Security and privacy

Ewan Sutherland

Executive Director

ewan@intug.net

INTUG contents

- promoting a culture of security
- storing traffic data
- authorising wire “taps”
- rights/obligations of employers
- protecting data on customers, staff, etc
- reporting cybercrimes
- complying with human rights
- paying for the above

INTUG scaring people

- netwars and information warfare
- cyberterrorism
- viruses, worms, trojan horses, etc
- ICC survey on unsecured WLANs

Computer Security Institute & FBI

- ninety percent of respondents detected computer security breaches within the last twelve months
- eighty percent acknowledged financial losses due to computer breaches
- forty-four percent were willing and/or able to quantify their financial losses, some US$455,848,000
- the most serious financial losses occurred through theft of proprietary information (26 respondents reported $170,827,000) and financial fraud (25 respondents reported $115,753,000).
- for the fifth year in a row, more respondents (74%) cited their Internet connection as a frequent point of attack than cited their internal systems as a frequent point of attack (33%).
- thirty-four percent reported the intrusions to law enforcement. (In 1996, only 16% acknowledged reporting intrusions to law enforcement.)

INTUG global legal instruments

- UN General Assembly resolutions
  - 55/63: Combating the criminal misuse of information technologies
  - 57/239: Creation of a global culture of cybersecurity
- Council of Europe (and others)
  - Cybercrime Convention
- OECD
  - Network security guidelines

INTUG cybercrime convention

- illegal access and interception
- interference to data and systems
- misuse of devices
- computer-related forgery and fraud
- offences related to child pornography
- aiding and abetting
- corporate liability
- expedited preservation and disclosure of stored computer data
- search, seizure and real-time collection of data
- interception of content

INTUG OECD Guidelines

- renewed in 2002
- adopted in December by General Assembly of United Nations
- continuing work on adoption
- endorsed by INTUG Council at Zurich

INTUG culture of security

- promote a culture of security among all participants as a means of protecting information systems and networks.
- raise awareness about the risk to information systems and networks; the policies, practices, measures and procedures available to address those risks; and the need for their adoption and implementation.
- foster greater confidence among all participants in information systems and networks and the way in which they are provided and used.

INTUG culture of security (2)

- create a general frame of reference that will help participants understand security issues and respect ethical values in the development and implementation of coherent policies, practices, measures and procedures for the security of information systems and networks.
- promote co-operation and information sharing, as appropriate, among all participants in the development and implementation of security policies, practices, measures and procedures.
- promote the consideration of security as an important objective among all participants involved in the development or implementation of standards.

INTUG reporting

- security measures rely on a realistic assessment of risks
- yet many (most?) events go unreported:
  - suppliers
  - users
- should we report more?
- would we get better assessment?

INTUG reactive policy making

- the long history of assassination and terrorism:
  - – Irish Republican Army
  - – Red Army Faction
  - – UNA bomber
- forensic capabilities of governments
  - – do they really need it?
  - – can they use the data?

INTUG over-reaction

- serious accusations of over-reaction at the expense of human rights and privacy
- Amnesty International
- UNHCR
- Electronic Privacy Information Center (EPIC)

INTUG human rights

- international provisions:
  - United Nations
  - Council of Europe
- national:
  - constitutions
  - specific legislation

INTUG data protection

- Data Protection Directive (95/46/EC)
- Communications Data Protection Directive (2002/??/EC)
- forthcoming “third pillar” legislation on data retention

INTUG European Union

- Data Protection Directive
- Communications Data Protection Directive
- Cybersecurity Task Force

INTUG USA

- A national strategy to secure cyberspace
- part of "homeland security“
- cyber incidents are increasing in number, sophistication, severity and cost.
- economy increasingly dependent on cyberspace
- a digital disaster strikes some enterprise every day
- fixing vulnerabilities before threats emerge will reduce risk.
- it is a mistake to think that past levels of cyber damage are accurate indicators of the future. Much worse can happen.
- common defence depends on a public-private partnership.
- everyone must act to secure their parts of cyberspace

INTUG policy work

- data retention
- implementation of Cybercrime Convention
- transposition of communications data protection directive
- review of EU data protection directive
- balance costs against improved security

INTUG conclusions

- problems cannot be solved nationally
- governments reacting, but not yet achieving a “culture of security”
- accusations of overly intrusive measures
- governments seem to ignore costs or pass them onto operators and thus to users
- how long need data be held?
- how do you ensure its security?

INTUG thank you

Ewan Sutherland

INTUG

Boulevard Reyers 80

B-1030 Brussels

+32.2.706.8255

http://www.intug.net/talks.html