IBM Security

Key findings from the 2017 Cost of Data Breach Study: Global Overview

BENCHMARK RESEARCH SPONSORED BY IBM SECURITY
INDEPENDENTLY CONDUCTED BY
PONEMON INSTITUTE

JUNE 2017

Peter Allor
Senior Security Strategist, IBM Security

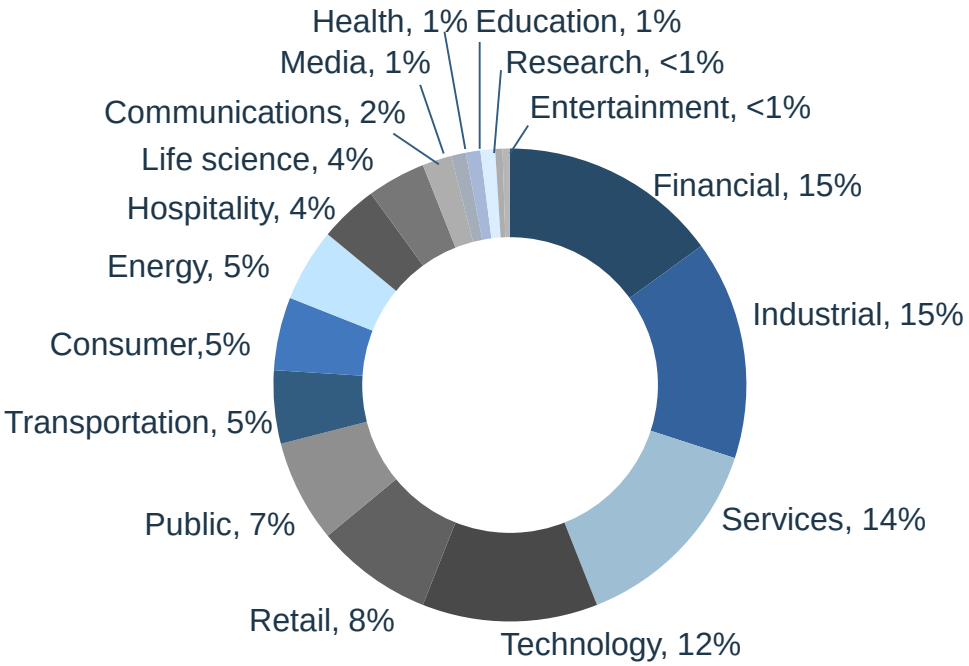
Ponemon INSTITUTE

IBM

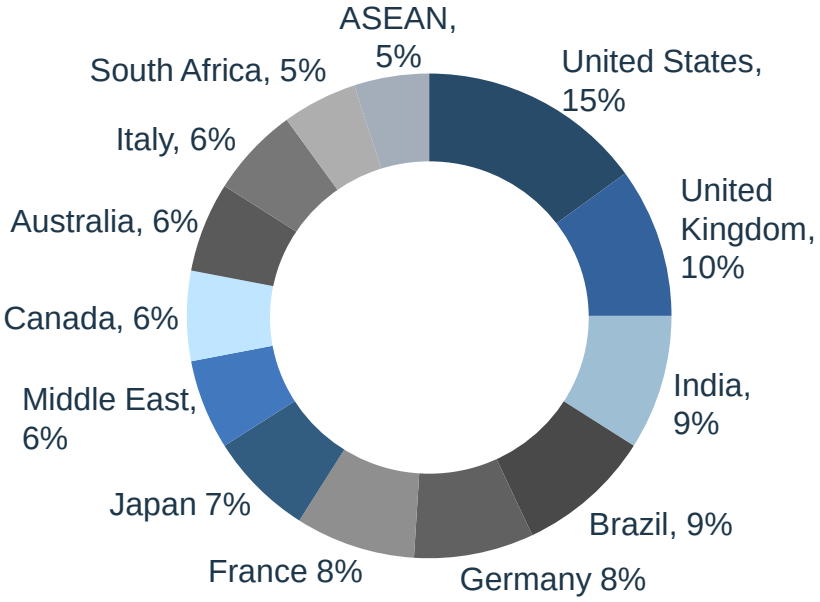
Approach and Terms

The 2017 Ponemon Cost of Data Breach Study covered 1,900 individuals across 419 companies in 13 countries or regions and 17 industries

Industries



Countries/regions



Understanding these terms will help you understand the report findings

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, a data breach involving between approximately 2,600 to slightly more than 100,000 compromised records

Participants

Organizations that experienced a data breach within the target incident range

Benchmark research

The unit of analysis is the organization; in a survey, the unit of analysis is the individual

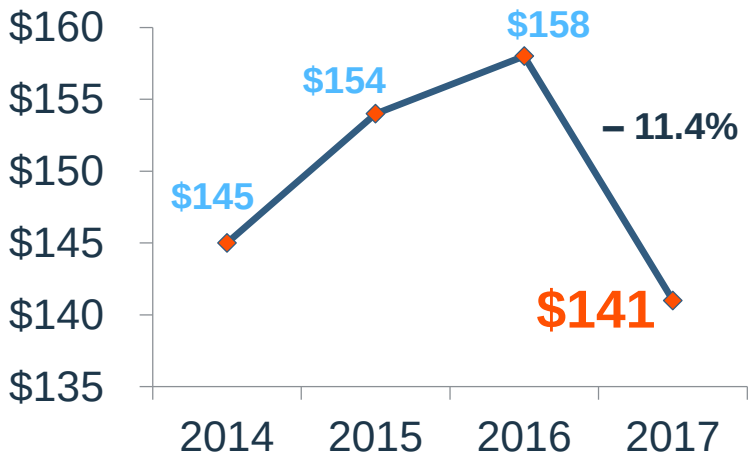
A mega-breach of more than 100,000 records is not considered typical. The cost data in this study cannot be used to calculate the financial impact of a mega-breach over 100,000 records.

