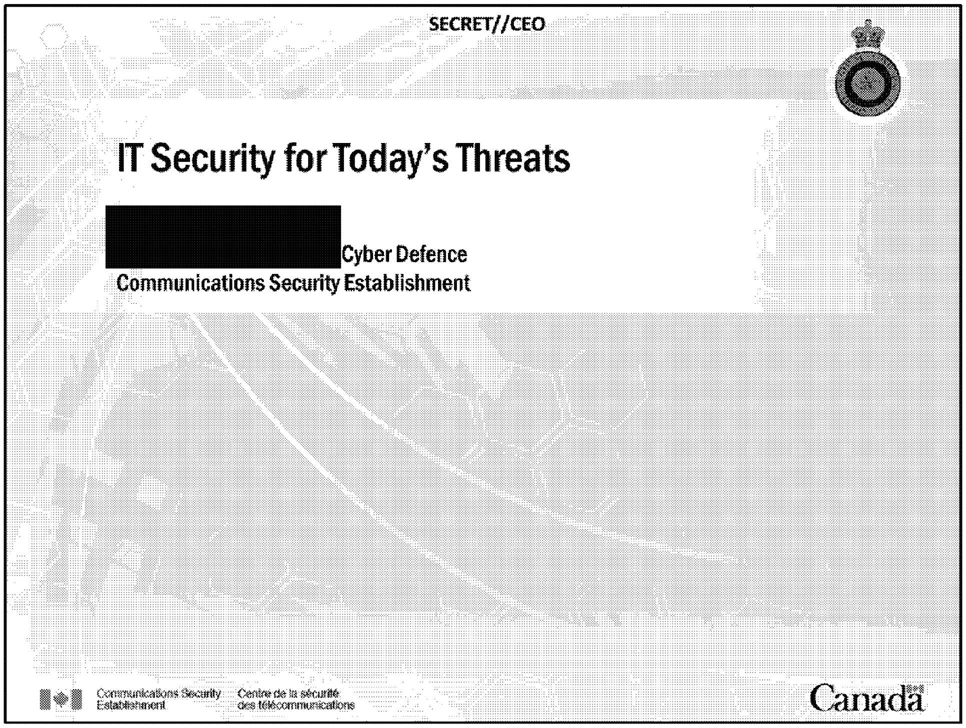


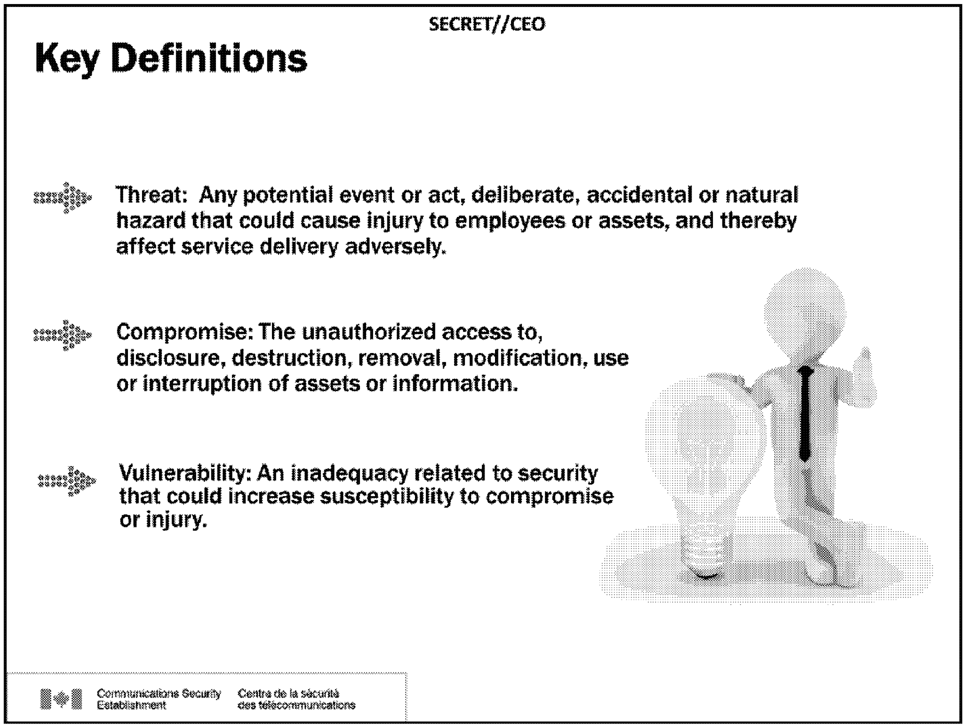
SECRET//CEO

IT Security for Today's Threats

[redacted] Cyber Defence
Communications Security Establishment

Communications Security Establishment
Centre de la sécurité des télécommunications

Canada



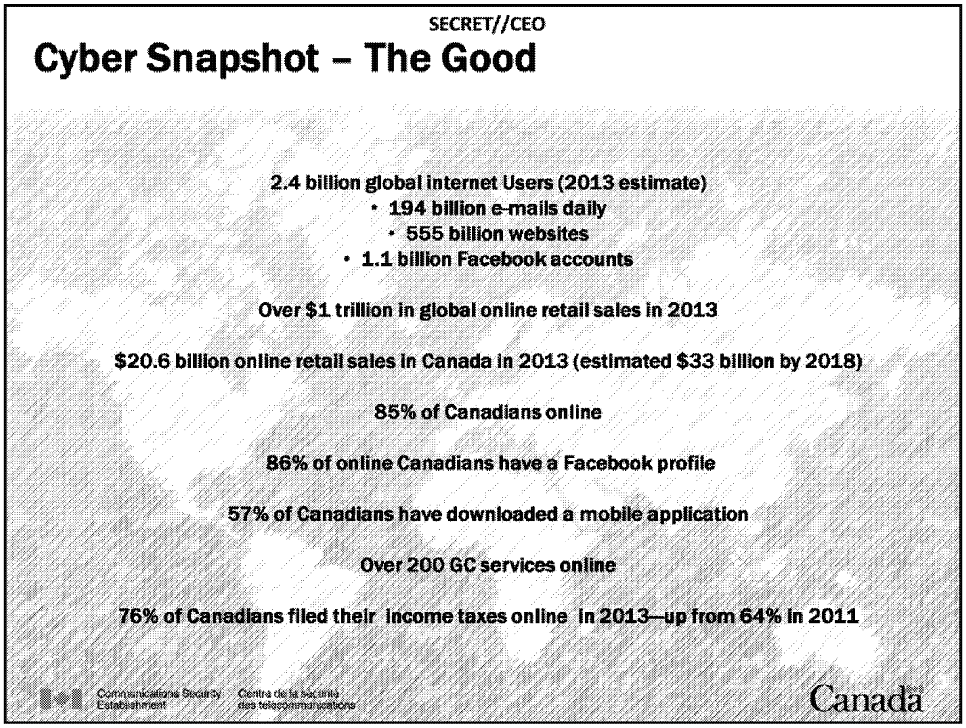
SECRET//CEO

Key Definitions

- Threat: Any potential event or act, deliberate, accidental or natural hazard that could cause injury to employees or assets, and thereby affect service delivery adversely.
- Compromise: The unauthorized access to, disclosure, destruction, removal, modification, use or interruption of assets or information.
- Vulnerability: An inadequacy related to security that could increase susceptibility to compromise or injury.

