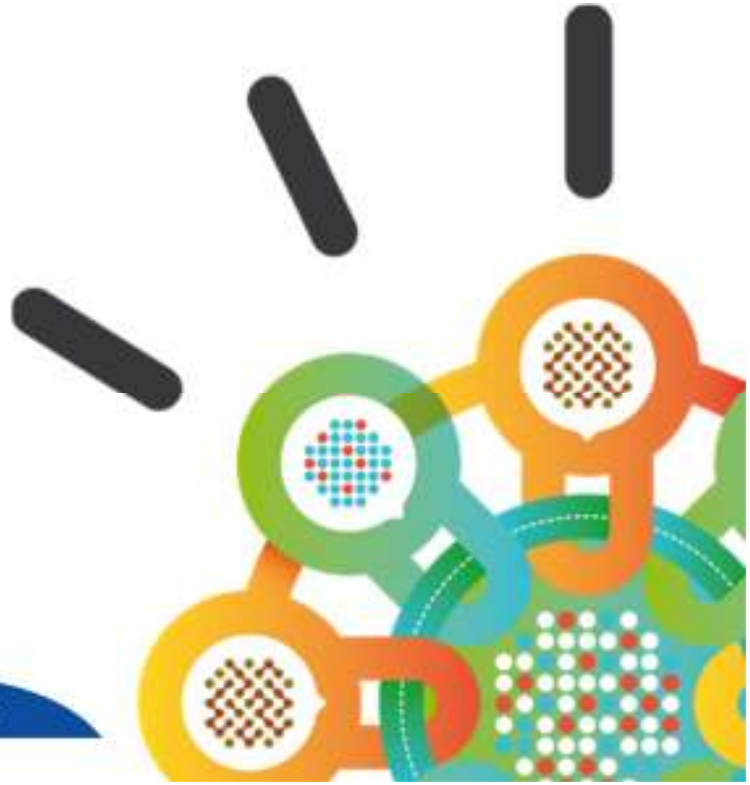
Key findings from the
2014 Cost of Data Breach Study: Global Analysis

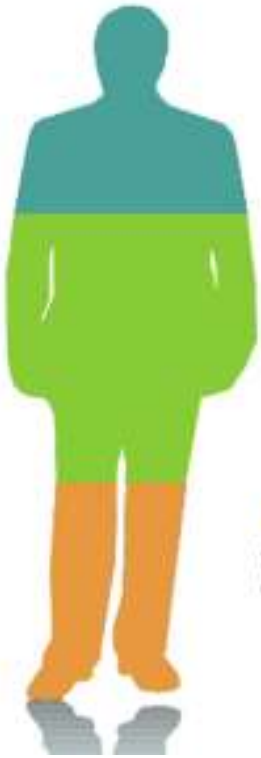
May 2014

Melbourne X Force Roadshow
29 July
Glen Gooding

Benchmark research sponsored by IBM
Independently conducted by
Ponemon Institute



IBM's investment in Security Research – Technical, IBM Enterprise, External



Influencers
Confident and prepared, influence the business strategically

Protectors
Less confident, prioritize security strategically but lack necessary structural elements