The Report

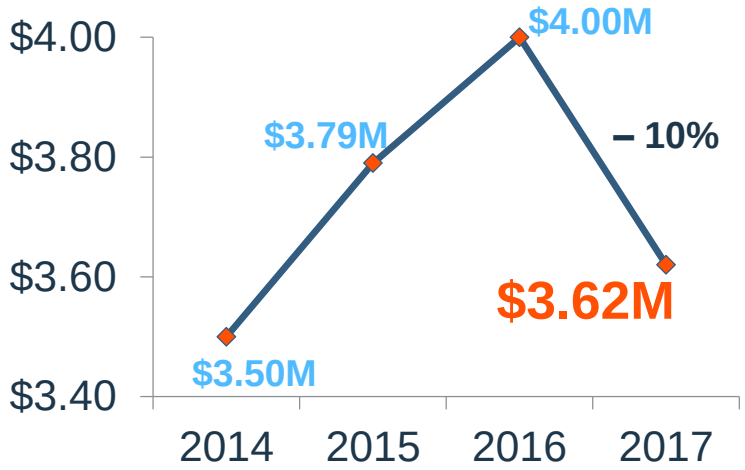
What goes up should come down

- The global average cost of a data breach is down over previous years
- 48% of the per-record 11.4% decrease over last year is due to the US dollar exchange rate
- The average size of a data breach increased 1.8% to 24,089 records

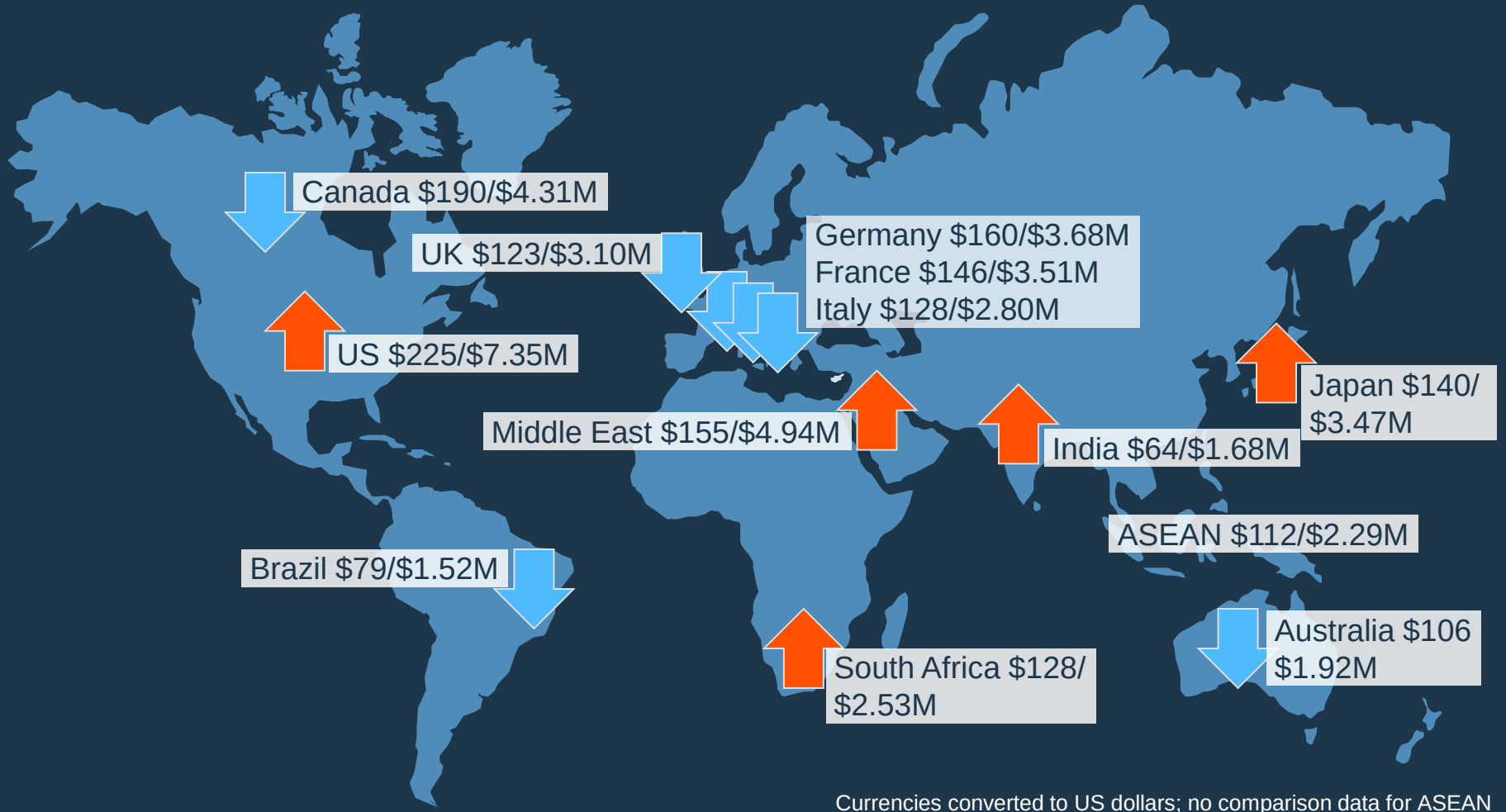
Global average cost per record
in US dollars



