DATA SCIENCE OR BLACK MAGIC – CYBERSECURITY THREATS IN CANADA

BCNET Conference – April 24th, 2018

Shawn Beaton

cira

BUILDING A BETTER ONLINE CANADA

.CA

2.7 million .CA domains with 100% uptime.

Cybersecurity Services

100,000 new cybersecurity threats blocked daily by D-Zone Firewall.

Registry Services

Robust top-level domain products and services.

We support initiatives that enhance Canadians' Internet experience:

Global Internet Leadership	• Support internet governance and standards through global organizations such as ICANN and CENTR
Canadian Initiatives	• **11** Internet Exchange Points nation-wide • **280,000+** internet performance tests conducted last year
Community Initiatives	• More than **$4.2 million** in grants to **102** projects through our Community Investment Program

~~BOTNETS~~, ~~DATA BREACHES~~, ~~DDOS~~, ~~RANSOMWARE~~, BITCOIN MINING IS THE NEW BLACK*

Low cost + easy money = perfect storm

What everyone is seeing

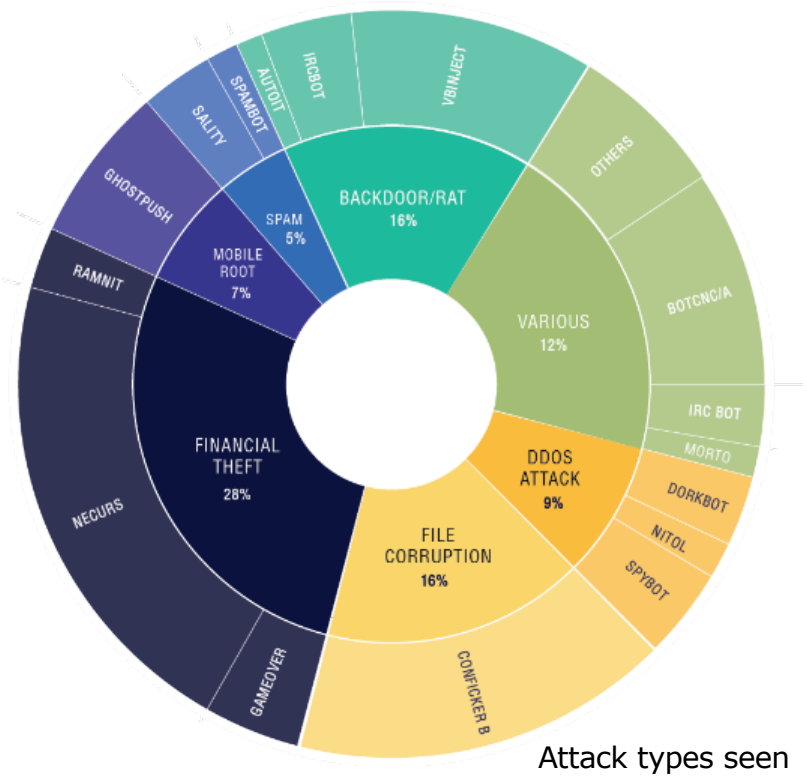
- ✓ Ransomware like Locky, CryptXXX, Cerber, Ghost Push, SAMSAM, Spora, Wannadie, SurLOcker (the list goes on and on) provide "professional" tools for hackers…and attacks have grown 752%
- ✓ Tools like Locky and Goldeneye are estimated to have raked-in $1 billion in 2017

What CIRA saw

- ✓ Botnets are on the rise with malicious queries across our global network reaching 101 million daily queries in Spring 2017[1]

1 Nomimum data science Q3 2017 security report

THEFT IS A TOP MOTIVATOR BUT THE REST OF THE "THREAT PIE" IS GROWING TOO



Attack types seen

CANADIAN PERSPECTIVE

- Cybersecurity costs us an estimated $2 billion
- Failed cybersecurity results in lost productivity
- Failed cybersecurity has out of pocket costs

IT WORLD CANADA

Follow

Search

CIO SECURITY MOBILE CLOUD AI RESEARCH EVENTS NEWS VIDEO BLOGS MORE SUBSCRIBE

Image by Daoleduc via GettyImages.ca

PRIVACY SECURITY

Canadian firm pays $425,000 to recover from ransomware attack

Howard Solomon @howarditwc
Published: July 13th, 2017

A major Canadian company was forced to pay $425,000 in Bitcoin over the weekend to restore its computer systems after suffering a crippling ransomware attack that not only encrypted its production databases but also the backups as well.

"They literally had no choice but to pay" because the backups were frozen, said

CYBERSECURITY INTERNET STATISTICS

Q3 2017 DDoS Attacks Key Facts

- Gaming top targeted industry
- Top target – 612 attacks (avg 7 / per day)

Compared to Q3 2016 (Yr Over Yr)

3%↓ Total DDoS attacks

2%↓ Infrastructure layer (3 & 4) attacks

2%↓ Reflection-based attacks

20%↑ Average number of attacks per target

Compared to Q2 2017 (Qtr Over Qtr)

8%↑ Total DDoS attacks

8%↑ Infrastructure layer (3 & 4) attacks

4%↑ Reflection-based attacks

13%↑ Average number of attacks per target

Q3 2017 Web Application Attacks Key Facts

- SQLi & LFI attacks – 85% of web app attacks
- USA top target **AND** sourced country

Compared to Q3 2016 (Yr Over Yr)

69%↑ Total web application attacks

217%↑ Attacks sourcing from the U.S.

62%↑ SQLi attacks

Compared to Q2 2017 (Qtr Over Qtr)

30%↑ Total web application attacks

48%↑ Attacks sourcing from the U.S.

