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
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
- Financial, 15%
- Industrial, 15%
- Services, 14%
- Technology, 12%
- Retail, 8%
- Public, 7%
- Transportation, 5%
- Consumer, 5%
- Energy, 5%
- Hospitality, 4%
- Life science, 4%
- Communications, 2%
- Media, 1%
- Health, 1%
- Research, <1%
- Entertainment, <1%

### Countries/regions
- United States, 15%
- United Kingdom, 10%
- India, 9%
- Brazil, 9%
- France, 8%
- Germany, 8%
- Japan, 7%
- Middle East, 6%
- Canada, 6%
- Australia, 6%
- Italy, 6%
- South Africa, 5%
- ASEAN, 5%
- United States, 15%
- United Kingdom, 10%
- India, 9%
- Brazil, 9%
- France, 8%
- Germany, 8%
- Japan, 7%
- Middle East, 6%
- Canada, 6%
- Australia, 6%
- Italy, 6%
- South Africa, 5%
- ASEAN, 5%
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.

**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
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
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

<table>
<thead>
<tr>
<th>Industry</th>
<th>Per-record Cost</th>
<th>Percent Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>Health</td>
<td>$380</td>
<td>Up 7%</td>
</tr>
<tr>
<td>Financial</td>
<td>$245</td>
<td>Up 10.9%</td>
</tr>
<tr>
<td>Services</td>
<td>$223</td>
<td>Up 7.2%</td>
</tr>
<tr>
<td>Education</td>
<td>$200</td>
<td>Down 18.7%</td>
</tr>
<tr>
<td>Life science</td>
<td>$188</td>
<td>Down 3.6%</td>
</tr>
<tr>
<td>Technology</td>
<td>$165</td>
<td>Up 13.8%</td>
</tr>
<tr>
<td>Retail</td>
<td>$154</td>
<td>Down 10.5%</td>
</tr>
<tr>
<td>Communications</td>
<td>$150</td>
<td>Down 8.5%</td>
</tr>
<tr>
<td>Industrial</td>
<td>$149</td>
<td>Down 4.5%</td>
</tr>
<tr>
<td>Energy</td>
<td>$137</td>
<td>Down 7.4%</td>
</tr>
<tr>
<td>Consumer</td>
<td>$132</td>
<td>Down 0.8%</td>
</tr>
<tr>
<td>Entertainment</td>
<td>$131</td>
<td>*</td>
</tr>
<tr>
<td>Hospitality</td>
<td>$124</td>
<td>Down 10.8%</td>
</tr>
<tr>
<td>Transportation</td>
<td>$123</td>
<td>Down 4.7%</td>
</tr>
<tr>
<td>Media</td>
<td>$119</td>
<td>Down 9.1%</td>
</tr>
<tr>
<td>Research</td>
<td>$101</td>
<td>Down 9.8%</td>
</tr>
<tr>
<td>Public Sector</td>
<td>$71</td>
<td>Down 11.3%</td>
</tr>
</tbody>
</table>

Percent change over 2016:

- Increase
- Decrease

Currencies converted to US dollars

*Comparative y-t-y data not available
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

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

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

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

**$3.62 million**

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)

<table>
<thead>
<tr>
<th>MTTI &lt; 100 days</th>
<th>MTTI &gt; 100 days</th>
<th>Total cost, in millions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2.80</td>
<td>$3.23</td>
<td>$3.83</td>
</tr>
<tr>
<td>$4.38</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MTTC &lt; 30 days</th>
<th>MTTC &gt; 30 days</th>
<th>Total cost, in millions</th>
</tr>
</thead>
<tbody>
<tr>
<td>$2.83</td>
<td>$3.18</td>
<td>$3.77</td>
</tr>
<tr>
<td>$4.35</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Currencies converted to US dollars
Hackers and criminal insiders continue to cause most data breaches

- Human error: 28% - $126 per record to resolve
- System glitch: 25% - $128 per record to resolve
- Malicious or criminal attack: 47% - $156 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

