions, synchronised with system information down to the code level," he explained. "Such technologies enable testers, software developers, and support staff to pinpoint the root cause of application flaws and iron out these bugs much more rapidly."

## Article search

## Directory search

Now you can [add your company](#)