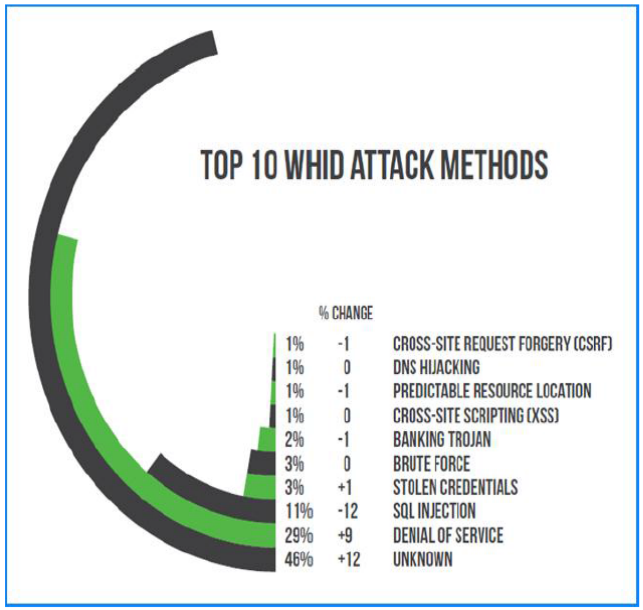
19%↑ SQLi attacks

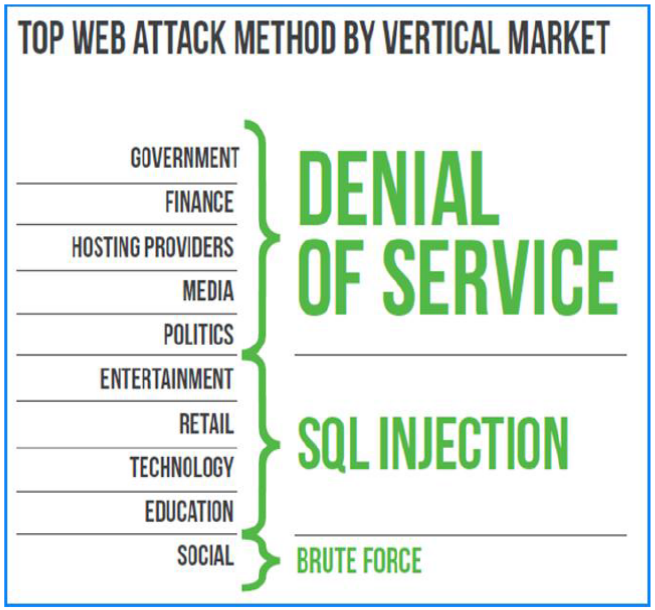
ATTACKS ARE HAPPENING EVERYWHERE

Attacks are sophisticated and varied…

…industry agnostic…

…and easier to organize, command and control



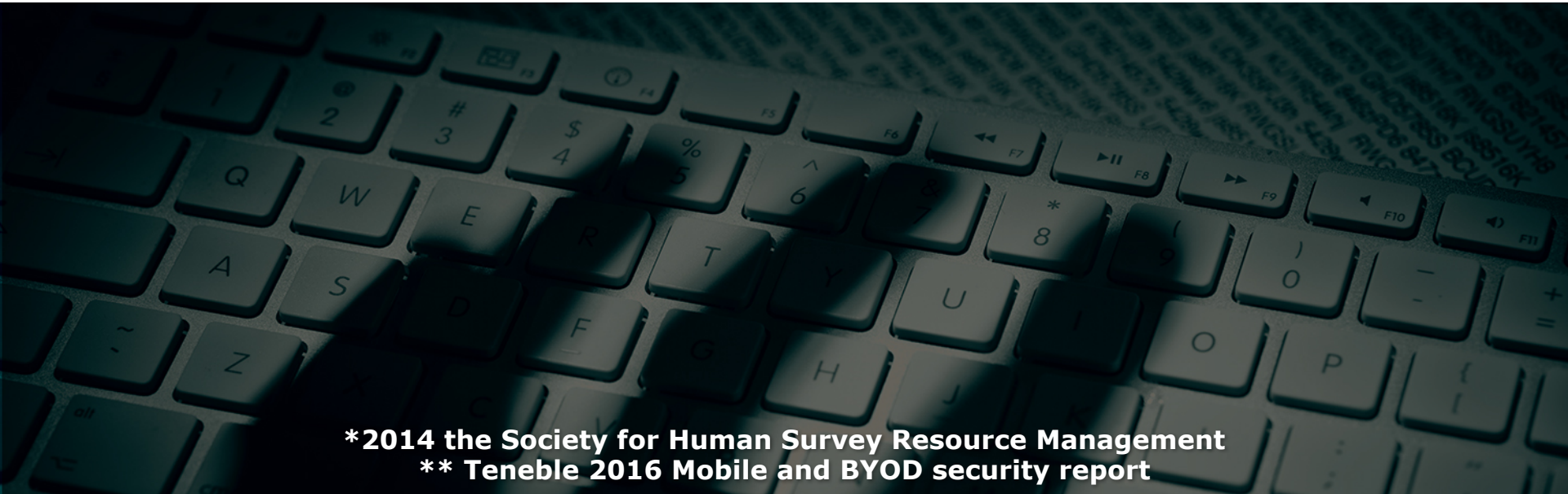


Source: Trustwave 2013 Global Security Report

Layers 3-5, Layer 7, DNS, Direct-to-Origin, Large, Small & Stealthy

HOME OFFICE WORKERS: BYOD AND SHADOW IT

- Telecommuting is offered by **59%** of companies*
- Full time telecommuting up by 20 percent
- **72%** of organizations offer at least some BYOD**
- Home users install all kinds of things on their home networks, part of the shadow IT dilemma



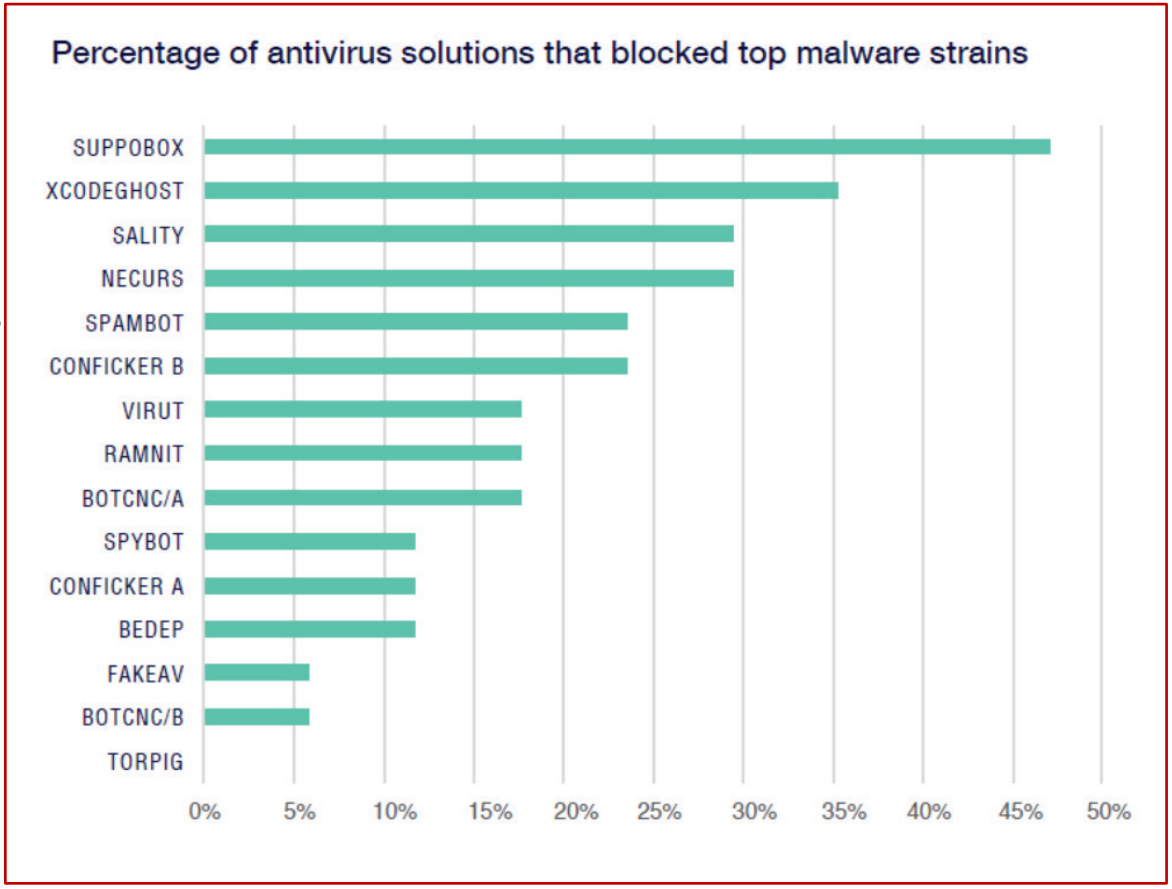
***2014 the Society for Human Survey Resource Management**
**** Teneble 2016 Mobile and BYOD security report**

