Public Safety Canada | Sécurité publique Canada

BUILDING A **SAFE** AND **RESILIENT CANADA**

The Canadian Cyber Incident Response Centre (CCIRC)

Presentation to the Disaster Recovery Information Exchange

September 13, 2017

Canada


massive data
wealth
prosperity
fourth industrial revolution
knowledge
entrepreneurship
global values
innovation
technology
pervasive connectivity
A WORLD GONE DIGITAL
intelligent transport
jobs
smart homes
3D printing
social media
cloud
Internet of Things
opportunity
advanced manufacturing
connected world


A WORLD GONE DIGITAL
cyber theft
spearphishing
ubiquitous
vulnerabilities
anonymity
disruption
censorship
asymmetric warfare
malicious code
pervasive connectivity
cybercrime
hackable transportation
job losses
hackable homes
pervasive risks
self-replication botnets
mass surveillance
Internet
of Things
non-attribution
news manipulation
vulnerable control systems

Cyber Security

WHAT

Protection of digital information and the infrastructure on which it resides

WHY

Maximize the benefits of digital life for Canadian citizens and businesses

Smartphones

Public Safety and utilities

The Internet

Computing

Commerce

Cyber Security is used everyday, by everyone, everywhere there is digital technology

Health care monitoring

Smart Apps

Social Media

Internet of Things devices

Transportation

So, what's new?

- Internet of Things
  - V2V, V2I, ITS, "Devices"
  - Smart Systems
  - People aren't things
- Cloud
  - Privacy, Responsibility and Ownership
- Blended Campaigns
  - Ukrainian Electrical Grid
  - Canadian Transit Organization
  - International Organizations
- Third Party Dependencies
  - "What do you mean our regulator compromised us?"
- "Shadow" OT
  - "What do you mean our city's vehicle traffic management system is on the Internet"?
- Information Operations
  - Social Engineering
  - Elections
- Data as the Target
  - Traditional espionage
  - Ransomware
  - Categorization by threat actor is becoming irrelevant
- Mobile Devices
  - "Where did my perimeter go?"

It's All About Understanding Risk

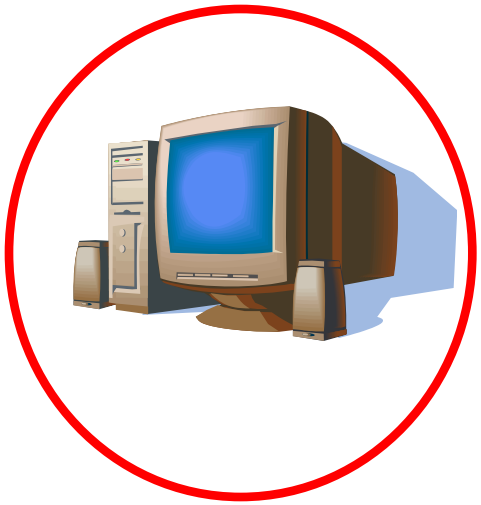
- "We're OK, there's an air gap."
  - Rural <-> Urban
  - Legacy <-> New
  - IT <-> OT
  - Physical <-> Virtual
- "We're all the same, right?"
  - Inconsistent adoption of technology
  - Legacy technologies
- "We're fine, the system will take care of that."
  - New interfaces and access points
  - Skill atrophy
  - Loss of visibility into all parts of a system
  - Cascading failures
  - Unexpected successes
  - Oh, Bill can override that…

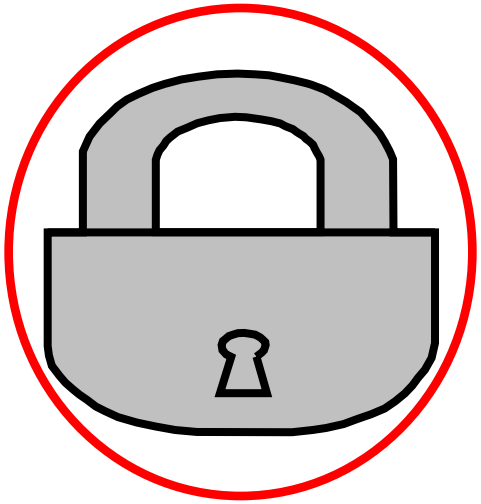
Basic (really really basic) Risk Mitigation

