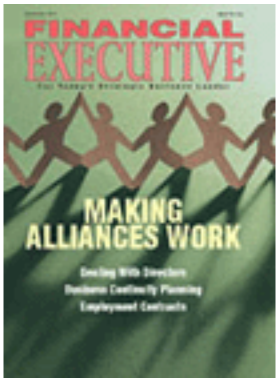
High Security, High Alert: 10 Future Trends



High Security, High Alert: 10 Future Trends

Financial Executive Magazine

December, 2001

Dr. James Canton – CEO and Chairman

Following the terrorist attacks, the Institute for Global Futures released its Top Ten Trends on the Future of High Tech Security Report. “These ten top trends are a recipe for how to prepare today for an extreme future where personal and economic threats will be common to our reality,” said the institute’s founder and CEO, Dr. James Canton. “New technologies may help protect us, but with a great cost to our privacy, while we deal with a new paradigm of risks never before imagined,” Canton added. “The key decision is, what are individuals, governments and organizations willing to do today to prevent future attacks. Without adopting an entirely new perspective on security, we will be vulnerable in the future.”

The Trends:

Economic Information Warfare (EIW) – Sophisticated attacks against entire economies, commerce and enterprises – will accelerate as a global threat.

Smart Watchers – A new generation of super-sensitive satellite and video-networked electronic surveillance – will be everywhere. Real-time personal face-scanning and suspicion-profiling tied to massive supercomputers, sensory-aware networks and data warehouses will determine risks, provide prevention strategies and intelligence on neutralizing threats.

National Identity Cards – Cards with embedded smart chips, containing an individual's entire genomic profile, will act as secure personal identifiers. They will wirelessly authenticate an individual's location, security clearance level and identity to a sea of intelligent networks tied to government, transportation, banking, telecom and enterprises.

Pandoras – The next generation of computer virus attacks will be self-mutating viruses created to destabilize, confuse and destroy critical electronic infrastructures essential to industry and government. These will be used by all sides as offensive and defensive weapons.

Sniffers – Designed to automatically sense, watch, search and identify individuals with critical information, weapons or bombs, these will be able to navigate physical, wireless and electronic spaces.

Secure-Wearables – Embedded, pinprick-sized, hyper-sensing bio-reactive nano-chips, personal PIN codes and GPS location monitoring will assist in security tracking and recovery after kidnappings or thefts.

DEPS (Digitally Engineered Personalities) – Personal sensors that live in the global telecom Internet network will provide 24/7, follow-you-anywhere security protection for individuals, enterprises and governments.

Biometric Authentication – Facial, eye, fingerprint and genomic scanning will be necessary to validate an individual's physical or virtual entry into electronic networks or physical areas. Security tattoos with bar-code scans will be popular and fashionable.

Biowar and Agri-Terrorism – Targeting the destruction of specific ecosystems, these will emerge as common threats to public health, soil, food and water resources.

Numerous personal privacy violations will occur, requiring new laws to protect and preserve individual freedoms.