Government of Canada | Gouvernement du Canada

National Cyber Protection

Securing the Network Economy

Send an e-mail. Use a bank machine. Fill a prescription. Buy groceries. Make a phone call.

Whether on the surface or behind the scenes, just about everything we do involves telecommunications networks. These networks bring voice, data, and video services to our homes and offices.

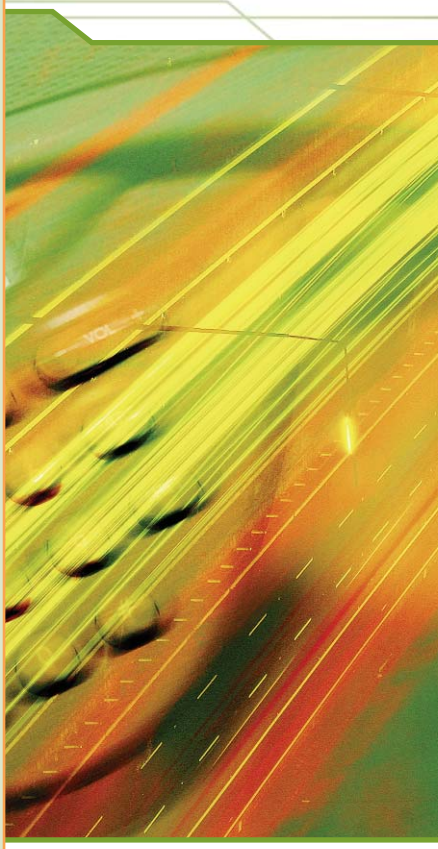
The "Network Economy" brings unprecedented efficiency and productivity to millions of Canadians…as long as the technology works. If networks go down, things we take for granted are not always available to us – phones, cash, computers, medication, even food.

Network environment

- Canadian networks are primarily owned and operated by private industry;
- Networks are interconnected both domestically and internationally;
- Canadian government, businesses and citizens have a strong and common need for secure and available networks;
- Network owners, operators, customers and suppliers all have an interest in the security of the networks and can impact its performance;
- Critical infrastructures are interdependent. For example, when electricity or telecommunications falter, everything from retail sales to banking, to medical services can be adversely affected.

Cyber threats and vulnerabilities

- Damage to equipment, applications and operating systems from viruses and worms;
- Terrorism, intelligence gathering and criminal activity on networks and information management systems;
- Insufficient audit and control measures;
- Internal corporate security breaches;
- Technology and equipment malfunction;
- Human error.



Protecting Cyber

Canada

Partnerships

- Protecting Canada's telecommunications networks is a job too big and too important for any one company or government;
- A partnership approach to cyber security provides the momentum, speed and flexibility required to address emergencies and the challenges presented by emerging technologies;
- Industry Canada, as the lead government department for telecommunications, has established the Canadian Telecommunications Cyber Protection Working Group (CTCP) to promote industry-to-industry, government-to-industry and industry-to-government co-operation in protecting Canadian networks;
- Industry Canada and the CTCP Working Group have established the Canadian Network for Security Information Exchange (CNSIE) to promote collaboration between a larger community of cyber security stakeholders such as the telecommunications, financial, energy, and vendor communities and other government departments;
- Collaboration has been established with domestic and international partners such as the Canadian Cyber Incident Response Centre (CCIRC), as well as the U.S. and U.K. Network Security Information Exchanges.

Partnership benefits

- Timely information from industry and governments on attacks, vulnerabilities, research and development, and government intelligence;
- Technical and operational network security best practices, e.g., Intrusion Protection Systems (IPS), firewalls, incident handling;
- A comprehensive incident handling approach that addresses prevention, detection, containment, education, and recovery;
- Exercises to test and improve response to an incident;
- Domestic and international partnerships with computer incident response teams, emergency responders, and critical industries, e.g., energy.
- Emergency contacts in government and industry.

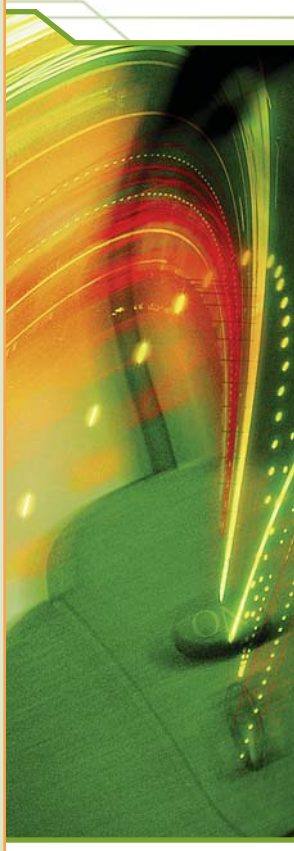
We rely heavily on telecommunications networks. In normal situations, they make our lives easier, providing quick and reliable access to people, services and information. In emergency situations, access to these networks and the services they provide can save lives.

Securing these networks is of paramount importance to Canadians and the Canadian economy. In today's society, security doesn't just mean securing the buildings and equipment. It includes securing networks from cyber threats and vulnerabilities.

For more information, visit our website at:

http://spectrum.ic.gc.ca/urgent

or call us toll-free at 1-866-266-9031.



Cat. No. Iu64-28/2005E
ISBN 0-662-41203-6
IC 54439