



Ponemon Institute's 2018 Cost of a Data Breach Study

September 18, 2018

Speakers



Deborah Snyder
CISO
State of New York



Dr. Larry Ponemon
Chairman and Founder
Ponemon Institute



Megan Powell
Product Marketing Manager
IBM Security

What is the TRUE cost of a data breach?

BENCHMARK RESEARCH SPONSORED BY IBM SECURITY
INDEPENDENTLY CONDUCTED BY
PONEMON INSTITUTE



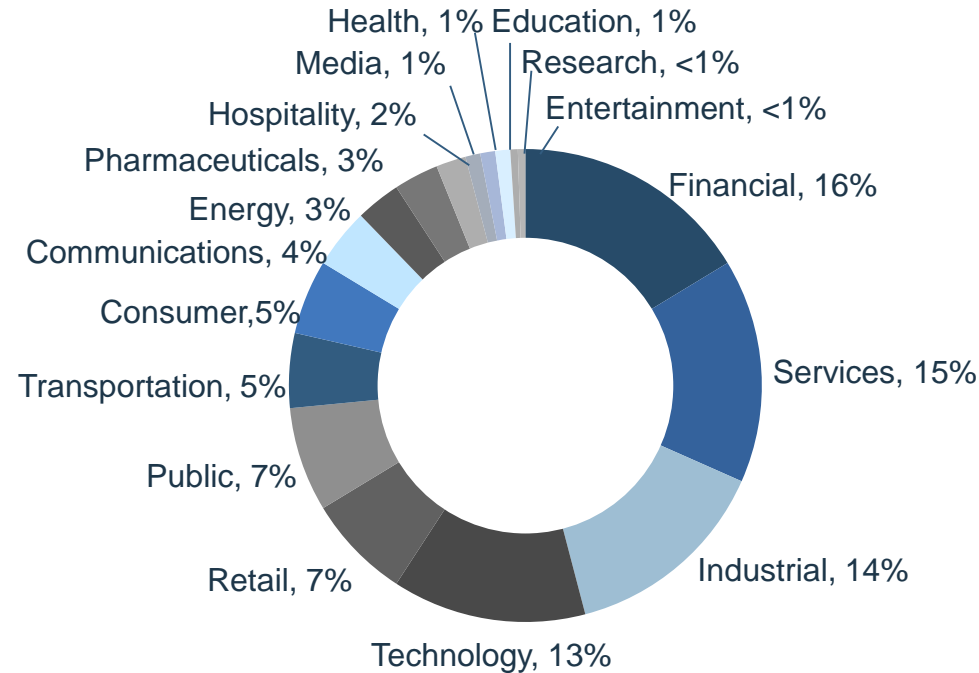
JULY 2018



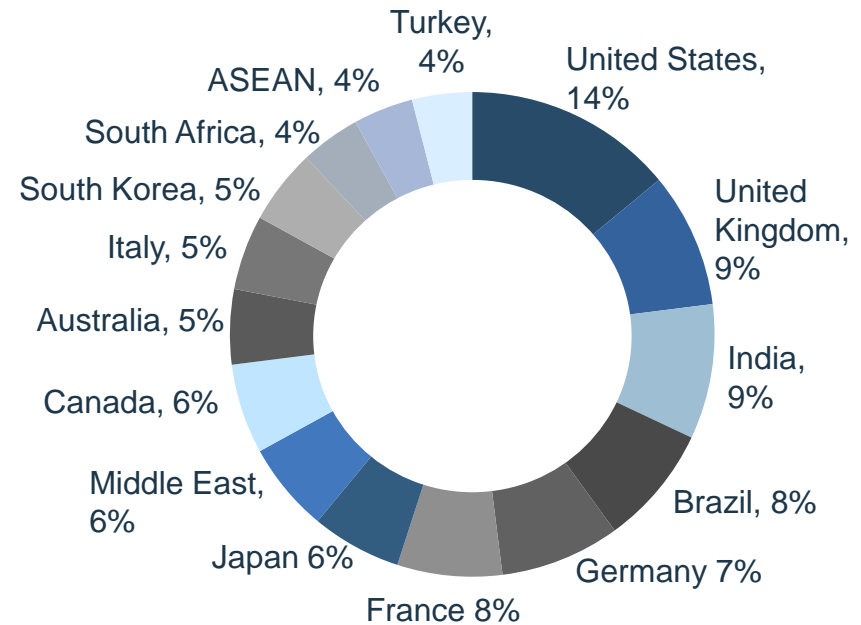
The 2018 Cost of a Data Breach Demographics

- 2,200+ interviews
- 477 companies
- 15 countries or regions
- 17 industries

Industries



Countries/regions



Are you focusing on the right things? What are the odds of....



