www.pwc.com/ca/security

Turnaround and transformation in cybersecurity

Key findings from The Global State of Information Security® Survey 2016 – Canadian Insights

Dec 2, 2015

Presented by:
Richard Wilson, Cybersecurity & Privacy Consulting

Methodology

The Global State of Information Security® Survey (GSISS) 2016, a worldwide study by PwC, *CIO* and *CSO*, was conducted online from May 7, 2015 to June 12, 2015.

- Readers of *CSO* and *CIO* and clients of PwC from 127 countries
- 37% respondents from North America, 30% from Europe, 16% from Asia Pacific, 14% from South America and 3% from the Middle East and Africa

www.pwc.com/gsiss

The Global State of Information Security® Survey 2016

10,040

Respondents

- 51% C-suite level
- 15% Director level
- 34% Other (e.g. Manager, Analyst, etc.)
- 39% Business and 61% IT (18% increase compared to 2014)

17

Industries represented

Top 5

- 22% Technology
- 10% Financial Services
- 8% Consulting/Prof. Services
- 7% Engineering/ Construction
- 7% Consumer Products & Retail

Reported annual revenues

- 34% at least US$1B
- 48% US$25 to $999M
- 26% less than US$100M
- 3% non-profit

Profile of Canadian respondents

157

Respondents

- 35% C-suite level
- 25% Director level
- 40% Other (e.g. Manager, Analyst, etc.)
- 34% Business and 66% IT (17% increase compared to 2014)

17

Industries represented

Top 5

- 19% Technology
- 12% Financial Services
- 9% Engineering/ Construction
- 9% Government Services
- 8% Agriculture

Reported annual revenues

- 31% at least US$1B
- 52% $25 to US$999M
- 21% less than US$100M
- 4% non-profit

Canadian insights:
Key themes and findings

4 global cybersecurity trends

1 ***Board Uncertainty:***
Driving cybersecurity as a strategic priority

2 ***Evolving goals of Threat Actors:***
Monitize data, organized hacktivism, reputational attacks, competitive advantage, 4th theatre of combat

3 ***Competition for resources:***
Supply and demand is out of balance

4 ***Technical Interconnection:***
Creating opportunity while balancing risks

2016 Canadian insights at a glance

160% increase in **detected incidents** in Canada (over 2014)

Incidents attributed to **foreign nation-states** increased the most (up **67%** over 2014) while **employees** continue to be the most cited **source of incidents** (**66%**)

Customer records continue to be the most targeted data (**36%**)

Attacks on IoT devices and systems are on the rise

Security spending increased by **82%** over 2014, currently at **5%** of IT spend

Average **financial loss** due to detected incidents is **$1M** (**18%** decrease from 2014)

Organizations are investing in core safeguards to better defend their ecosystems against evolving threats

65% **58%**

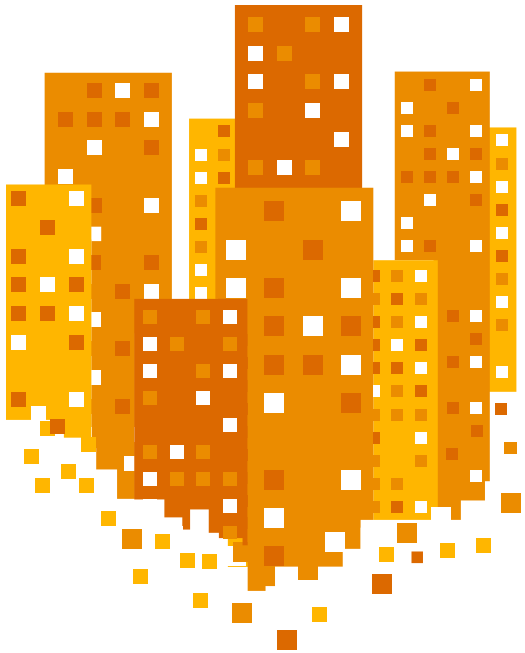
Have an overall information security strategy

