IBM Security

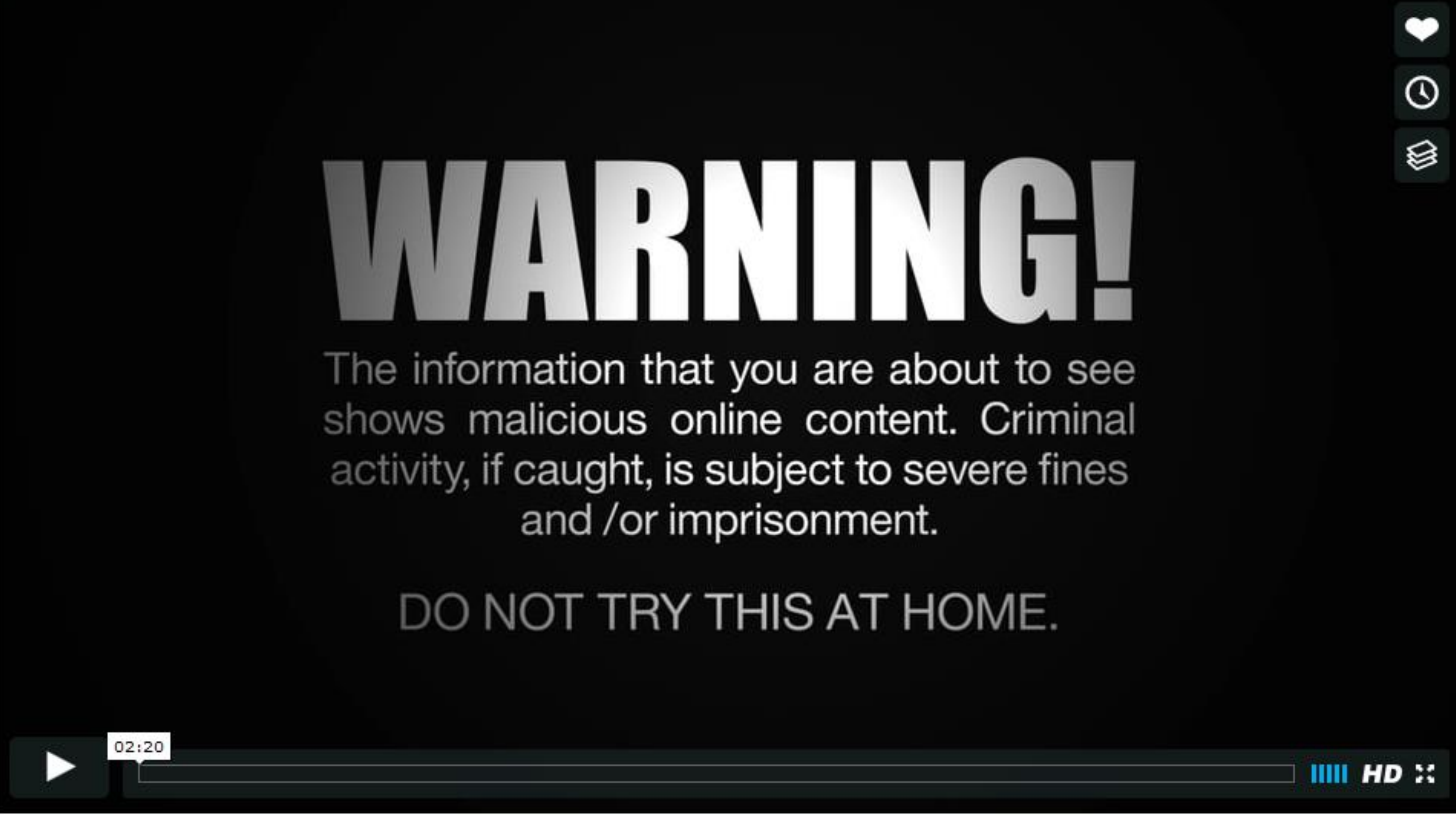
Outthink Threat: *Can Cognitive Change the Odds?*

Diana Kelley
Executive Security Advisor
@dianakelley14

February 2017

Agenda

- The “Game” has Changed
- Threat Trends
- Cost of Data Breach: Canada
- Security as an Immune System
- Cognitive: The Next Era



WARNING!

The information that you are about to see shows malicious online content. Criminal activity, if caught, is subject to severe fines and /or imprisonment.

DO NOT TRY THIS AT HOME.

IBM X-Force monitors and analyzes the changing threat landscape

Coverage

20,000+ devices under contract

15B+ events managed per day

133 monitored countries (MSS)

3,000+ security related patents

270M+ endpoints reporting malware

Depth

25B+ analyzed web pages and images

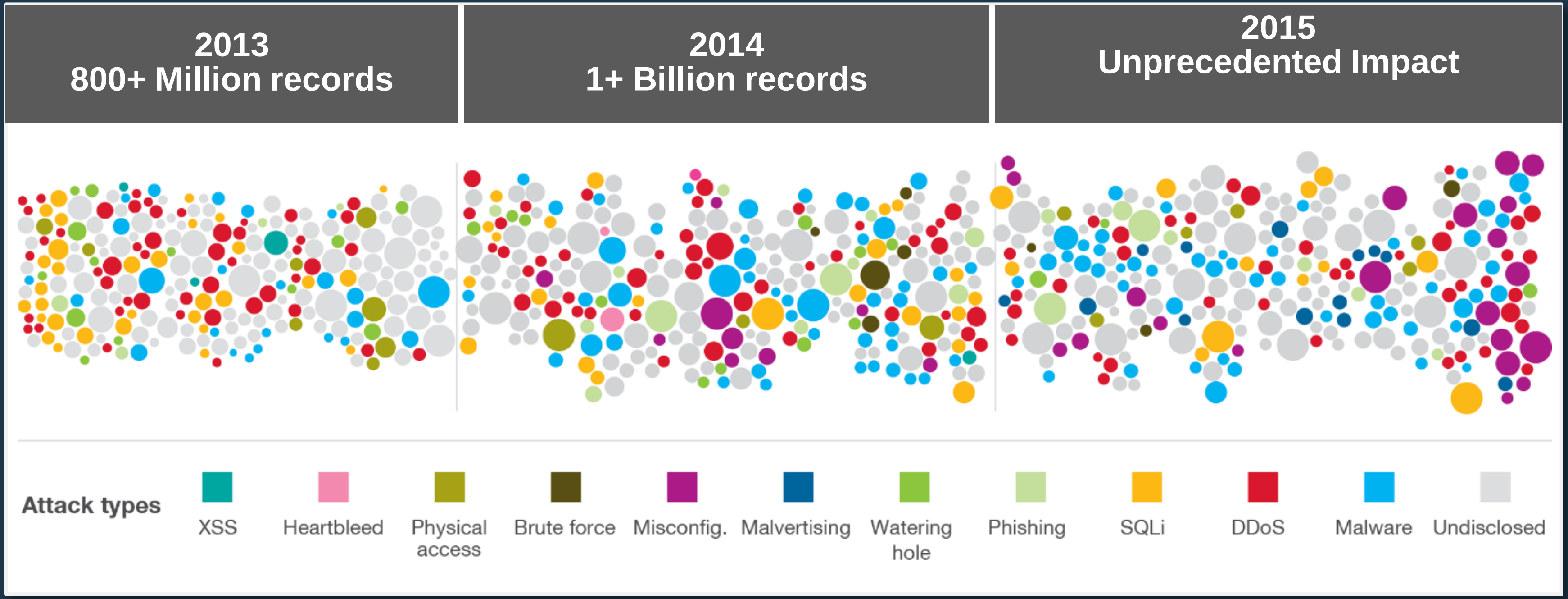
12M+ spam and phishing attacks daily

96K+ documented vulnerabilities

860K+ malicious IP addresses

Millions of unique malware samples

Breaches Continue to Increase



Healthcare mega-breaches set the trend for high value targets of sensitive information