- IT - ASD's Essential Eight
  - **Application Whitelisting**
  - **Patch applications**
  - Disable untrusted macros
  - Harden user applications
  - **Restrict administrative privileges**
  - Use multi-factor authentication
  - **Patch Operating Systems**
  - Backup important data daily

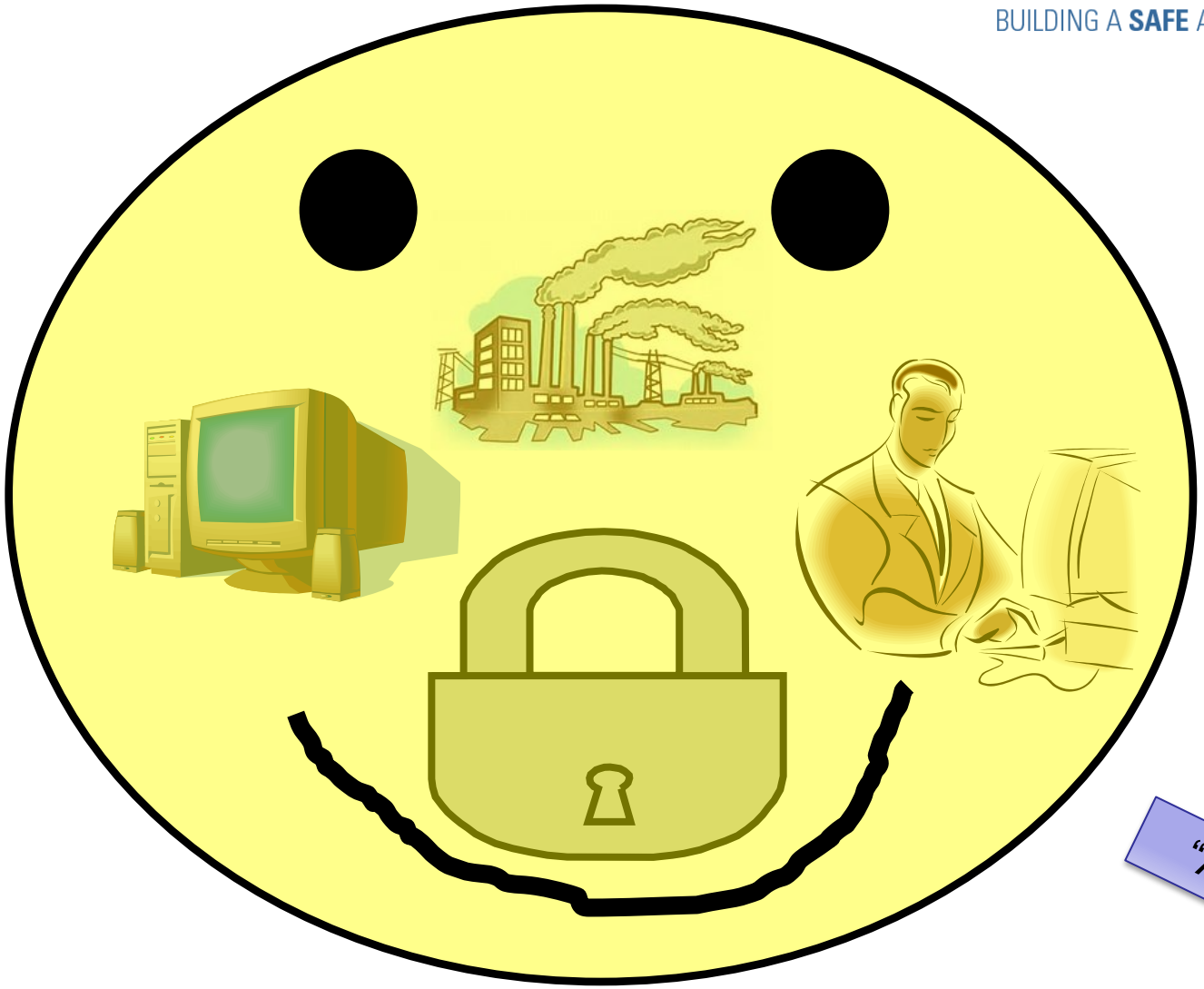
- OT – ICS-CERT's Seven "Strategies"
  - **Application Whitelisting**
  - **Ensure proper configuration/patch management**
  - **Reduce your attack surface area**
  - Build a defendable environment
  - Manage authentication
  - Implement secure remote access
  - Monitor and Respond