Communications Security Establishment Centre de la sécurité des télécommunications

Definitions from the PGS.



SECRET//CEO

Cyber Snapshot – The Good

2.4 billion global internet Users (2013 estimate)
- 194 billion e-mails daily
- 555 billion websites
- 1.1 billion Facebook accounts

Over $1 trillion in global online retail sales in 2013

$20.6 billion online retail sales in Canada in 2013 (estimated $33 billion by 2018)

85% of Canadians online

86% of online Canadians have a Facebook profile

57% of Canadians have downloaded a mobile application

Over 200 GC services online

76% of Canadians filed their income taxes online in 2013—up from 64% in 2011

Communications Security Establishment Centre de la sécurité des télécommunications Canada

Sources:

- Chief’s GTEC speech
- Internet World Stats-Usage and Population Statisitcs
- The Ipsos Canadian inter@ctive Reid Report 2012
- Forrester Research
- CRA Annual Report to Parliament 2012-2013

Storyline: Cyber around the globe

Past 10 years – exponential evolution of the internet

In 2010 – 1.7 Billion internet users – est. by 2015 +10 billion

2/3 of cdns bank and file taxes on line

CII – oil&gas, power, water, public transportation, air traffic control

Industry – instant mass marketing

Not yet exhausted potential opportunities of internet use

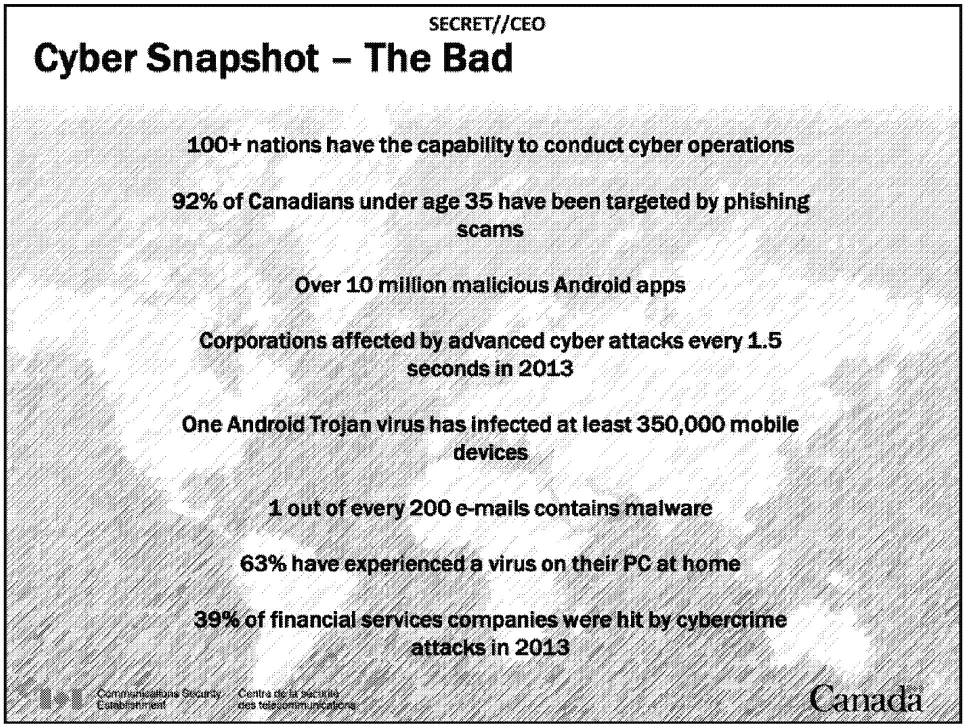
IMAP Retail industry Global Report 2009 (Clearwater Corporate Financing LLP)

Global retail sales $14 B in 2009 – 14.5 % growth over 2008

Online sales 2009 – $349 B – for top retailers on lines = 6.6% of all sales

- 130 B in US

2014 on line sales forecast – 779 Billion by 2014



SECRET//CEO

Cyber Snapshot – The Bad

100+ nations have the capability to conduct cyber operations

92% of Canadians under age 35 have been targeted by phishing scams

Over 10 million malicious Android apps

Corporations affected by advanced cyber attacks every 1.5 seconds in 2013

One Android Trojan virus has infected at least 350,000 mobile devices

1 out of every 200 e-mails contains malware

63% have experienced a virus on their PC at home

39% of financial services companies were hit by cybercrime attacks in 2013

Communications Security Establishment Centre de la sécurité des télécommunications

Canadä

Storyline: Cyber around the globe

Past 10 years – exponential evolution of the internet

In 2010 – 1.7 Billion internet users – est. by 2015 +10 billion

2/3 of cdns bank and file taxes on line

CII – oil&gas, power, water, public transportation, air traffic control

Industry – instant mass marketing

Not yet exhausted potential opportunities of internet use

IMAP Retail industry Global Report 2009 (Clearwater Corporate Financing LLP)

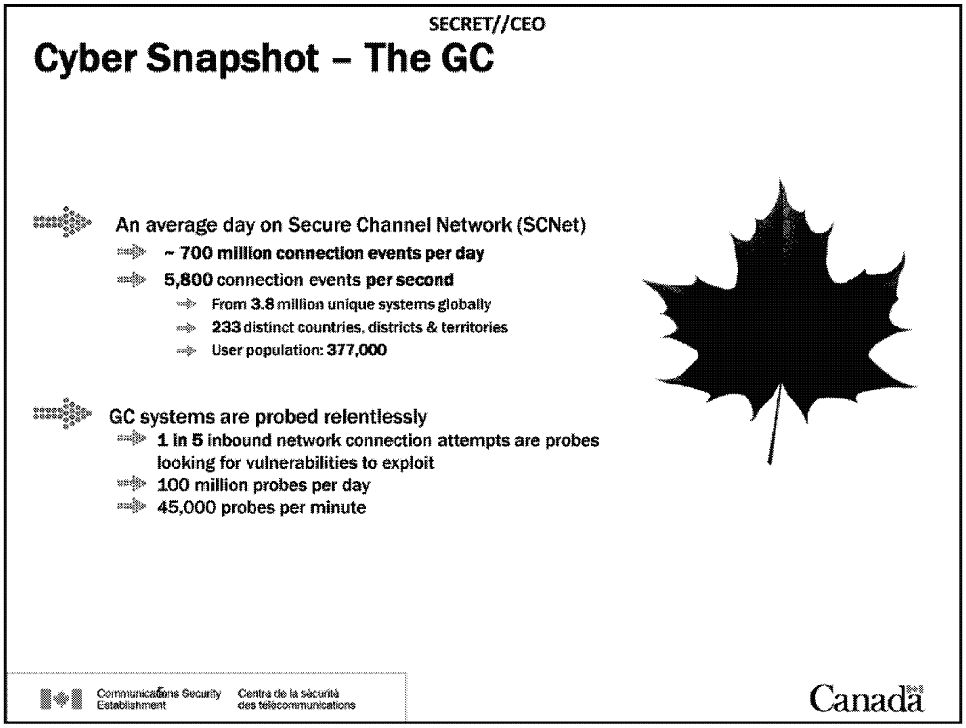
Global retail sales $14 B in 2009 – 14.5 % growth over 2008