average time to identify data breach

201 days*

average cost of a U.S. data breach

$7M*

*Source: Ponemon 2016 Cost of a Data Breach Study: Global Analysis

Key Trends

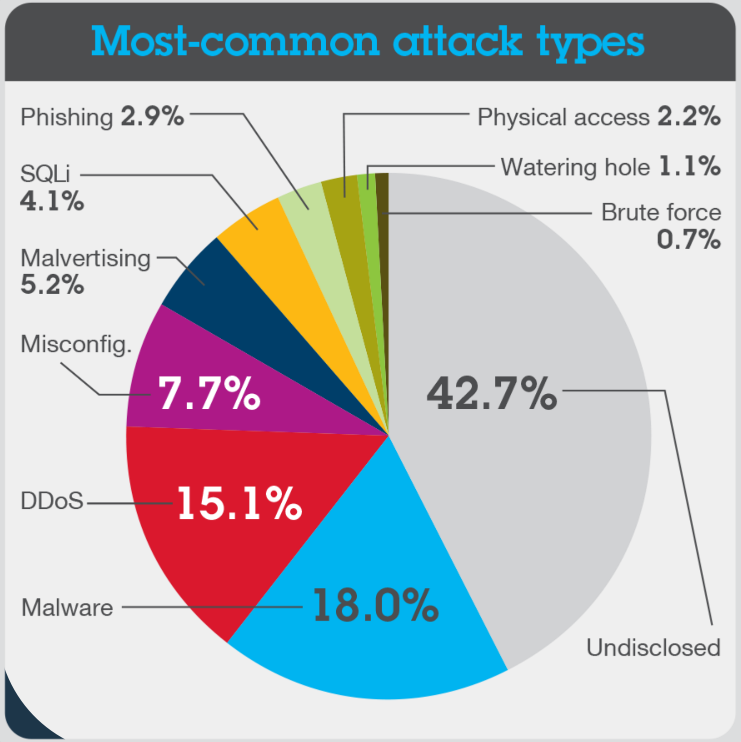
Focus on High Value Targets

Sophistication of Attack Techniques

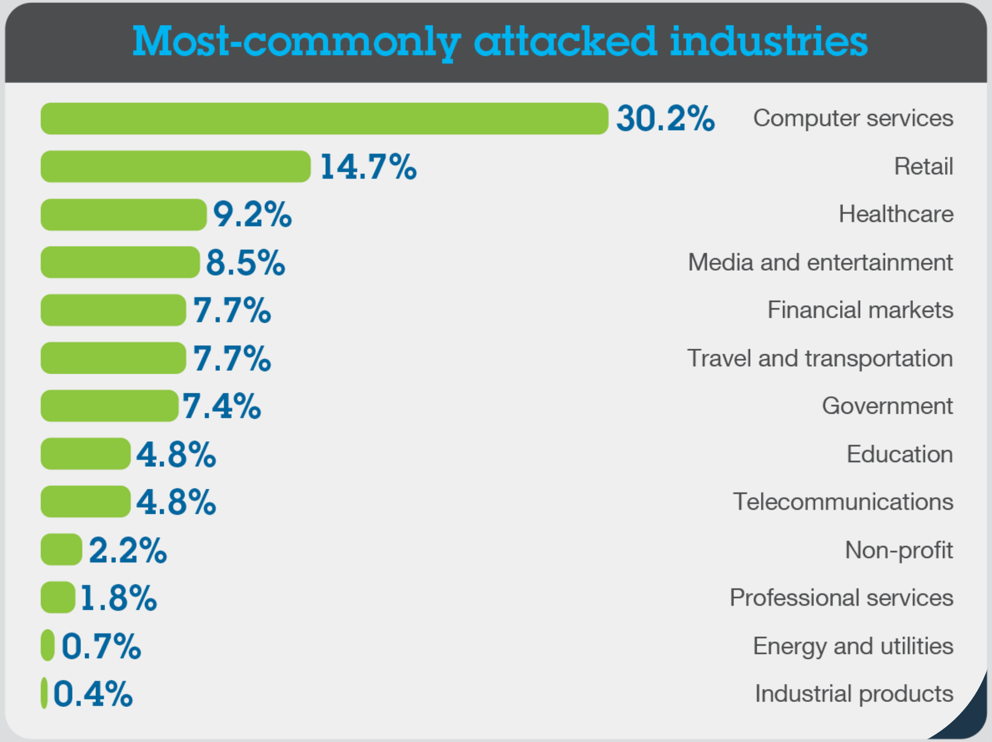
Breaches without Borders

A Need for Security Basics

Classic attacks like SQLi, Malware & DDoS Continue to be Successful



Most-common attack types



Most-commonly attacked industries

Source: IBM X-Force Threat Intelligence Report - 2016

Canada 2016 CODB at a Glance v. Global

2016 Cost of Data Breach Study: Canada

Benchmark research sponsored by IBM
Independently conducted by Ponemon Institute LLC
June 2016

- 24 Canadian companies participated
  - Global: 383 companies in 12 countries
- $6.03 million (CAD) is the average total cost of data breach
  - Global: $4M (USD)
- $278 (CAD) is the average cost per lost or stolen record
  - Global: $158 USD
- 10.6% increase in cost per lost or stolen record
  - Global: 15% increase

Download report for free here: http://www-03.ibm.com/security/data-breach/

Find Earlier + Eradicate Faster = Significant Cost Savings

Figure 17. Mean time to identify the breach event (MTTI)