Seams





Harmony



"Artist" Alert

Cyber Incidents

Unavoidable part of the digital age, as computers are complex and imperfect

Happen all the time, and more frequently than is admitted

Range in impact:
- business-as-usual (virus infection)
- business-altering (data breach)
- national emergency (power outage)

Change over time as rapidly as technology evolves

Rarely affect only one victim

Can be prevented, detected, managed and mitigated with the right tools and knowledge

Cyber Incidents and Notifications - 2016

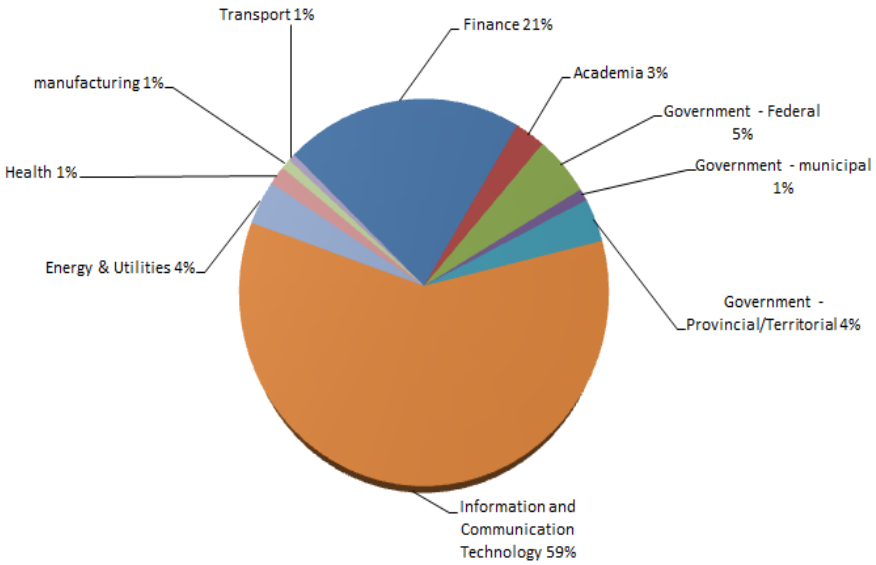
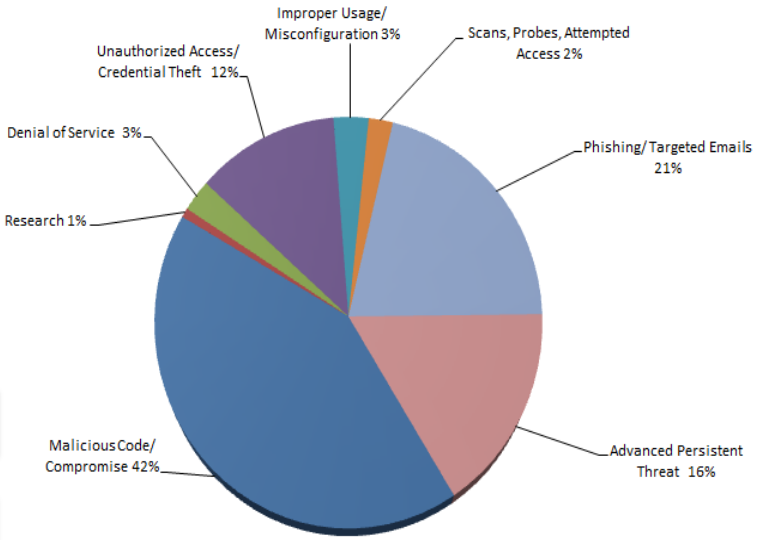


Figure 1: Percentage of Total Incidents by Sector

N = 1594

Figure 2: Percentage of Total Incidents by Type



Potentially Compromised Hosts: 882,126

Potentially Vulnerable Hosts: 2,712,005

Canadian Cyber Incident Response Centre (CCIRC)

OUR VISION

Impact of Cyber Incidents on Canadians is minimized

OUR MISSION

Support Canadian critical infrastructure and businesses in preventing, detecting, and mitigating cyber incidents

