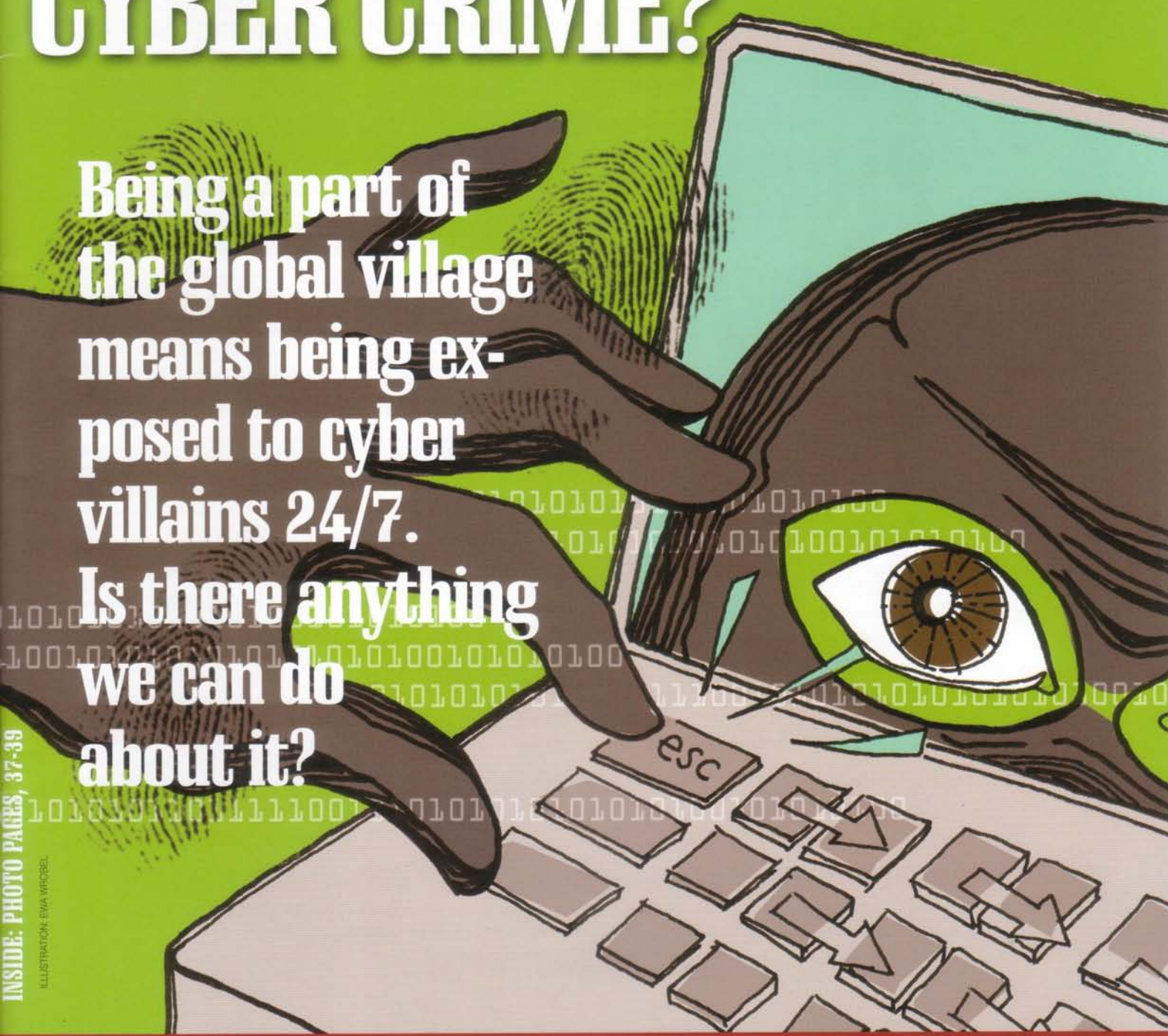
American
INVESTOR

JUNE 2009
Vol. XIX, No. 5 • ISSN 1506-3240

www.amcham.com.pl

CAN WE CRUSH CYBER CRIME?

Being a part of the global village means being exposed to cyber villains 24/7. Is there anything we can do about it?



INSIDE: PHOTO PAGES, 37-39

ILLUSTRATION: EWA WRÓBEL

U.S. Visa Waiver Program

Managing Multiplicity

ART EWA WRÓBEL

Digital mind games

As technological advancement in computer network systems continues to develop at a rapid pace, so does the potential threat of downing systems by a third party. Today, data security is the new battlefront for the defense industry and for your business too.

By Adam Kapitan Bergmann

The author is a Managing Director at PricewaterhouseCoopers responsible for Aerospace, Defense & Security in Central & Eastern Europe. He previously was In-Country Program Manager for the Lockheed Martin Poland F-16 Program and is a founding member of AmCham's Defense & Security Committee.

The pen is said to be mightier than the sword. In the current global economy, when so much of the world depends on IT infrastructure, the mouse has become mightier than the bomb. *American Investor* readers are all too aware of in-your-face online scams and nuisance e-mails promising cash rewards for helping recover money blocked in Third World countries. What may not be as obvious is the link between criminal use of the Internet and terrorism—and, indeed, the use of the Internet as a method of modern warfare.