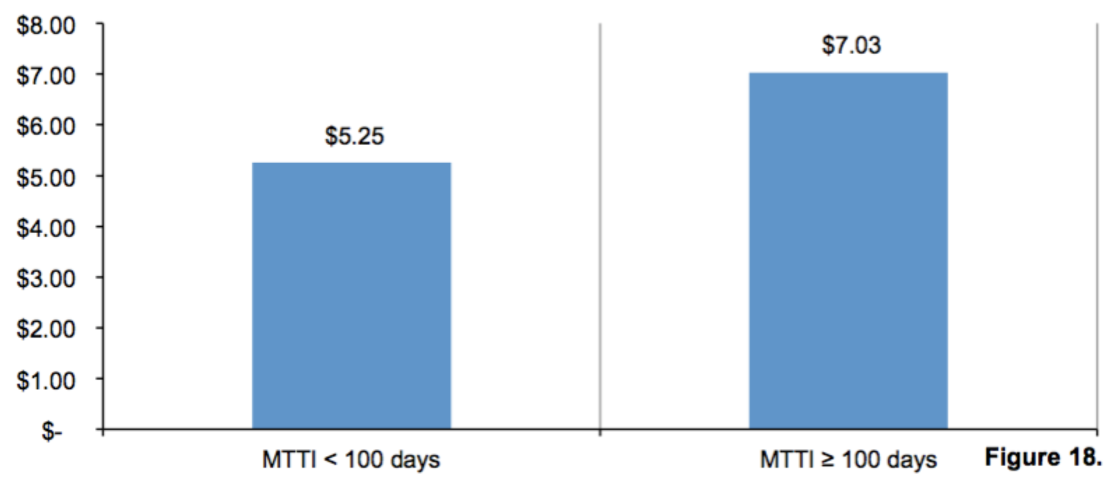
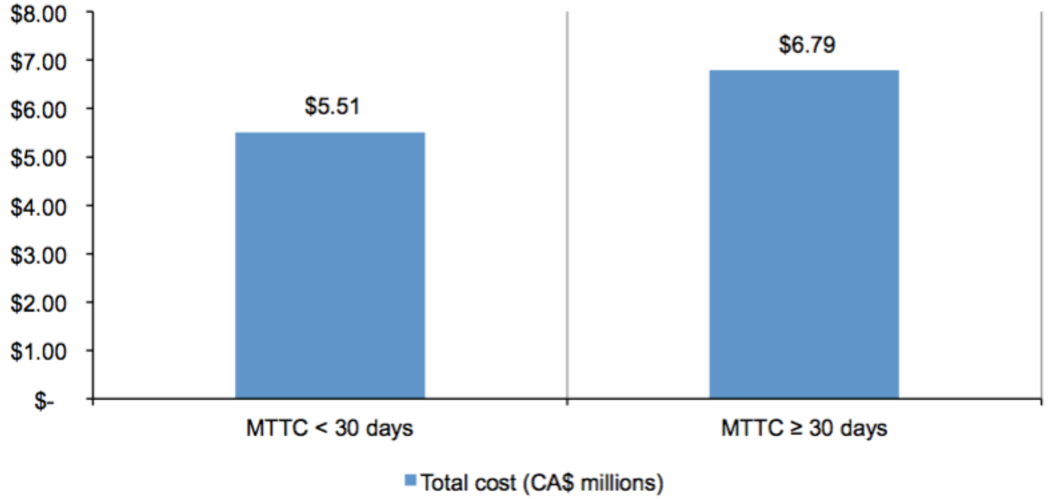
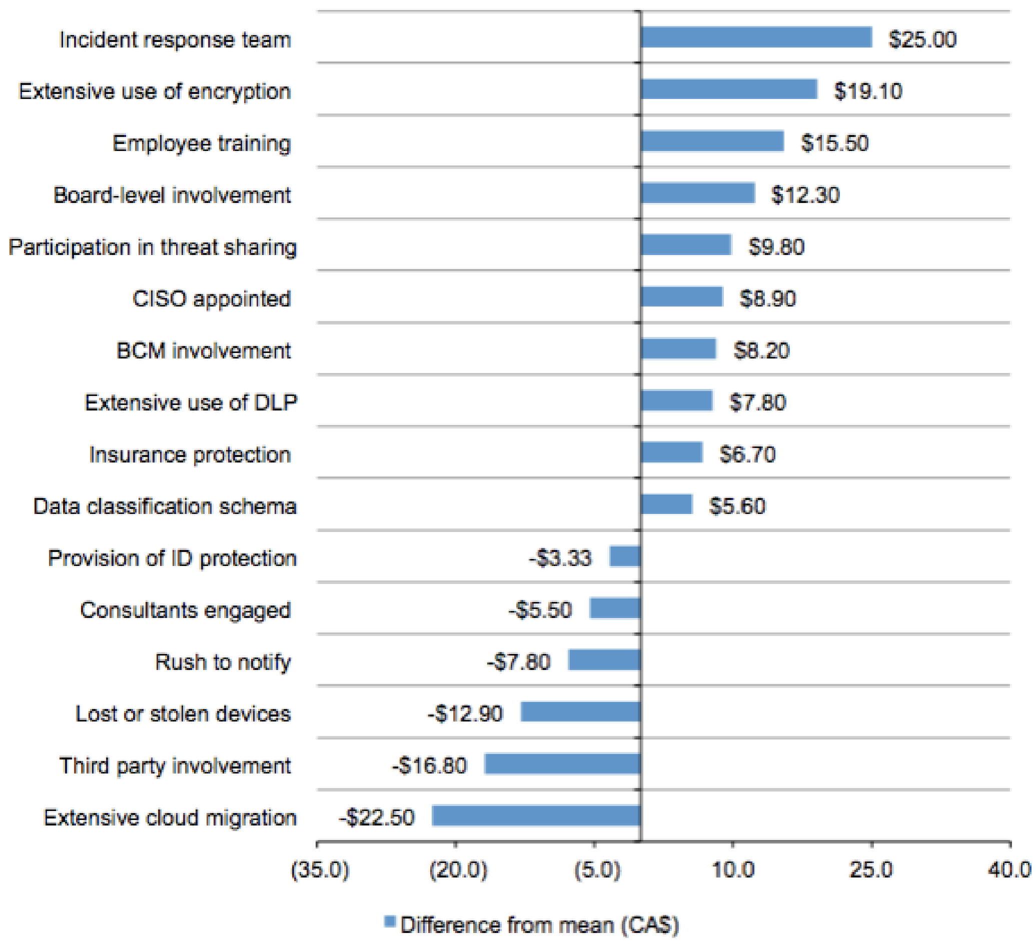


Figure 18. Mean time to contain the breach event (MTTC)