Winning the
Powerball?

1
in

292,201,338



Getting struck by
lightning?

1
in

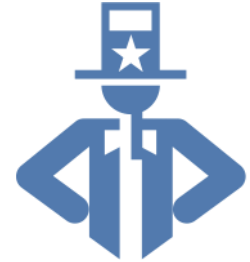
1,083,000



Finding a pearl
in an oyster?

1
in

12,000



Getting an IRS
audit?

1
in

160

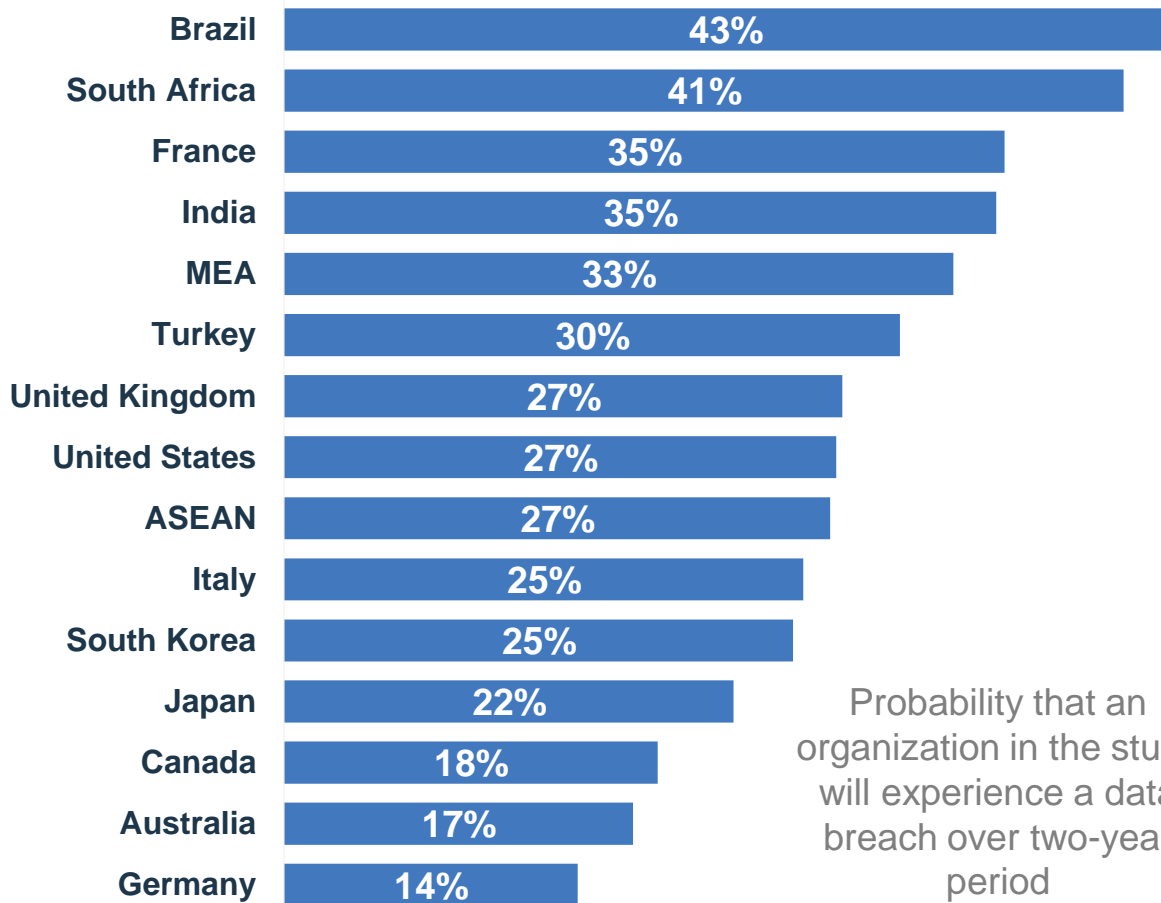
The odds are much greater that you will experience a data breach



Experiencing a data breach?