OUR APPROACH

TRUST

We are here to help

We understand that incidents happen

We are not a regulator or investigator

RELATIONSHIPS

Always happy to take a call, 24/7, 365

Long term relationships with our partners

Work in concert with private sector solution providers

INNOVATION

We evolve as cyber incidents evolve

Human-speed and machine-speed

Partner and outcome driven

CCIRC'S ROLES

PEOPLE

Dedicated, innovative, credible, trusted

RESPONSE

Canada's proven computer security incident response team

ANALYTICS

World-class data analytics and generation of value-add cyber incident knowledge

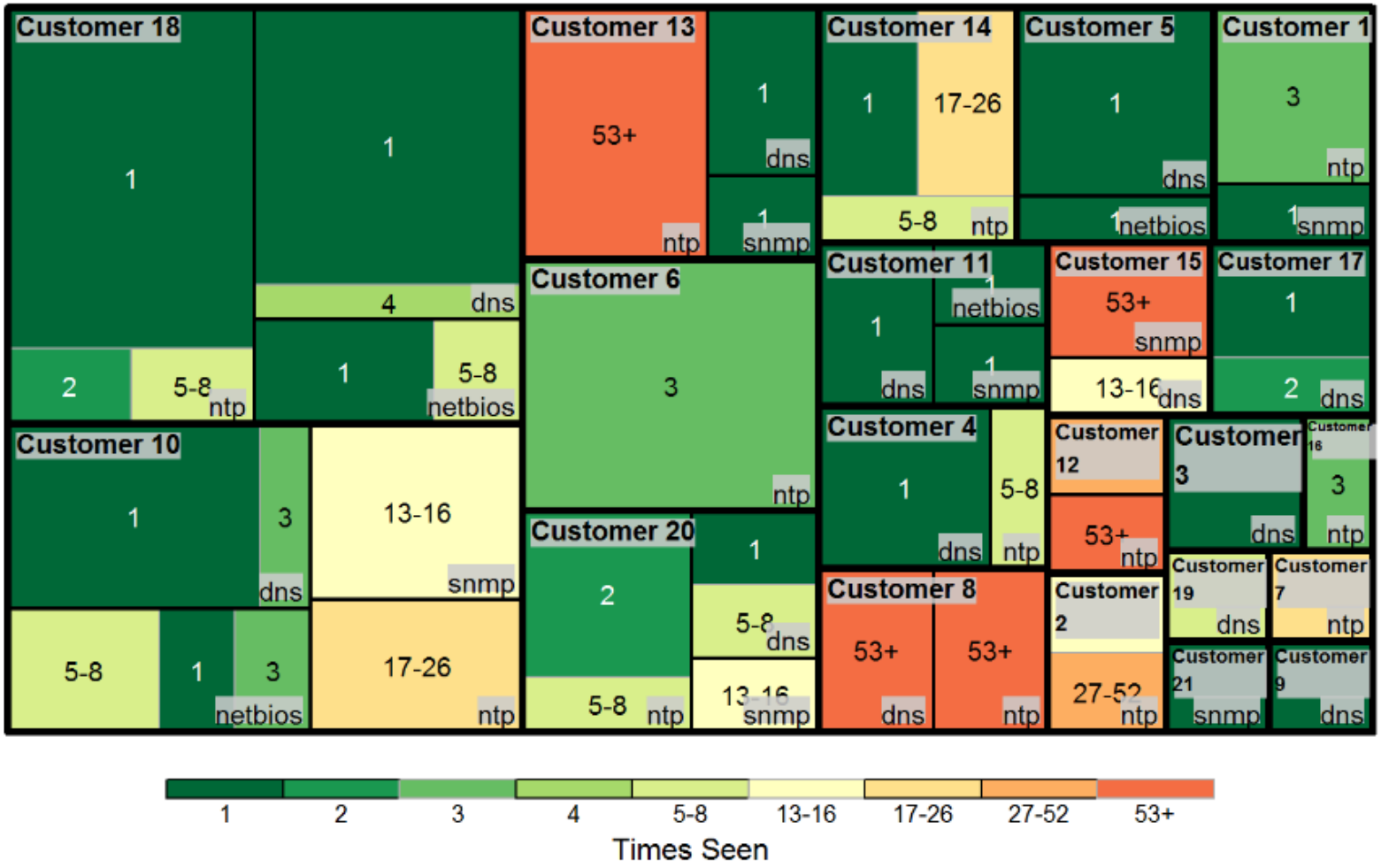
PARTNERS

Federal agencies, domestic partners, international CERT community

OUR FOUNDATION

NCTNS Municipal Stats Since 2013

Vulnerable Service Events - Government (Municipal)



ps.cyberincident-cyberincident.sp@canada.ca

www.publicsafety.gc.ca/ccirc