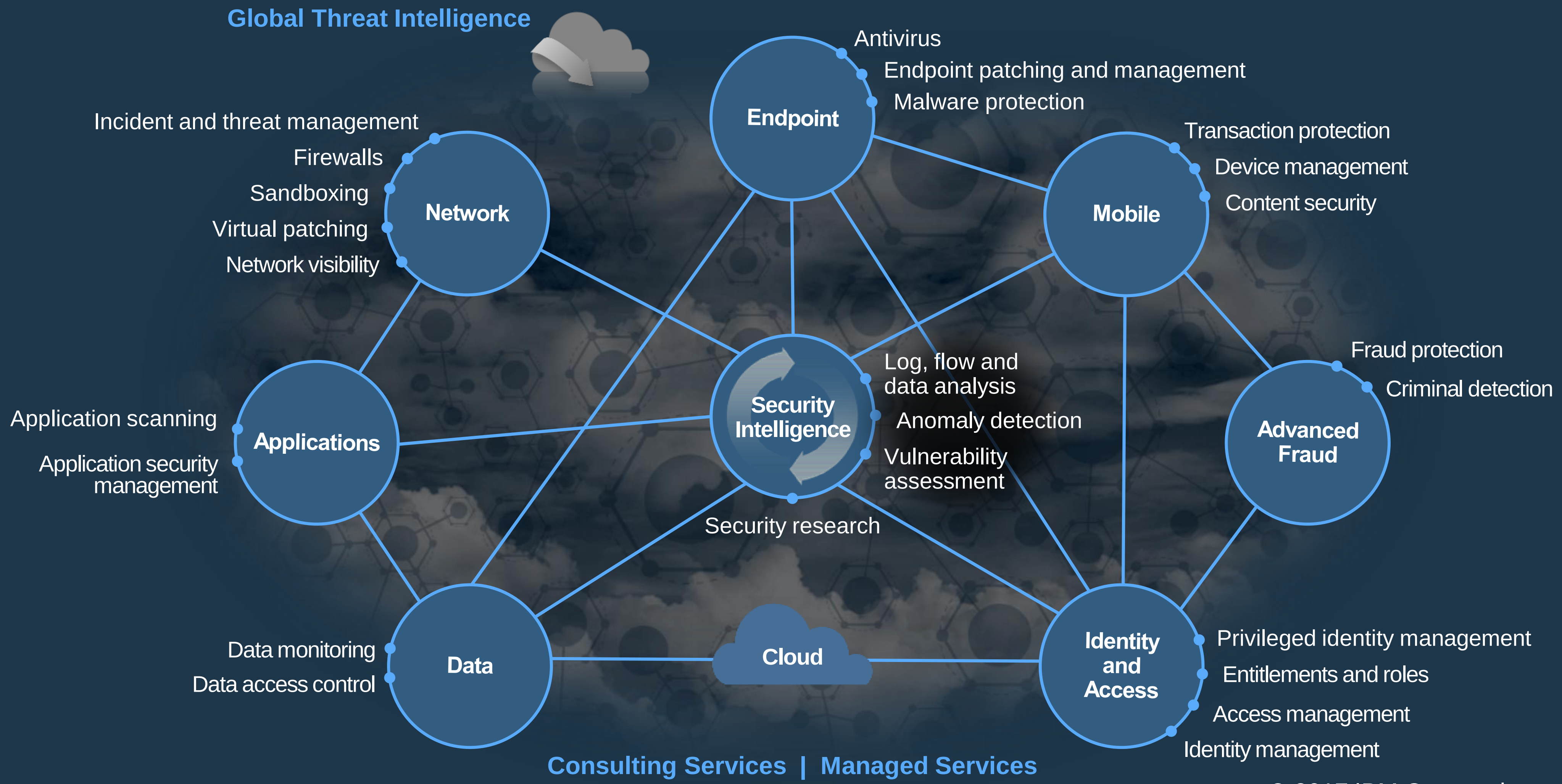


Factors the Increase/Decrease Recovery Costs

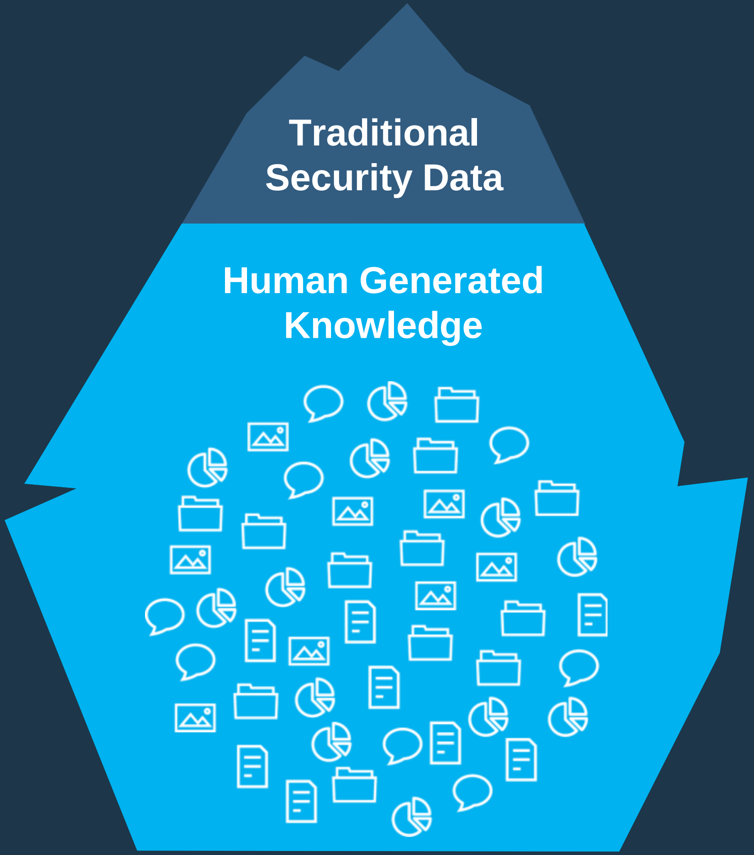
Figure 7. Impact of 16 factors on the per capita cost of data breach
Measured in Canadian dollars



Establish security as an immune system



A tremendous amount of security knowledge is created for human consumption… **but most of it is untapped**



- Security events and alerts
- Logs and configuration data
- User and network activity
- Threat and vulnerability feeds