"As a good Canadian dresses in layers…

…so too needs to be their cybersecurity"

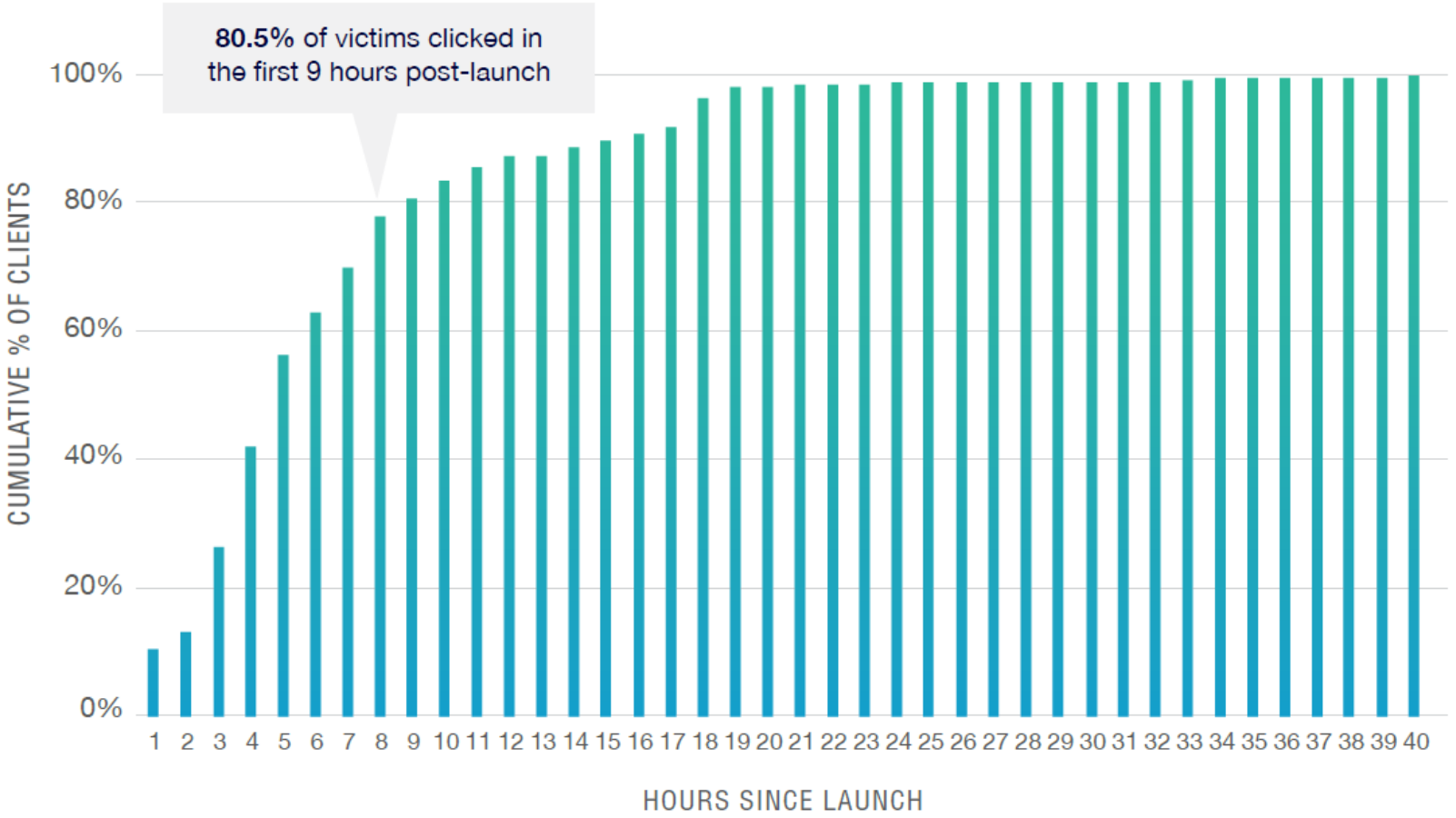
DEFENCE IN DEPTH

- Every security tool responds differently to threats
- During a zero-day situation there is a global fog-of-war
- Having multiple defensive layers is a recommended best practice to protect your organization



Think antivirus is good enough? We analyzed top solutions to see how effective they were at blocking malware

SPEED SAVES



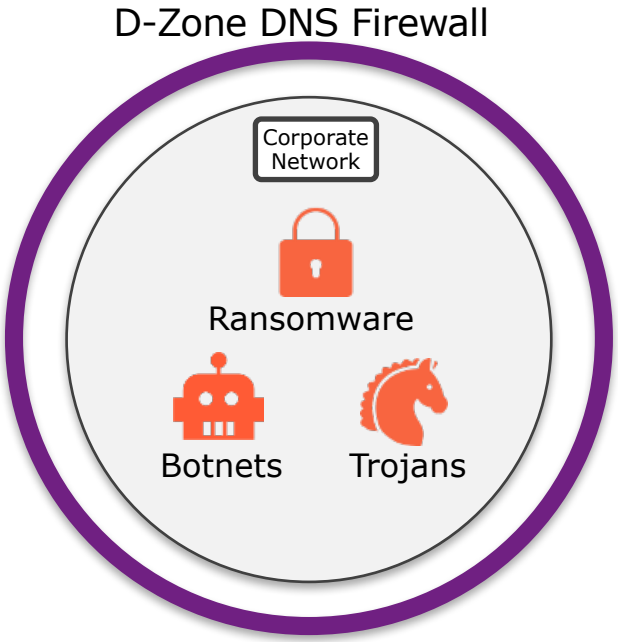
"Being able to block new threats as they come in has reduced our impacted user rate by 80 - 90%"

