

Subscription Services

Affiliates



COMPUTERWORLD\*


NetworkWorld\*

CIO  
CANADA

itFocus

CIO Government  
CANADA Review

it  
Job  
universe.ca

Enter your  QUICKLINK number to go directly to that article.

[Advanced Search](#)

> Knowledge Centres

## Security

Security Products, Practices and Infrastructure

## Enterprise Infrastructure

- Data Centre
- Servers and Mainframes
- Storage and Storage Sub-Systems
- Operating Systems
- Systems Management
- Peripherals

## Communications Infrastructure

- Network and Management Planning
- Performance Management and Monitoring
- Network Devices

## Information Architecture

- Service Oriented Architectures
- Messaging and Collaboration
- Databases
- Data Warehousing
- Identity Management

## Integrating IT

# Cyber-crime strides in lockstep with security

By: Ernest DaSilva & IDGNS

IT World Canada (25 Jan 2006)

Information Security made great strides last year.

Sadly, so did cyber-crime.

In the U.S. - according to a recent FBI study - almost 90 per cent of firms experienced computer attacks last year despite the use of security software.

So what happened in 2005?

In a year when rootkits went mainstream and malware went criminal, information security improved.

There was no global pandemic like the Slammer or Blaster worm juggernaut. There was no malware with a replication magnitude of the order of Code Red, Slammer, Nimda, or the Iloveyou virus. With the notable exception of PHP worms, even the Linux side had fewer popular viruses and worms.

Advertisement

Patching got easier. Not only did more and

- Development Environments
- Tools and Languages
- Project Management
- Middleware / Utilities
- Outsourcing and Application Service Providers (ASP)

Departmental and End User Computing

- Personal Systems and Peripherals
- Personal and Portable Devices
- Personal and Office Productivity Applications
- Small-Area Networking (SAN)
- Help Desk and End-User Support

Enterprise Business Applications

- Enterprise Resource Planning (ERP)
- Business Intelligence and Data Mining
- Enterprise Portals
- Knowledge Management
- Knowledge Worker Tools
- Open Source and Linux

Extended Enterprise

more sophisticated patch management tools arrive from every sector, but there were fewer patches to deploy. Administrators

got better at blocking hackers and malware. And end users don't click on every file attachment they receive.

But security onslaughts attain greater significance as the year saw the metamorphosis of cyber malice into a highly organized and sophisticated international crime syndicate, where the likes of 'phishing' and 'spamming' have gone through drastic evolution.

Eighty-seven per cent of the more than 2,000 public and private enterprises that took part in the FBI survey said that they had undergone one or the other kind of security attack. Virus, spyware and adware top the list where a significant amount of businesses faced systems and data sabotage. One third of the companies detected port scans of their systems, a method used by attackers to identify vulnerable PCs to sneak in, the

- Supply Chain Management (SCM)
- Customer Relationship Management (CRM) and Customer Self-Service
- Online Retailing and Ecommerce

■ Security

- Security Products, Practices and Infrastructure
- Disaster Recovery / Business Continuity
- Hacking and Viruses
- Alerts, Patches and Fixes
- Privacy Issues

■ Voice Data and IP

- Carriers and Service Providers
- Protocols and Standards
- Hardware, Software and Emerging Applications
- Regulatory Issues

■ IT Workplace

survey said.

A staggering 98 per cent of survey respondents said they used antivirus software, of which nearly 84 per cent still suffered a virus attack.

According to U.S.-based security and communications software vendor MicroWorld Technologies Inc. in

Farmington Hills, Mich., many antivirus software products fail to prevent virus attacks because they work in a reactive way with known virus signatures, and hence cannot take on newer threats. Enterprises must reevaluate the kind of technology and effectiveness of many leading antivirus and security software they use.

The stuff that is getting by our defenses is more dangerous: Malware went criminal. Most of today's malware exists to steal confidential information, send spam, or steal identities. Now, malware is getting harder to remove, hiding better, and contains more tricks and exploits than ever.

IT managers and system administrators reported spyware and viruses were the most common problem, followed by port scans, sabotage of data or networks, and adult pornography. While not necessarily illegal, adult pornography is against the policy of most organizations, the study noted.

- o Human Resources Issues
- o Hiring and Retention
- o Careers and the Job Market
- o Salaries and Benefits
- o Education and Training
- o Consulting and Contracting

Leadership

- o Issues for CIOs
- o Budgeting / IT Alignment
- o Value Management and ROI
- o Human Capital Management
- o Best Practices
- o Industry News

E-Government

- o Case Studies and Best Practices From Canada and Internationally
- o Legal and Government Policy Issues
- o Management Issues
- o Privacy and Security

Wireless and Mobile Computing

More than 50 per cent of hacking attempts came from within the U.S. and from China, as many organizations were able to trace where intrusion attempts originated. But hackers are using computers that are under their control but located in other countries, combined with the use of proxies to make detection more difficult.

The FBI said a Romanian hacker could use a proxy computer in China to gain access to a compromised computer in the U.S., leading to a false conclusion that the attack originated in the U.S.

Antivirus software is widely used, and most organizations also have firewalls in place, the survey said. But 44 per cent reported that intrusions came from within their own organizations, and "this is a strong indicator that internal controls are extremely important and should not be underemphasized while concentrating efforts on deterring outside hackers," the FBI said.

Nearly two-thirds of those surveyed had implemented event logging on their network, a measure the FBI said is a crucial element in tracking crime. And half of those stored the logs on a remote protected server.

[Copyright Information](#) [Privacy Policy](#) [Site Map](#) [About Us](#) [Media Centre](#) [Reprint Services](#) [Mobile](#) [Feedback](#) [Contact Us](#)



[PC World Canada](#) [Bio-IT World](#) [CIO Titles](#) [CMO](#) [ComputerWorld Titles](#) [CSO](#)

[Darwin](#) [GamePro](#) [Infoworld](#) [Games.net](#) [ITJobUniverse](#) [JavaWorld](#) [MacCentral](#)

[MacWorld](#) [Network World Titles](#) [PCWorld](#) [Playlist](#) [IDG WorldWide Network](#)

©2005 ITworldcanada.com All rights reserved.