Online sales 2009 – $349 B – for top retailers on lines = 6.6% of all sales

- 130 B in US

2014 on line sales forecast – 779 Billion by 2014

Sources (respectively): John Forster, Canadian Press, Kaspersky Lab, SC Magazine, Infosecurity Magazine, 2012 Fact Guide Internet World Stats, IT Pro)



SECRET//CEO

Cyber Snapshot – The GC

- An average day on Secure Channel Network (SCNet)
  - **~ 700 million connection events per day**
  - **5,800** connection events **per second**
    - From **3.8** million unique systems globally
    - **233** distinct countries, districts & territories
    - User population: **377,000**
- GC systems are probed relentlessly
  - **1 in 5** inbound network connection attempts are probes looking for vulnerabilities to exploit
  - 100 million probes per day
  - 45,000 probes per minute

Communications Security Establishment Centre de la sécurité des télécommunications 5

Canadä

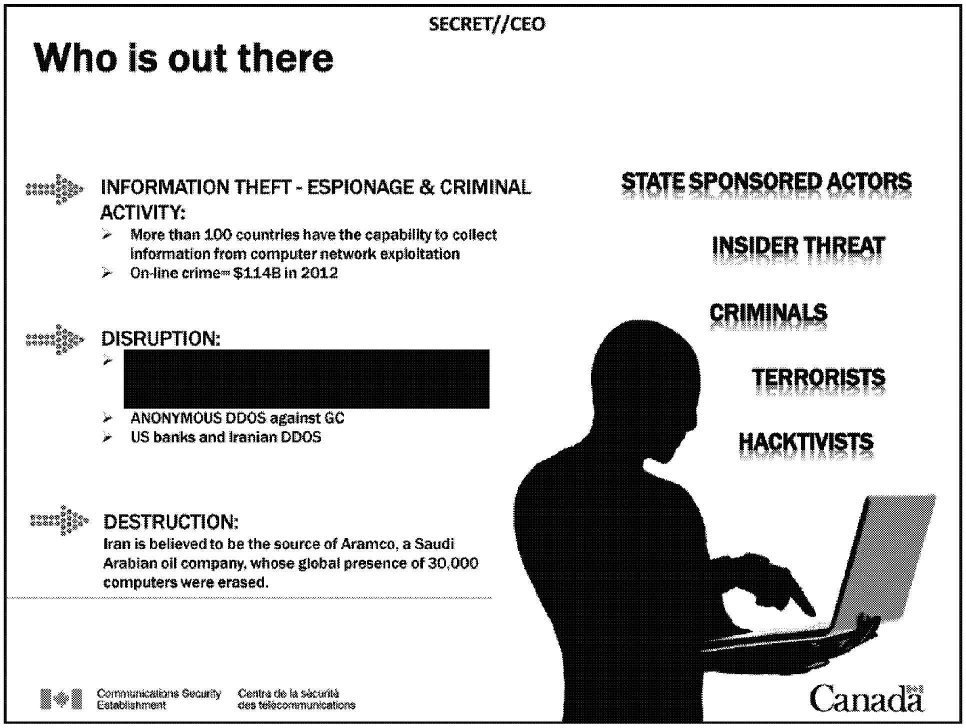
Storyline: What this means for the GC

20 TB data daily

2 million emails

Incidents – anomalous – 1 m

- signature based – 2000 – [redacted]



SECRET//CEO

Who is out there

INFORMATION THEFT - ESPIONAGE & CRIMINAL ACTIVITY:

- More than 100 countries have the capability to collect information from computer network exploitation
- On-line crime= $114B in 2012

DISRUPTION:

- [redacted]
- ANONYMOUS DDOS against GC
- US banks and Iranian DDOS

DESTRUCTION:

Iran is believed to be the source of Aramco, a Saudi Arabian oil company, whose global presence of 30,000 computers were erased.

STATE SPONSORED ACTORS

INSIDER THREAT

CRIMINALS

TERRORISTS

HACKTIVISTS

Communications Security Establishment   Centre de la sécurité des télécommunications

Canada

Storyline: Intents and evolution

ADD: Insider threat (Snowden)

What are some examples of each. Lets start with the obvious Deliberate.

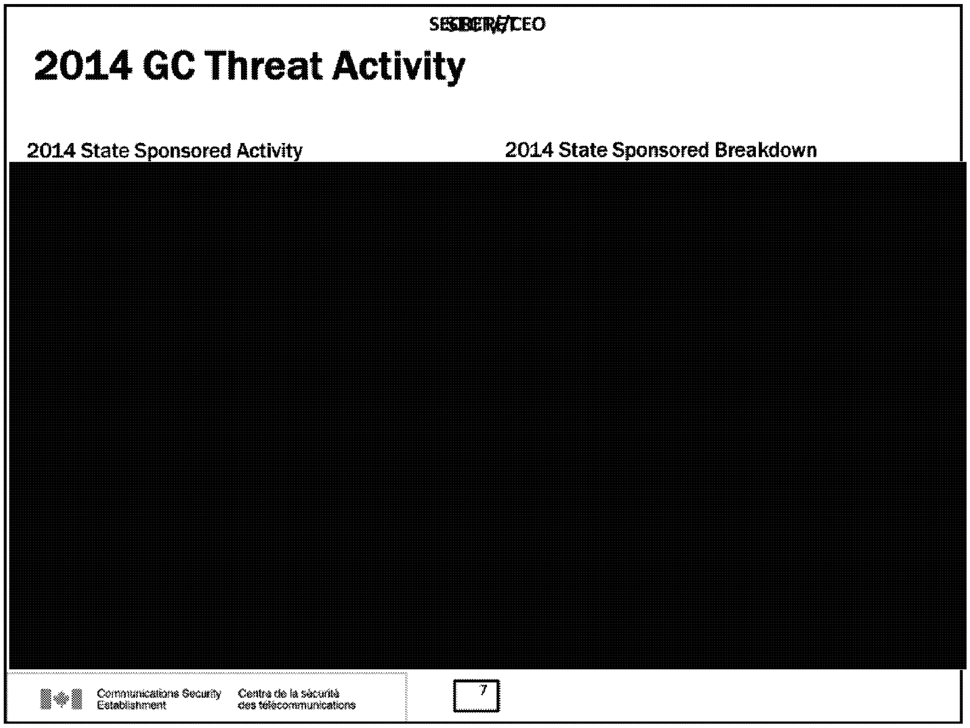
Deliberate Events

- Social engineering
- Eavesdropping
- Phishing
- Theft
- Denial of Service (DoS)
- Sabotage/Defacement
- SPAM

Accidental Events

- Human error
- Technical flaws or failures

- Industrial accidents
- Fires, spills, etc



SECRET//CEO

2014 GC Threat Activity

2014 State Sponsored Activity

2014 State Sponsored Breakdown

[redacted]

Communications Security Establishment

Centre de la sécurité des télécommunications

7

Slide used by Chief for [redacted] – updated with current stats (January – June 2014); quarter 3 stats currently unavailable.