1 in 4

(Global average 28%)



Probability that an organization in the study will experience a data breach over two-year period

Global findings at a glance

\$3.86M / 6.4% 

Average total cost of data breach

\$148 / 4.8%

Average cost per record lost or stolen

24,615 / 2.2% 

Average number of breached records

27.9%

Likelihood of a recurring material breach over two years



419 companies participated
Currency: US dollar

Per-record costs for top three industries



\$408 Health

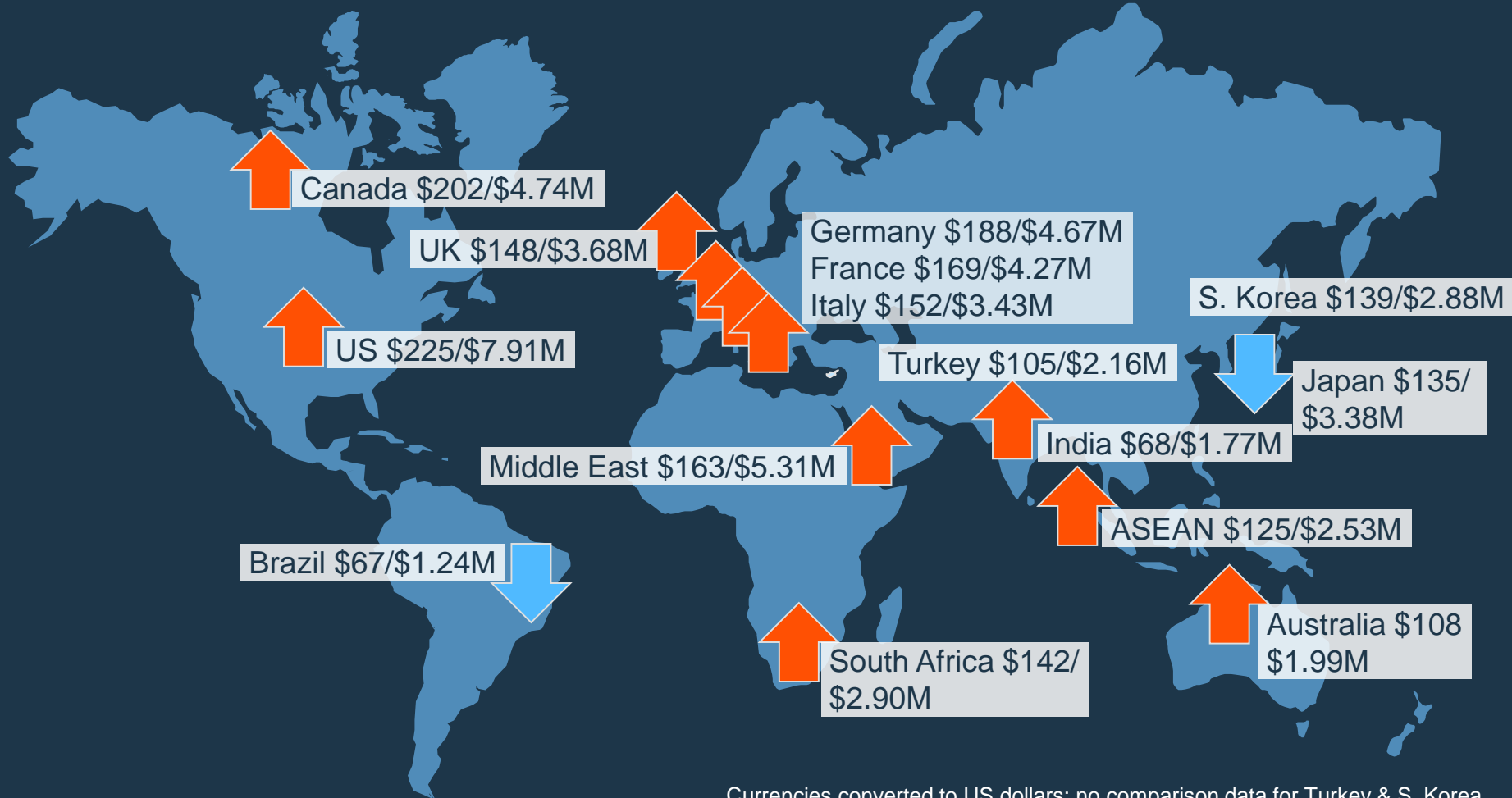


\$206 Financial



\$181 Services

Costs and trends vary widely across countries in the study



Currencies converted to US dollars; no comparison data for Turkey & S. Korea