57% **53%**

Employee training and awareness programs

55% **52%**

Have security baselines / standards for third parties



50% **54%**

Have a CISO in charge of security

50% **49%**

Conduct threat assessments

54% **48%**

Active monitoring analysis of security intelligence

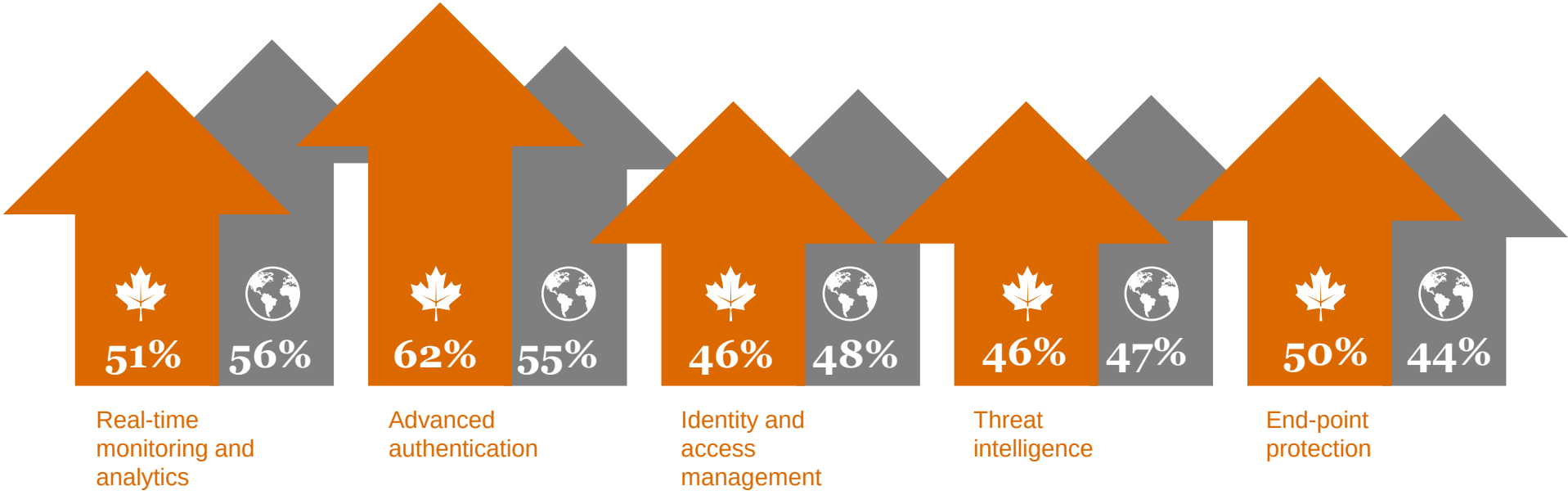
Risk-based frameworks can help organizations to design, measure and monitor progress towards an improved cyber program

	Canada	Global
NIST Cybersecurity Framework	41%	35%
ISO27001	29%	40%
SANS Critical Controls	24%	28%
ISF Standard of Good Practice	22%	26%
Other	17%	18%
None	8%	8%
Do not know	13%	11%

Cloud-based security services provide advanced capabilities that are scalable, quicker to deploy, cost-effective and reduce need for in-house expertise

64% ***Use cloud-based cybersecurity services***
(vs 69% globally)

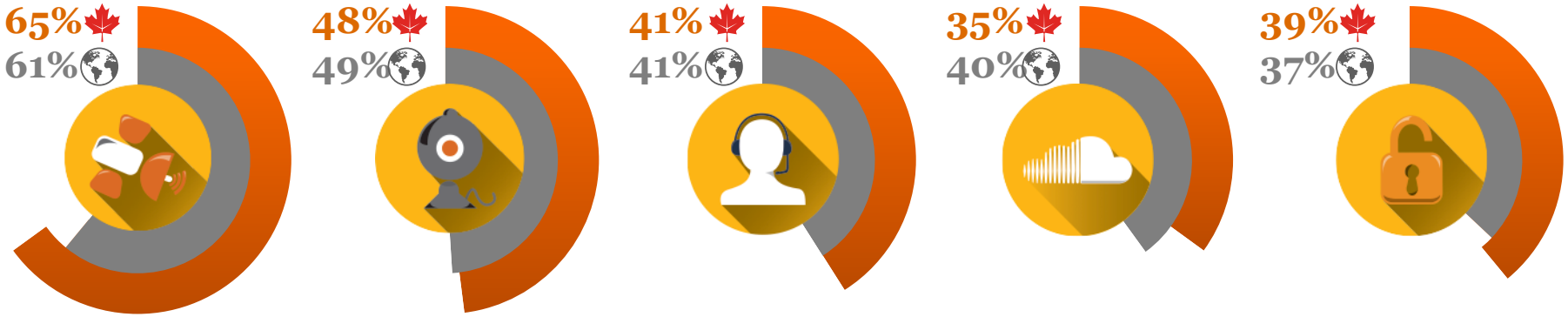
Adoption of cloud-based cybersecurity services



