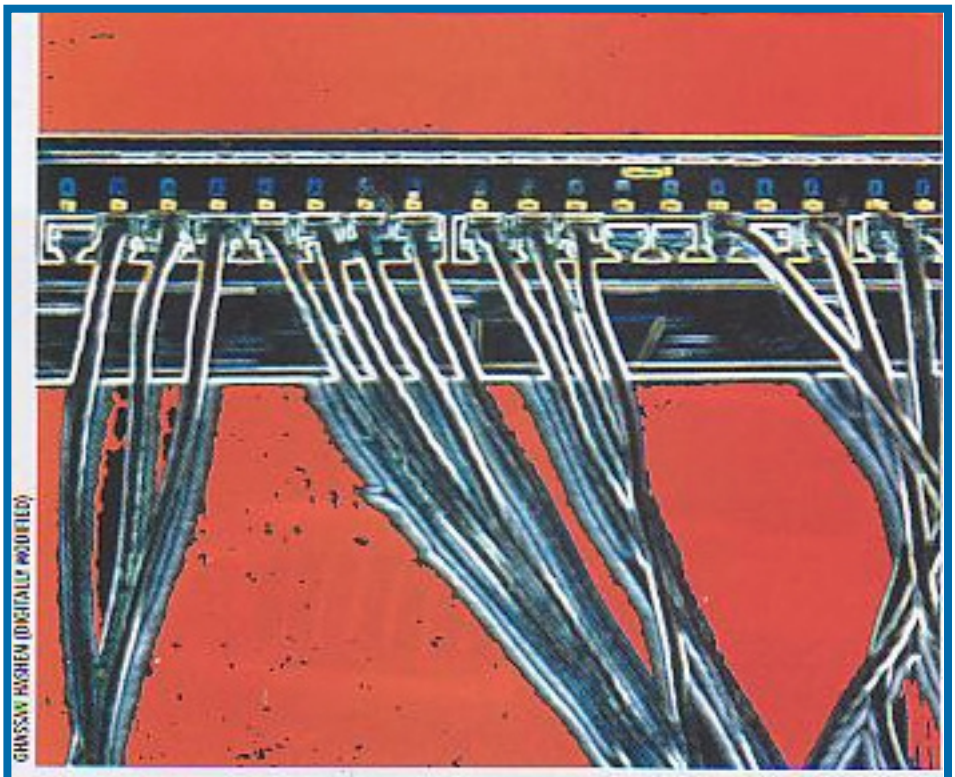
Name of Publication: Business Monthly (Egypt's leading monthly magazine)
Date of Publication: December 03 (exact week unknown yet)
Page(s) in Publication: 34, 35 (Feature)

(see next pages)



GHASSAN HASHEM (DIGITALLY MODIFIED)

CYBERCRIME

REGION'S IT SYSTEMS FACE GROWING THREATS

The cyber world is threatened by intruders and viruses just as the real world faces its own terrorists and health scares. As the hacker finds new ways to access computer systems illegally, countermeasures become necessary, and Cold War-style defense budgets must be equal to the task. With ever-increasing dependence on IT systems for life's necessities, failure has the potential for disaster.

Persistent threats from intruders continue to plague public and private sector computer systems alike. IT security specialists, meanwhile, fear that the lack of maturity of defensive software in the Middle East makes the region particularly prone to cyber-attack – and the huge recovery costs that result.

The ongoing risk of intrusion, corruption and data theft, therefore, continue to make security a top priority, according to IDC, a major global-market intelligence and advisory firm, which specializes in information technology. IDC expects worldwide spending on data security to reach more than $116 billion by 2007.

Such enormous spending is a reaction to a recent escalation both in the frequency of cyber-attacks and in their complexity and virulence. The overall rate of cyber-attacks on companies increased by 19 percent from the first half of 2002 to mid-2003, while the prevalence of blended threats, such as the recent Slammer Worm and Blaster Worm, increased by 20 percent in 2003 alone. These attacks affect all computer users – from the home user whose hard drive crashes wiping out the only extant copy of aunt Bertha's corn bread recipe, to the multinational bank that has its depositors' accounts shuffled and re-dealt.

Downtime spent recovering from attack, loss of corporate information and risk of liability involved in stolen confidential information all contribute to an enormous amount of potentially avoidable damage to the organizational bottom line. Particularly exposed are Internet enterprises (e-businesses), especially to the cost of downtime business loss. In governmental organizations, meanwhile, the stakes are even higher: the security and economic well-being of entire populations can be threatened.

At the last GITEX convention, the premier event in the Middle East showcasing IT innovations, held from October 19 to 23 in Dubai, a number of multinationals in the cyber-security field hinted at a desire to penetrate the region's markets more effectively. Security solutions provider Advanced German Technology (AGT), for example, has partnered with a number of European IT security-systems developers to bring new products into the Middle East, including virtual private networks and intrusion detection systems.

AGT managing director Mario Grossmann sees the worldwide IT security threat as both an opportunity and a challenge. "We, as a security supplier, have a responsibility to bring the best available weapons to the battle against

viruses, intrusion and manipulation," he said. "If we can raise the level of maturity in systems protection in this market, we will have contributed to the financial, economic and defensive well-being of its people."

Another potential key to the Middle East market is Arabic-language capability. While the operating systems of most multinational or large regional companies are in English, some firms are developing Arabic-based systems. Where security solutions are software-based, language capability becomes vital. ASTEC, a German firm looking to get into the Middle Eastern market in partnership with AGT, for example, has developed the first secure library-management system, winning the company a contract to safeguard the German defense ministry's library. ASTEC has also launched an Arabic-language project, along with the Egyptian Ministry of Irrigation & Water Resources, to create a secure library for the Aswan High Dam Museum.

In Egypt, the IT sector had a relatively slow start, and still lags behind the countries of the Gulf in electronic sophistication, especially in the banking sector. Until recently, the capability for ATM transactions was comparatively limited, and most banks didn't have database-to-branch interconnections. Electronic transfers moved at a relative snail's pace, while modern banking facilities – such as the direct deposit of wages and salaries – were virtually non-existent.

All this is currently being addressed. Egyptian bankers who have spent their careers overseas are being brought home to reorganize and modernize local systems. ATMs are going up at a feverish pace, and the establishment of inter-branch connectivity is well under way.

It would be comforting to know that investment in IT security is climbing in tandem.

ALEXANDER FUCHS