[redacted]

State Sponsored

[redacted]

[redacted]

Note – also detected limited state sponsored activity [redacted] in Q1

SECRET//CEO

2013 State Sponsored Actor Activity

[redacted]

Communications Security Establishment
Centre de la sécurité des télécommunications

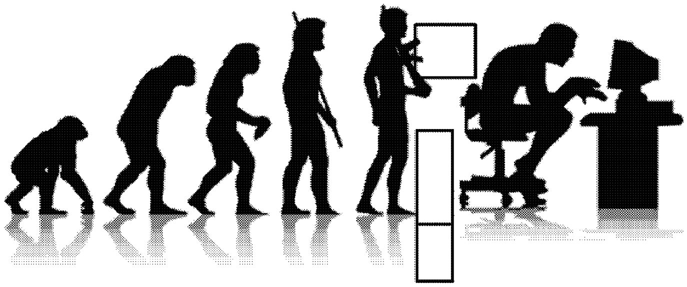
SECRET//CEO

Open Source Threat Activity (Malware)

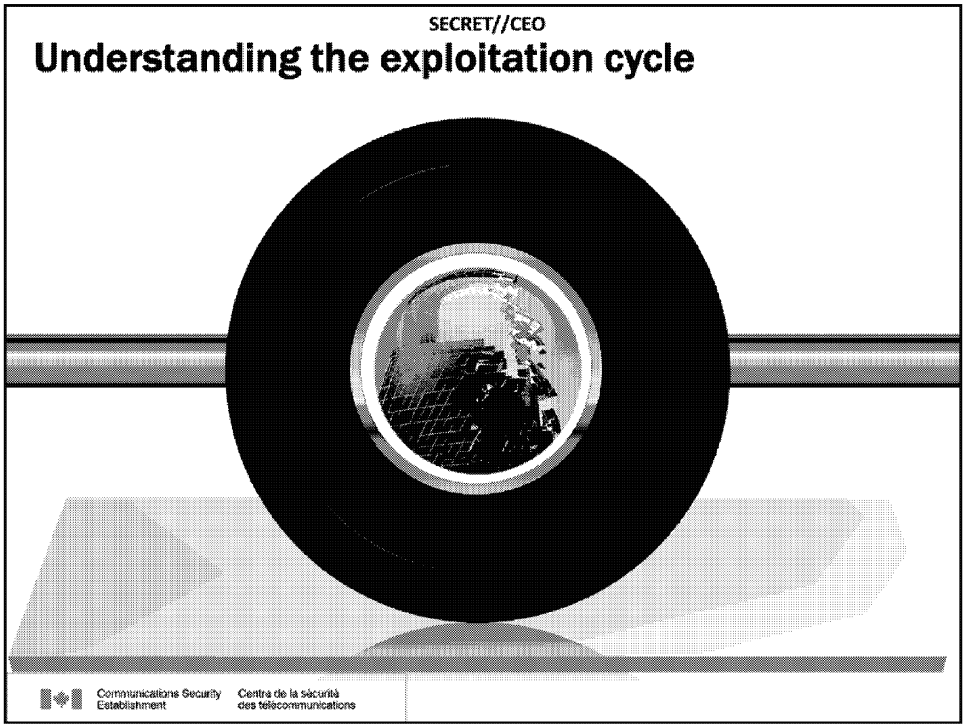
[redacted]

SECRET//CEO

The threat actor has evolved



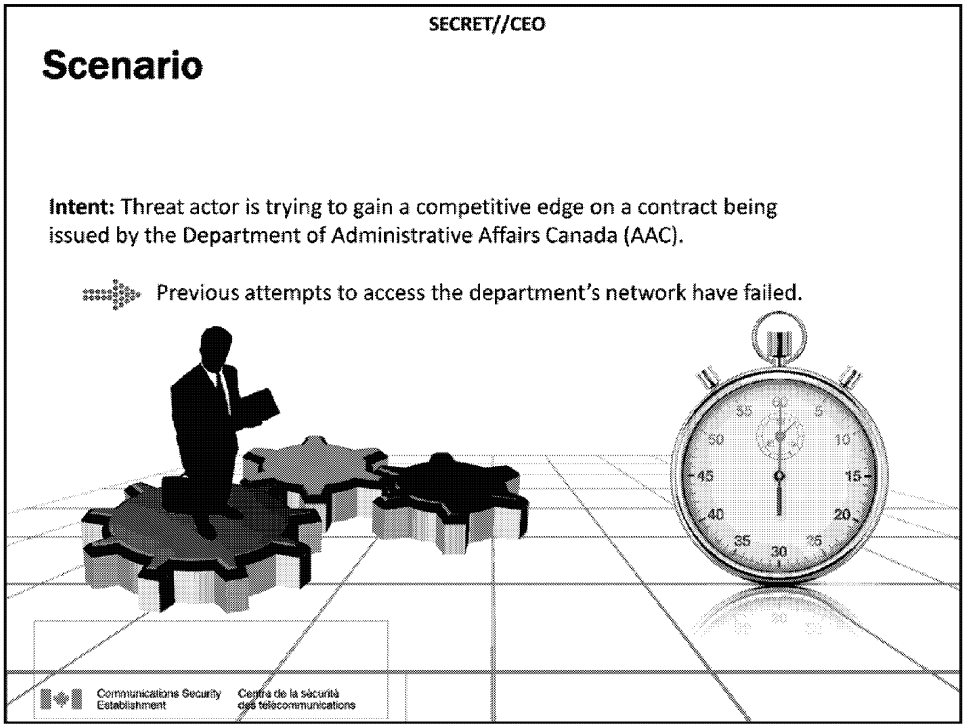
Communications Security Establishment
Centre de la sécurité des télécommunications



SECRET//CEO

Understanding the exploitation cycle

Communications Security Establishment
Centre de la sécurité des télécommunications