Growing number of organizations are using big data analytics for cybersecurity

54% ***of Canadian respondents use big data analytics for cybersecurity*** (vs 59% globally)

Benefits of data-driven cybersecurity



Better understanding of external threats

Better understanding of internal threats

Better understanding of user behaviour

Better visibility into anomalous network activity

Improved ability to quickly identify & respond to security incidents

Advanced authentication is replacing passwords to improve trust and experience for customers, employees and business partners

	Canada	Global
Software tokens	61%	63%
Hardware tokens	59%	61%
Cryptographic keys	60%	61%
Biometrics (fingerprints, etc.)	42%	59%
Multifactor authentication	57%	53%
Smartphone tokens	48%	50%
Other	18%	22%

Over the past three years the number of organizations that embrace external collaboration has steadily increased

63%

of Canadian respondents formally collaborate with others in the industry on cybersecurity (up 28% from last year)

Benefits of external collaboration

62% 56%

Share & receive information from peers

40% 46%

Share & receive information from ISACs

46% 42%

Improved threat intelligence & awareness

42% 40%

Share & receive information with government

42% 37%

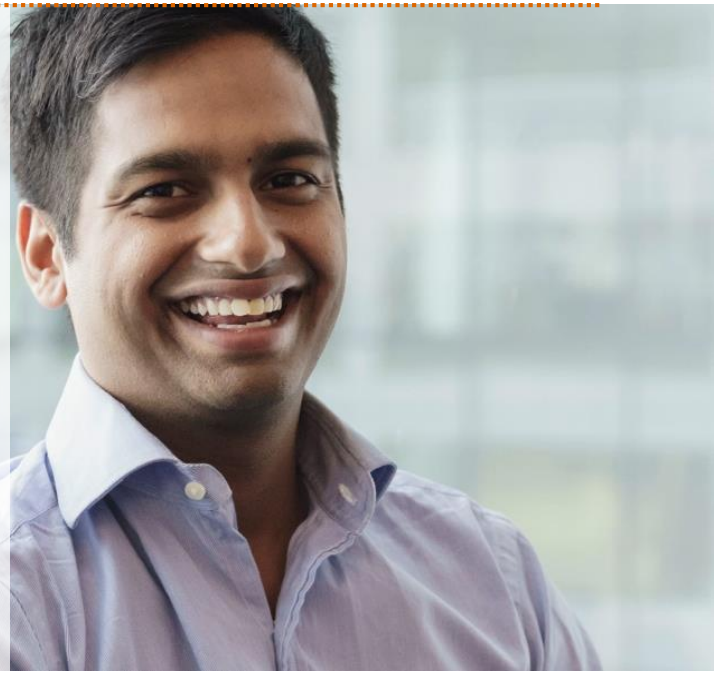
Share & receive information from law enforcement

Purchase of cybersecurity insurance is on the rise to mitigate the financial impact of security incidents

59% ***of Canadian companies have purchased cybersecurity insurance*** (up 32% from last year)

Incident-related losses covered by cybersecurity insurance

Personally identifiable information	**50%**	47%
Payment card data	**37%**	41%
Damage to brand reputation	**36%**	36%
Incident response	**28%**	31%



As organizations continue to grow through mergers and acquisitions, the cybersecurity practices and potential liabilities of a target company have become serious risks

