TOP 10 IT SECURITY ACTIONS & BEYOND

ISACA Annual Meeting

June 14th, 2018

Communications Security Establishment
Centre de la sécurité des télécommunications

Canada

CSE's ROLE IN CYBER SECURITY

CYBER SECURITY LEAD IN CANADA

ACCESS TO UNIQUE FOREIGN INTELLIGENCE

AHEAD OF EMERGING THREATS

MONITOR GC SYSTEMS 24/7 FOR CYBER THREATS

SAFEGUARDS CANADA'S MOST IMPORTANT INFORMATION

Communications Security Establishment

Centre de la sécurité des télécommunications

Canada

CYBER: WHY IT'S IMPORTANT

Cyber is:

- Integrated into every Canadian's everyday life
- A key part of all aspects of the government agenda: economic prosperity, innovation, defence and security
- Critical to democracy and democratic institutions
- Canada's wealth, innovative business sector, diplomatic relationships and military partnerships make it an attractive target

Successful compromises can:

- Affect Government services to citizens
- Compromise Canadians' personal information
- Harm Canada's economy and national security
- Undermine Canadians' trust and confidence

Communications Security Establishment   Centre de la sécurité des télécommunications

Canada

CYBER TRENDS

2014

JANUARY | **TARGET**
110M financial records stolen

APRIL | **HEARTBLEED**
900 records stolen from CRA

JUNE | **NATIONAL RESEARCH COUNCIL (NRC)**

2015

MAY | **INTERNAL REVENUE SERVICE (IRS)**
330,000 US tax records stolen

JUNE | **OFFICE OF PERSONNEL MANAGEMENT (OPM)**
21.5M records stolen of US government employees

2015

JULY | **GC DDOS ATTACKS**
> 12 websites of federal departments crippled
ASHLEY MADISON
37M user's account information leaked

2016

OCTOBER | **MIRAI BOTNET**
Infected IoT devices worldwide. DDOS attack on DNS provider DYN

2017

MAY | **WANNACRY** (RANSOMWARE)
>300,000 computer infected
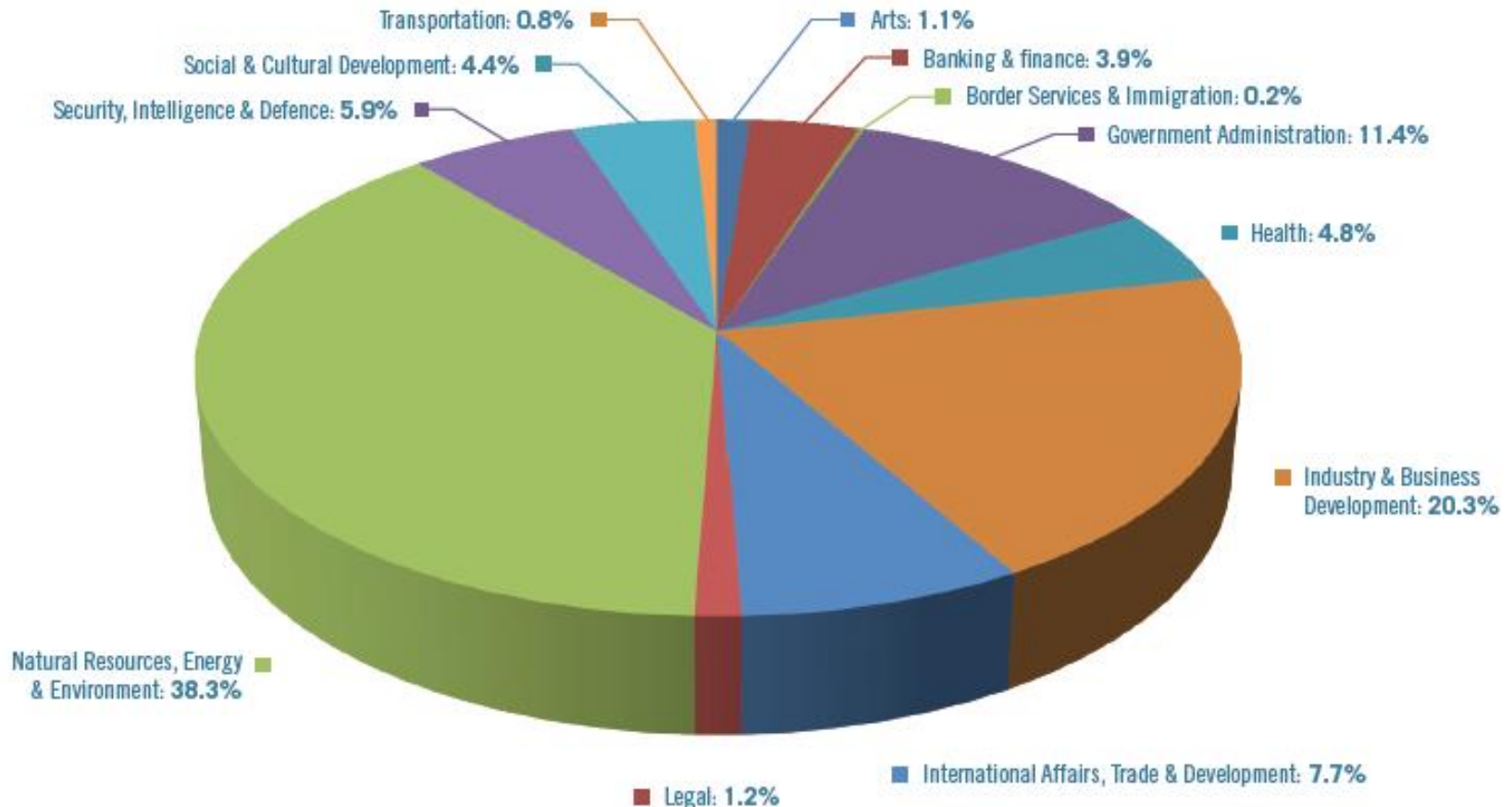
JULY | **EQUIFAX**
145M US personal info leaked