SECRET//CEO

Scenario

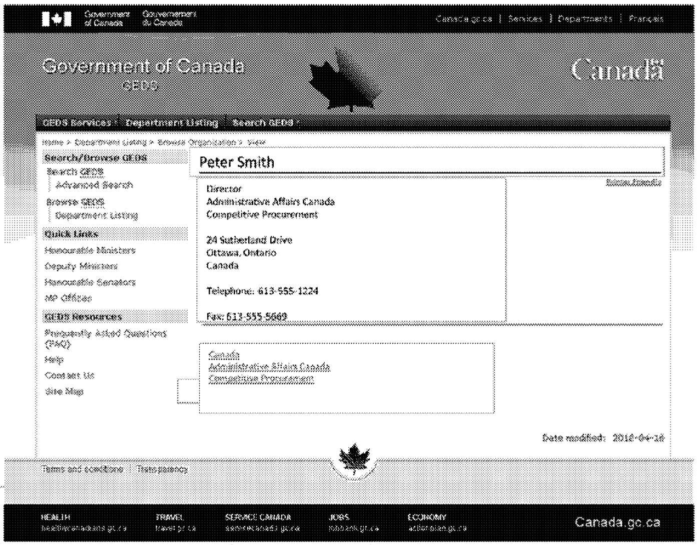
Intent: Threat actor is trying to gain a competitive edge on a contract being issued by the Department of Administrative Affairs Canada (AAC).

Previous attempts to access the department's network have failed.

Communications Security Establishment
Centre de la sécurité des télécommunications

SECRET//CEO

Step I: It all begins with GEDS



Peter Smith

Director
Administrative Affairs Canada
Competitive Procurement

24 Sutherland Drive
Ottawa, Ontario
Canada

Telephone: 613-555-1224

Fax: 613-555-5669

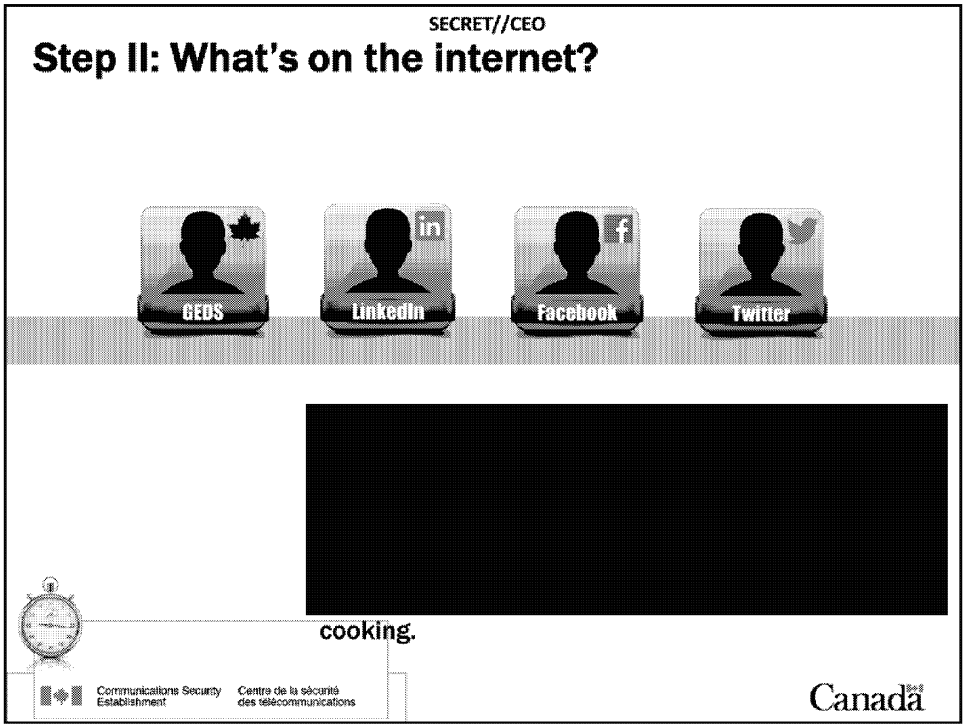
Canada
Administrative Affairs Canada
Competitive Procurement

Date modified: 2012-04-16

Communications Security Establishment
Centre de la sécurité des télécommunications

- [illegible]
- Bird, Ali, Senior Advisor, 613-555-9675
- Chan, Rick, Executive Assistant, 613-555-2802
- Cox, Chris, Analyst, 613-555-9635
- Coady, Anne, Administrative Officer, 613-555-5695

Canada



SECRET//CEO

Step II: What's on the internet?

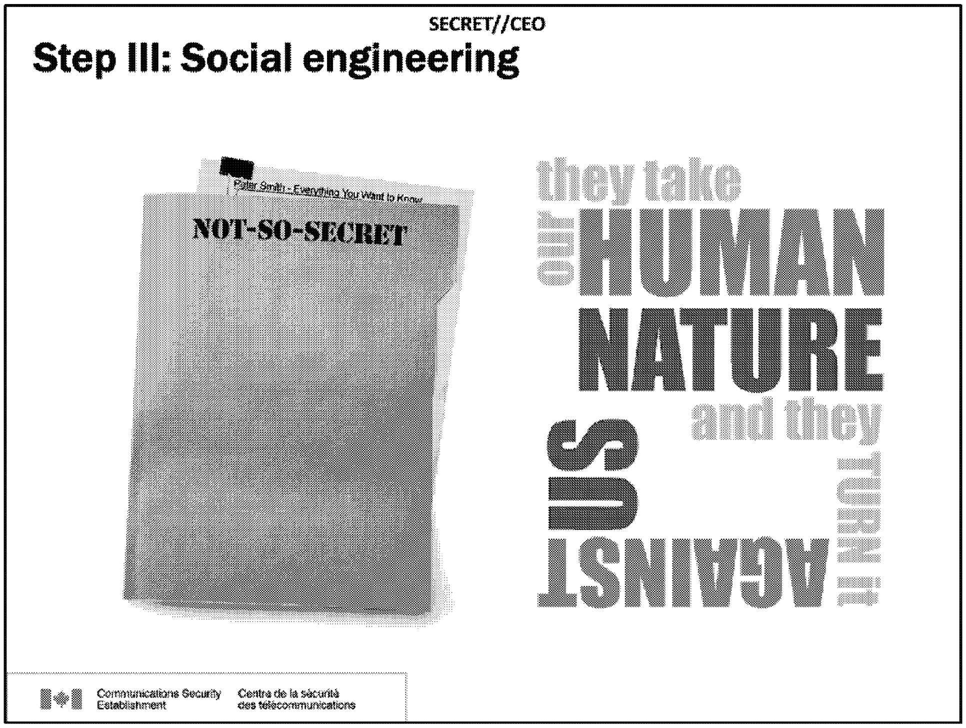
GEDS
LinkedIn
Facebook
Twitter

[redacted]

cooking.