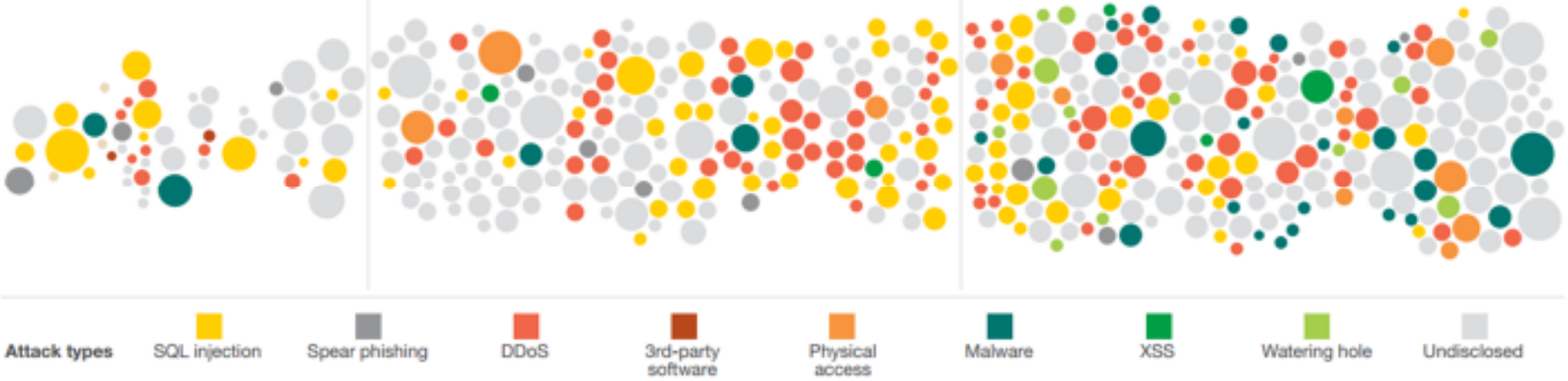
Responders
Least confident, focus largely on protection and compliance

Ponemon INSTITUTE

We are in an era of continuous breaches

Attackers are relentless, victims are targeted, and the damage toll is rising

2011	2012	2013
Operational Sophistication	**Near Daily Leaks of Sensitive Data**	**Relentless Use of Multiple Methods**
IBM X-Force® declared **Year of the Security Breach**	**40% increase** in reported data breaches and incidents	**500,000,000+ records** were leaked, while the future shows no sign of change



Source:
IBM X-Force Threat Intelligence Quarterly – 1Q 2014

Note: Size of circle estimates relative impact of incident in terms of cost to business.

The 2014 Cost of Data Breach Study: Global Analysis—definitions and key facts

- **Data breach:** An event in which an individual's name plus a medical record or financial record or debit card is potentially at risk
- **Data record:** Information that identifies the natural person (individual) whose information has been lost or stolen in a data breach
- **Incident:** For this study, an incident is a data breach involving between 2,415 to slightly more than 102,000 compromized records
- **Benchmark research:** For this benchmark study, the unit of analysis is the organization; in survey research, the unit of analysis is the individual

11 countries

16 industries

314 organizations

A mega-breach of more than 100,000 records is not considered typical. The cost data in this study cannot be used to calculate the financial impact of a mega-breach.

Global and country-level averages show that the cost of a data breach is on the rise.

Cost per record* in 2013

Global average

$145

9%

year-to-year increase

Highest countries

$201 in the U.S.

$195 in Germany

Lowest countries

$70 in Brazil

$51 in India

Cost per incident* in 2013

Global average

$3.5M

15%

year-to-year increase

Highest countries

$5.9M in the U.S.

$4.7M in Germany

Lowest countries

$1.6M in Brazil

$1.4M in India

*Currencies converted to US dollars

Global and country-level averages show that the cost of a data breach is on the rise.

Cost per record* in 2013

Global average

$145

9%

year-to-year increase

$135

In Australia

Cost per incident* in 2013

Global average

$3.5M

15%

year-to-year increase

Highest countries

$5.9M in the U.S.

$4.7M in Germany

$1.6M in Brazil

$1.4M in India

Lowest countries

*Currencies converted to US dollars

Global and country-level averages show that the cost of a data breach is on the rise.

