15. Survival planning for business: a view from Nokia

Urho Ilmonen

I. Current threat assessment

Nokia produces telecommunications equipment, which is a non-military, neutral and universally beneficial technology.[1] Good communications are important for democracies and dictators alike. Accordingly, the company believes that it neither poses a threat to anyone nor is a specific target for anyone except ordinary criminals. On current company analysis, non-state assailants should not have any interest in harming the company.

Nokia believes that security can be created by sound business practices and careful processes. The company's threat scenarios include as the worst root causes of threats: (*a*) employees who are careless and over-trusting; (*b*) subcontractors who also work with the company's competitors and implement lax security measures; (*c*) poor information security that compromises data; (*d*) industrial espionage by competitors, either alone or with the assistance of state investigation agencies; (*e*) 'social engineering' specifically as a means of industrial espionage;[2] and (*f*) specific environments in the so-called emerging markets which pose new threats to personnel security, such as kidnappings and ransom activities, and can give rise to large-scale armed robbery of valuable cargoes.

II. What has changed after 11 September 2001?

The attacks of 11 September 2001 were a tragic act committed against innocent people by a new player in the international league of aggression. The action came as a shock, especially because of the surprise and generally perceived injustice, and because it happened in a country that had not experienced domestic warfare for a very long time. Such an attack would not have come as such a shock for people in Grenada, Israel, Kosovo, Lebanon or similar places, or indeed in Europe, which was ravaged by war and massive bombings not such a long time ago. For the risk assessments of non-US companies, not much changed as an immediate result of the attacks. Co-location with offices of large US companies was considered a risk, and defence and other industries that were considered high-risk targets became more alert. However, politically

[1] See the Nokia Internet site at URL <http://www.nokia.com>.

[2] On the social engineering methods of compromising computer security see, e.g., the Computer Emergency Response Team (CERT) Internet site at URL <http://www.cert.org/incident_notes/IN-2002-03.html>.

a great deal changed in the world, including the role of the United Nations, and this will change our lives dramatically for a long time to come.

III. Why is security needed and what is the focus?

Security is a basic need of all people. According to the Maslow hierarchy of basic human needs, security is ranked just below air, food and water.[3] Business entities also need security to be able to carry out their activities with as little interference from criminals, terrorists or the authorities as is possible and feasible. Important changes in this equation have occurred after September 2001, and some of them are more welcome than others.

The main focus of corporate security activities remains on the threat scenarios mentioned above. Awareness training should tackle the problem of careless employees and fend off most of the risk of social engineering. Sound, well-enforced processes should be able to meet most of the information security challenges. Efficient, well-applied emergency response plans and business continuity plans can help in preparing for and minimizing the effects of crises. Nokia sees this as its primary task. On the other hand, federal security requirements tend to steer the focus of corporate security towards sometimes costly actions which have only a limited effect on general domestic security and sometimes dramatic effects on business. This is not necessarily the focus the private sector would like to have.

IV. Vulnerabilities and attacks increase

The world has become increasingly dangerous, not least with regard to the security of information systems. Research conducted by the Computer Emergency Response Team Coordination Center (CERT/CC) of Carnegie Mellon University shows that incidents breaching information security systems have increased exponentially, from under 10 000 in 1999 to 76 404 in 2003 (and still rising), while known system vulnerabilities increased over the same period from under 500 to 1993 (albeit currently on a declining trend).[4]

The complexity of systems and the vast deployment of global data networks have put both the public and private sectors in a new situation. So far we have not seen proof of deliberate, coordinated terrorist-initiated attacks on data systems. Should terrorists exploit these abundant vulnerabilities—and it seems likely that they may soon—our society will find itself in a new, challenging situation.

[3] On the theory of Abraham Maslow's hierarchy of basic human needs see, e.g., URL <http://web.utk.edu/~gwynne/maslow.HTM>.

[4] CERT is a worldwide network of national and regional teams for the collection and dissemination of computer security threats, vulnerabilities, incidents and incident response. CERT/CC is operated by the Software Engineering Institute of Carnegie Mellon University, Pittsburgh, Pennsylvania. On CERT/CC see URL <http://www.cert.org/>. See also chapter 2 in this volume.

V. Emergency response and business planning

Crises occur because of disasters of a natural, political and terrorist nature, and society must be prepared for them. The private sector has to shoulder its responsibility vis-à-vis its employees, their families, its stakeholders and its customers. This requires contingency planning—preparing for the unforeseeable. However, preparations can only be taken up to a level deemed reasonable in the light of the current threat assessment.

During the war in Iraq in 2003, Nokia had Emergency Response Plans (ERPs) drafted and tested in all the countries affected. A special support team with intimate knowledge of all the sites, all the people and all the plans was made available to follow the situation closely, 24 hours a day and 7 days a week. Deployment of the ERPs was decentralized. Each country manager had an independent right to pull out his or her people, and had the financial means and arrangements for this at his disposal at all times. Business Continuity Plans (BCPs) remain in place and are continuously updated.

VI. Partnership with the authorities?

There is truth in the saying that the road to hell is paved with good intentions. This should be kept in mind when contemplating responses to the post-11 September 2001 security situation, if actions are to be avoided that could in any way support the disruptive goals of terrorists.

Pressing requests are being made to business to participate in the fight against terrorism. As an example, the US Customs–Trade Partnership Against Terrorism (C-TPAT)[5] is being promoted as a voluntary programme to improve logistics security. From the point of view of the private sector, it is not voluntary, it is costly, and it leaves the private sector's own security situation unchanged. Corporations thus perceive no advantage with this system, not least because it is being pursued without extra funding and with only negative incentives for participation. Is this the way for the public sector to motivate the private sector? Is this the way to promote true partnership? What started as an initiative to improve logistics security in the delivery channels for imports to the United States has amounted to something bordering on an illegal obstacle to the free movement of goods.

Business operates by business principles. Shareholder value and profit are important, as are continuity and corporate social responsibility. Is not business entitled to a reasonably safe operating environment in exchange for the taxes it pays? Companies tend to become concerned if they are faced with strict measures and demands for partnership that do not make indisputable sense from the standpoint of sound cost–profit analysis.

[5] On the C-TPAT see URL <http://www.customs.ustreas.gov/xp/cgov/import/commercial_enforcement/ctpat/>, and chapter 19 in this volume.

VII. Conclusions

This brings the discussion back to the opening remarks. First, it should be acknowledged that governments are generally acting in the best and noblest interests. The parts of the private sector which are engaged directly in their efforts, as security contractors, are obviously acting in their own best business interests and as such need to be controlled by their principals. How good a job the regimes involved make of this has an immense effect on the public perception of the efficiency of the partnership. Everyone travelling to and within the United States by air has been experiencing the immense effort to maintain air travel security. How efficient this really is, and at what cost in terms of both finance and civil liberties, remains to be seen once the system starts to work in the way it was intended. What remains puzzling is why the USA cannot learn from the experience in Europe, where full luggage screening is carried out reasonably cheaply and efficiently, and without infringing on civil liberties.

The solution proposed here is a partnership based on equality. What is needed are truly efficient public-sector measures that do not unduly infringe on civil liberties or on the freedom of business. The public–private sector partnership must be based on give and take, equality, trust and mutual respect. This is surely feasible: it already works in many countries with very good effect. More work is needed, and everyone needs to participate. The private sector cannot lean back and say ‘you do it, we will pay taxes’, and the public sector cannot lean forward and say ‘you have to do it, we have determined that this is in your own best interest’. A real discussion, real controls, real incentives and, above all, *reasonableness* is what is needed.