– Trent University

THE THREAT IS ALREADY INSIDE

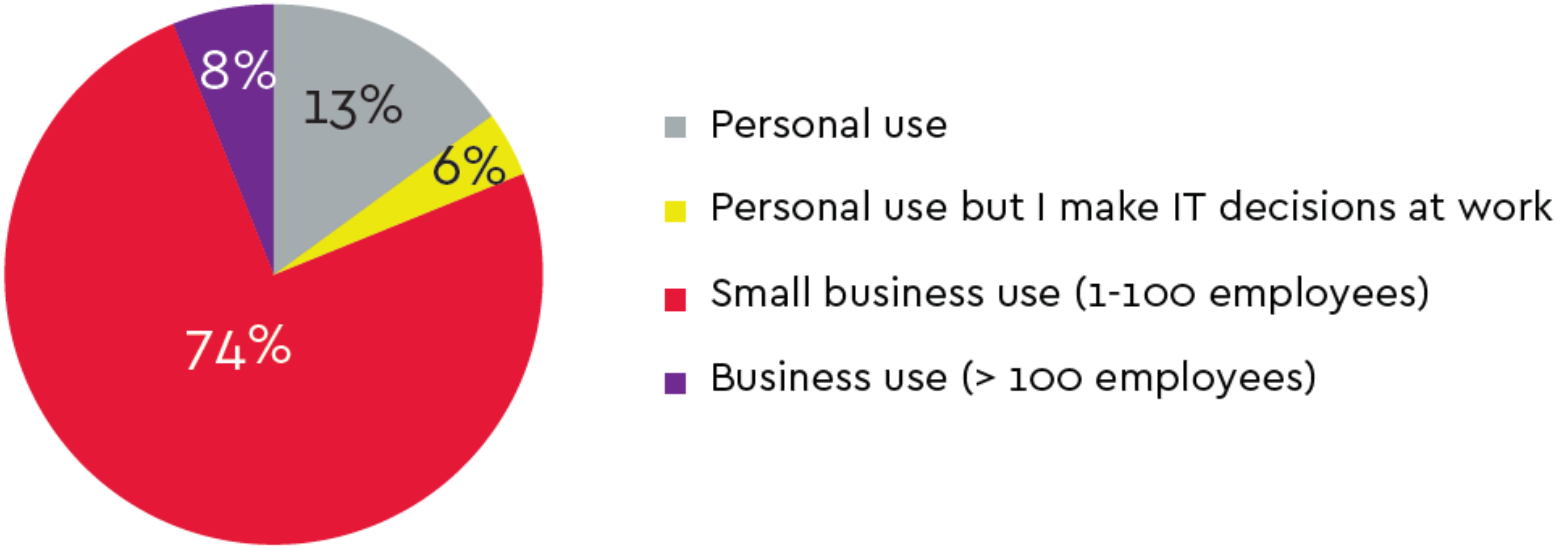
- 100% of organizations that have deployed D-Zone DNS Firewall already had undetected malware and botnets on their network – some very serious like key-loggers

- D-Zone picked-up the malware as it tried to call home to the host server

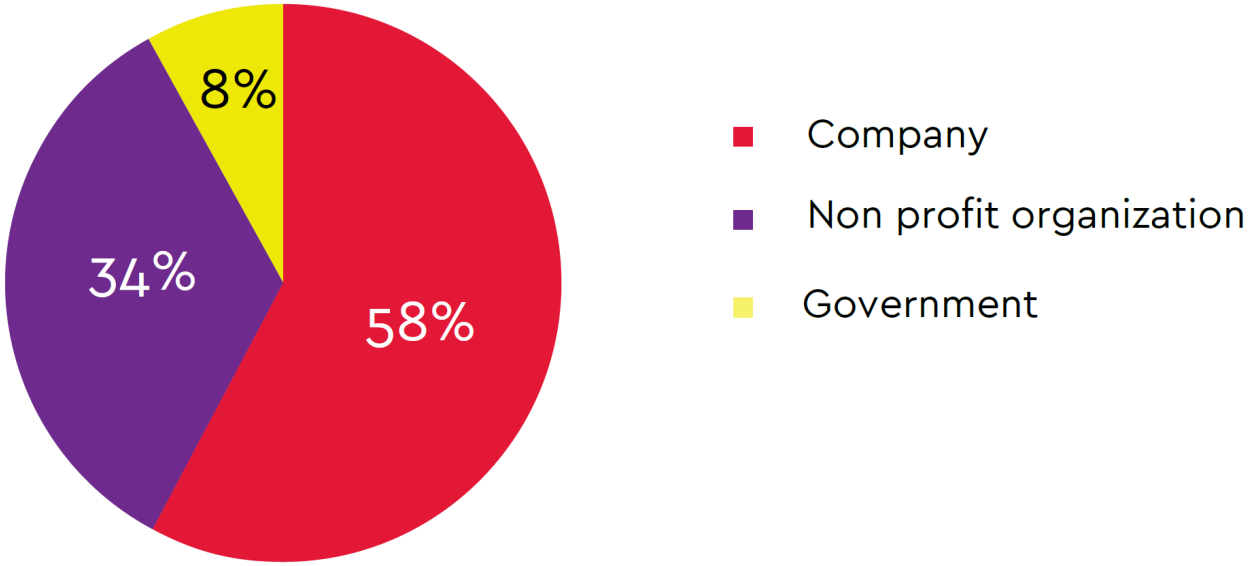


CIRA CYBERSECURITY SURVEY - RESPONDENT BREAKDOWN

We asked questions relevant to the circumstances of the respondents



ORGANIZATIONAL TYPES RESPONDING



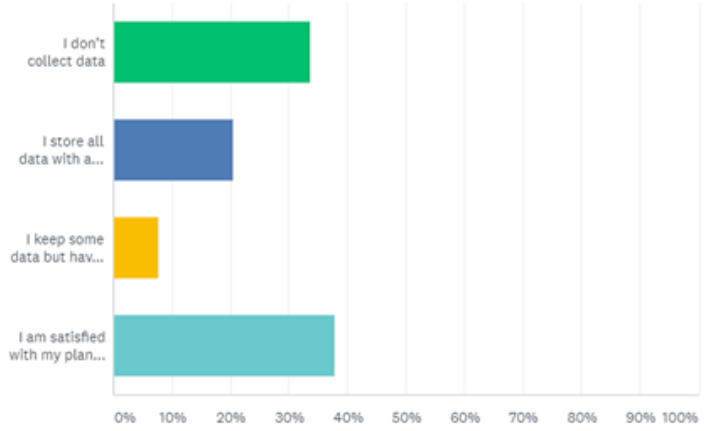
SUMMARY OF CONCLUSIONS

- ✓ Awareness of threats is high
- ✓ Concern about threats is high
- ✓ Cyber-attacks are having a real impact
- ✓ Most individuals are living on a hope and prayer
- ✓ Organizations are using several cybersecurity solutions
- ✓ The bad guys are still getting in

DATA CONCERN

Some organizations don’t appear to have a concern about customer data – will new PIPEDA* rules change this?

If you collect and store customer data electronically, do you have documented plans to keep it secure? Select the option that best describ you.



ANSWER CHOICES	RESPON
I don't collect data	33.68%
I store all data with a service provider like a hosting company, cloud accounting company (like Freshbooks) or online storefront provider (like Shopify) so I don't have security documents and plans	20.52%
I keep some data but have no documented plans to secure it and don't know where to start – it worries me	7.84%
I am satisfied with my plans to keep the customer data I store safe	37.96%
TOTAL	

*The Personal Information Protection and Electronic Documents Act (PIPEDA) - amendments related to **mandatory reporting** have been passed in the Digital Privacy Act, 2015. These amendments may come into effect sometime this year or next. GDPR in Europe already has this.