Cost per record* in 2013

Global average

$145

9%

year-to-year increase

$135

In Australia

Cost per incident* in 2013

Global average

$3.5M

15%

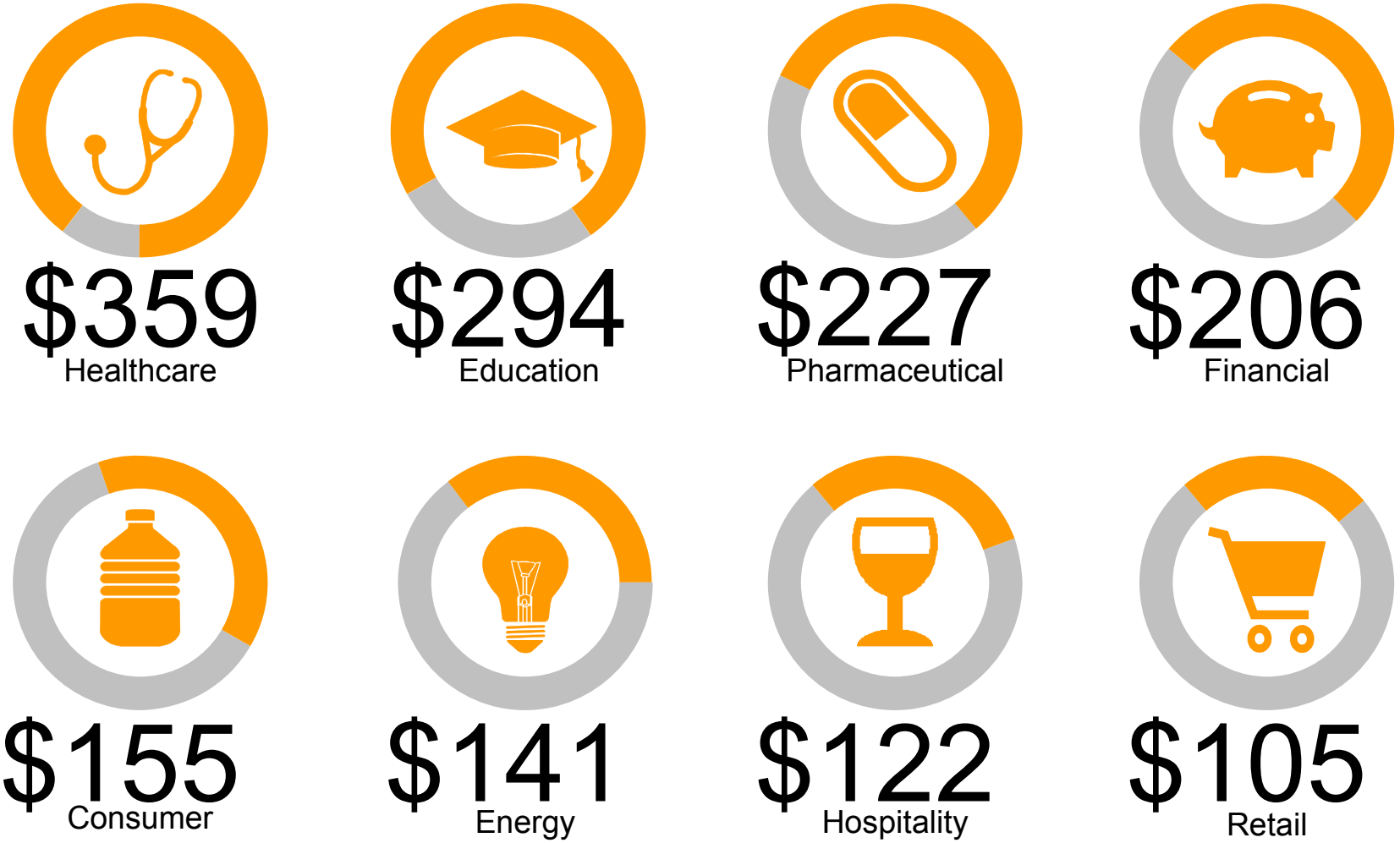
year-to-year increase

$2.6M

In Australia

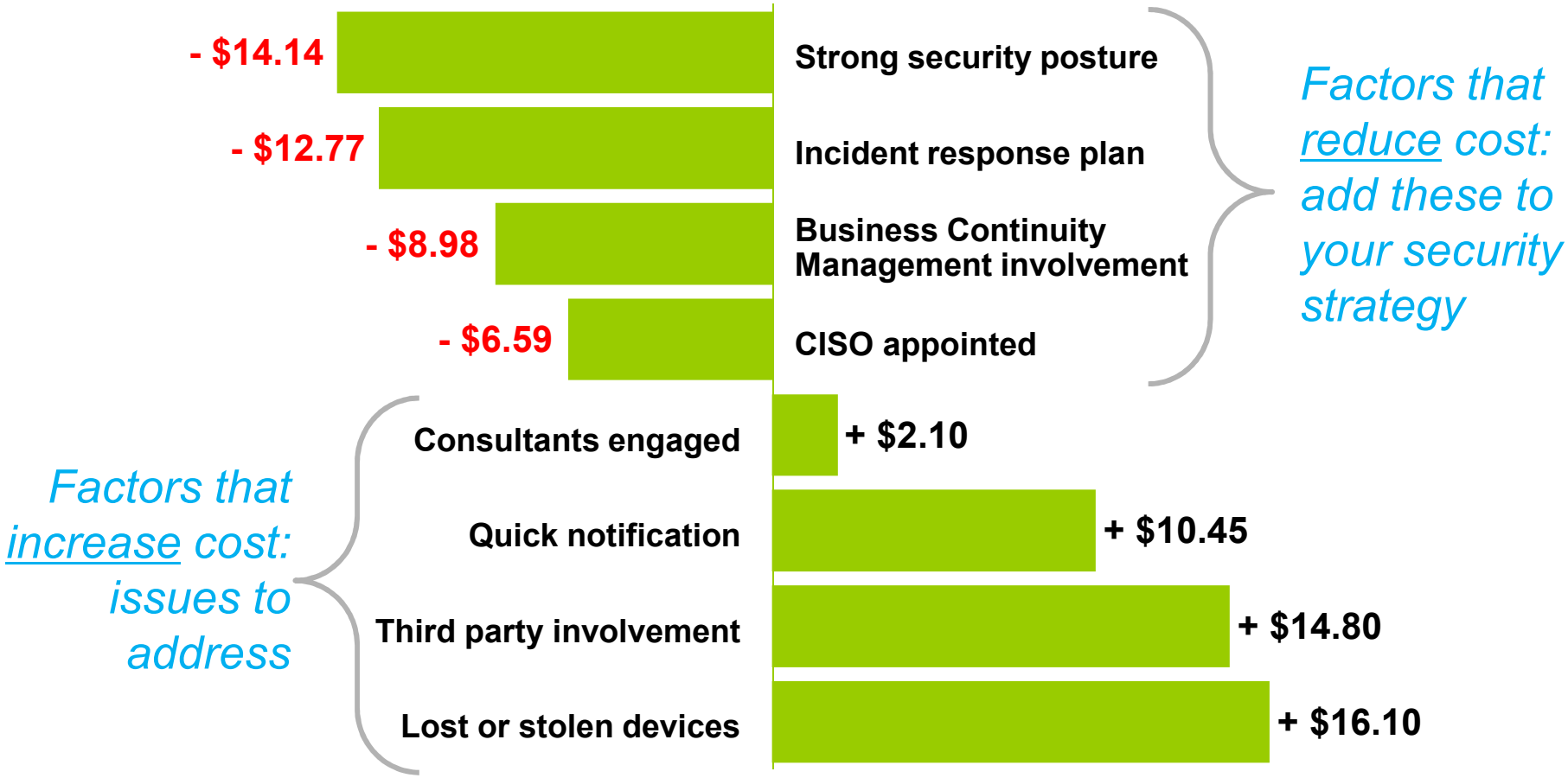
*Currencies converted to US dollars

Highly regulated industries have the highest per-record data breach costs.



Currencies converted to US dollars

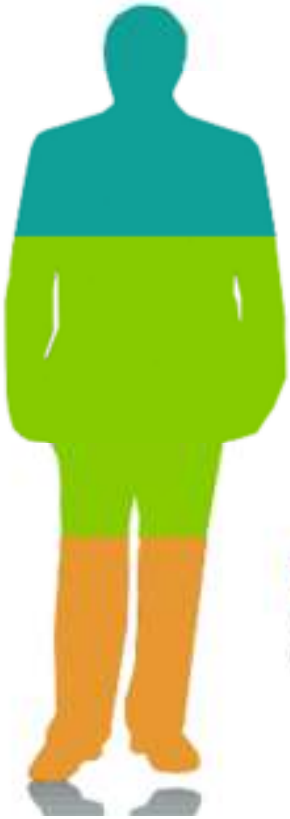
You can raise or lower your per-record cost of a data breach by addressing these eight influencing factors.