United States at a glance

\$7.91M / 7%↑

Average total cost of data breach

\$233 / 3%↑

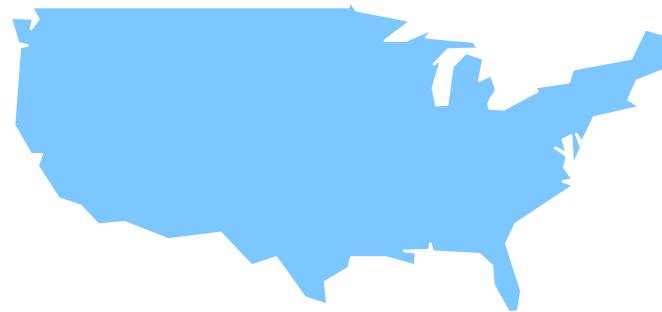
Average cost per record lost or stolen

31,465 ↑

Average number of breached records

\$4.20M ↑

Average cost of lost business



15 years in the study
65 companies participated
Currency: US dollar

Industries with the highest abnormal churn rate

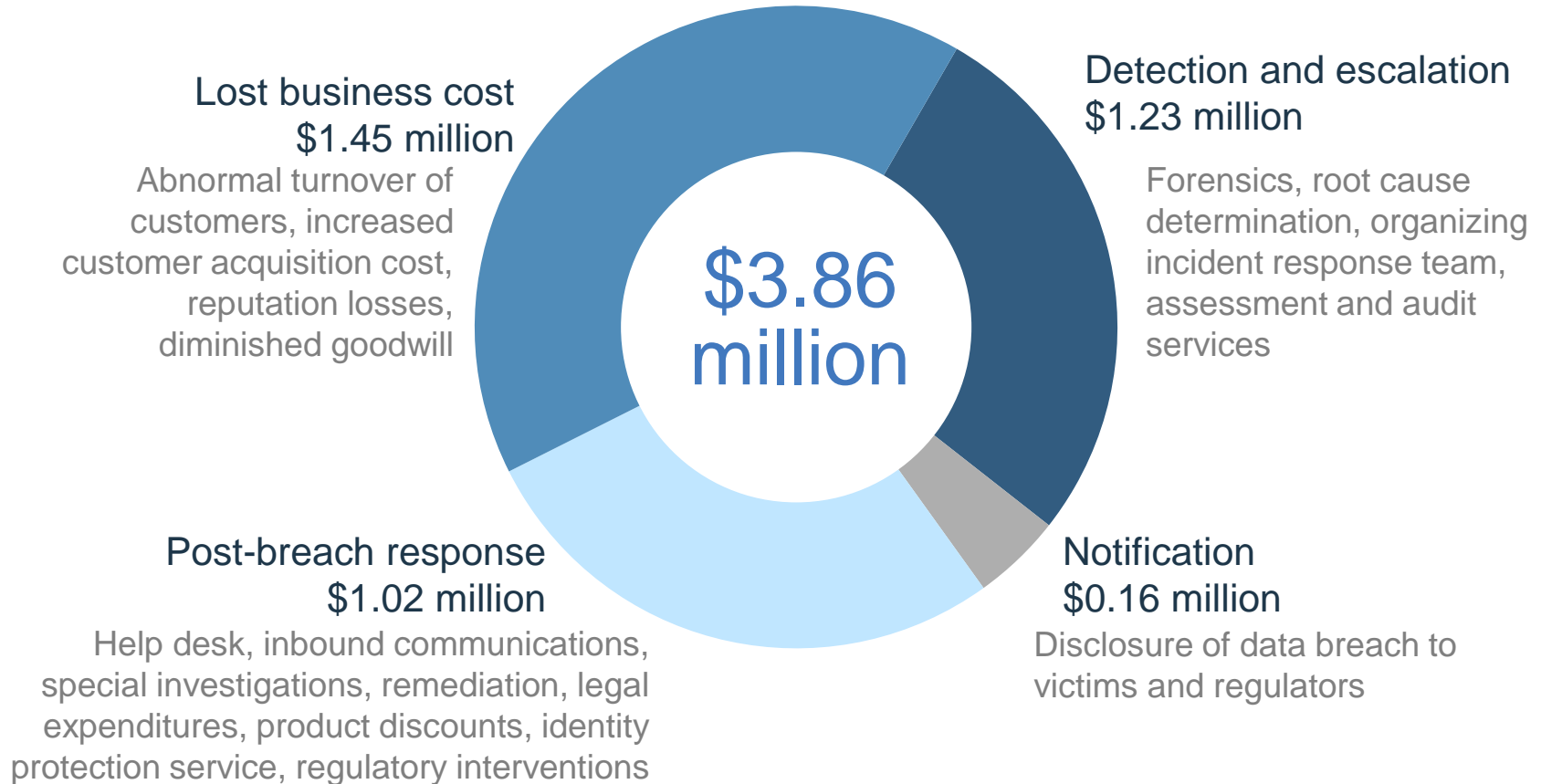
7.5% Financial

6.7% Health

6.3% Pharmaceuticals

The largest component of the total cost of a data breach is lost business

Components of the \$3.86 million cost per data breach



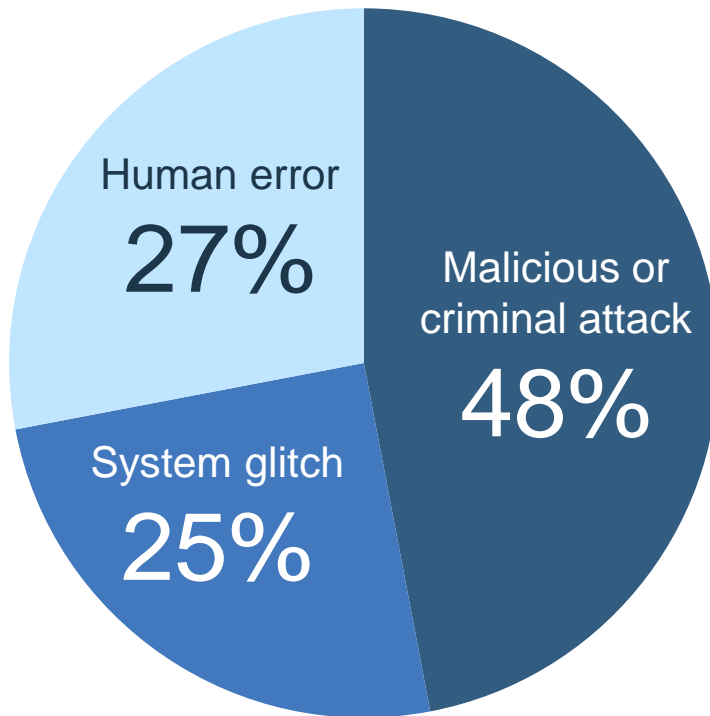
Currencies converted to US dollars

Public Sector Organizations at a Glance

- 32 public sector organizations (6.7% of the total benchmark sample)
- Per capita cost for public sector organizations is \$75 per compromised record
- Total average cost for public sector organizations is \$2.3 million
- Top factors that **decrease** breach cost for public sector organizations:
 - Extensive use of encryption
 - Formation of an IR team
 - Employee training
- Top factors that **increase** breach cost for public sector organizations:
 - 3rd party involvement in the breach
 - Compliance failure
 - Extensive cloud migration
- Mean time to identify the breach is 190 days
- Mean time to contain the breach is 57 days