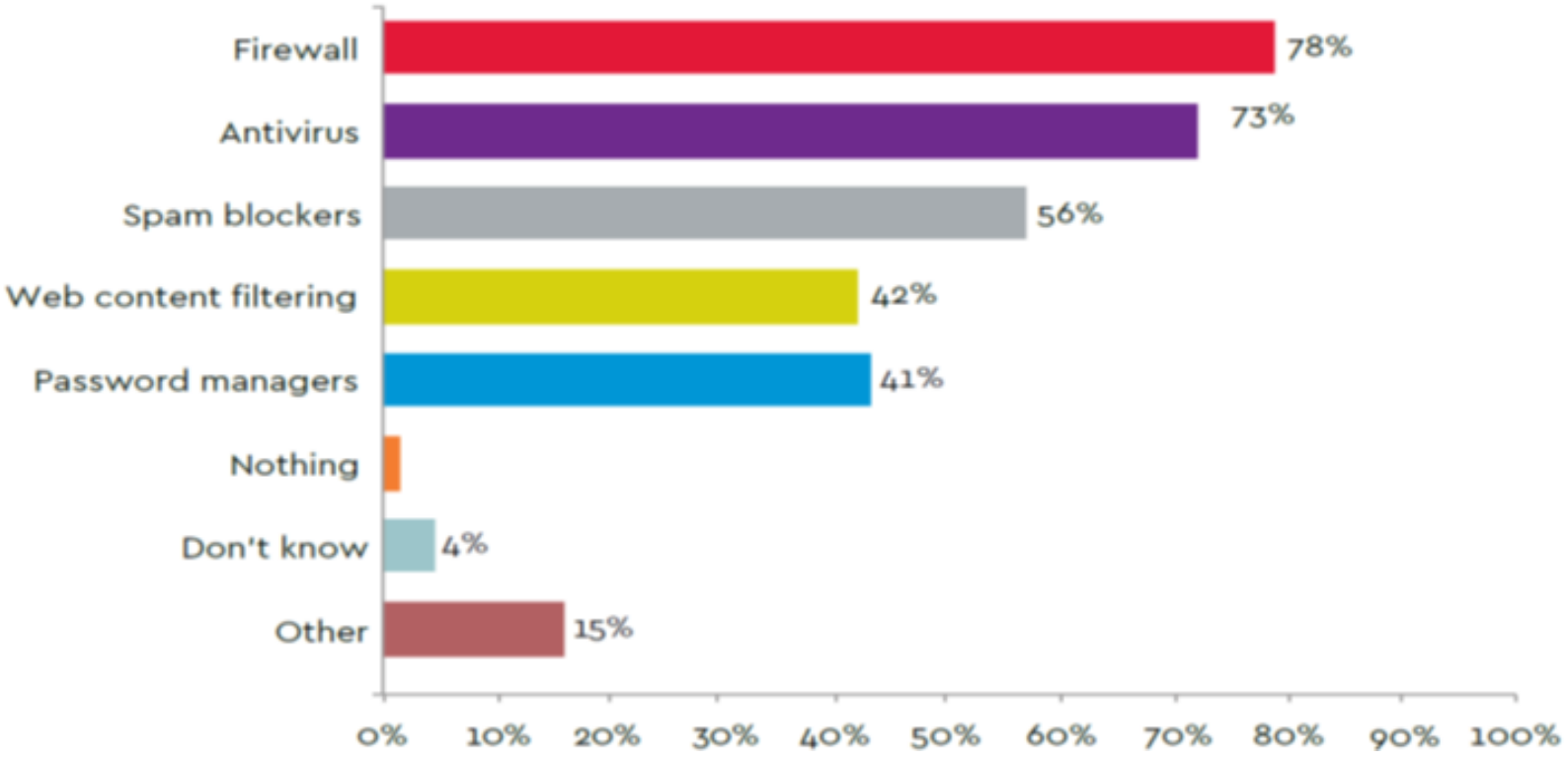
WHAT WE KNOW

79% of companies collect data from individuals.

21% of users trust companies with their data

- BSI Group

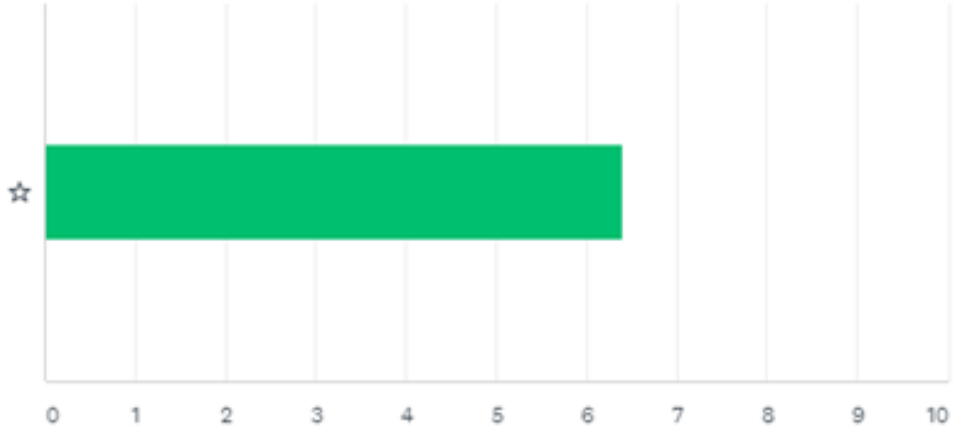
LARGER ORGANIZATIONAL LAYERS



- Larger organizations report 2X more problems
- With money to invest in application and data-layer security it is no surprise that the #1 reported layer is endpoint security (i.e. stopping humans from messing-up)

CONFIDENCE IN PLATFORMS VS. MALWARE

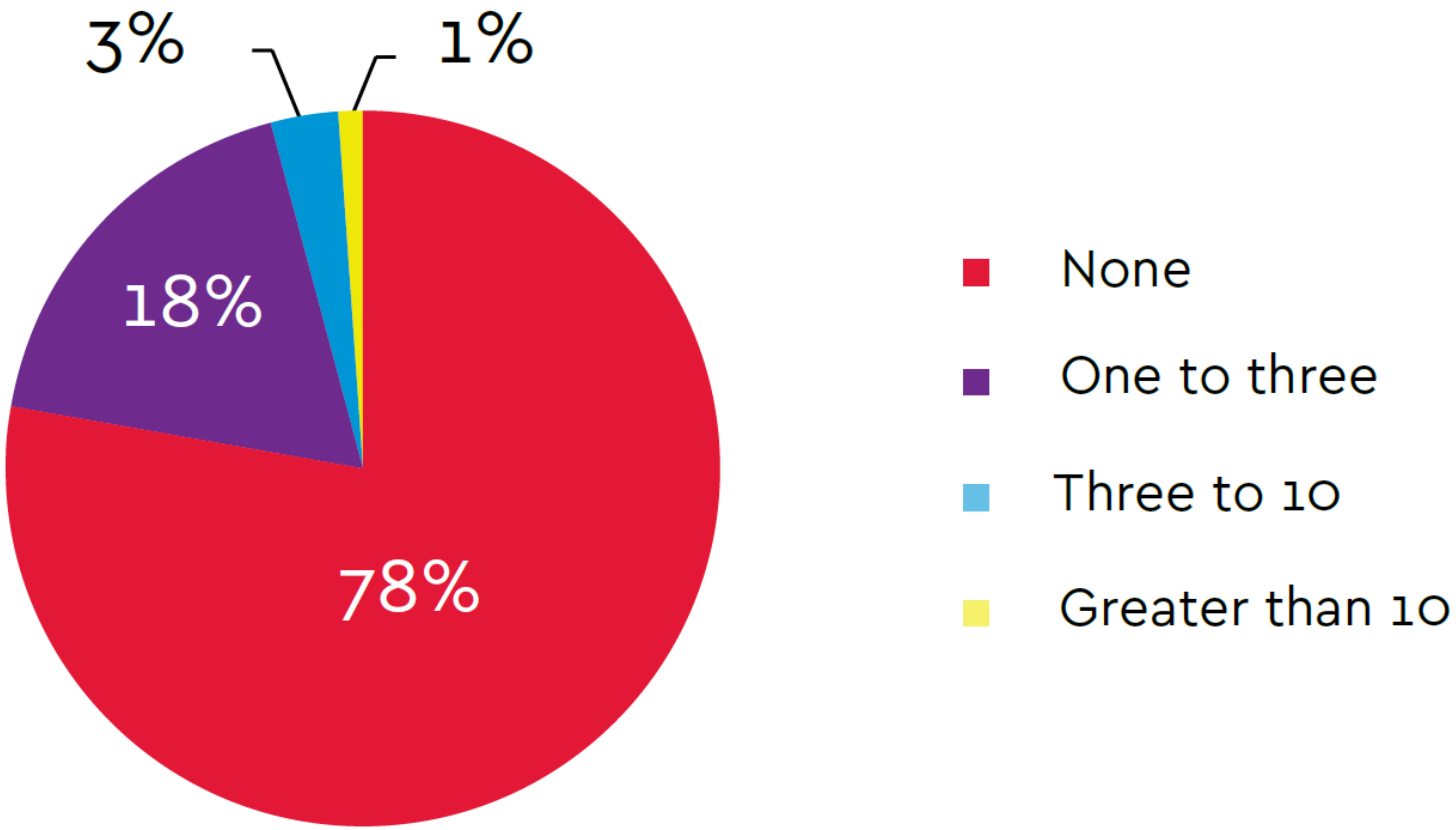
How confident are you in your security tools to protect you from malware and phishing?