Global average cost per incident
in millions of US dollars

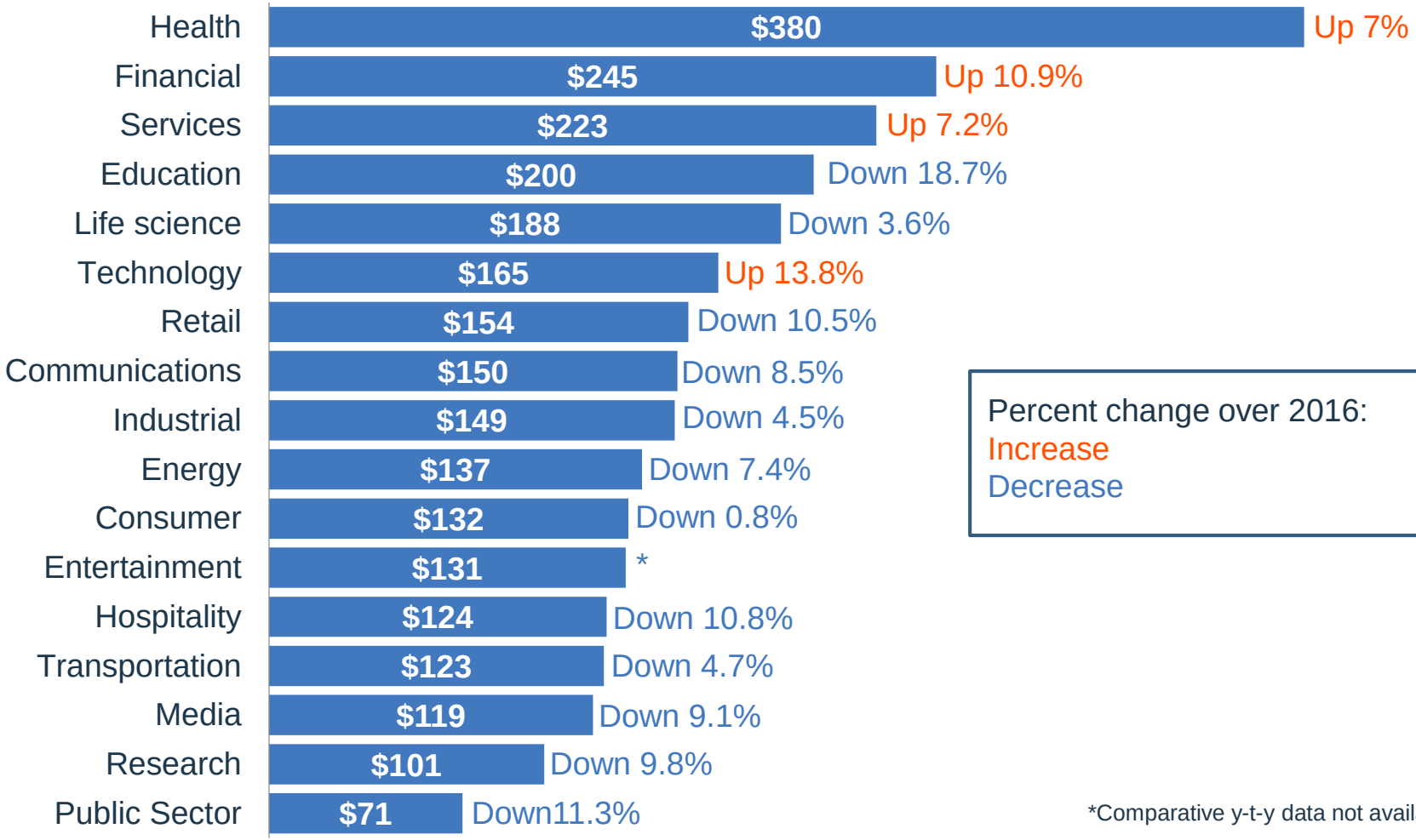


Costs and trends vary widely across countries in the study



Currencies converted to US dollars; no comparison data for ASEAN

The per-record cost of a data breach also varies widely by industry

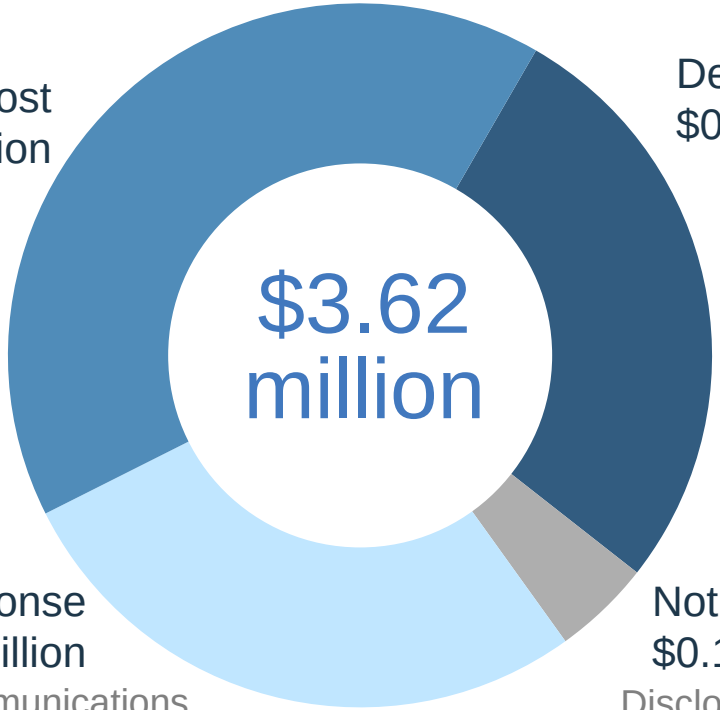


*Comparative y-t-y data not available

Currencies converted to US dollars

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

Components of the $3.62 million cost per data breach



Lost business cost
$1.51 million
Abnormal turnover of customers, increased customer acquisition cost, reputation losses, diminished goodwill

Detection and escalation
$0.99 million
Forensics, root cause determination, organizing incident response team, identifying victims

Ex-post response
$0.93 million
Help desk, inbound communications, special investigations, remediation, legal expenditures, product discounts, identity protection service, regulatory interventions