In the past, an attack on a country invited reprisals either political or military, and the potential loss of life and treasure. As witnessed by the cyber war waged against Estonia, it is now possible for unknown attackers to cripple the infrastructure of a country without sending tanks across the border. Whereas oil, steel and access to uranium were once required to to becoming a military power, now the only limiting factor is access to the Internet and knowledge of computers. In previous conflicts, the targets were physical. Now the same effect can be achieved by overloading IT infrastructure and denying access to banking, government services and communications.

In a recent conference sponsored by AmCham dedicated to Internet security, two specific statements summed up the current state of the global economy and the new set of threats. One: the Internet is the only space where the good guys, the bad guys and the regulators all share the same limited infrastructure. Two: the Internet allows non-state actors to attack traditional superpowers without risk of immediate reprisal.

These concepts may seem distant from day-to-day business operations in Poland, but there are risks and threats in this area of which all should be aware. The aerospace and defense sector is often a bellwether of military and political realities. During the Cold War, preparedness was quantified by numbers of aircraft, ships and bombs. During the AmCham monthly meeting in May 2007, Lockheed Martin President & CEO Robert J. Stevens stated that his company was shifting focus towards becoming a global security company. U.S. Defense Secretary Robert Gates recently announced a major shift of defense spending priorities which will entail cuts to many traditional weapons programs in exchange for development of new technology to fight insurgencies and terrorism around the globe. We in Poland should take notice that the threats have changed.

Today, aerospace and defense companies are facing a host of critical challenges, forcing executive teams to focus intensely on the most important priorities: the relentless pursuit of innovation without compromising intellectual property, developing international markets and managing global supply chains without violating export controls and regulations, and providing access to crucial data without increasing vulnerability to targeted hacking or state-sponsored electronic espionage.

Common to every one of these challenges is the crucial need to protect sensitive information as it travels back and forth across decentralized internal networks, expanding supply chains and international borders, according to a worldwide security survey by PricewaterhouseCoopers, *CIO Magazine* and *CSO Magazine* of more than 7,000 CEOs, CFOs, CIOs, CSOs, vice presidents and directors of IT and information security from 119 countries.

By comparing your own company to the aerospace and defense industry, which is one of the most regulated and IT-savvy

sectors, you may be able to assess where your business lies in terms of threats and new risks to your sensitive data.

Safeguarding information, assets and initiatives requires knowledge, particularly knowing where deficiencies lie and having the ability to address them. Here's a brief overview of the critical areas that may deserve your attention, and a few insights on what these trends mean for your business.

Of the aerospace and defense respondents to the worldwide security survey, 90% say their company has a dedicated senior security executive, and 75% report that they have an overall information security strategy in place. Yet a surprisingly large number of the sector's IT and business managers "don't know what they don't know."

Protecting intellectual property, confidential information and other sensitive data

Opportunities to remediate gaps abound. At risk are vast quantities of important data, such as system designs, testing and assessment results, and strategic business plans. The A&D industry has reached well beyond the risks posed by laptop loss or theft, and made enormous strides in encrypting data in databases, file sharing, backup tapes, and removable media. But the shadow story here is that almost half the sector hasn't yet done so. At the same time, only 40% have an accurate inventory of where personal data for employees and customers are collected, transmitted and stored.

The human factor

As penalties for compliance violations rise, remediating gaps will require a closer focus on the weakest link: people. Failure to protect against electronic transfer of export-controlled information can result in heavy fines, criminal charges, imprisonment, denial of export privileges and customs seizure.

Sourcing, collaboration and strategic alliances

Trust is not a strategy. As A&D companies expand supply chains across international boundaries, partnering arrangements can involve multiple countries, companies and contractors. Few companies are fully aware of the risks they face if they do not require all overseas suppliers and partners to abide by the same stringent set of rules and regulations.

SECURITY HINTS:

Security gaps have the power to wreck your business. All too often we think we have adequate security measures in place, but unless the threat is constantly monitored it is easy to fall behind. Regular review is the only answer in order to ensure that your security strategy, approach and structure remain fit to deliver your business objectives.

1 Tighten spending alignment with objectives.

While 90% of aerospace and defense respondents believe their organization's security policies are aligned with objectives, only 76% say the same about security spending.

2 Get your business-continuity/disaster-recovery plan in place.

As the implications of expanding global supply chains continue to evolve, planning to weather a major disruption in operations is crucial to sustaining growth and market share.

3 Take a risk-based approach.

Don't "boil the ocean." Given the volume of data at risk across so many different systems and access points, place a higher priority on the most sensitive information and the systems at highest risk.

4 Maximize opportunities to integrate security with compliance and risk management.

Addressing critical security, privacy and compliance priorities on a "siloed" or fragmented basis costs more, and often yields much less effective results.

5 Kick your incident-response planning into higher gear.

When a security breach occurs, taking the right steps can prevent major impacts to your business and protect evidence critical to pursuing legal recourse or reducing compliance penalties.