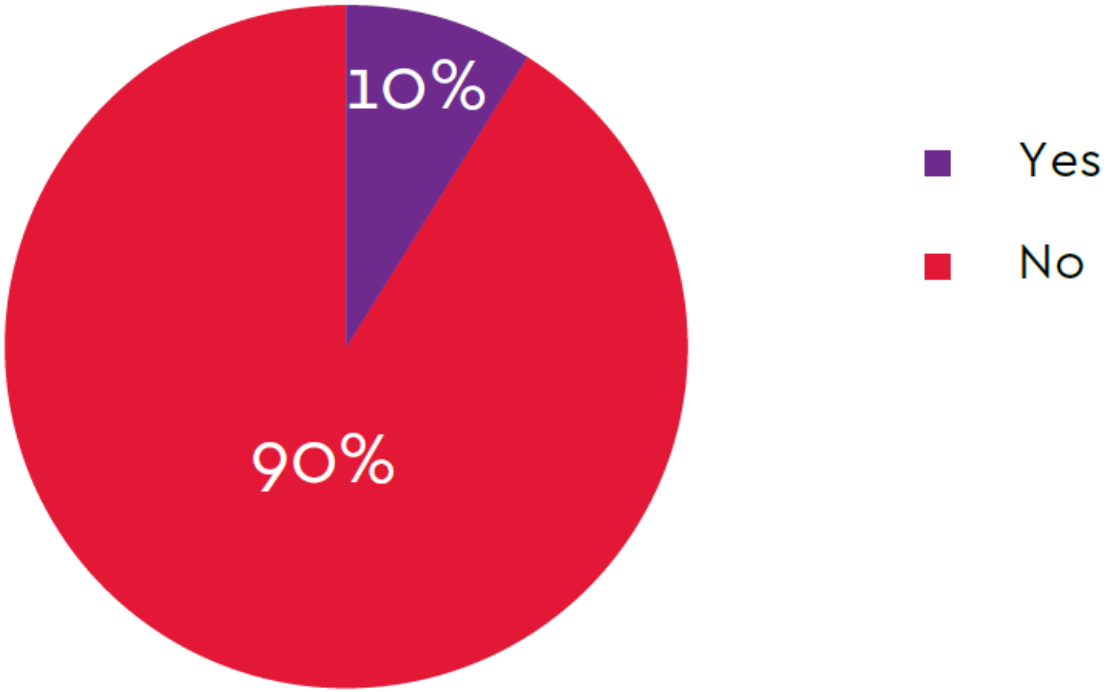
	OUR INVESTMENT IS NOT ENOUGH TO BE CONFIDENT	(NO LABEL)	(NO LABEL)	(NO LABEL)	SOMEWHAT CONFIDENT	(NO LABEL)	(NO LABEL)	(NO LABEL)	(NO LABEL)	VERY CONFIDENT
☆	3.96% 8	1.49% 3	4.95% 10	5.94% 12	20.30% 41	10.89% 22	16.83% 34	18.32% 37	8.91% 18	8.42% 17