OCTOBER | **YAHOO**
3B user's data compromised

GOVERNMENT OF CANADA CYBER EVENTS IN 2016 BY SECTOR

WHAT ARE THREAT ACTORS INTERESTED IN? EVERYTHING!
GOVERNMENT OF CANADA CYBER EVENTS IN 2016 BY SECTOR

Transportation: 0.8%
Arts: 1.1%
Social & Cultural Development: 4.4%
Banking & finance: 3.9%
Security, Intelligence & Defence: 5.9%
Border Services & Immigration: 0.2%
Government Administration: 11.4%
Health: 4.8%
Industry & Business Development: 20.3%
Natural Resources, Energy & Environment: 38.3%
International Affairs, Trade & Development: 7.7%
Legal: 1.2%

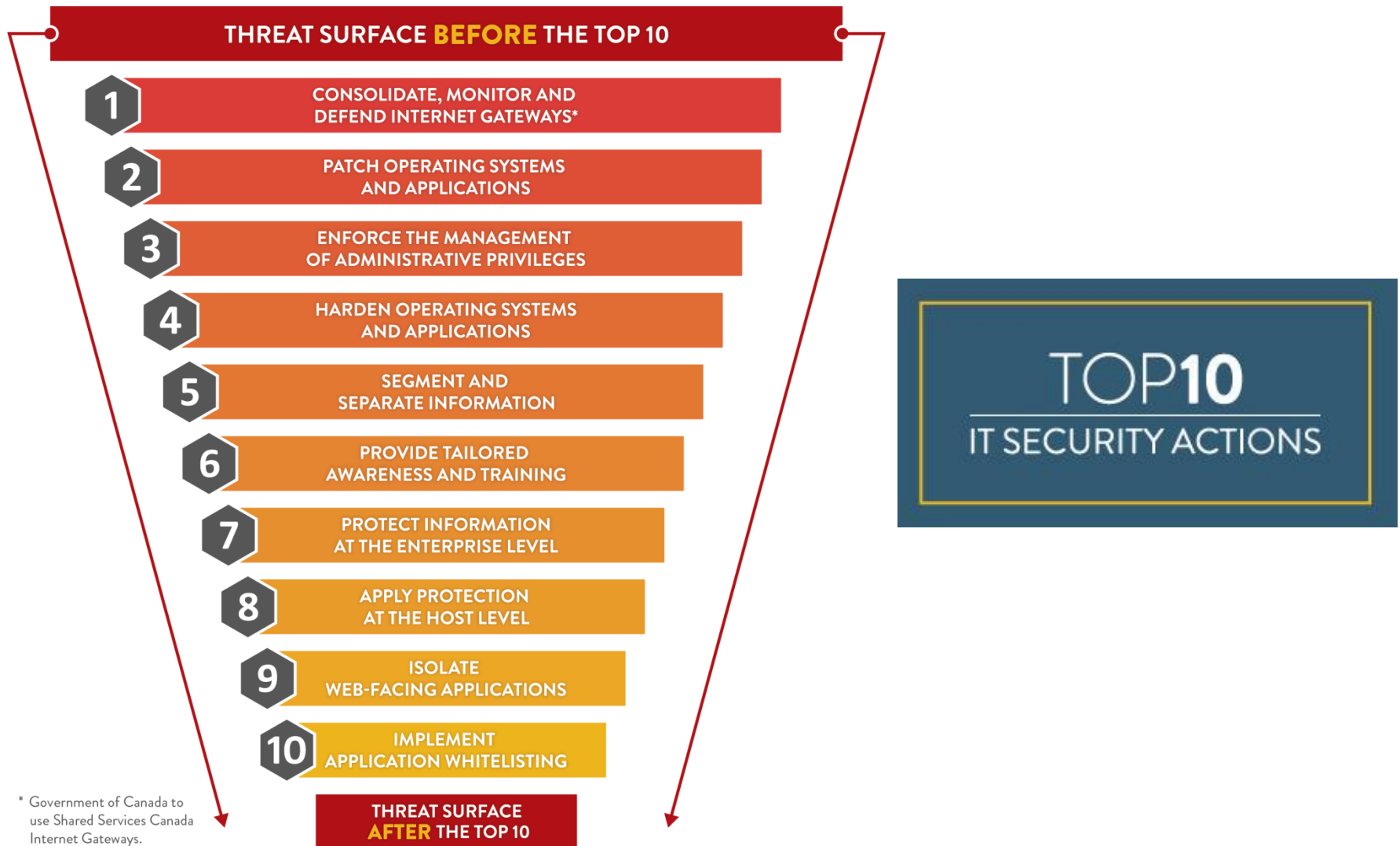Communications Security Establishment   Centre de la sécurité des télécommunications