Communications Security Establishment
Centre de la sécurité des télécommunications

Canada



SECRET//CEO

Step III: Social engineering

Peter Smith - Everything You Want to Know

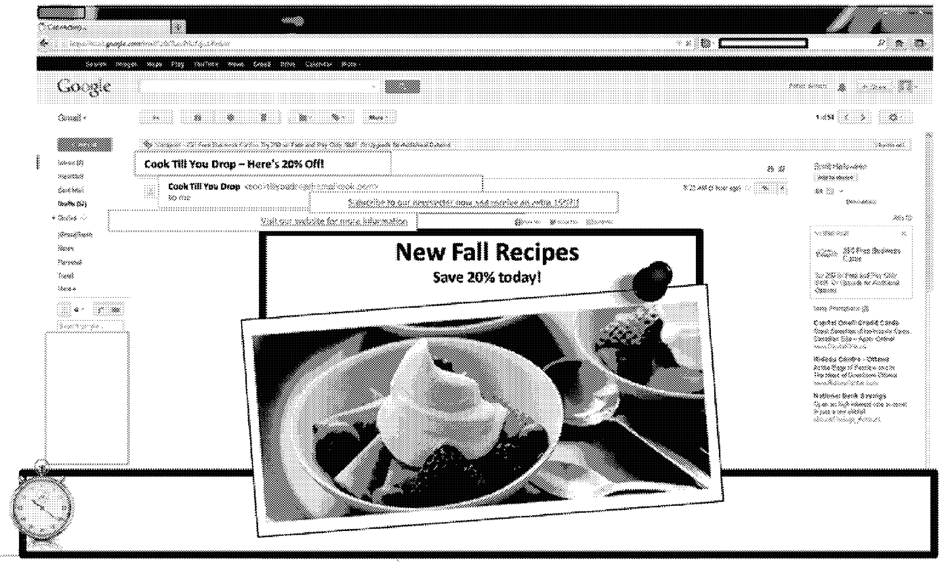
NOT-SO-SECRET

they take our HUMAN NATURE and they TURN it AGAINST US

Communications Security Establishment Centre de la sécurité des télécommunications

15

Step IV: Time to go phishing



Cook Till You Drop – Here's 20% Off!

Cook Till You Drop

Subscribe to our newsletter now and receive an extra 15%!!!

Visit our website for more information

New Fall Recipes

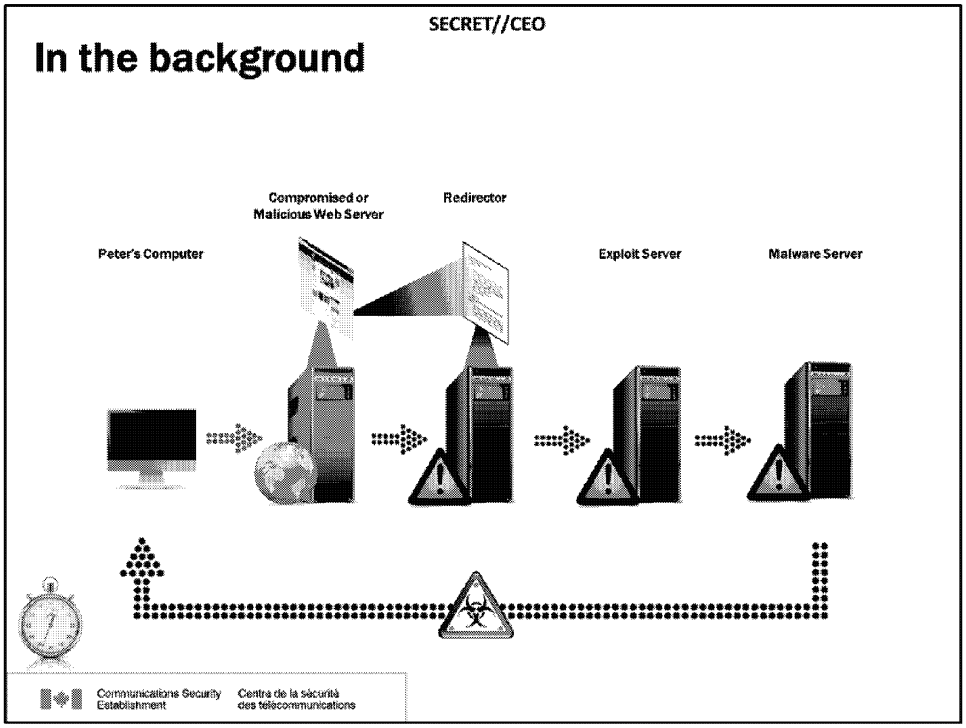
Save 20% today!

SECRET//CEO

Step V: Watch that "seed" grow

Communications Security Establishment
Centre de la sécurité des télécommunications

17



SECRET//CEO

In the background

Peter's Computer

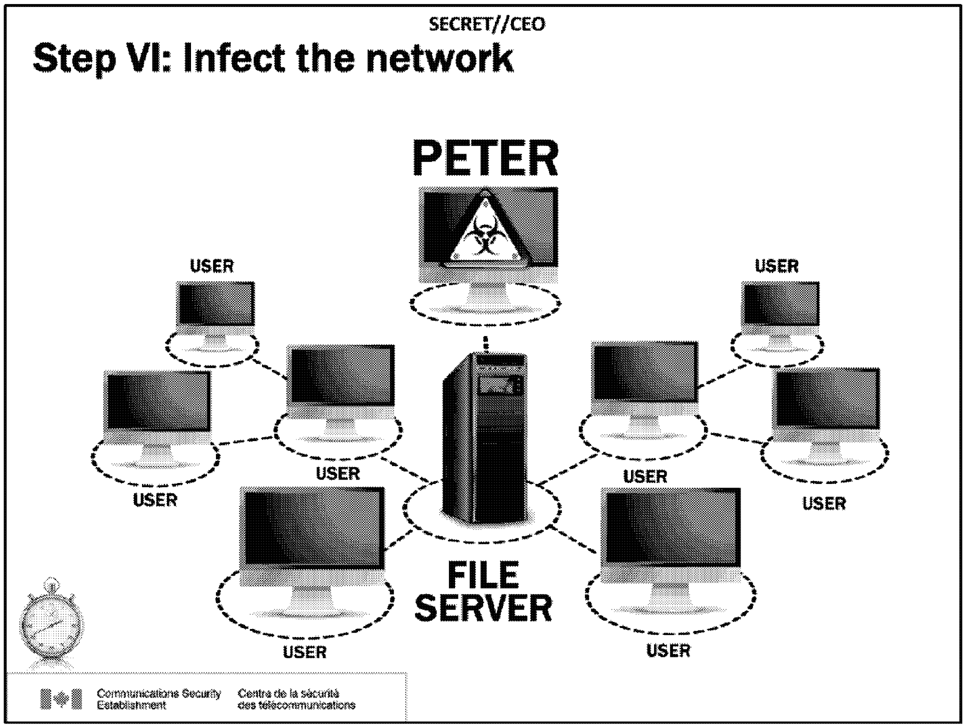
Compromised or Malicious Web Server

Redirector

Exploit Server

Malware Server

Communications Security Establishment
Centre de la sécurité des télécommunications