<table>
<thead>
<tr>
<th>Country</th>
<th>Probability (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>South Africa</td>
<td>41%</td>
</tr>
<tr>
<td>India</td>
<td>40%</td>
</tr>
<tr>
<td>Brazil</td>
<td>39%</td>
</tr>
<tr>
<td>France</td>
<td>36%</td>
</tr>
<tr>
<td>Middle East</td>
<td>32%</td>
</tr>
<tr>
<td>United States</td>
<td>27%</td>
</tr>
<tr>
<td>ASEAN</td>
<td>26%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>26%</td>
</tr>
<tr>
<td>Japan</td>
<td>24%</td>
</tr>
<tr>
<td>Italy</td>
<td>23%</td>
</tr>
<tr>
<td>Australia</td>
<td>17%</td>
</tr>
<tr>
<td>Germany</td>
<td>15%</td>
</tr>
<tr>
<td>Canada</td>
<td>15%</td>
</tr>
</tbody>
</table>
What you can do to help reduce the cost of a data breach

Amount by which the cost-per-record was lowered

- Incident response team: $19.30
- Extensive use of encryption: $16.10
- Employee training: $12.50
- Business Continuity Management involvement: $10.90
- Participation in threat sharing: $8.00
- Use of security analytics: $6.80 *
- Use of DLP: $6.20
- Data classification: $5.70
- Insurance protection: $5.40
- CISO appointed: $5.20
- Board-level involvement: $5.10 *
- CPO appointed: $2.90 *

Savings are higher than 2016
* No comparative data

Currencies converted to US dollars
The study also found factors that increase the per-record cost

Amount by which the cost-per-record was increased

- Third party involvement: ($16.90)
- Extensive cloud migration: ($14.13)
- Compliance failures: ($11.20)
- Extensive use of mobile platforms: ($8.80)
- Lost or stolen devices: ($7.60)
- Rush to notify: ($5.50)
- Consultants engaged: ($2.70)
- Provision of ID protection: ($2.00)

Additional costs are higher than 2016

* No comparative data

Currencies converted to US dollars
How organizations are spending their IT security budgets in relation to a breach

- Prevention: 31%
- Detection: 29%
- Remediation: 20%
- Containment: 20%

IT SECURITY SPEND
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 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

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

Go to [ibm.com/security/data-breach](http://ibm.com/security/data-breach) and see what the data breach numbers look like for you.

Go to [ibm.com/security/data-breach](http://ibm.com/security/data-breach) to see the global study or a country-specific study.

Go to [ibm.com/security/services](http://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.

New this year! [Cost Calculator tool](http://ibm.com).
Q & A
THANK YOU

FOLLOW US ON:

ibm.com/security
securityintelligence.com
xforce.ibmcloud.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.
The incidence of malicious attack varies considerably by country

<table>
<thead>
<tr>
<th>Region</th>
<th>Malicious or criminal attack</th>
<th>System glitch</th>
<th>Human error</th>
</tr>
</thead>
<tbody>
<tr>
<td>Middle East</td>
<td>59%</td>
<td>22%</td>
<td>19%</td>
</tr>
<tr>
<td>United States</td>
<td>52%</td>
<td>24%</td>
<td>24%</td>
</tr>
<tr>
<td>France</td>
<td>50%</td>
<td>19%</td>
<td>31%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>50%</td>
<td>23%</td>
<td>28%</td>
</tr>
<tr>
<td>Japan</td>
<td>48%</td>
<td>24%</td>
<td>28%</td>
</tr>
<tr>
<td>Australia</td>
<td>48%</td>
<td>24%</td>
<td>28%</td>
</tr>
<tr>
<td>Canada</td>
<td>48%</td>
<td>22%</td>
<td>30%</td>
</tr>
<tr>
<td>Germany</td>
<td>46%</td>
<td>34%</td>
<td>20%</td>
</tr>
<tr>
<td>Brazil</td>
<td>44%</td>
<td>25%</td>
<td>31%</td>
</tr>
<tr>
<td>South Africa</td>
<td>43%</td>
<td>29%</td>
<td>29%</td>
</tr>
<tr>
<td>India</td>
<td>41%</td>
<td>33%</td>
<td>26%</td>
</tr>
<tr>
<td>ASEAN</td>
<td>40%</td>
<td>25%</td>
<td>35%</td>
</tr>
<tr>
<td>Italy</td>
<td>40%</td>
<td>24%</td>
<td>36%</td>
</tr>
</tbody>
</table>

- Malicious or criminal attack
- System glitch
- Human error