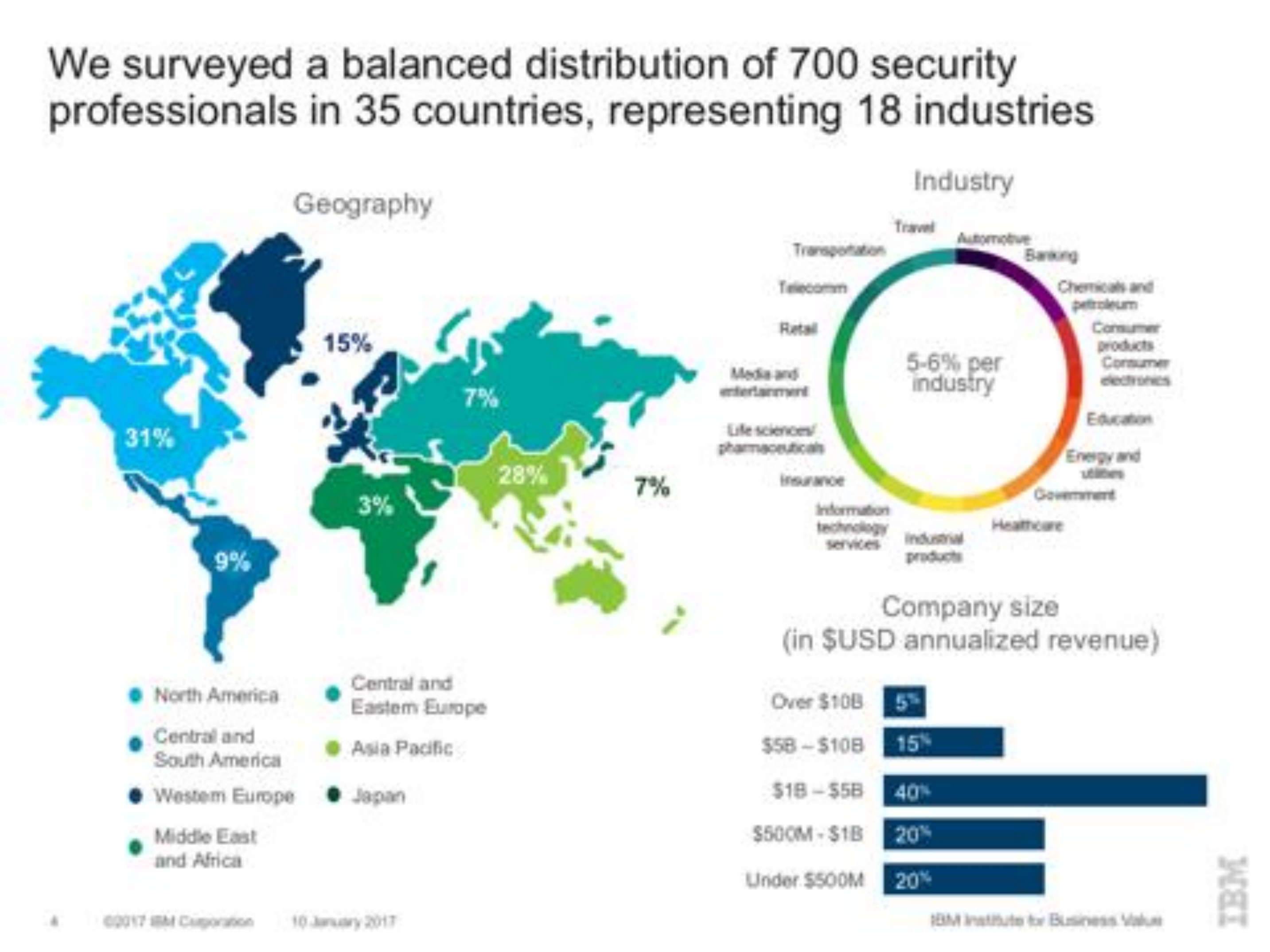
A universe of security knowledge
Dark to your defenses

Typical organizations leverage only 8% of this content*

Examples include:

- Research documents
- Industry publications
- Forensic information
- Threat intelligence commentary
- Conference presentations
- Analyst reports
- Webpages
- Wikis
- Blogs
- News sources
- Newsletters
- Tweets

Can Cognitive Help?

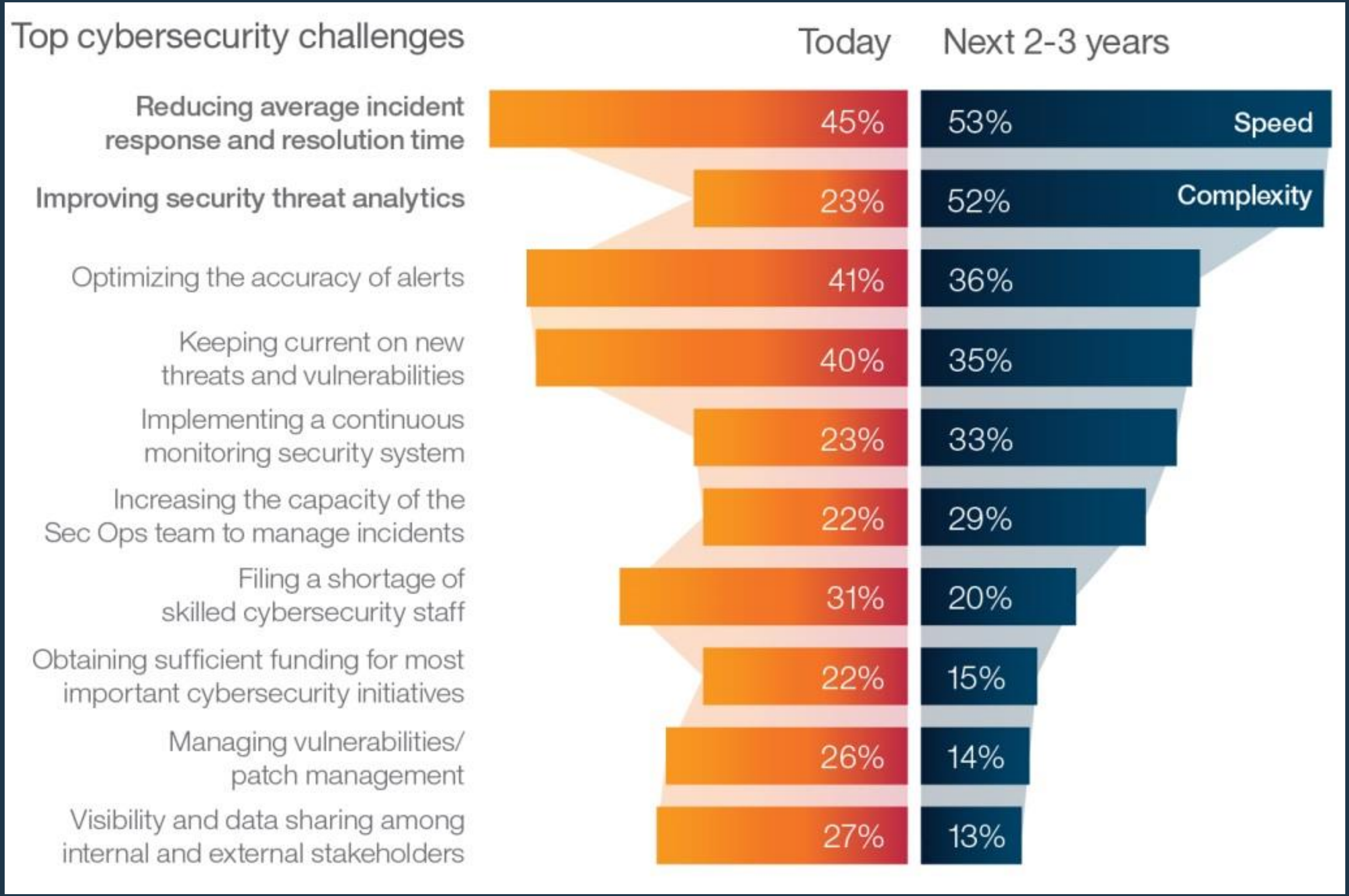


We surveyed a balanced distribution of 700 security professionals in 35 countries, representing 18 industries

