Security Journal, **2007**, **20,** (9–11)
© 2007 Palgrave Macmillan Ltd 0955–1622/07 $30.00
www.palgrave-journals.com/sj

Security in the 21st Century

Peter Grabosky
Australian National University, Canberra, ACT 0200, Australia.
E-mail: Peter.Grabosky@anu.edu.au

Security Journal (2007) **20,** 9–11. doi:10.1057/palgrave.sj.8350036

Lessons

If there is one thing that the past two decades have taught us, it is that nothing ever stays still for long. Problems and solutions that were barely foreseeable in 1986 are commonplace today. One has no reason to doubt that dramatic changes will continue to take place between now and year 2026. Security solutions have never been enduring. The best minds in security have been, and will continue to be, challenged by the cleverest and most resourceful members of the criminal elite.

Trends

In Western industrial societies at least, two general trends were looming on the horizon in 1986 that have profoundly influenced security since then. The first is technology; the second is the changing role of the state.

The widespread development and application of digital technology, and its exponential takeup beginning in the mid-1980s, have changed the way we live. For the most part, this has been a profoundly enriching experience. Education, entertainment, commerce, health services, banking, communications and a host of other daily activities are more accessible than ever before. Opportunities abound in all of these domains, thanks to the facilitative capacities of technology. Ordinary citizens are empowered as never before. Unfortunately, so too are criminals.

The pervasiveness of digital technology now means that we have become very dependent on information systems, and this dependency lends itself to criminal exploitation.

The information systems of banks and other financial systems are attractive targets for electronic thieves and extortionists. Fraudulent solicitations can be sent by spammers to millions of recipients instantly and at negligible cost. Digital technology lends itself perfectly to the production and dissemination of child pornography. Viruses and worms can quickly degrade information systems around the world. As a result, information security has become a growth industry of the 21st century.

The second major trend that emerged during the 1980s was a significant transformation in the role of the state. The Thatcher and Reagan revolutions brought about profound change in governance. Most significant among these was the withdrawal of the state from many activities that were previously regarded as central state functions. In many countries, publicly owned assets and infrastructure, from telephone systems to government buildings to national railways, shipping companies and airlines, were sold off. The management of prisons was contracted out to private companies. Citizens were called upon to be more self-reliant and resourceful, and to bear more responsibility for their health insurance, their retirement income, and their education. The term "user-pays" became common in many places.

This devolution of responsibility has also extended to the realm of security. Citizens with assets to protect are now strongly urged to protect them with their own resources. The rise of the private security industry had become apparent by the mid-1980s, but few would have predicted the extent of its continued growth. Governments themselves turned to the private sector for security services that had previously been provided by state police. Today, the first person one encounters when entering the headquarters of the Australian Federal Police in Canberra is not a police officer, but rather a private security guard.

Another trend, not unrelated to the two noted above, is what is commonly termed globalization. By this, we mean the increasing movement across borders of people, money, ideas and information, good and services, and viruses – both microbial and digital.

In some respects, the globalization of commerce reinforces the devolution of responsibility for asset protection. When a company is engaged in petroleum exploration in a contested area of Colombia, for example, it cannot rely on the resources of the Colombian state to protect its assets. Trade secrets are valuable, and economic intelligence may be worth more to a government than political intelligence. A company doing business in a foreign country may find that law enforcement agents of the host nation, far from being the greatest source of protection, may actually pose the greatest risk.

A final related trend is the growing tension between security and personal freedom. Technology has not only provided unimagined opportunities for law abiding citizens and criminals, it has also provided the state with surveillance capability of which George Orwell would have been proud. In the United Kingdom, closed circuit television cameras are ubiquitous. The post-9/11 environment has seen unprecedented state surveillance of financial transactions and telecommunications.

Moreover, private institutions have also invested in surveillance technology. In some instances, private information is a simple by-product of commercial activity. I am not troubled when Amazon.com suggests a book in which I might be interested, based on my previous purchases through their facilities. I would be troubled, however, if my or anyone else's government, or anyone else, had access to my reading lists or to the websites that I visit.

The future

One has no reason to doubt that technology will continue to advance, and that the increase in capacity will be accompanied by a decrease in cost. And the likelihood that the security industry will shrink is very low indeed. Under these conditions, what do we need to know about security?

We live in an age when money does not grow on trees (as if it ever did). So the consumers of security services will need to determine which of the security solutions available to them are effective and efficient. Continuous analysis and evaluation of specific technologies, and security services more generally, will become a fact of life. Whether the efficiency and effectiveness of security products and services will be assessed by market forces, or by the regulatory activities of governments, is a matter that will depend to a significant extent on the role of the state. The role of research in determining what works, and at what price, should become more prominent.

Of no less importance, are the consequences of security for our personal freedoms. Personal privacy will remain under great pressure, whether at the hands of the state, or of private enterprise. Governments in particular, given their capacity for surveillance, should be attentive to potential infringements of human rights. Since so much public life today takes place on private property, private enterprise, for its part, may face pressures to avoid gratuitously invading the privacy of clients, customers or members of the general public. In both cases, the vigilance of individuals and of public interest organizations will be instrumental.

And finally, researchers should be mindful of the unintended consequences of security initiatives. Those who conceive or implement security solutions may do so without considering the possibility of collateral damage. Comprehensive analysis of downside risk is important; so too is post-mortem analysis in the event of failure. Engineers dwell on bridge failures and airplane crashes not because they want to do away with bridges or air travel, but because they want to make both safer. Researchers on security would do well to adopt a wider perspective on risk with a view towards optimizing security and human freedom.