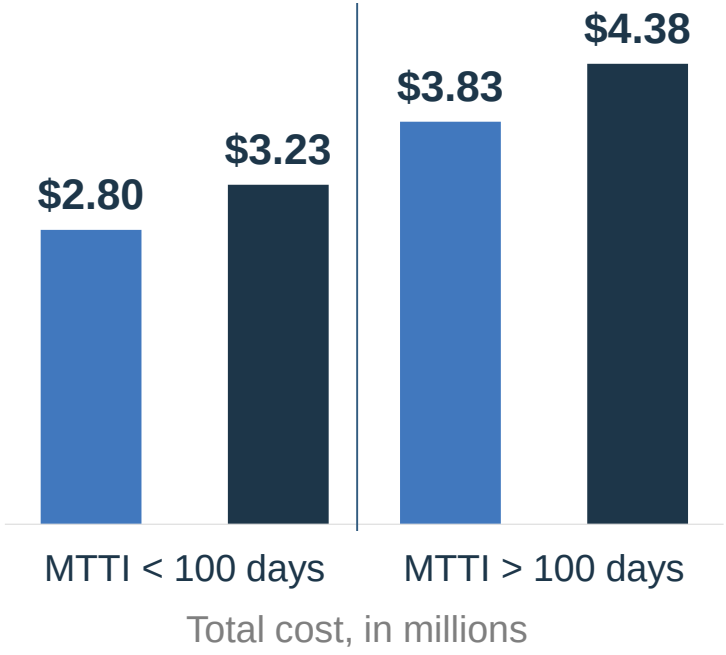
Notification
$0.19 million
Disclosure of data breach to victims and regulators

Currencies converted to US dollars

Gaining visibility and responding faster help to reduce costs

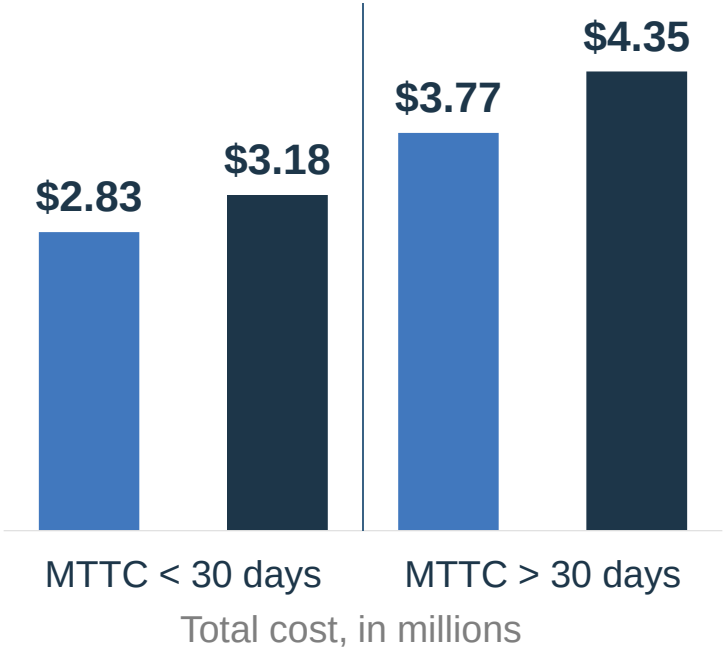
Mean time to identify (MTTI)

(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)

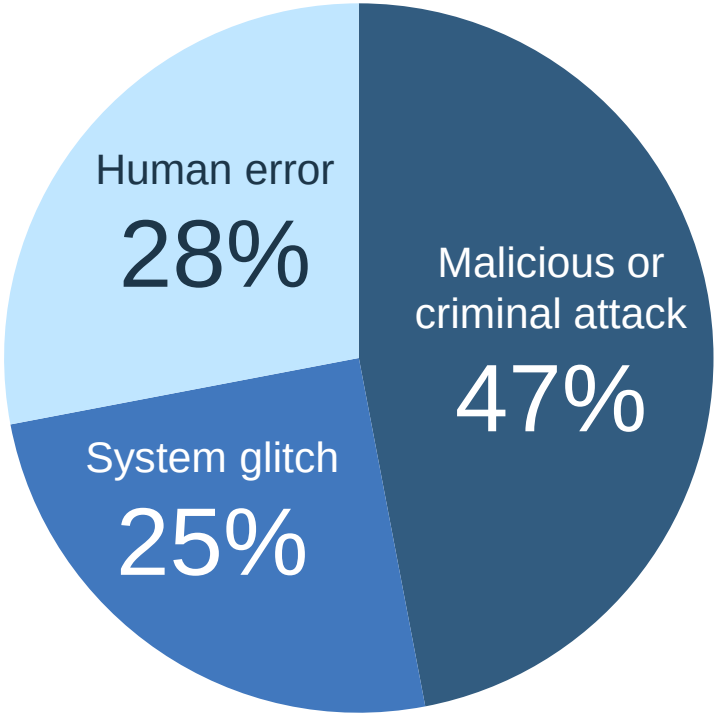


FY 2017 FY 2016

Currencies converted to US dollars

Hackers and criminal insiders continue to cause most data breaches

$126
per record to resolve



$156
per record to resolve

$128
per record to resolve

Currencies converted to US dollars

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 960,000

Being in a car accident on a 1,000-mile trip?

1 in 366

Dating a millionaire?