Currencies converted to US dollars

Finding a Strategic Voice (2012) – IBM's findings in alignment with Ponemon Institute

And their roles are evolving with growing **authority, accountability** and **impact** across the enterprise.



Influencers

Confident and prepared, influence the business strategically

Protectors

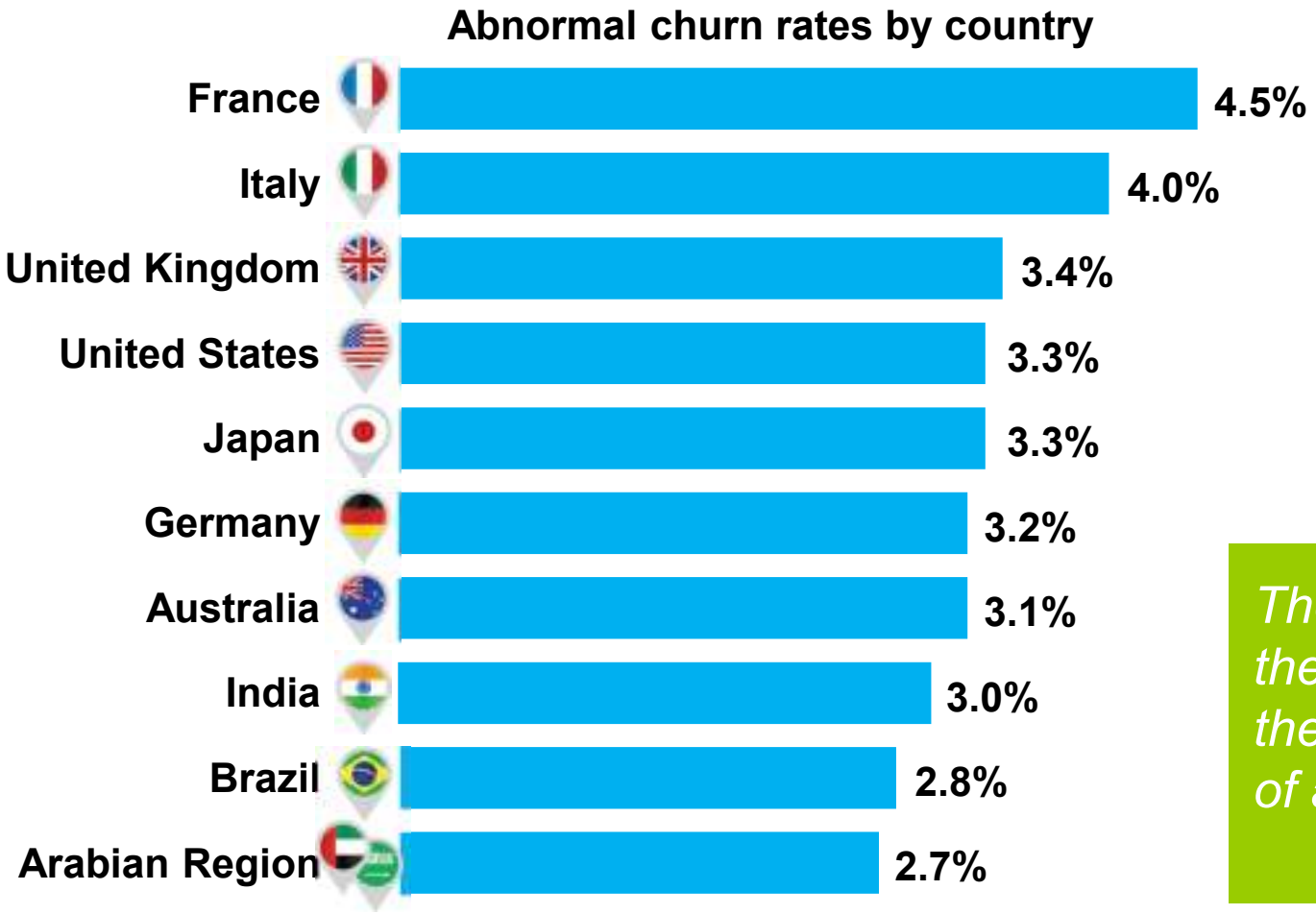
Less confident, prioritize security strategically but lack necessary structural elements

Responders

Least confident, focus largely on protection and compliance

How they differ

Customer churn following a data breach—and the related impact on the organization's reputation—is a key contributor to increased cost.