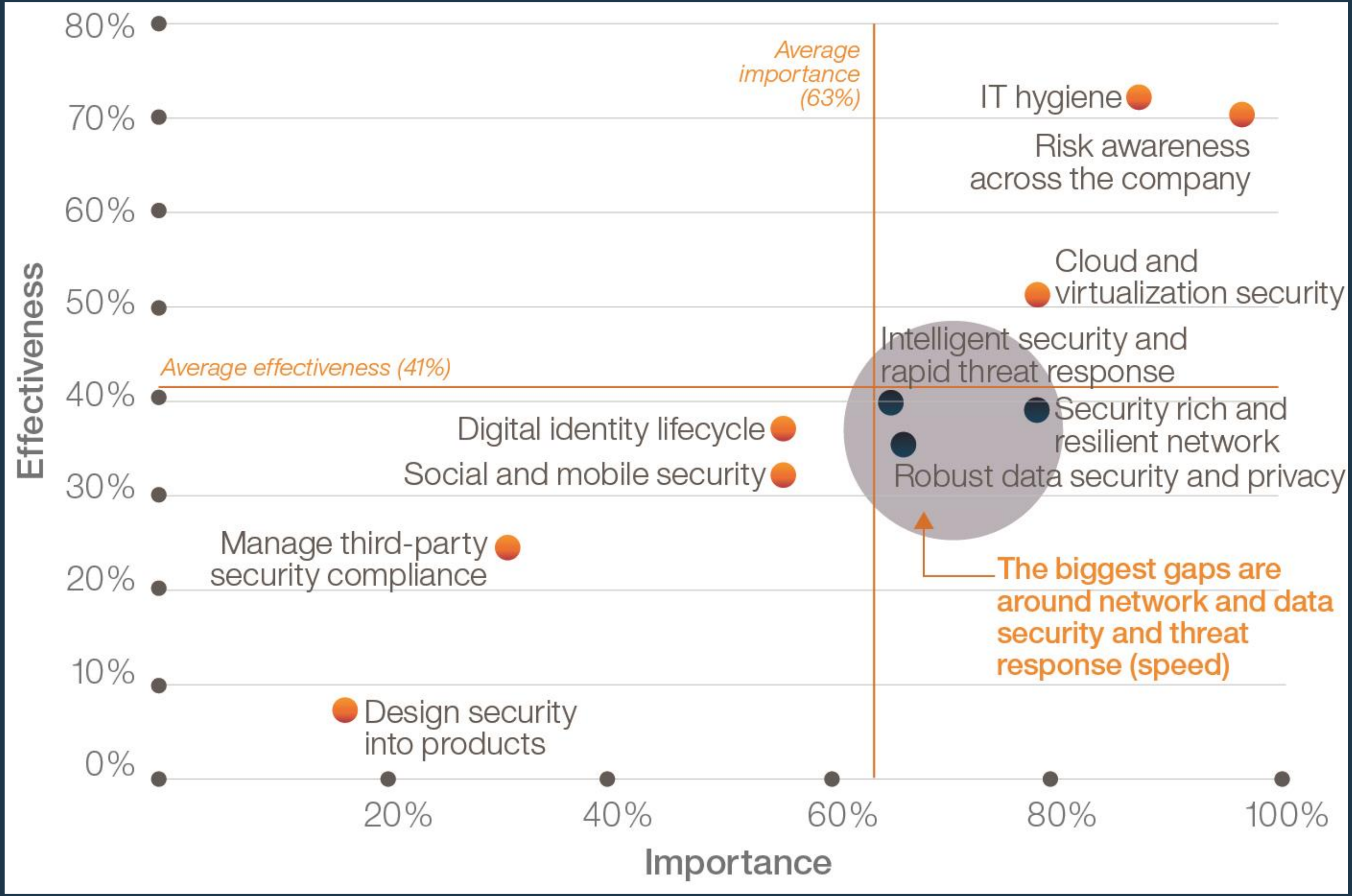
4 ©2017 IBM Corporation 10 January 2017 IBM Institute for Business Value

IBM

Challenges around Response Speed – Analytics



Network, data protection, speed are the weakest areas for most



The biggest gaps are around network and data security and threat response (speed)

Three Critical Gaps

Intelligence gap

#1 most challenging area due to insufficient resources is threat research (65% selecting)

#3 highest cybersecurity challenge today is keeping current on new threats and vulnerabilities (40% selecting)

Speed gap

The top cybersecurity challenge today and tomorrow is **reducing average incident response and resolution time**

This is despite the fact that **80%** said their incident response speed is much faster than two years ago

Accuracy gap

#2 most challenging area today is optimizing accuracy alerts (too many false positives)

#3 most challenging area due to insufficient resources is threat identification, monitoring and escalating potential incidents (61% selecting)

Addressing gaps while managing cost and ROI pressures

EY sees how Cognitive Security Can Help

Seeing internal and external challenges

A rapid pace of technological change and adversaries advancing their tools and techniques

Digital innovation and transformation efforts within organizations are pushing the enterprise flat – how do you move fast with digital transformation without creating a more porous perimeter?

Reducing overall risk with cognitive security solutions

Cognitive security solutions could:

- Provide better threat intelligence, helping to understand potential attacks in the future
- Act as an expert advisor for a security operations analyst, it could not only enhance their expertise, but also may help to adapt and evolve security controls based on what the system has learned over time
- Help to manage GRC, deciphering the different requirements from multiple regulatory agencies

"There is a massive amount of noise out there, the human brain can't process everything on a day to day basis – we need something to help, something like AI or cognitive technologies."

Chad Holmes, Principal and Cyber Strategy, Technology and Growth Leader (CTO) at Ernst & Young LLP

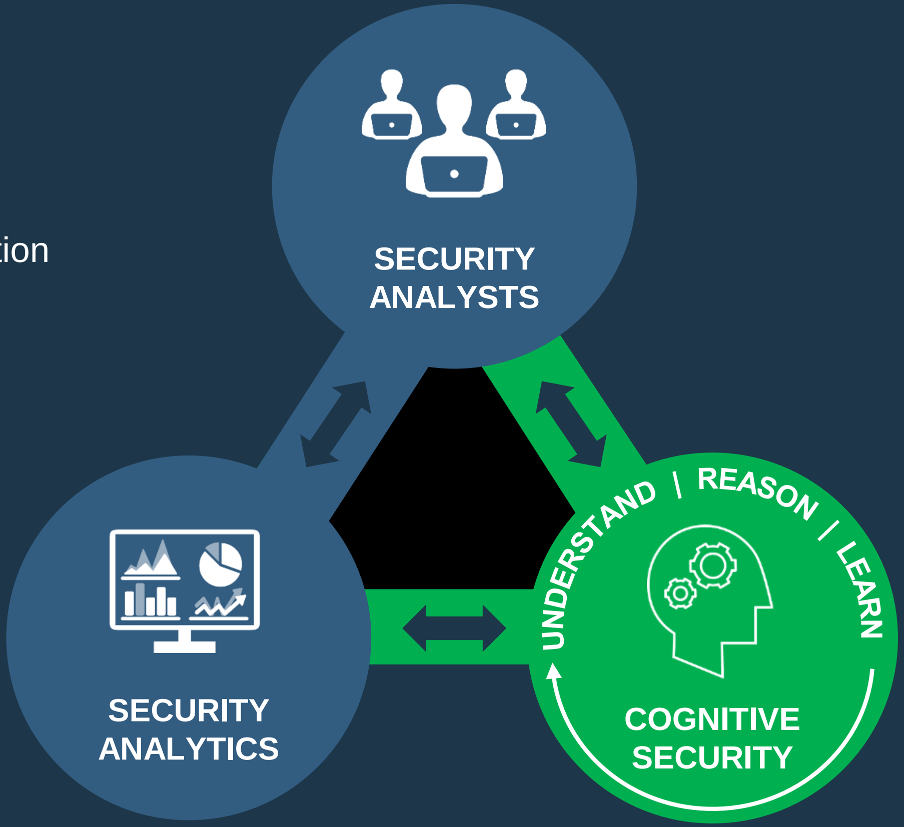
Cognitive systems bridge this gap and unlock a new partnership between security analysts and their technology