78%

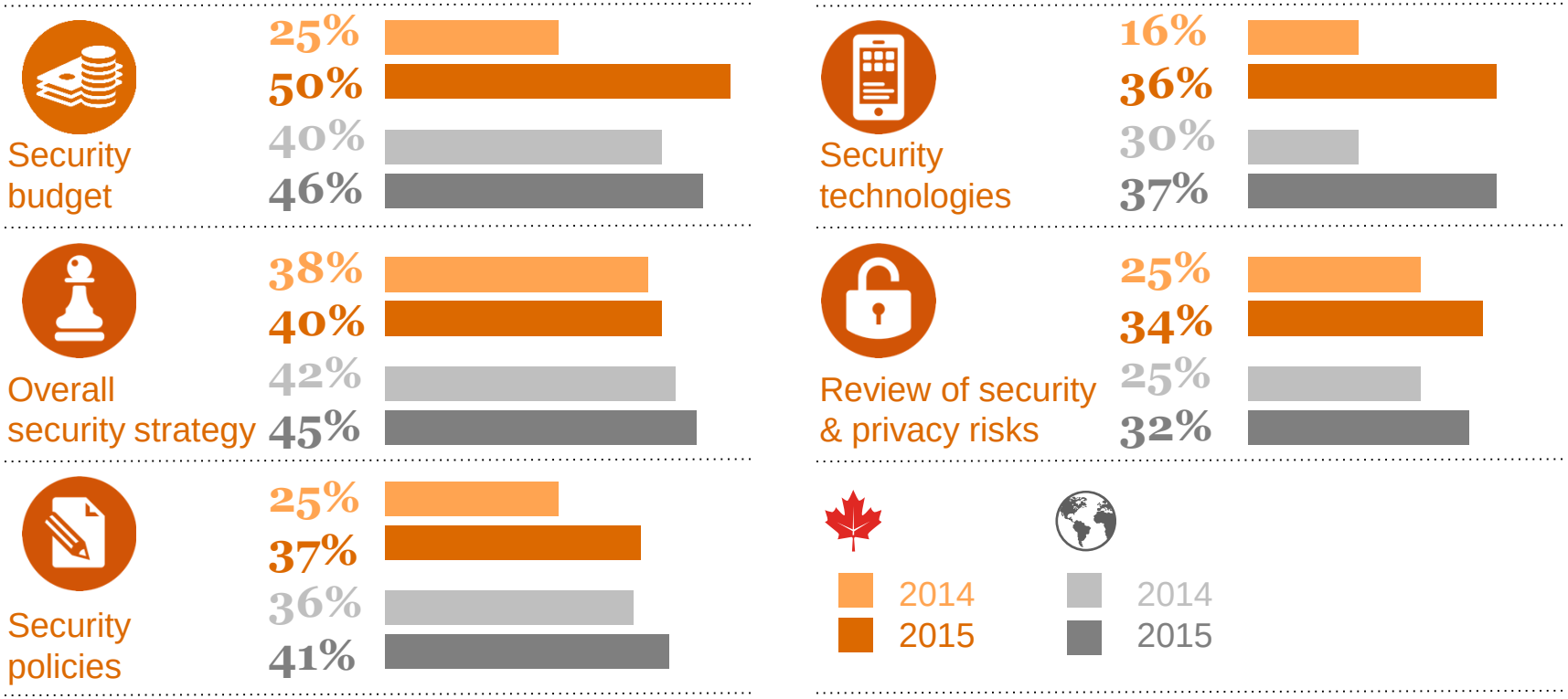
A Freshfields survey of 214 global dealmakers found that 78% of respondents believe cybersecurity is not analyzed in great depth or specifically quantified as part of the M&A process.

Cybersecurity risks of target companies should be considered across three areas:

1. The nations in which the target company is headquartered and operates
2. The industry in which the organization operates
3. The company's individual security practices and incident history

Board participation in cybersecurity programs continues to grow

Board participation in cybersecurity



For more information, please contact:

Richard Wilson, Partner, Consulting
+1 416.941.8374
richard.m.wilson@ca.pwc.com

Sajith (Saj) Nair, Partner, Consulting
+1 416 815 5185
s.nair@ca.pwc.com

David Craig, Partner, Risk Assurance
+1 416 814 5812
david.craig@ca.pwc.com

Lori-Ann Beausoleil, Partner, Forensics
+1 416 687 8617
lori-ann.beausoleil@ca.pwc.com

PwC simplifies complex cybersecurity challenges across the full spectrum of services for our clients:

- Strategy & Transformation
- Implementation & Operations
- Privacy & Consumer Protection
- Incident Response

Visit **www.pwc.com/gsiss** to explore the data further.
www.pwc.com/ca/security