SECRET//CEO

Step VI: Infect the network

Communications Security Establishment
Centre de la sécurité des télécommunications

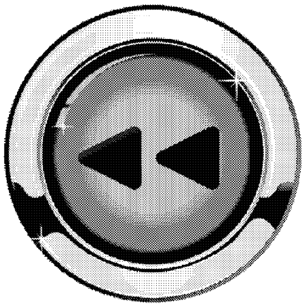
SECRET//CEO

Threat actor now has control

Communications Security Establishment Centre de la sécurité des télécommunications

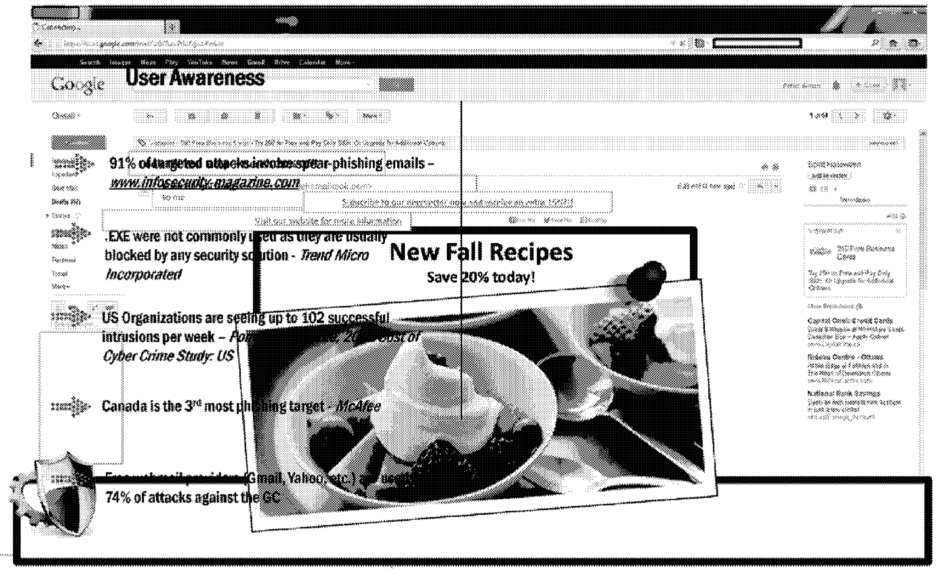
- Screen captures
- Creating accounts and accessing all information within accounts (i.e. Outlook information)
- Obtaining complete departmental account names and passwords
- Creating network map to guide compromises
- Uploading tools to compromise other PC/Severs in the Network
- Identifying databases and their versions
- Listing running processes and process information
- Stopping software from running (i.e. antivirus)
- Replacing valid software malicious one
- Covertly transfer files out to a specific server
- Delete information & takedown network
- Launch attacks to other networks
- Cost of mitigation = extremely high

Rewind



SECRET//CEO

Rewind: Mitigation strategy



User Awareness

- 91% of targeted attacks involve spear-phishing emails – *www.infosecurity-magazine.com*
- .EXE were not commonly used as they are usually blocked by any security solution - *Trend Micro Incorporated*
- US Organizations are seeing up to 102 successful intrusions per week – *Po… 20… Cost of Cyber Crime Study: US*
- Canada is the 3rd most phishing target - *McAfee*
- Free webmail providers (Gmail, Yahoo, etc.) are used…
- 74% of attacks against the GC

Subscribe to our newsletter now and receive an extra 15%!!!

Visit our website for more information

New Fall Recipes

Save 20% today!

Communications Security Establishment

Centre de la sécurité des télécommunications

SECRET//CEO

Rewind: Mitigation strategy

3rd Party Application Patching

- Peter was running a vulnerable version of a browser [illegible] (i.e. Java). Many exploits were available for Peter's pl[illegible] version. One was used to allow malware to be downloaded onto his system.
- Timely updates of 3rd Party applications (i.e. PDF viewer, MS Office, ActiveX objects and other web b[illegible]s) allows patching of vulnera[illegible] and limits [illegible]e and the time the system can be exploited.
- 98% of GC compromises [illegible] sh[illegible] after patches are disclosed by vendor.

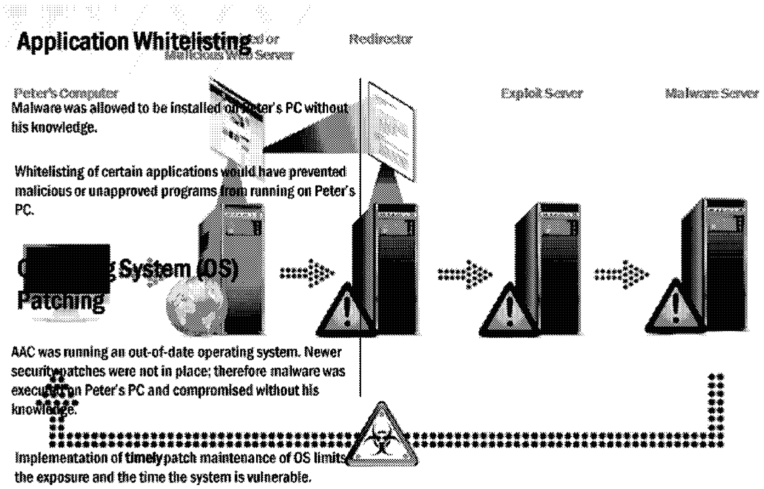
Communications Security Establishment Centre de la sécurité des télécommunications

SECRET//CEO

Rewind: Mitigation strategy

Application Whitelisting

- Malware was allowed to be installed on Peter's PC without his knowledge.
- Whitelisting of certain applications would have prevented malicious or unapproved programs from running on Peter's PC.