Human Expertise

- Common sense
- Morals
- Compassion
- Abstraction
- Dilemmas
- Generalization

Security Analytics

- Data correlation
- Pattern identification
- Anomaly detection
- Prioritization
- Data visualization
- Workflow



Cognitive Security

- Unstructured analysis
- Natural language
- Question and answer
- Machine learning
- Bias elimination
- Tradeoff analytics

How to Prepare

Recognize your weaknesses	Look at the primary weaknesses and vulnerabilities within your organization. How are they connected? What is a priority? Evaluate your intelligence, speed and accuracy.
Become educated about cognitive security capabilities	Take a holistic and formal approach to learn about cognitive security solutions. There could be many misconceptions in your organization from a capability, cost and implementation perspective.
Define an investment plan	It is difficult to build an investment case when a technology is new and unproven – focus on the fact that cognitive security is a capability that can improve the overall effectiveness of security operations.
Look to augment your capabilities, no matter your maturity	Cognitive security solutions are an emerging technology area, and its unique characteristics can benefit organizations of all sizes. Whether you are *Pressured, Prudent* or *Primed,* there are things you can do.

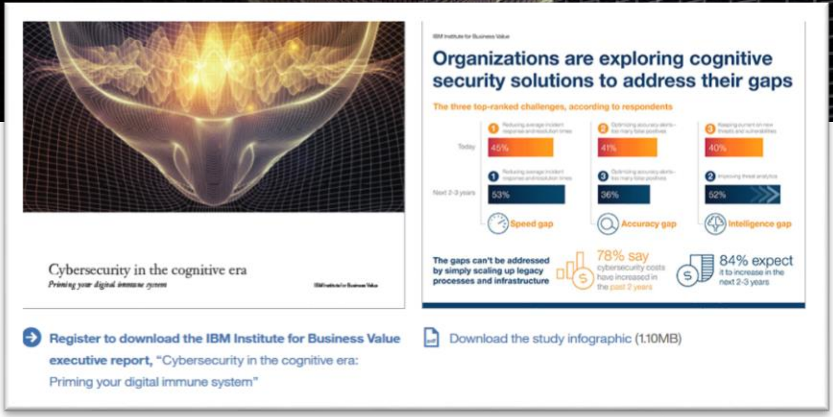
Learn more about the study: Cybersecurity in the cognitive era

Visit ibm.com/security/cognitive to download the report

Read the blog at Securityintelligence.com

Cybersecurity in the cognitive era

Priming your digital immune system



Cybersecurity in the cognitive era
Priming your digital immune system

IBM Institute for Business Value

Organizations are exploring cognitive security solutions to address their gaps

The three top-ranked challenges, according to respondents

Today
Next 2-3 years
1 Reducing average incident response and resolution times
45%
2 Optimizing accuracy alerts–too many false positives
41%
3 Keeping current on new threats and vulnerabilities
40%
1 Reducing average incident response and resolution times
53%
3 Optimizing accuracy alerts–too many false positives
36%
2 Improving threat analytics
52%
Speed gap
Accuracy gap
Intelligence gap

The gaps can't be addressed by simply scaling up legacy processes and infrastructure

78% say cybersecurity costs have increased in the past 2 years

84% expect it to increase in the next 2-3 years

Register to download the IBM Institute for Business Value executive report, "Cybersecurity in the cognitive era: Priming your digital immune system"

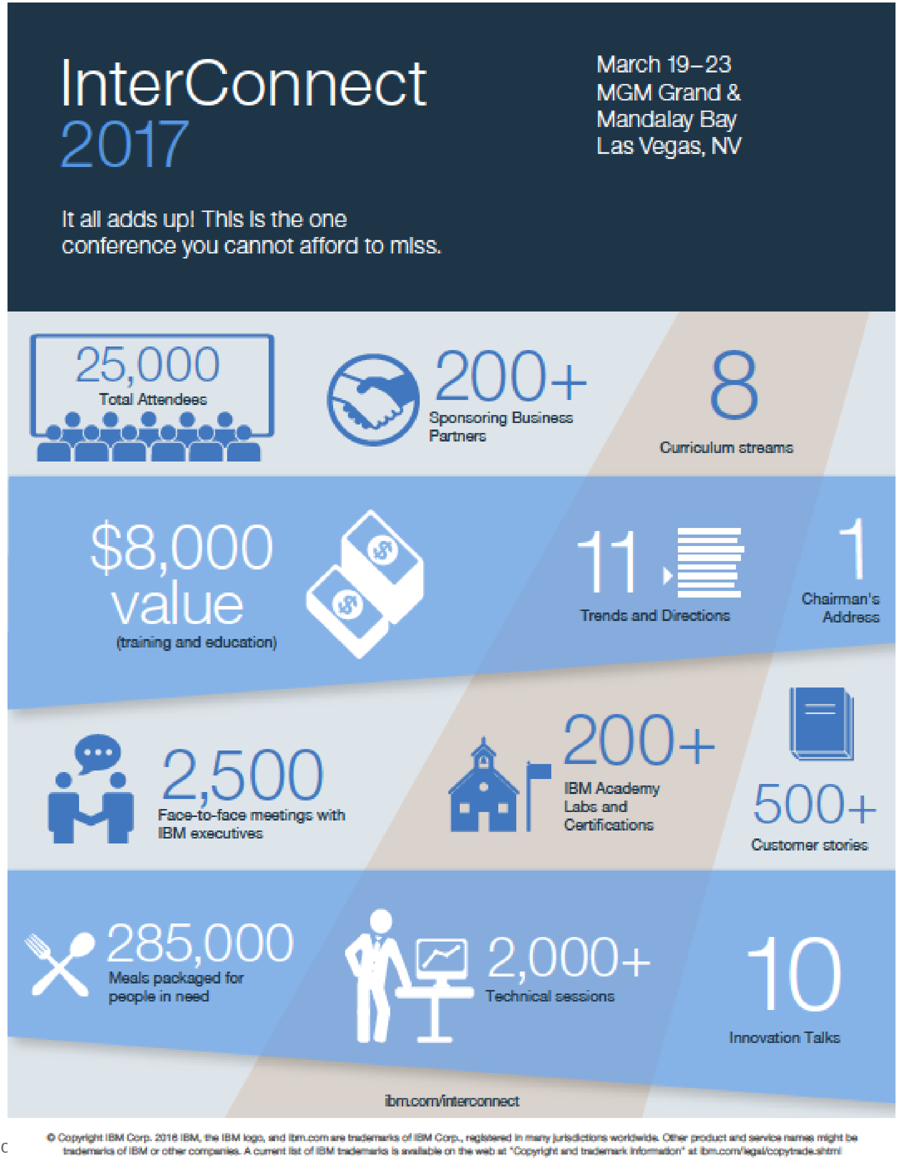
Download the study infographic (1.10MB)