The more churn there is, the higher the per-record cost of a data breach

Abnormal churn rate also varies widely by industry.

6.2%
Pharmaceutical

6.1%
Financial

5.9%
Healthcare

3.0%
Consumer

2.9%
Hospitality

2.8%
Energy

2.4%
Education

1.3%
Retail

Currencies converted to US dollars; refer to the study for data on all 16 industries

Other components of the cost of a data breach include detection, notification, post-event costs and lost business.

Cost category	Highest country (average cost per incident)	Typical components
Detection and escalation	$1.3M Germany	Forensics, assessment, audit services, crisis team management, internal communications
Notification	$509K United States	Contact databases, regulatory requirement research, outside experts, postal expenditures, inbound communications setup
Post-data breach costs	$1.6M United States	Help desk, inbound communications, investigations, remediation, legal costs, product discounts and other special offers
Lost business	$3.3M United States	Abnormal turnover, increased customer acquisition costs, reputation losses, diminished goodwill

Other components of the cost of a data breach include detection, notification, post-event costs and lost business.

Cost category	Highest country (average cost per incident)	Australian Figures	Typical components
Detection and escalation	$1.3M Germany	$.99M 3RD Highest	Forensics, assessment, audit services, crisis team management, internal communications
Notification	$509K United States	$54K 7th Highest	Contact databases, regulatory requirement research, outside experts, postal expenditures, inbound communications setup
Post-data breach costs	$1.6M United States	$.76M 7th Highest	Help desk, inbound communications, investigations, remediation, legal costs, product discounts and other special offers
Lost business	$3.3M United States	$.78M 7th HIghest	Abnormal turnover, increased customer acquisition costs, reputation losses, diminished goodwill

Malicious or criminal attacks are the leading root cause of a data breach…and result in the highest cost per record.