DDOS ATTACKS IN THE LAST 12 MONTHS

22% of organizations experienced a user-impacting DDoS attack

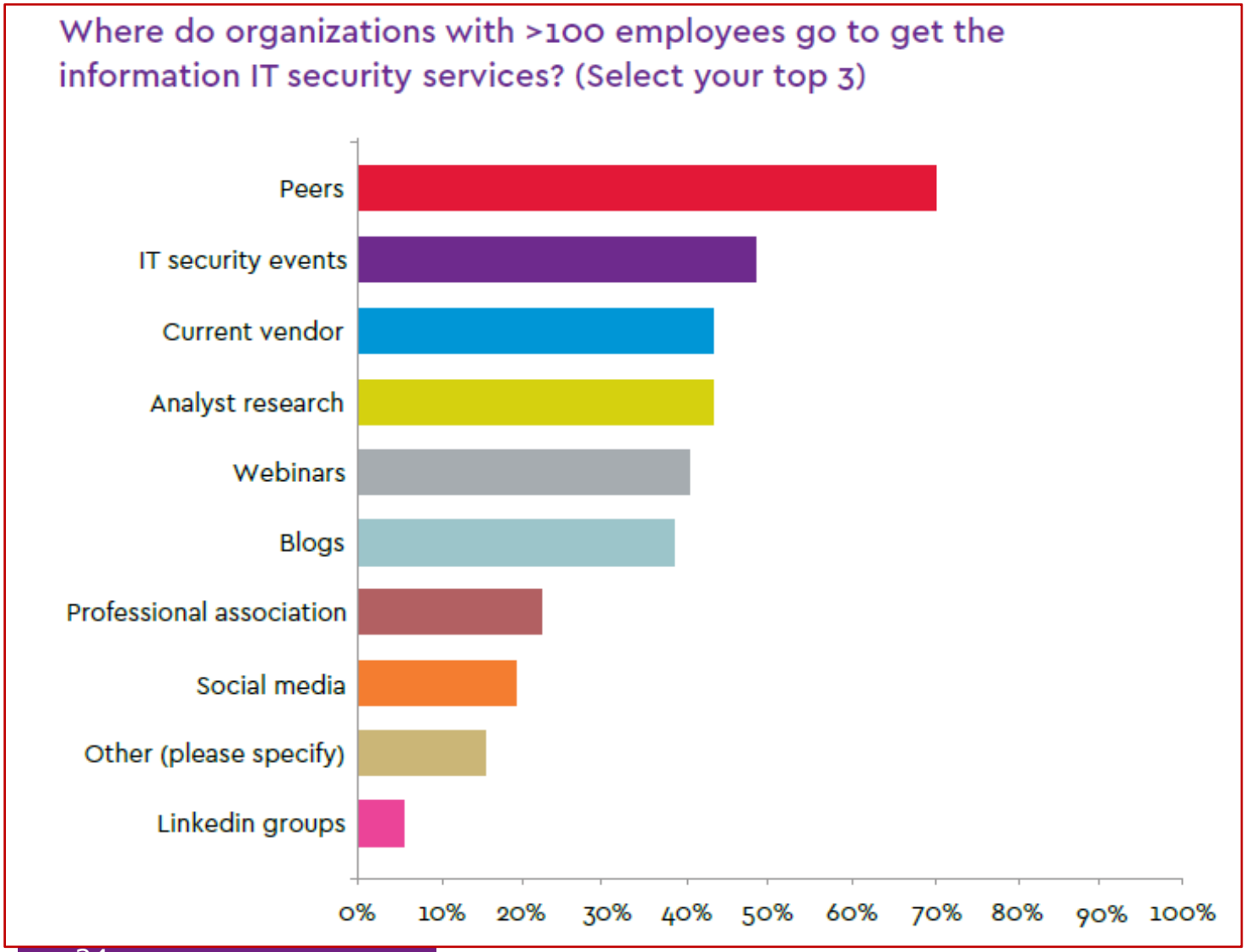


10% OF ORGANIZATIONS HAVE HAD THEIR ONLINE PRESENCE BROUGHT DOWN IN THE LAST 24 MONTHS



32% OF ORGANIZATIONS REPORT AN EMPLOYEE GAVE AWAY INFORMATION IN A PHISHING ATTACKB

WHERE DO IT PEOPLE REPORT GOING TO LEARN



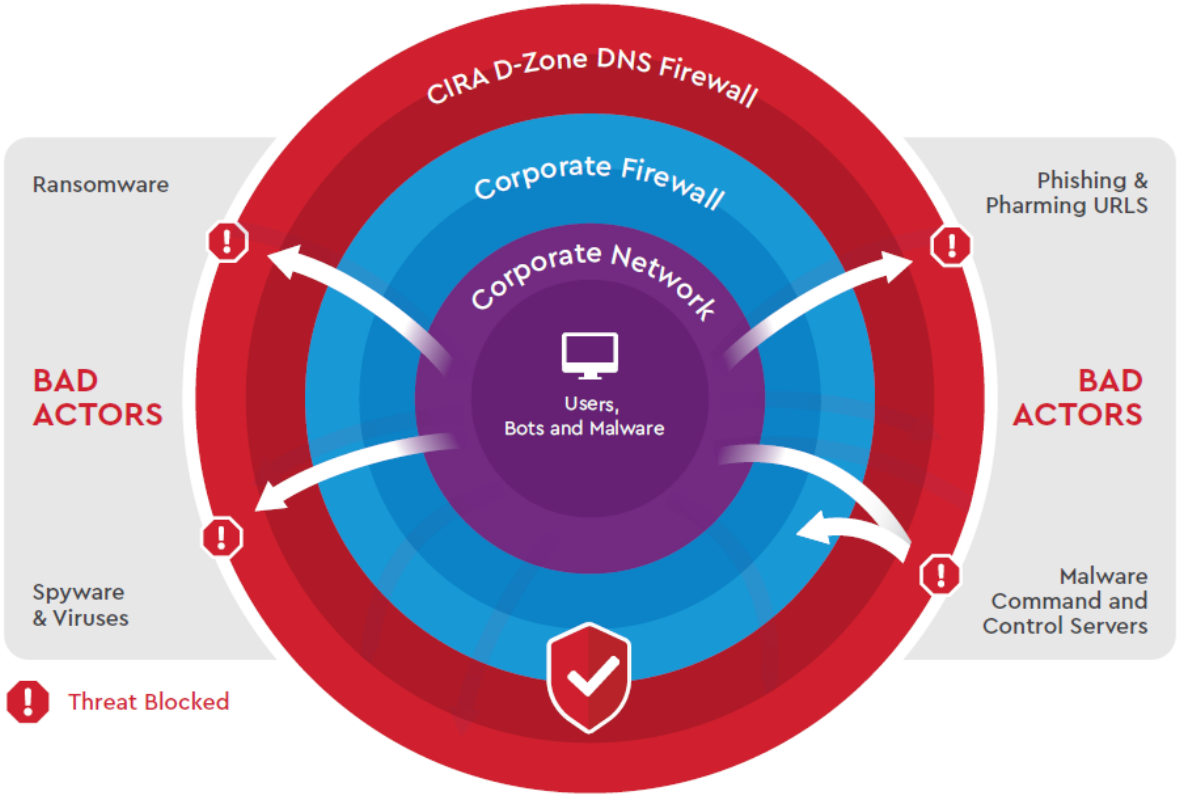
It is getting late, so let’s wrap this up

SUMMARY

We aren’t winning and it is costing us a lot of resources

- Organizations are investing a lot in security
- The bad guys are still getting in. Organizations report:
  - 19% report successful ransomware attacks
  - 22% report successful DDoS attacks
  - 32% report successful phishing attacks

AND NOW A MESSAGE FROM OUR SPONSOR



Detect

Real time and historical analysis of global DNS data to detect security threats

Feed

Policy enabled recursive DNS servers are updated with real-time threat feeds

Enforce

Servers examine DNS transactions and block domain and IP security threats and filtered sites and categories