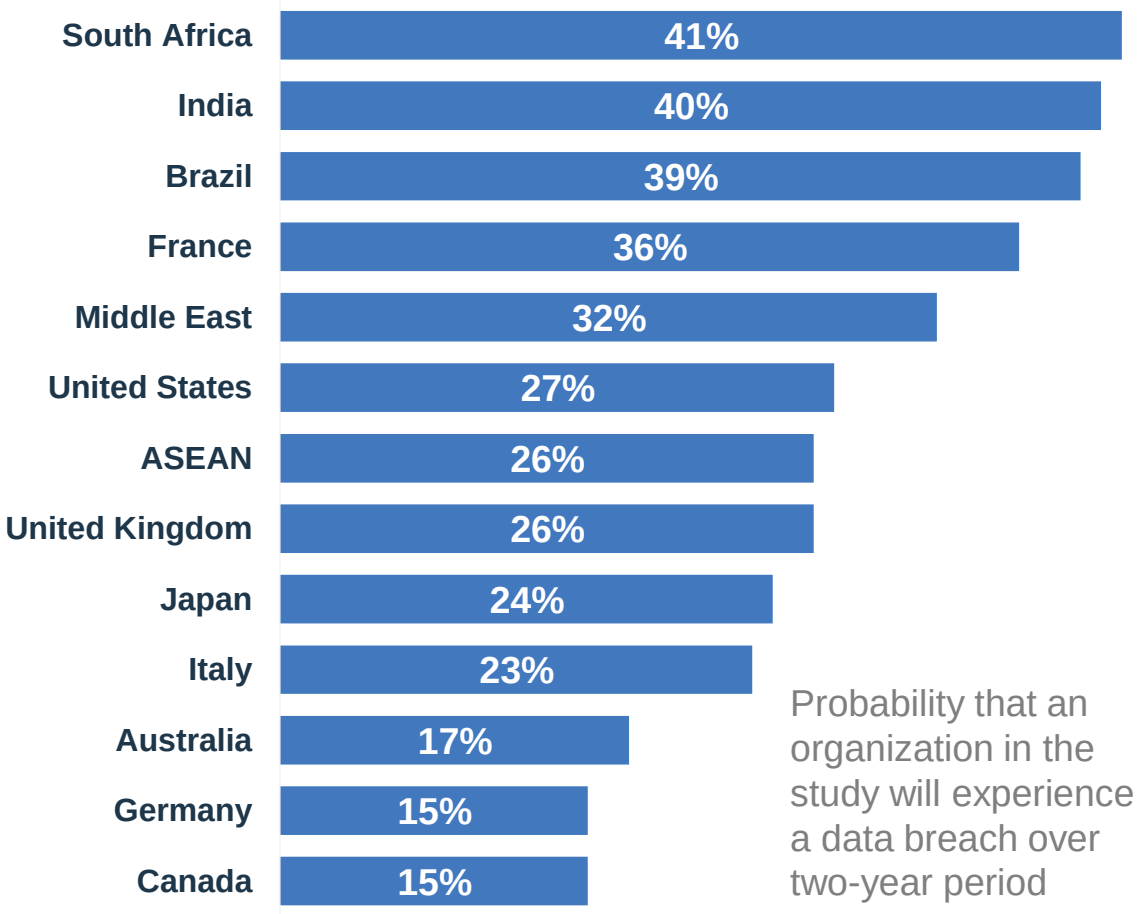
1 in 220

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

Experiencing a data breach?

1 in 4

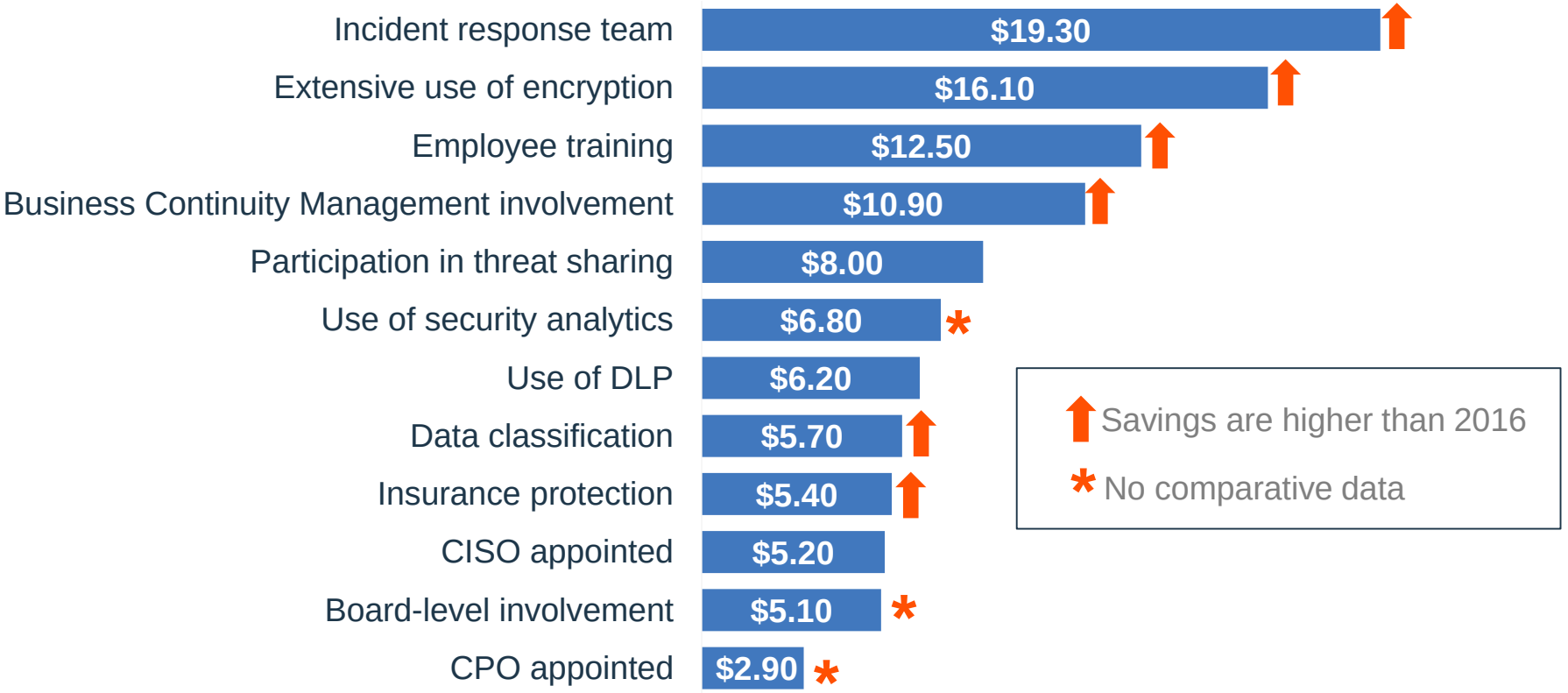
(Global average 28%)



