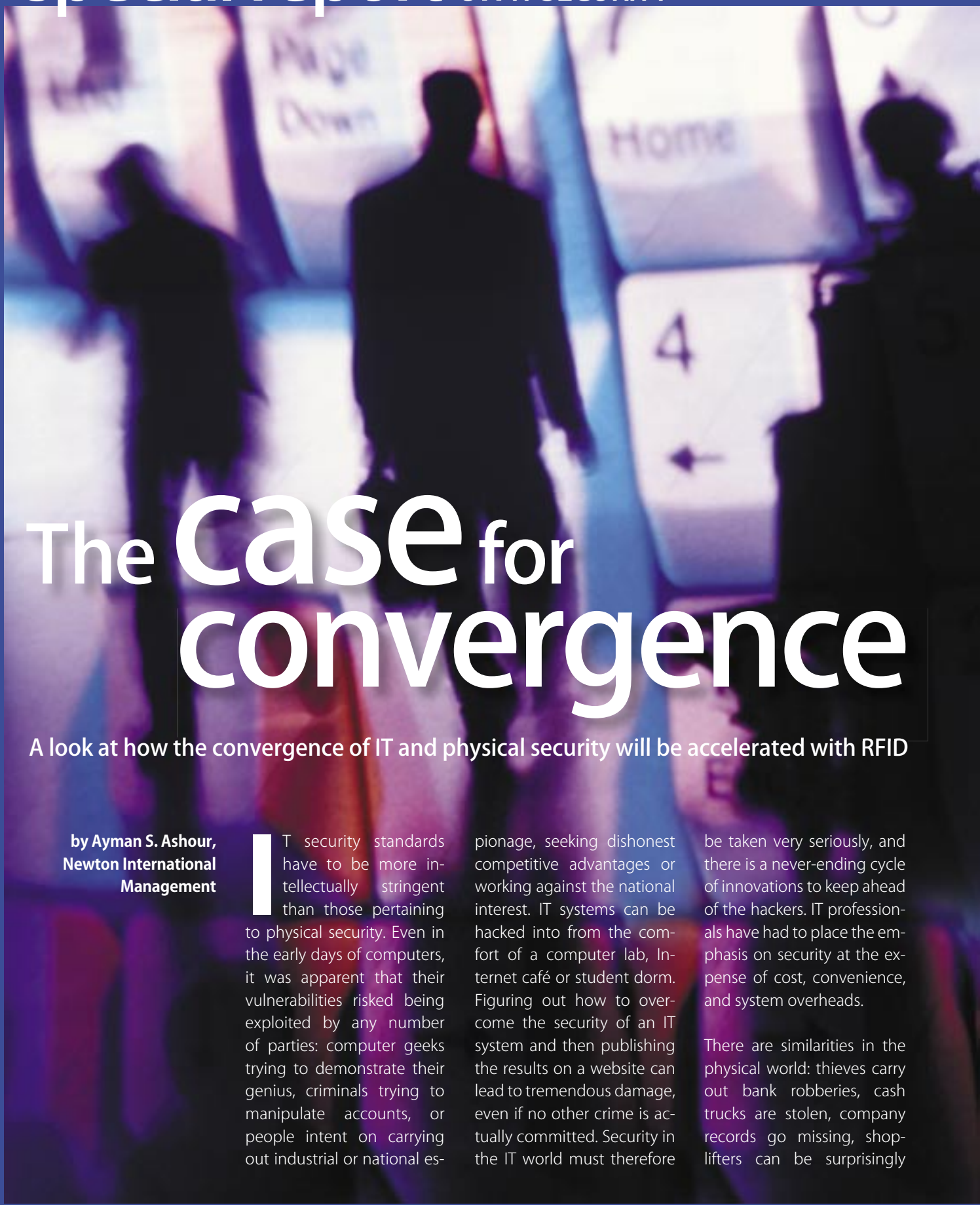

The case for convergence

A look at how the convergence of IT and physical security will be accelerated with RFID

by Ayman S. Ashour, Newton International Management

IT security standards have to be more intellectually stringent than those pertaining to physical security. Even in the early days of computers, it was apparent that their vulnerabilities risked being exploited by any number of parties: computer geeks trying to demonstrate their genius, criminals trying to manipulate accounts, or people intent on carrying out industrial or national espionage, seeking dishonest competitive advantages or working against the national interest. IT systems can be hacked into from the comfort of a computer lab, Internet café or student dorm. Figuring out how to overcome the security of an IT system and then publishing the results on a website can lead to tremendous damage, even if no other crime is actually committed. Security in the IT world must therefore be taken very seriously, and there is a never-ending cycle of innovations to keep ahead of the hackers. IT professionals have had to place the emphasis on security at the expense of cost, convenience, and system overheads.