IBM at Reboot

@IBM

Drop off your feedback form for a FREE Gift at IBM Booth # 18

Time	Topic	Speaker	Role	Where
February 8 9: 00 AM – 12:00 PM	IBM Workshop – Safe guarding the data when legacy defenses are not enough	Walid Rjaibi	IBM Global CTO for IBM Data Security	Lecture Theatre
February 9 1:35 PM – 2:10 PM	IBM Keynote – The Emerging Era of Cognitive Security	Diana Kelley	IBM Global Executive Security Advisor	Salon AB
February 9 2:15 PM – 2:45 PM	Keeping Data Safe: Guardium Data Protection case study	Raki Robert	Technical Sales Engineer - Canada & Caribbean Data Security, IBM Security	Lecture Theatre
February 10 11:05 AM – 12:15 PM	Concurrent Panel Session - Panel B: Ransomware: Are You the Next Digital Hostage?	Charles Davis	IBM Global Executive Security Architect	Lecture Theatre
February 10 2:15 PM – 3:30 PM	Concurrent Panel Session - Panel B: Digital Government Platforms / Government as a Platform	Paul Lewis	IBM Canada Executive Consultant	Lecture Theatre



InterConnect 2017

March 19–23
MGM Grand &
Mandalay Bay
Las Vegas, NV

It all adds up! This is the one conference you cannot afford to miss.

25,000 Total Attendees

200+ Sponsoring Business Partners

8 Curriculum streams

$8,000 value (training and education)

11 Trends and Directions

1 Chairman's Address

2,500 Face-to-face meetings with IBM executives

200+ IBM Academy Labs and Certifications

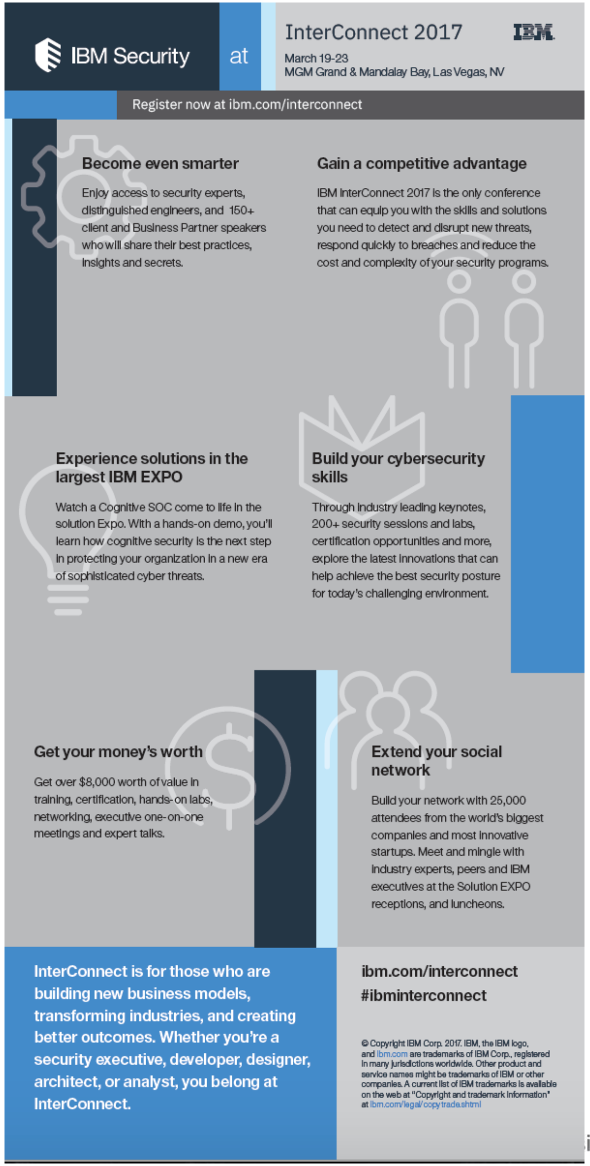
500+ Customer stories

285,000 Meals packaged for people in need

2,000+ Technical sessions

10 Innovation Talks

ibm.com/interconnect



IBM Security at InterConnect 2017

March 19-23
MGM Grand & Mandalay Bay, Las Vegas, NV

Register now at ibm.com/interconnect

Become even smarter

Enjoy access to security experts, distinguished engineers, and 150+ client and Business Partner speakers who will share their best practices, insights and secrets.

Gain a competitive advantage

IBM InterConnect 2017 is the only conference that can equip you with the skills and solutions you need to detect and disrupt new threats, respond quickly to breaches and reduce the cost and complexity of your security programs.

Experience solutions in the largest IBM EXPO

Watch a Cognitive SOC come to life in the solution Expo. With a hands-on demo, you'll learn how cognitive security is the next step in protecting your organization in a new era of sophisticated cyber threats.

Build your cybersecurity skills

Through industry leading keynotes, 200+ security sessions and labs, certification opportunities and more, explore the latest innovations that can help achieve the best security posture for today's challenging environment.

Get your money's worth

Get over $8,000 worth of value in training, certification, hands-on labs, networking, executive one-on-one meetings and expert talks.

Extend your social network

Build your network with 25,000 attendees from the world's biggest companies and most innovative startups. Meet and mingle with industry experts, peers and IBM executives at the Solution EXPO receptions, and luncheons.

InterConnect is for those who are building new business models, transforming industries, and creating better outcomes. Whether you're a security executive, developer, designer, architect, or analyst, you belong at InterConnect.

ibm.com/interconnect
#ibminterconnect

Learn more about IBM X-Force

IBM Security

No. 1	enterprise security software vendor in total revenue
25	industry analyst reports rank IBM Security as a **LEADER**
130+	countries where IBM delivers managed security services
12K+	clients protected *including…*
90%	of the Fortune 100 companies

Join IBM X-Force Exchange
xforce.ibmcloud.com

Visit our web page
ibm.com/security/xforce

Watch our videos
IBM Security YouTube Channel

View upcoming webinars & blogs
SecurityIntelligence.com

Follow us on Twitter
@ibmsecurity

IBM Security

THANK YOU

FOLLOW US ON:

🌐 ibm.com/security

🌐 securityintelligence.com

🌐 xforce.ibmcloud.com

@ibmsecurity

▶ youtube/user/ibmsecuritysolutions

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM®