AUSTRALIAN IT

Click here to print this page

Security cannot rely on market

Karen Dearne
MARCH 09, 2004

INDUSTRY experts say market forces have failed to deliver adequate IT security and warn that cyberspace threats have already reached "a worst case" scenario.

Business and security leaders say governments cannot expect the private sector to secure the nation's critical information infrastructure nor defeat the problems of crime in cyberspace.

Declaring 2003 "the worst-ever year for worms, viruses and security breaches that cost of billions of dollars" — speaker after speaker told the 13th annual RSA Conference in San Francisco that privacy and security issues must be solved "right now" and demanded government assistance.

But US Homeland Security presidential adviser General John Gordon told the conference private industry would have to do more to help the US Government in the war on terrorism.

Terrorist groups have not launched an attack through cyberspace, "but the potential is there", he says.

In particular, industry would have to improve software quality.

"It cannot be beyond our ability to write code with a reduced set of vulnerabilities," General Gordon says.

The information security conference, which began as a cryptographers meeting, is now a mainstream business forum attracting more than 10,000 participants and a trade show with about 250 security vendors.

Microsoft's chief Trustworthy Computing strategist Scott Charney said in spite of more being done in security than before, "we have reached a point of market failure".

Former White House IT security adviser Richard Clarke has reached the same conclusion, saying all cyberspace indicators went off the charts last year.

"The dollar value of damage caused by worms and viruses tripled in 2003. If that wasn't market failure, somebody needs to tell us what market failure is," he says.

Clarke says there is no reason to believe 2004 is going to be any better, "so we had better reopen the dialogue between industry and government".

Business Software Alliance chief executive Robert Holleyman says the industry

group has been telling Washington "very loudly" the status quo is not adequate.

"We do not have the culture of security awareness that we need to have," he says.

"We're missing it by a long, long mile. But we cannot raise the overall level of security if the issue remains solely within the technical community. Governance is the hook the BSA is using to foster the debate in corporate boardrooms."

Meanwhile, many governments around the world have been attempting to solve privacy and security problems through regulation.

In the US, businesses are subject to a raft of new laws.

Clarke says he has long argued that attempts to regulate cyberspace are a "bad idea" because governments "would do it stupidly".

But that stance always came with a rider: if the markets failed to create strong security products or failed to cause people to adopt satisfactory processes, then the authorities would step in.

"Market failure was our escape hatch," he says.

"Maybe if things really weren't working, then in extremes the government would have to become involved. But things are already so bad that I would argue it's no longer a matter of whether the government should regulate or not, it's a question of whether we can write regulations that work. What can we do to improve things like HIPAA (Health Insurance Portability and Accountability Act) so we're getting some value back from the regulations that do exist?"

Charney, who was chief of the US Justice Department's computer crime and IP section for nine years before joining Microsoft, believes the Government cannot reasonably expect businesses to secure the IT networks that underpin commerce and society.

He says that in the 1990s markets were not demanding security and vendors weren't building it.

But at the same time, the US Government "essentially decided that market forces would have the largest role to play" in securing the US's critical information infrastructure.

"The rationale was that the private sector designed, deployed and maintained this infrastructure, therefore it had a responsibility to protect it," Charney says.

"As a result, even as the president's commission of critical infrastructure protection was issuing its report in 1996, we as a society delegated public safety and national security to market forces. But, in fact, markets are not designed to do public safety and national security. You can't make a case for privatising public safety.

"Imagine if you are robbed and a policeman comes to your house, you say 'there's the guy', and the cop says, 'For 50 bucks I'll chase him'. You say, 'No, you don't understand, he's got a knife too' and the cop says 'Then it's 100 bucks'. So we don't do it ... instead we fund public safety and national security through taxes, make everyone pay for it and just do it."

Charney says September 11 was not a cyber event per se, but it was a huge cyber-event for a lot of companies.

For many companies without disaster recovery plans and redundant systems, it was very much an IT event, and it cost them millions.

More importantly, "it became an issue of wow, there are risks and threats we have not anticipated, there is a dependence on IT infrastructure, and everyone started reassessing risks and threats".