There are similarities in the physical world: thieves carry out bank robberies, cash trucks are stolen, company records go missing, shoplifters can be surprisingly

creative, and inmates escape from prisons. Issues of physical security are, as such, just as old as the notions of possession, ownership or custody. Over the years, security professionals have developed methods to deal with physical vulnerabilities, yet in the world of physical security finding equilibrium has been a complex task. Physical security professionals have much greater experience than their IT counterparts in balancing security with privacy, convenience, and cost. As in the IT world, the challenges facing physical security professionals are being made ever more difficult, as news of vulnerabilities spreads via the media and Internet.

Courtesy of Gemplus

With users such the US Government taking a leading role, the technology for manufacturing dual interface contact/contactless controllers is likely to develop further

IT security: threats from everywhere

Whereas exploiting physical security vulnerabilities requires the physical presence of a perpetrator, IT security professionals have to contend with threats from virtually anywhere. To probe the security of a building the criminal has to be physically present – he has to try out various keys or look for an open window. An IT criminal can do the same while sitting comfortably sipping a cup of coffee in front of a computer screen. What are the implications of this for the world of identification? And what does all of this have to do with convergence? There is little doubt that identification is fundamental to security and the degree to which physical and IT security converges will depend on the degree to which common and reproducible identity can be used across the physical and virtual worlds.

Numerous IT systems, including many in vital industries, still recklessly rely on passwords for identification

In the last few years, hackers have used the Internet to illustrate how to decode and/or copy important RFID physical security products such as low frequency car immobilizers and access control proximity cards. In other words, the tools to make fake tokens that can be used to gain access to our cars and our offices are right there on the worldwide web for all would be criminals to see! Most security professionals view this to be of limited impact: car immobilizers will not deter a determined thief committed to stealing a specific car and many access control systems are used for access management rather than security. Access control systems for sensitive or more secure locations may employ extra security such as scramble pads, biometrics, or a combination of some or all of these.

Nevertheless, over the years, major access control users have generally accepted the lower levels of security offered by low frequency access control cards in return for convenience, reliability and relatively low cost. To

Unlke with physical security, the threats to IT security come from everywhere: criminals can hack IT systems from the comfort of an Internet café or their own home, for example

date, in many markets and for many users, the move from low frequency 125kHz to 13.56MHz technology seemed to occur not because of security but rather the increased functionality and multi-application capabilities made possible by smart card technology.

Passwords still dominate IT access

Huge investments have been made in the world of IT security yet identification continues to be a weak link. A relatively small percentage of IT systems employ smart cards with PKI for validation but numerous systems, including many in vital industries, recklessly continue to rely on passwords for identification. Leading market research firms have been projecting major growth in the use of smart cards for IT access for many years, but this growth continues to disappoint and trail expectations.

IT professionals need to issue new identification to users because although their current physical security IDs are convenient, they are not secure enough for IT. The current reality is that, for physical security, most access control cards utilize low frequency 125kHZ or 13.56MHz RFID memory cards and the relatively low numbers utilizing smart cards for IT security have standardized on contact micro-controller cards. The dilemma outlined earlier remains - physical security professionals balance convenience, cost and security whereas IT security professionals rely either on passwords or opt for a truly secure solution using PKI verification. For physical security professionals, the move back to contact technology is unthinkable; RFID has solved numerous problems from vandalism and maintenance of readers, to speed and convenience for users. Yet it is equally unthinkable for IT security professionals to offer a solution to the issue of secure ID replacing passwords without PKI verification, and therefore, a crypto-secure smart card. Until now, this has been the picture: the virtual world relying on passwords or having to issue new contact based smart cards!

Dual interface contact/ contactless cards

The last five years have underscored security risks and have resulted in increased awareness of the risks of cyber terrorism and identity theft. The US Government has launched massive programs aimed at ensuring its employee and contractor IDs are both secure and interoperable. In this, the US Government is actually leading by example and proving that it is possible to create, implement and manage a single ID program spanning physical and IT security applications spread over multiple geographical locations. It is hard to think of a more complex application for a single ID than within such a mammoth employer. It appears that the ID technology used, at least initially, by the various US Government programs will be based on contact technology with RFID interface.

With a user as large as the US Government, the technology for manufacturing dual interface contact/contactless controllers is likely to develop further, resulting in lower costs and increased reliability for the ID cards. Much more significant, perhaps, will be the wider use of contactless crypto controllers in ePassports, national IDs, and banking applications. It is expected that this will further drive down the price of RFID based crypto controllers, to the point that they become the norm, replacing low frequency and high frequency RFID cards for physical security. Then, and only then, will truly converged identity solutions be possible across physical and IT security.