Canada

WHAT IS THE TOP 10 IT SECURITY ACTIONS?

- The Top 10 is a practical list of IT security actions departments can take to be more secure

- Has been condensed from the Top 35 for ease of use and to focus departmental efforts

- Developed based on CSE's analysis of the cyber threat activity trends that impact Government of Canada (GC) Internet-connected network

Communications Security Establishment   Centre de la sécurité des télécommunications

Canada

IMPLEMENT THE TOP 10

THREAT SURFACE BEFORE THE TOP 10

1 CONSOLIDATE, MONITOR AND DEFEND INTERNET GATEWAYS*

2 PATCH OPERATING SYSTEMS AND APPLICATIONS

3 ENFORCE THE MANAGEMENT OF ADMINISTRATIVE PRIVILEGES

4 HARDEN OPERATING SYSTEMS AND APPLICATIONS

5 SEGMENT AND SEPARATE INFORMATION

6 PROVIDE TAILORED AWARENESS AND TRAINING

7 PROTECT INFORMATION AT THE ENTERPRISE LEVEL

8 APPLY PROTECTION AT THE HOST LEVEL

9 ISOLATE WEB-FACING APPLICATIONS

10 IMPLEMENT APPLICATION WHITELISTING

THREAT SURFACE AFTER THE TOP 10

* Government of Canada to use Shared Services Canada Internet Gateways.

TOP10
IT SECURITY ACTIONS

Communications Security Establishment Centre de la sécurité des télécommunications

Canada

OBSERVATIONS

- Since the TBS Security Policy Information Notice (SPIN 2015-01) was issued in 2015:
  - Many GC departments and agencies have incorporated elements into their departmental investment plans and internal IM/IT audit assessment
  - Perception is that it is easier for large departments to implement as they have the dedicated resources
  - For small and medium agencies, there is a lack of resources dedicated to IT security
  - A strong desire for a community wide effort to share best-practices and initiatives
  - Top 10 is an excellent start but security requires continuous improvement and additional guidance is needed

MOVING FORWARD WITH ITSG-33

- ITSG-33 (*IT Security Risk Management: A Lifecycle Approach*) provides guidance pertaining to:
  - IT Security Risk Management Activities
  - Security Implementation Process
  - Security Control Catalogue & Profiles

- How to transition from Top 10 to ITSG-33?
  - Top 10 are only the first steps to increasing a department's security posture
  - Top 10 activities correspond directly to ITSG-33 security controls
  - Your "Business Need for Security" will help determine what security controls are required

Communications Security Establishment   Centre de la sécurité des télécommunications

Canada

KEY TAKEAWAYS

- The environment is complex and the threats are diverse
- CSE has additional tools that can help make your organization more secure moving beyond the Top 10

CSE-CST.GC.CA/ITS
itsclientservices@cse-cst.gc.ca

@CSE_CST

WE ARE CYBER SECURITY

Communications Security Establishment
Centre de la sécurité des télécommunications

Canada