Virulent worms Nimda and Code Red followed almost immediately, and suddenly cybersecurity had become "a burning issue" that sparked the "incredible activity" seen in the past couple of years.

Charney says that although he is not as anti-regulation as some in the industry, people must realise it actually takes time for markets to react to new circumstances.

"Part of the difficulty is that the products most people are using today were built in a time when the threat model was completely different," he says.

"If you look at the difference between Windows Server 2000 and WinServer 2003, for example, in relation to Blaster, on WS2000 the worm propagates across the internet, on WS2003 it doesn't propagate — it's still a problem, it affects the machine, but it doesn't spread. Why? Because the product is designed differently because of the new threats."

Charney says businesses are paying more attention to corporate governance and there is a fast-growing security market.

He says: "The question is now two-fold. What could the government do, if anything, to incentivise good security? And would regulation actually move the ball forward if the ball is already rolling. Secondly, we have to recognise that even if we all devote our time to this, it's still going to take time to fix the problem. It's hard to migrate off legacy systems; many custom applications and software packages don't support the newer stuff. So we're in a very tough period, and this will continue for a while."

Regulators will need to be careful not to go down a path that won't promote the best practices and will freeze technologies in today's state.

"If anything, we have to be adaptable to make products and services ever more secure as threat models change," he says.

Holleyman says the BSA is concerned at the lack of boardroom commitment to security within organisations.

BSA launched a CEO-led task force that found there was general agreement over the types of standards and practices that should be undertaken, but "the gap was the executive management team, the corporate boardrooms", he says.

To address the gap, BSA developed a Framework for Action, released in October, that now forms the basis of a security initiative for businesses in partnership with the Department of Homeland Security.

Holleyman says there has been a lot of work on security across the software development life cycle.

"But, is any of this going to be effective? Who is going to listen? We have to find the right forums to talk the issues; we need government as a partner, and we need to talk about this internationally.

"This is one of key points, because we can't simply deal with this challenge within US borders, security has to be a process that we undertake internationally." Holleyman believes the US has a unique opportunity for leadership in this area.

"We also have huge risks," he says.

"If we make mistakes; if we choose an overly regulatory hand rather than letting the private sector lead; if we fossilise technologies rather than encouraging companies to implement innovative solutions, then those mistakes will be repeated around the world.

"I like to think that we can get it right, that we can find a way to make governance a key issue.

"If we can get US senior business people talking with their peers around the world, in partnership with government, if we advance this mission with other governments, we really do have a chance to raise the bar, to recognise that the status quo is not acceptable, and that significant progress can be made."

Karen Dearne attended RSA Conference 2004 in San Francisco as a guest of RSA Security Australia.

Self-regulation fails, but regulator won't act

SECURITY consultant and former US cyberspace tsar Richard Clarke says private-sector governance can work, but some situations demand government action.

Example one

"ISPs in general do nothing about security, and if they did do some very basic things, well, there might not be spam.

"The Federal Communications Commission has the legal authority, granted by Congress, to regulate ISPs, but it has chosen not to use that power.

"Two years ago, they got the ISPs to come up with a voluntary set of guidelines, and at the time FCC chairman Mike Powell said: 'If you don't live up to these voluntary guidelines, I will regulate you'.

"Well, guess what, ISPs haven't lived up to the guidelines, and Powell hasn't regulated.

"The market is not forcing the ISPs to do anything about security. Turns out it's not a big market differentiator.

"Here's a case where perhaps we should involve the government and say: 'FCC, Congress has given you the power, take the voluntary guidelines and make them compulsory.'"

Example two

"Banking and finance are already regulated by the Gramm-Leach Bliley Act, but the

industry itself doesn't think that's enough.

"The industry thinks there should be strong regulation, so they're looking at creating their own security standards for software, for procurement, for self-regulation, and that's a good thing.

"I think we're seeing, in banking and finance, owners and operators of infrastructure now beginning to demand more secure products and they are going to set the standards they want providers to meet.

"If the industry can get together and hold together on this — tell the vendors to meet tougher standards for software development, live up to higher levels of quality control and provide higher levels of insurance in software for security purposes or they won't buy their next new products — that would be a form of regulation.

"That would probably be market forces, and that may happen."

This report appears on australianIT.com.au.