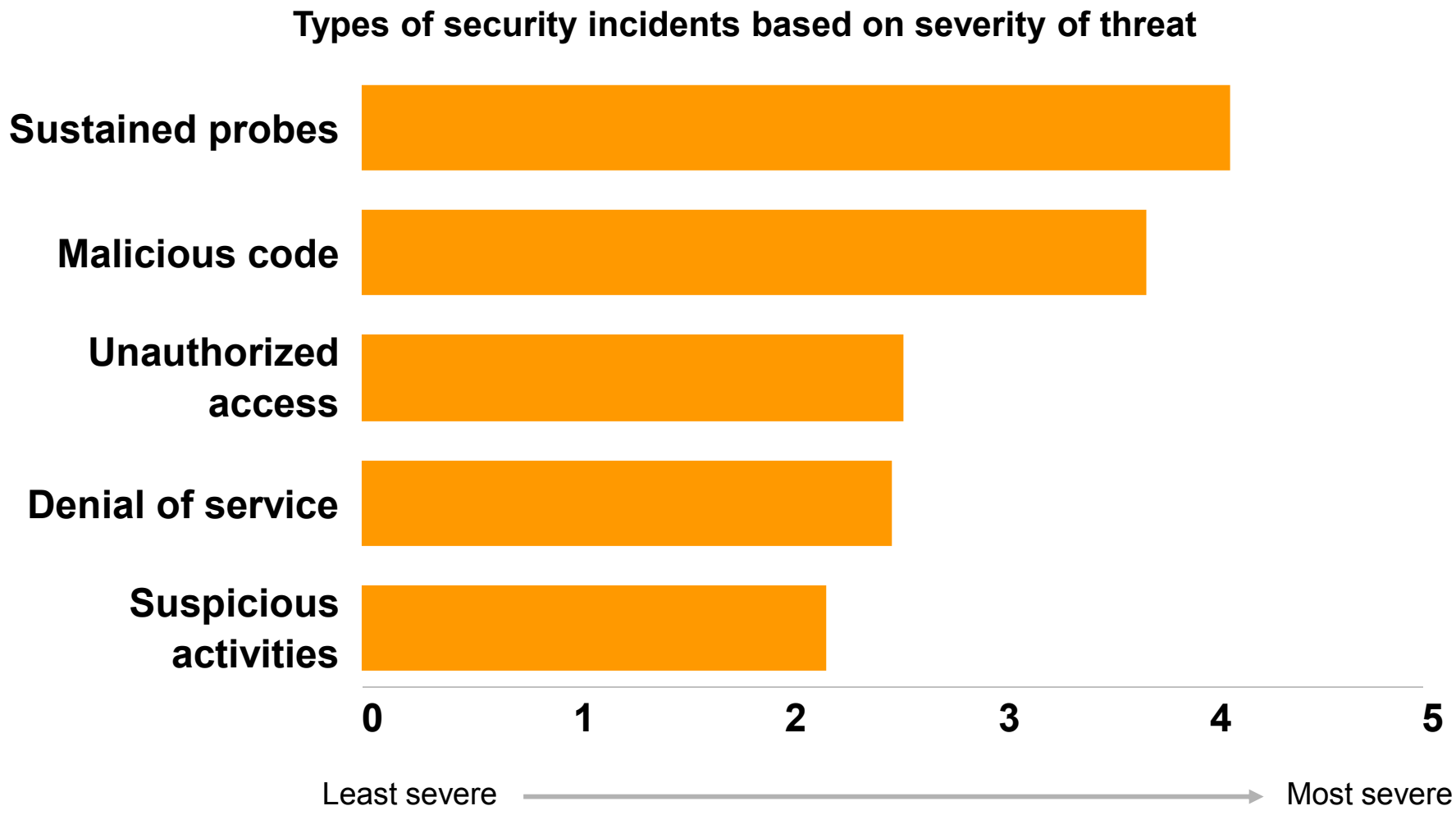
$117
per record

$159
per record

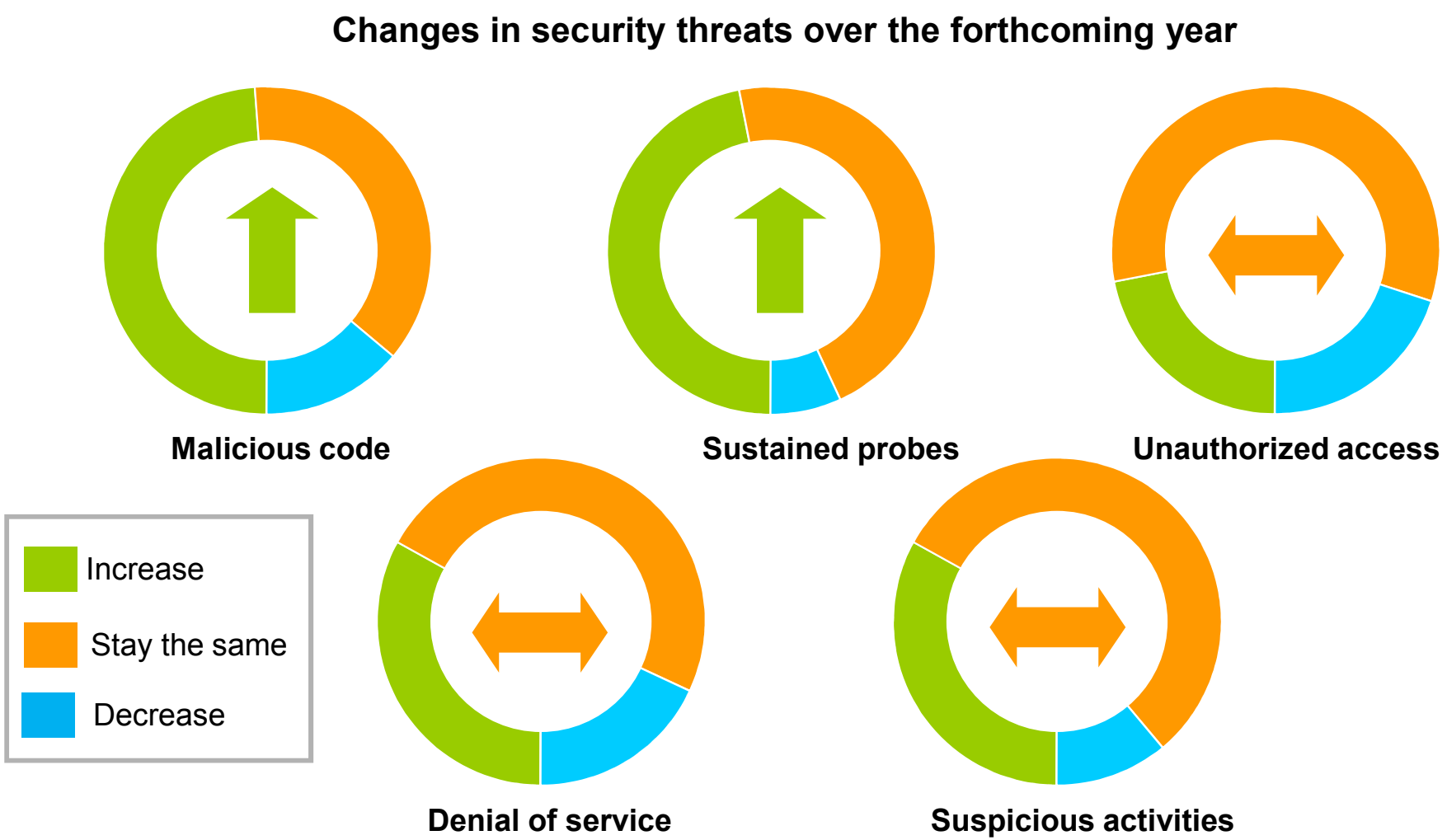
$126
per record

Currencies converted to US dollars; rounding errors may apply

Five types of malicious attack are most likely to keep IT security executives and managers awake at night.



Malicious code and sustained probes are projected to increase significantly over the course of 2014.



Organizations studied believe there is much room for improvement in their current security postures.

Do you have a security strategy to protect your:

Information assets?

55% Said NO

Online presence?

58% Said NO

IT infrastructure?

62% Said NO

What is the ideal amount to invest in security strategies over the next 12 months?