Hackers and criminal insiders continue to cause most data breaches

\$128
per record to resolve



\$157
per record to resolve

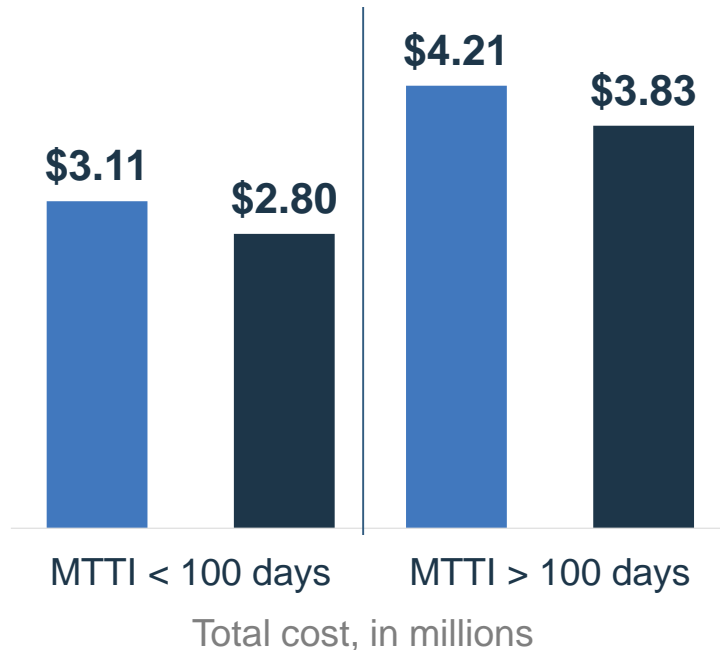
\$131
per record to resolve

Currencies converted to US dollars

Gaining visibility and responding faster help to reduce costs

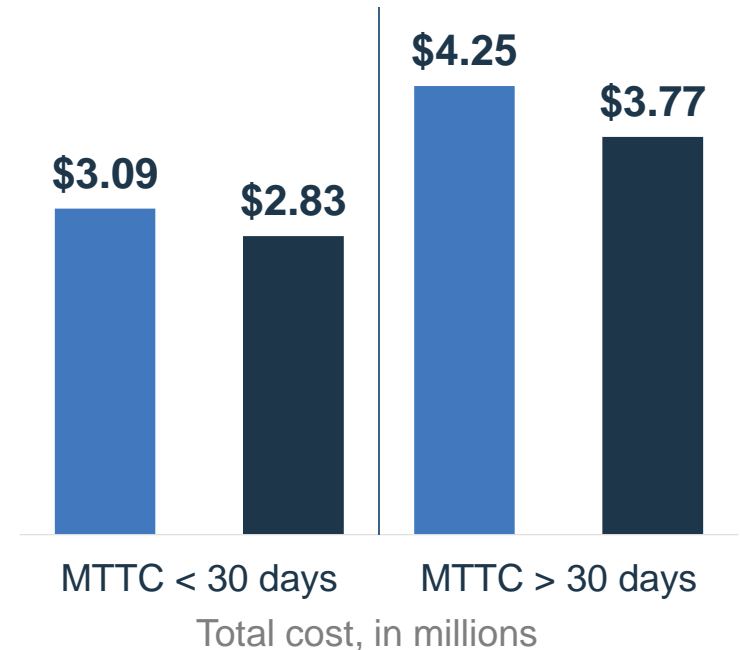
Mean time to identify (MTTI)

(The time it takes to detect that an incident has occurred)




Mean time to contain (MTTC)

(The time it takes to resolve a situation and ultimately restore service)



■ FY 2018 ■ FY 2017

Currencies converted to US dollars

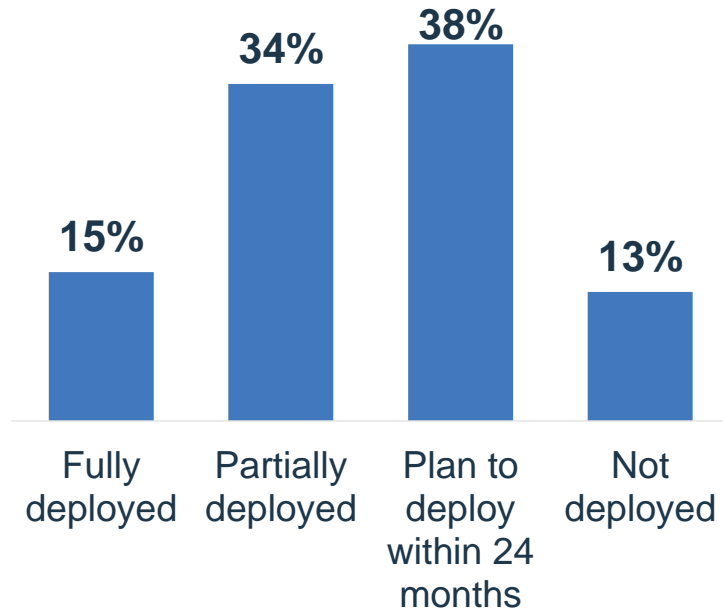


New this year:

