



Special Threat Briefing

David McMahon

National Security Advisor, Bell Canada.

05 November 2009

Think outside of the box

20%

80/20 THEORY OF SECURITY ARCHITECTURE

Traditional Enterprise Security Architecture, policies and standards are **only 20** per cent effective at preventing cyber attacks from penetrating an organization today.

The remaining **80** per cent, require innovative Security Architecture design, most of which can **only** be accomplished with carrier grade services.

Citizen

1 incident per year

Traditional Risk Management

- No Threat Picture
- Basic Policies, Standards, Laws
- Protective Safeguards
- Emergency Planning

Business

10 incident per year

Active Risk Management

- Limited threat picture
- Policies, Standards, Laws
- Active Technical controls
- Defensive Safeguards
- Incident management

Carriers

10⁹ incident per year

Proactive Risk Management

- Decisively engaged with the threat
- Policies, Standards, Laws ineffective
- Deep Prediction and interdiction
- Highly dynamic tradecraft

Data set represents 70 percent of everything

160 Gbps ...30 percent growth/year

2.3 Petabytes per day with TV

45 Billion e-mails/month

50 million IP addresses

27 million connections

46 percent of consumer space

80 percent of enterprise

90 percent Government and CI

Evil

80000 zero-day/day

54 Gbps malicious traffic

1 Billion value of recovered bandwidth

1.5 Million compromise PCs

21 million botnet connections per month

4.8 Gbps botnet traffic put to ground

44 billion bad e-mails/month

1 Trillion Incidents/year

In perspective...

50 petabytes the entire works of humankind, from the beginning of recorded history, in all languages

200 petabytes of malicious traffic was stopped in the cloud in Canada/year

1 exabyte all phone calls, and e-mail of Canadians for a year

5 exabytes is all words ever spoken by human beings

12 exabytes is the sum of human-produced information

Crime and consequences

5 billion was spent on IT security last year

100 billion estimated cyber crime losses
in Canada last year

1 crime in Canada

477 technology specific offences in 2001



Teenagers

Hackers

Threat agents

Organized Crime

Terrorism

Espionage



Arms race

20000 machine Botnet can DDOS
the government and safety sectors

\$3000 dollars cost to rent

50,000 machine Botnet

- 9 GBPS uplink flood
- 22.5 GBPS downlink flood

Robot Networks

Threat data

Decisively Engaged
Cyberwar

Estonia NATO example

Perimeter defences

Theoretical limitations

Laying siege to network fortresses

and why Internet is not good enough for your corporate backbone...
Secure network architectures require trusted routing and
PROACTIVE defence in depth.

You can not manage
what you can not measure

Proactive cyber defence

Carrier security

An ounce of prevention is worth a pound of cure

Deep perception
Core intelligence

“Buying your enterprise time and precision.”

*“**Proactive Cyber Defence** means acting in anticipation to oppose an attack against computers and networks. It represents the dynamic between purely offensive and defensive action; interdicting and disrupting an attack or a threat’s preparation to attack, either pre-emptively or in self-defence.”*