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

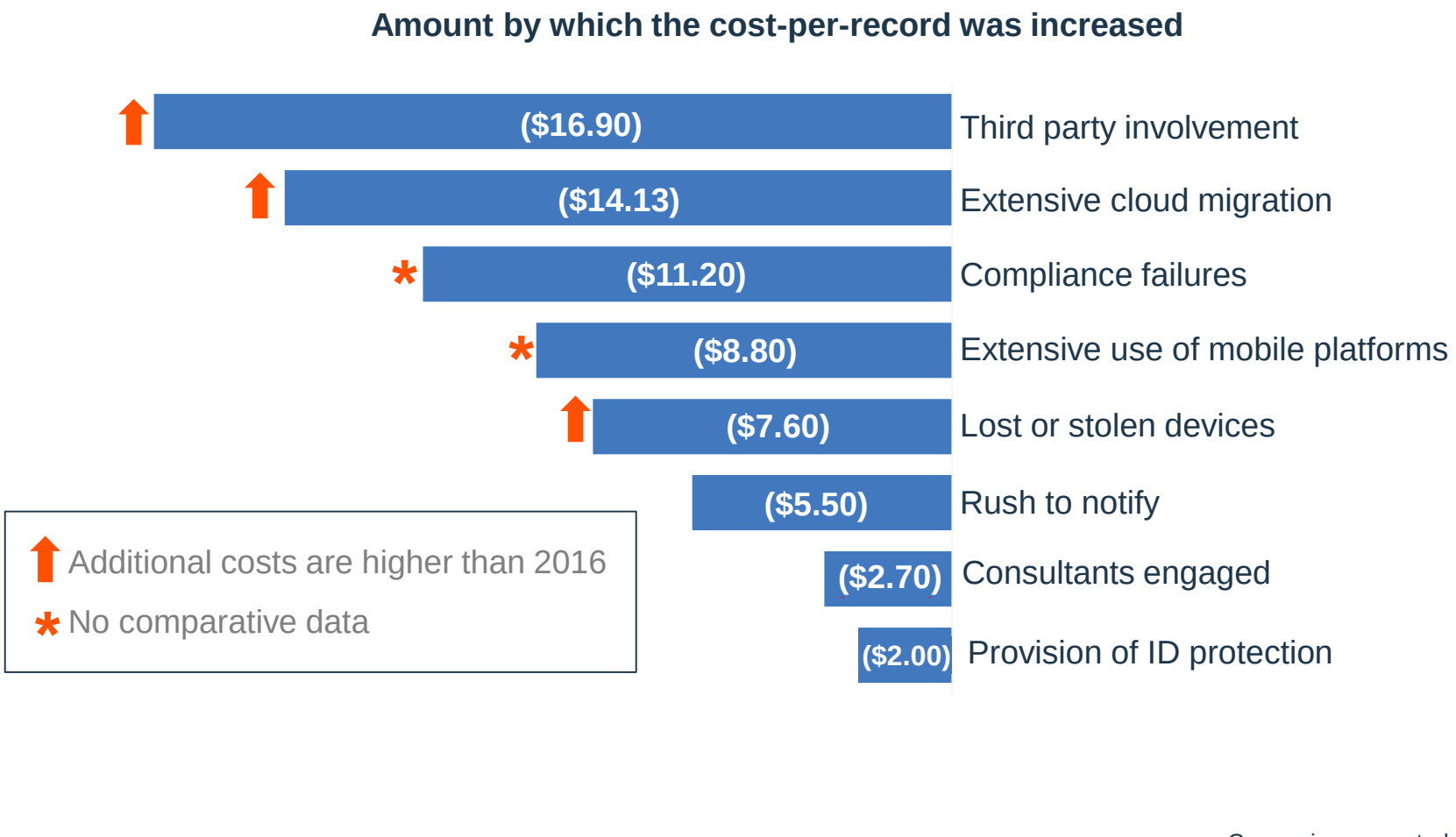
What you can do to help reduce the cost of a data breach