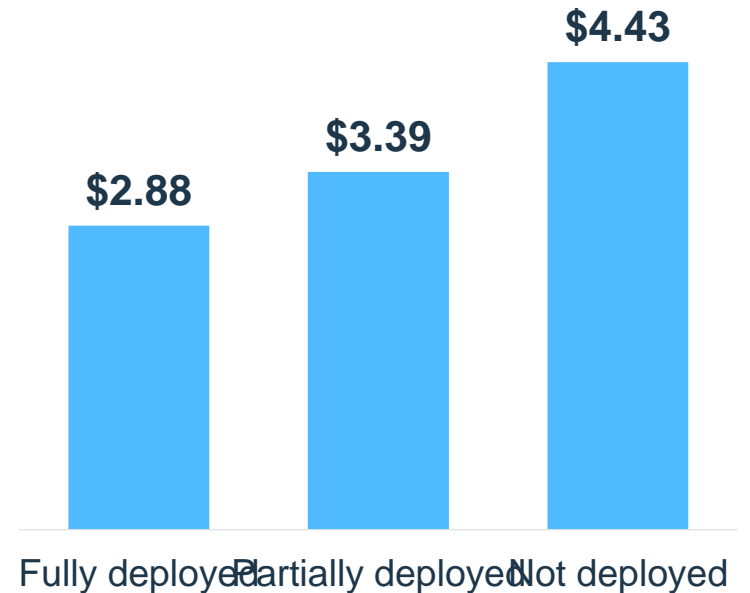
The impact of security automation

The current state of security automation: our findings

Current state of security automation



Cost impacts by level of deployment

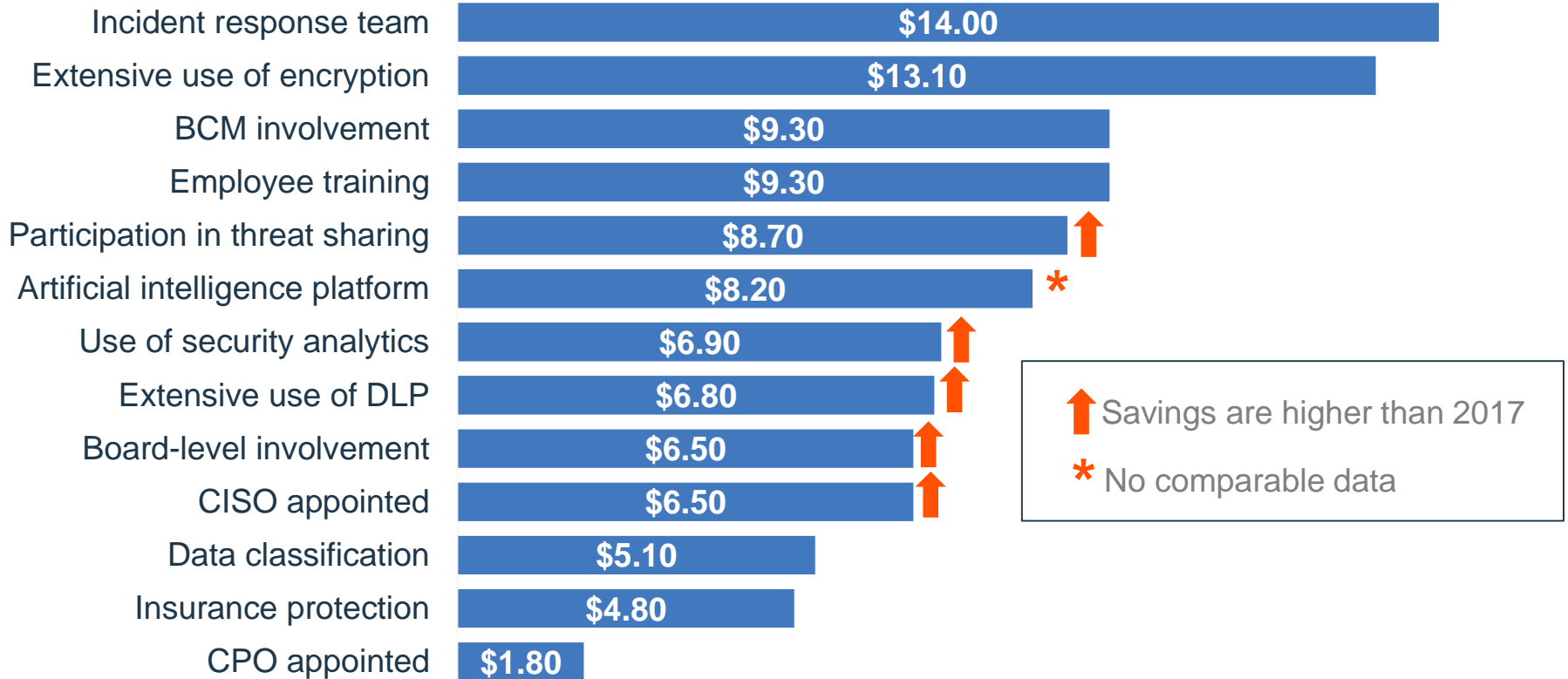


Average total cost, in millions

Currencies converted to US dollars

What you can do to help reduce the cost of a data breach

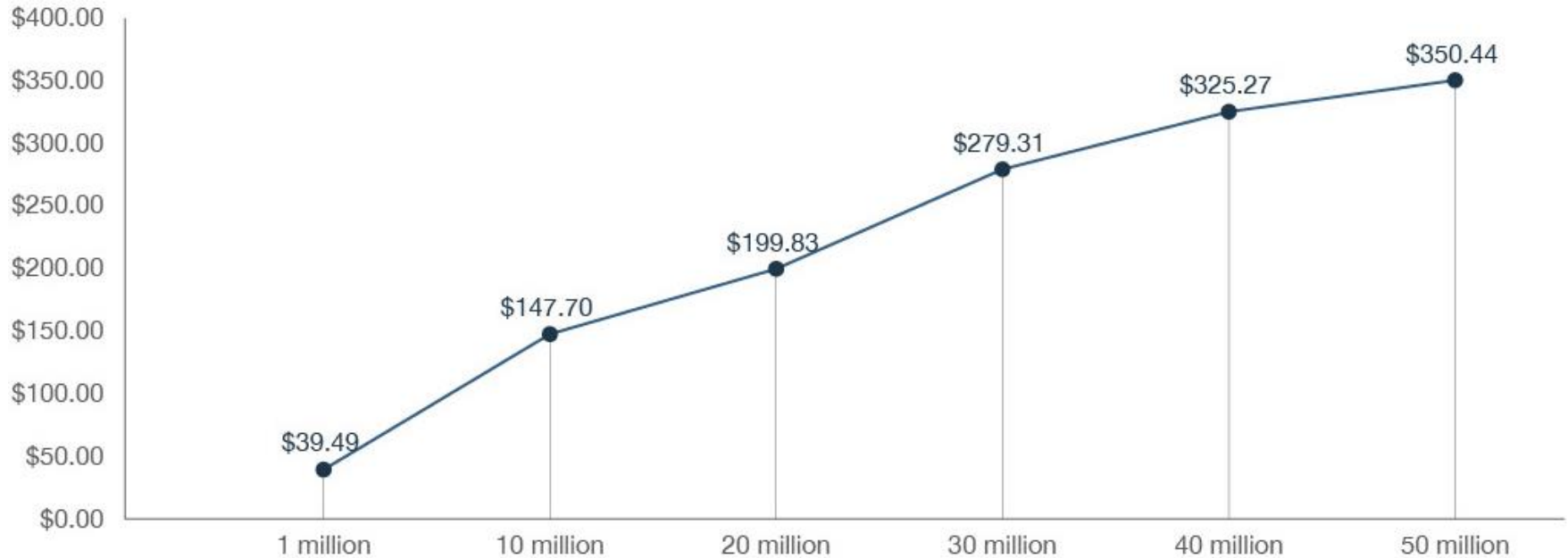
Amount by which the cost-per-record was lowered



Currencies converted to US dollars

**Also new this year:
The mega breach**

The average total cost of a mega breach



Key takeaways from this year's study

1

Lost business is the biggest financial consequence of a data breach

2

A proactive approach to incident response can significantly reduce cost and impact of a breach

3

Disruptive technologies like cloud and mobile add complexity and cost

4

Having the right skills, expertise and knowledge—from operations to the C-Suite—can impact an organization's ability to reduce the cost of a data breach

5

Investing in security technologies such as analytics, SIEM and encryption can help prevent breaches as well as reduce cost

6

Visibility across the incident life cycle is critical to identifying threats, prioritizing response and identifying data at risk

Engage with the numbers





Go to [ibm.com/security/data-breach](https://www.ibm.com/security/data-breach) and register to download the report, see what the data breach numbers look like for you in the calculator, and take a security posture self-assessment

Go to [ibm.com/security/services](https://www.ibm.com/security/services) to learn how IBM Security Services can help in your journey to reduce impact of and exposure to a data breach



THANK YOU

FOLLOW US ON:

-  ibm.com/security
-  securityintelligence.com
-  xforce.ibmcloud.com
-  [@ibmsecurity](https://twitter.com/ibmsecurity)
-  youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2017. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

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.

Questions



Contact Information

Dr. Larry Ponemon

Chairman and Founder
Ponemon Institute
Larry@Ponemon.org

Megan Powell

Product Marketing Manager
IBM Security
megan.powell@ibm.com
[linkedin.com/in/meganmitchellpowell/](https://www.linkedin.com/in/meganmitchellpowell/)

Amy Glasscock

Senior Policy Analyst
NASCIO
aglasscock@NASCIO.org

Meredith Ward

Senior Policy Analyst
NASCIO
mward@NASCIO.org

Follow Us



@NASCIO



/NASCIOmedia



/NASCIOmedia



National Association of State
Chief Information Officers
(NASCIO)