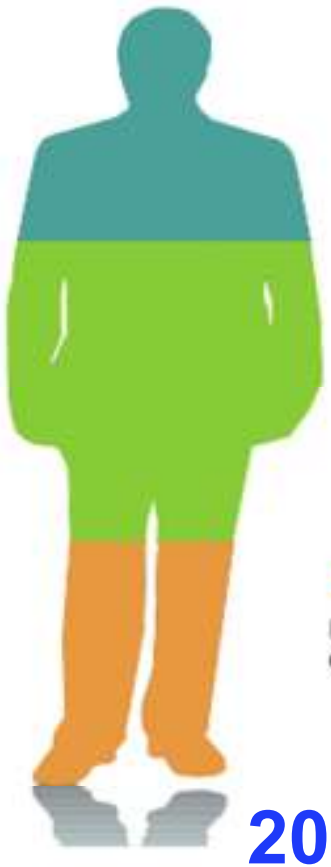
$14M

50% funding gap

What do you anticipate your budget for security will be over the next 12 months?

$7M

2014 CISO Assessment - Participation



Influencers
Confident and prepared, influence the business strategically

Protectors
Less confident, prioritize security strategically but lack necessary structural elements

Responders
Least confident, focus largely on protection and compliance

2012

2013

2014 ??

Your view

Next steps

Visit **ibm.com**/services/costofbreach

and register to receive the global study or a country-specific study

Visit **ibm.com**/services/security

to learn how IBM Security Services can help protect your organization

Visit www.ponemon.org

to learn more about Ponemon Institute research programs