Amount by which the cost-per-record was lowered



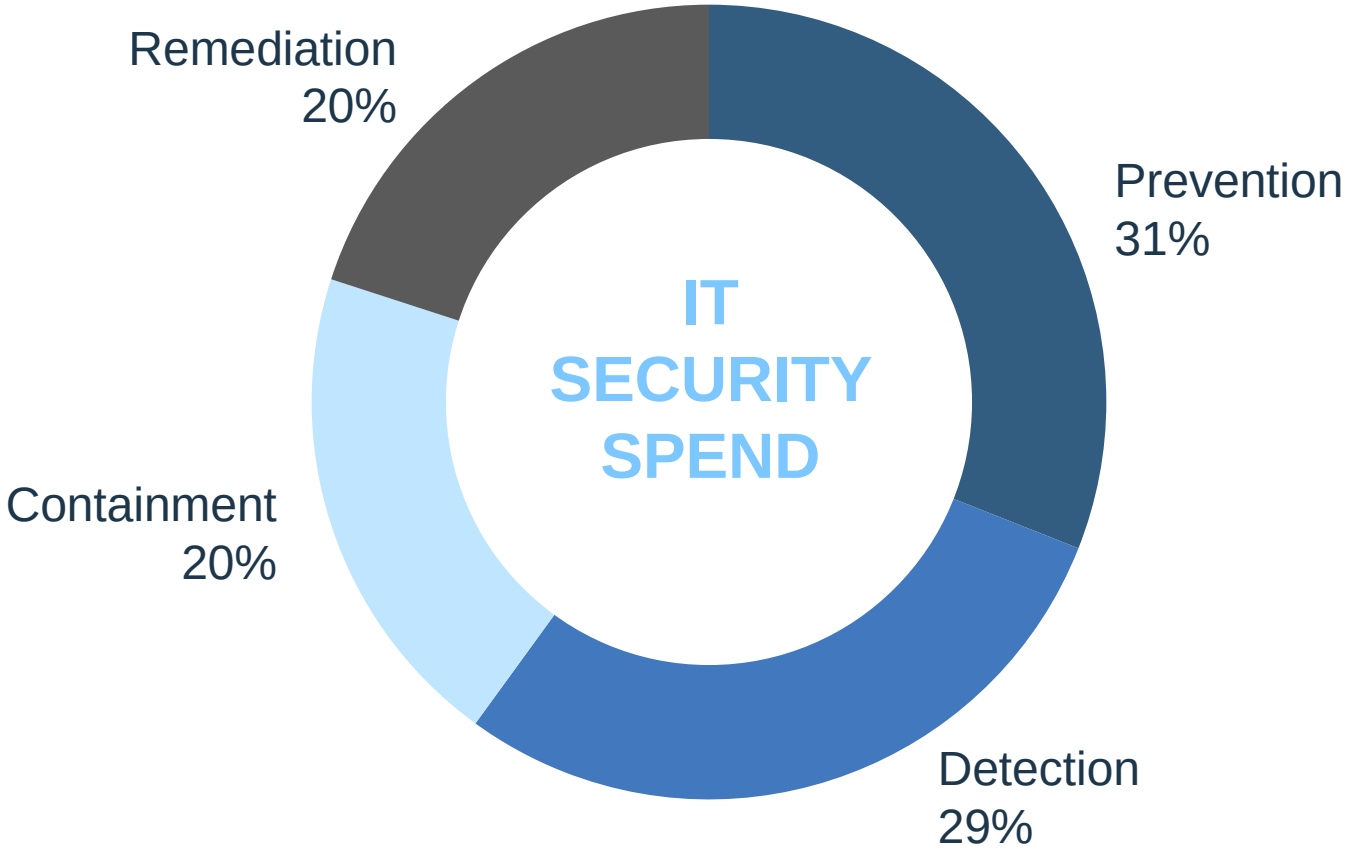
Currencies converted to US dollars

The study also found factors that increase the per-record cost



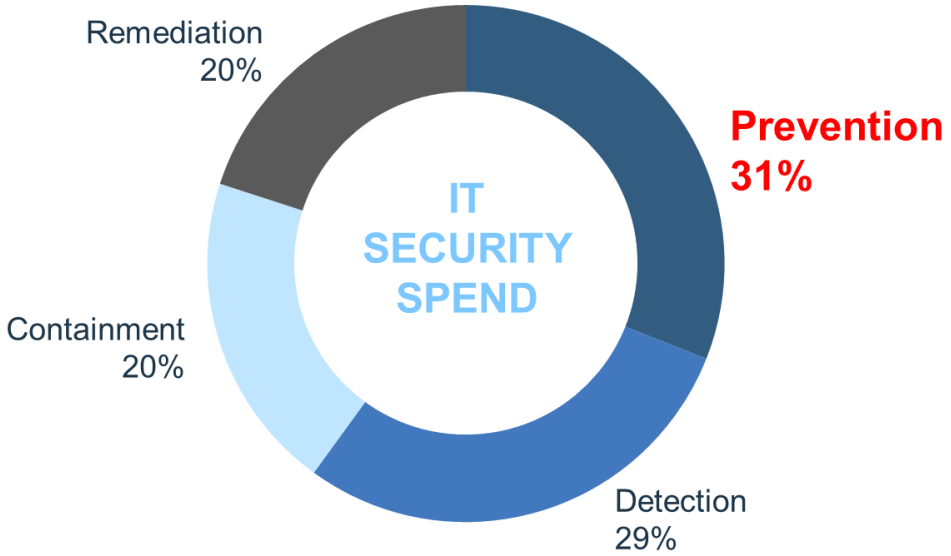
Currencies converted to US dollars

How organizations are spending their IT security budgets in relation to a breach



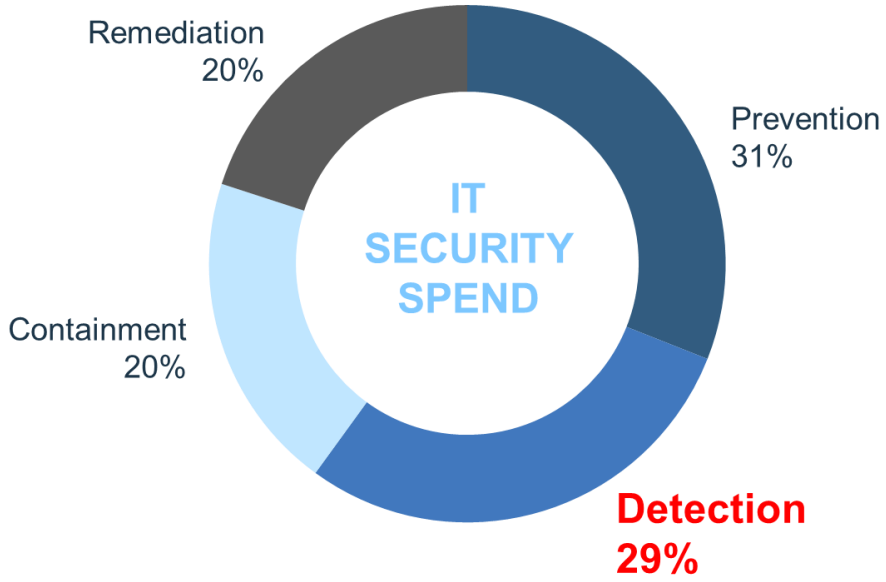
Prevention: When prevention works

- Agile incident management:
  - Which levers will your organization need to pull in the event of a widespread breach?
- Account privilege segregation
- Privileged password “checkout”
- Time-limited privileged access