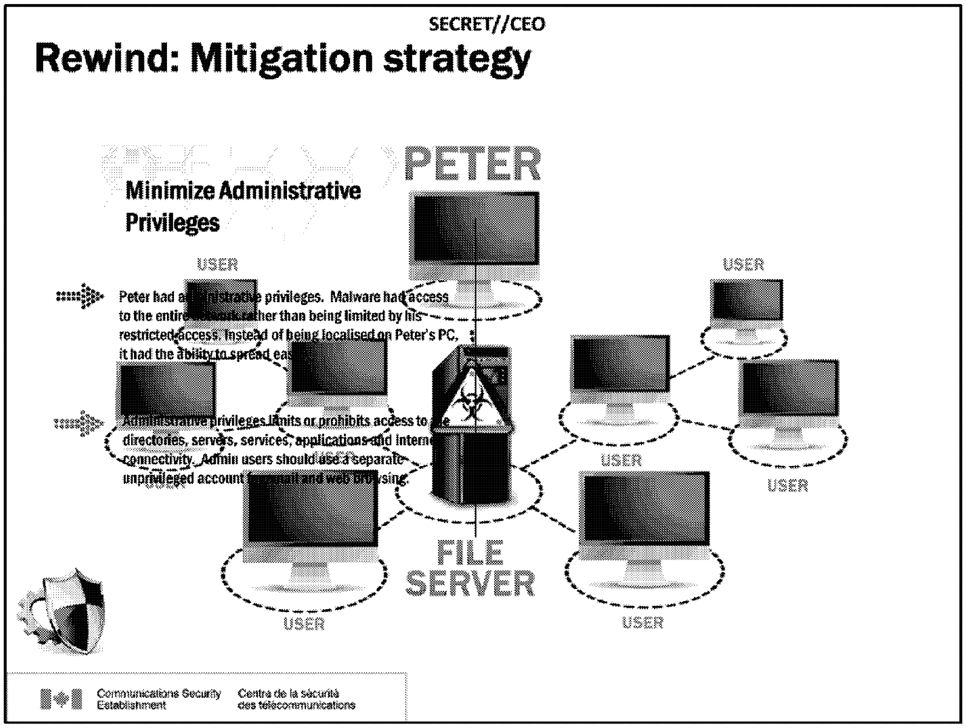


Operating System (OS) Patching

- AAC was running an out-of-date operating system. Newer security patches were not in place; therefore malware was executed on Peter's PC and compromised without his knowledge.

Implementation of timelypatch maintenance of OS limits the exposure and the time the system is vulnerable.

Communications Security Establishment Centre de la sécurité des télécommunications



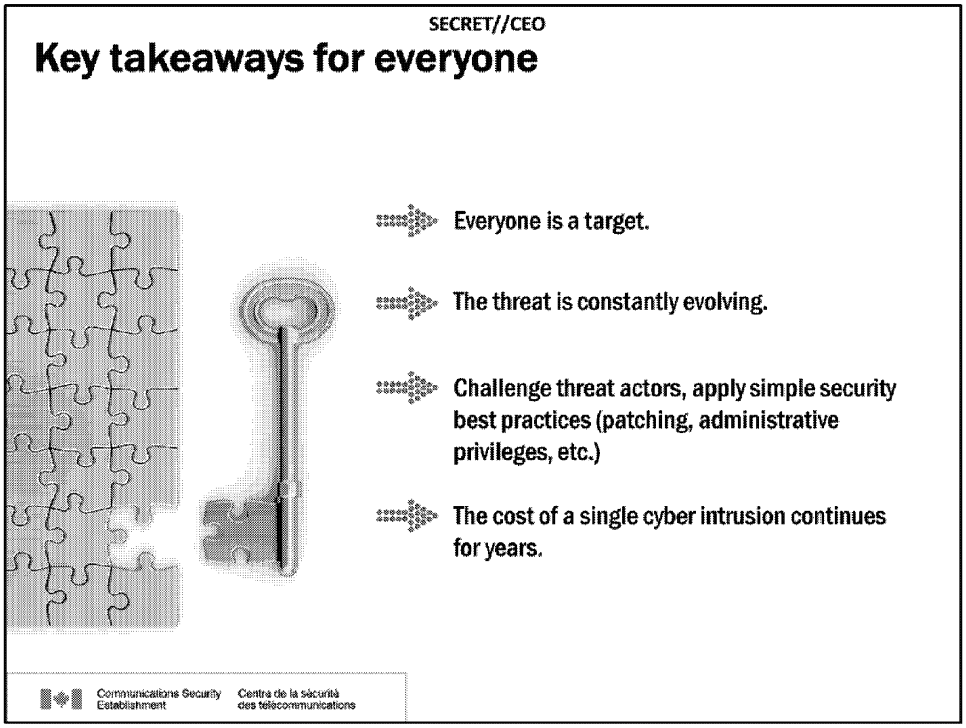
SECRET//CEO

Rewind: Mitigation strategy

Minimize Administrative Privileges

- Peter had administrative privileges. Malware had access to the entire network rather than being limited by his restricted access. Instead of being localised on Peter's PC, it had the ability to spread easily.
- Administrative privileges limits or prohibits access to file directories, servers, services, applications and internet connectivity. Admin users should use a separate unprivileged account for email and web browsing.

Communications Security Establishment
Centre de la sécurité des télécommunications

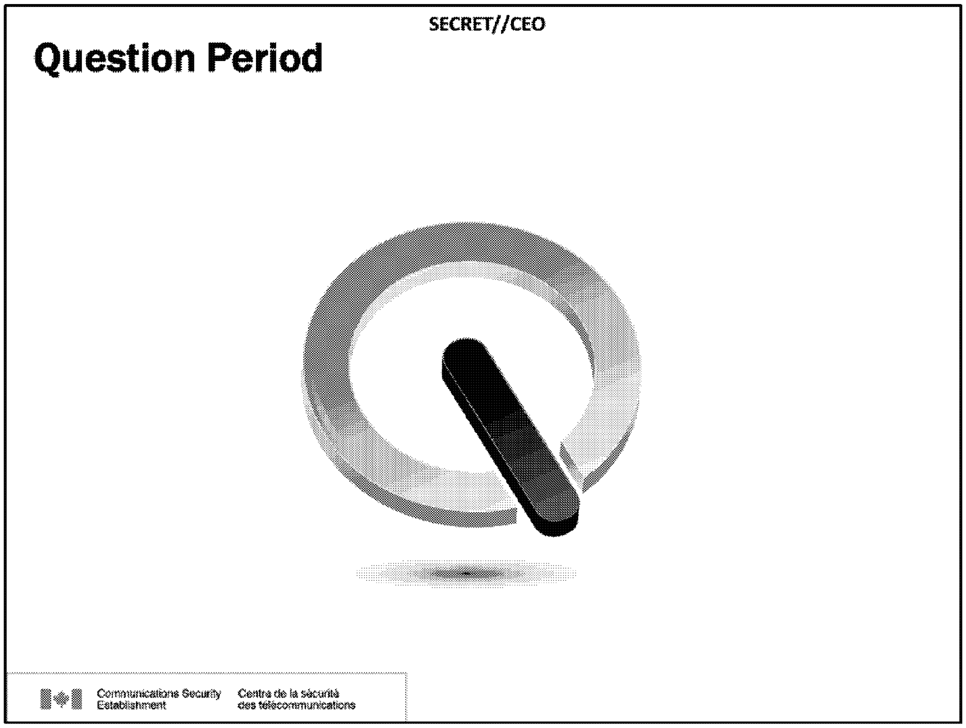


SECRET//CEO

Key takeaways for everyone

- Everyone is a target.
- The threat is constantly evolving.
- Challenge threat actors, apply simple security best practices (patching, administrative privileges, etc.)
- The cost of a single cyber intrusion continues for years.

Communications Security Establishment Centre de la sécurité des télécommunications



SECRET//CEO

Question Period

Communications Security Establishment
Centre de la sécurité des télécommunications