Report

Malicious activity is identified and reported

Mitigate

Locate and quarantine infected devices

IN THE NEWS THIS WEEK

IT WORLD CANADA

CIO SECURITY MOBILE CLOUD AI RESEARCH EVENTS NEWS VIDEO BLOGS MOR

Image by Monsitj from GettyImages.ca

PRIVACY SECURITY TELECOMMUNICATIONS

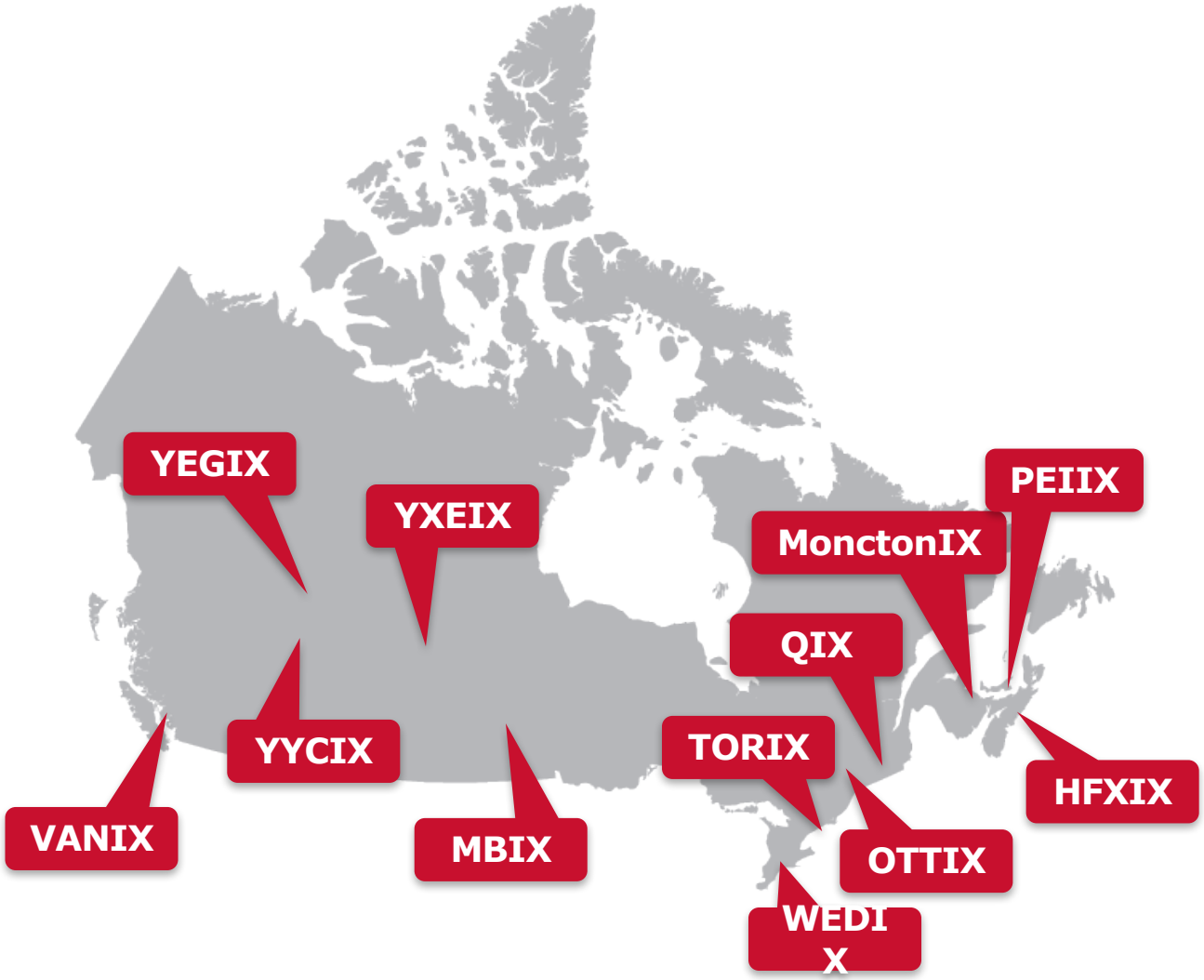
Canadian IXPs join secure routing initiative to close Internet loopholes

Howard Solomon @howarditwc
Published: April 23rd, 2018

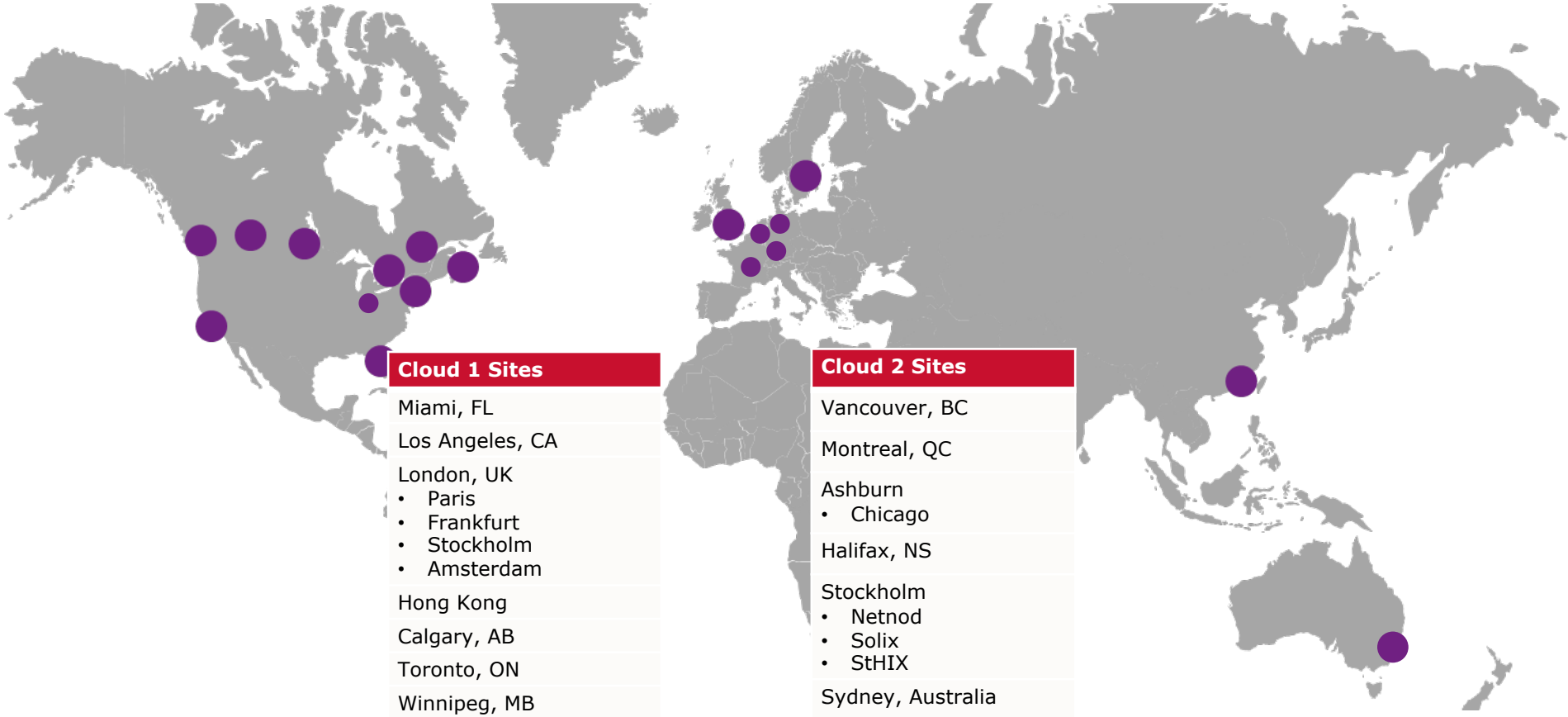
CIRA HELPS BRING THE INTERNET TO CANADA

Helping support a cross-country network of Internet Exchange Points

- ✓ Faster
- ✓ More Reliable
- ✓ Sovereign



A GLOBAL DNS SERVICE FOR CANADA



Cloud 1 Sites
Miami, FL
Los Angeles, CA
London, UK • Paris • Frankfurt • Stockholm • Amsterdam
Hong Kong
Calgary, AB
Toronto, ON
Winnipeg, MB

Cloud 2 Sites
Vancouver, BC
Montreal, QC
Ashburn • Chicago
Halifax, NS
Stockholm • Netnod • Solix • StHIX
Sydney, Australia

D-ZONE DNS FIREWALL KEY BENEFITS

A cloud-based firewall that uses the DNS to block malware

- ✓ Blocks users from clicking on nefarious urls
- ✓ Blocks malware that gets on your network from calling out to its command and control servers
- ✓ Located in Canadian data centers for performance and data sovereignty
- ✓ Unique data science adds over 100,000 new malicious domains every single day

Questions?