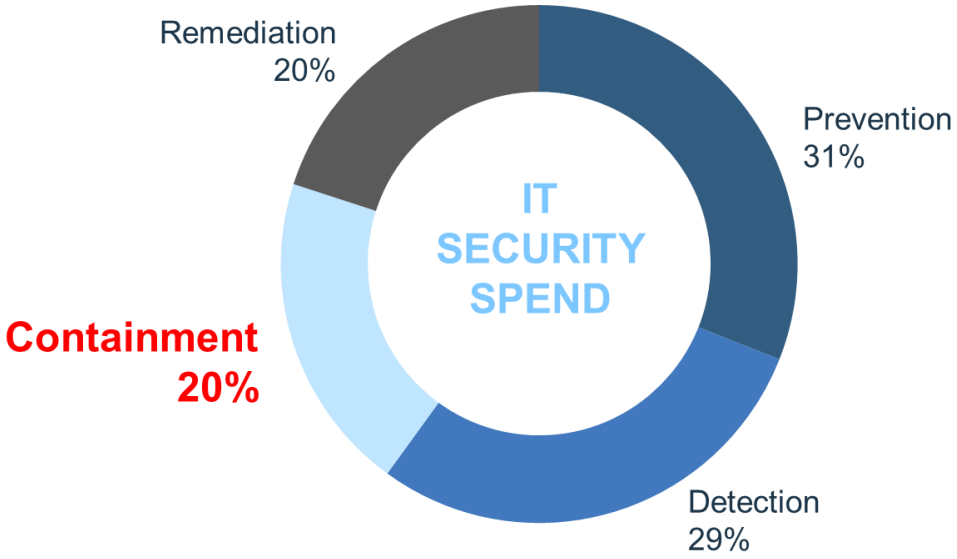
Detection: Worth the investment?

- Organization was undergoing active attack on a daily basis
- Knew what tools the attacker was using, but was concerned there were areas of enterprise they weren't seeing
- Worked with organization to install an EDR solution
- Identified attacker activity on hosts in real time



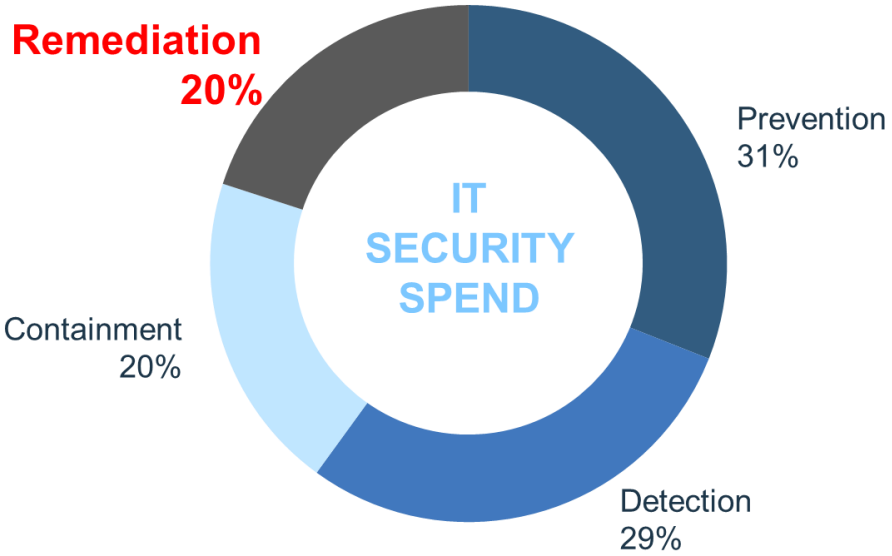
Containment

- WannaCry
  - Robust patching
  - Offline backups
  - Sensitive data segmented



Remediation

- Shamoon v2
- Destructive malware in the environment
- Recover data and get business running again as fast as possible
- Prevent similar capability from causing disruption in the environment in the future



Key takeaways from this year's study

1. Lost business is the biggest financial consequence of a data breach
2. Breaches that occur during cloud implementations and involve mobile add complexity and cost
3. 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
4. A proactive approach to incident response can significantly reduce cost and impact of a 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

Organizations are making investments and seeing results, but there remains much room for improvement

Global average percentage of **companies that**:

41%

Have a data security strategy

43%

Participate in threat intelligence sharing

52%

Deploy security intelligence systems including SIEM

48%

Deploy advanced identity and access management tools

59%

Extensively use encryption or cryptographic tools

56%

Outsource some or all of security operations or infrastructure

Where you should be focusing today…and the IBM Security Services

Client pain point	IBM Security Services solution
• Doesn't have a CSIRT or an Incident Response Team	• IBM X-Force Incident Response and Intelligence Services (IRIS)
• Doesn't have SIEM or use security analytics • Needs greater visibility	• Security intelligence and optimization consulting services • Managed SIEM (QRadar-based) • Endpoint Managed Security • Managed Security Services
• Lack of maturity • Gaps in security posture • Compliance and regulatory issues	• Security strategy, risk and compliance consulting services
• Extensive use of cloud	• Cloud security strategy
• Data and application security gaps • Extensive use of mobile platforms	• Managed data protection services for Guardium • Critical data protection program • Application Security Services for web and mobile apps • IBM X-Force Red security testing services

See the numbers

New this year! Cost Calculator tool

Go to **ibm.com**/security/data-breach and see what the data breach numbers look like for you

Go to **ibm.com**/security/data-breach to see the global study or a country-specific study

Go to **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

Q & A

IBM Security

THANK YOU

FOLLOW US ON:

ibm.com/security

securityintelligence.com

xforce.ibmcloud.com

@ibmsecurity

youtube/user/ibmsecuritysolutions

WGP03611USEN-00

The incidence of malicious attack varies considerably by country