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**
- Financial, 16%
- Services, 15%
- Industrial, 14%
- Technology, 13%
- Public, 7%
- Retail, 7%
- Transportation, 5%
- Consumer, 5%
- Communications, 4%
- Energy, 3%
- Pharmaceuticals, 3%
- Hospitality, 2%
- Research, <1%
- Entertainment, <1%
- Health, 1%
- Education, 1%

**Countries/regions**
- United States, 14%
- United Kingdom, 9%
- India, 9%
- Brazil, 8%
- France, 8%
- Germany, 7%
- Turkey, 4%
- ASEAN, 4%
- South Korea, 5%
- Italy, 5%
- Australia, 5%
- Canada, 6%
- Middle East, 6%
- Japan, 6%
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

(Globally average 28%)

<table>
<thead>
<tr>
<th>Country</th>
<th>Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Brazil</td>
<td>43%</td>
</tr>
<tr>
<td>South Africa</td>
<td>41%</td>
</tr>
<tr>
<td>France</td>
<td>35%</td>
</tr>
<tr>
<td>India</td>
<td>35%</td>
</tr>
<tr>
<td>MEA</td>
<td>33%</td>
</tr>
<tr>
<td>Turkey</td>
<td>30%</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>27%</td>
</tr>
<tr>
<td>United States</td>
<td>27%</td>
</tr>
<tr>
<td>ASEAN</td>
<td>27%</td>
</tr>
<tr>
<td>Italy</td>
<td>25%</td>
</tr>
<tr>
<td>South Korea</td>
<td>25%</td>
</tr>
<tr>
<td>Japan</td>
<td>22%</td>
</tr>
<tr>
<td>Canada</td>
<td>18%</td>
</tr>
<tr>
<td>Australia</td>
<td>17%</td>
</tr>
<tr>
<td>Germany</td>
<td>14%</td>
</tr>
</tbody>
</table>

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

- Canada: $202/$4.74M
- US: $225/$7.91M
- Brazil: $67/$1.24M
- UK: $148/$3.68M
- France: $169/$4.27M
- Italy: $152/$3.43M
- Germany: $188/$4.67M
- Turkey: $105/$2.16M
- India: $68/$1.77M
- ASEAN: $125/$2.53M
- South Africa: $142/$2.90M
- Japan: $135/$3.38M
- S. Korea: $139/$2.88M
- Middle East: $163/$5.31M
- Australia: $108/$1.99M

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:

- **Lost business cost**: $1.45 million
  - Abnormal turnover of customers, increased customer acquisition cost, reputation losses, diminished goodwill

- **Detection and escalation**: $1.23 million
  - Forensics, root cause determination, organizing incident response team, assessment and audit services

- **Post-breach response**: $1.02 million
  - Help desk, inbound communications, special investigations, remediation, legal expenditures, product discounts, identity protection service, regulatory interventions

- **Notification**: $0.16 million
  - Disclosure of data breach to victims and regulators

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

- Malicious or criminal attack: 48%
- Human error: 27%
- System glitch: 25%

$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)

<table>
<thead>
<tr>
<th>MTTI &lt; 100 days</th>
<th>MTTI &gt; 100 days</th>
</tr>
</thead>
<tbody>
<tr>
<td>$3.11</td>
<td>$2.80</td>
</tr>
<tr>
<td>$4.21</td>
<td>$3.83</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>MTTC &lt; 30 days</th>
<th>MTTC &gt; 30 days</th>
</tr>
</thead>
<tbody>
<tr>
<td>$3.09</td>
<td>$2.83</td>
</tr>
<tr>
<td>$4.25</td>
<td>$3.77</td>
</tr>
</tbody>
</table>

Total cost, in millions

Currencies converted to US dollars

FY 2018 FY 2017
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

- Fully deployed: $2.88
- Partially deployed: $3.39
- Plan to deploy within 24 months: $4.43
- Not deployed: 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

<table>
<thead>
<tr>
<th>Action</th>
<th>Savings (US dollars)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incident response team</td>
<td>$14.00</td>
</tr>
<tr>
<td>Extensive use of encryption</td>
<td>$13.10</td>
</tr>
<tr>
<td>BCM involvement</td>
<td>$9.30</td>
</tr>
<tr>
<td>Employee training</td>
<td>$9.30</td>
</tr>
<tr>
<td>Participation in threat sharing</td>
<td>$8.70</td>
</tr>
<tr>
<td>Artificial intelligence platform</td>
<td>$8.20</td>
</tr>
<tr>
<td>Use of security analytics</td>
<td>$6.90</td>
</tr>
<tr>
<td>Extensive use of DLP</td>
<td>$6.80</td>
</tr>
<tr>
<td>Board-level involvement</td>
<td>$6.50</td>
</tr>
<tr>
<td>CISO appointed</td>
<td>$6.50</td>
</tr>
<tr>
<td>Data classification</td>
<td>$5.10</td>
</tr>
<tr>
<td>Insurance protection</td>
<td>$4.80</td>
</tr>
<tr>
<td>CPO appointed</td>
<td>$1.80</td>
</tr>
</tbody>
</table>

Savings are higher than 2017

* No comparable data

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 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 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
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.

WGP03611USEN-00
Questions
Contact Information

Dr. Larry Ponemon
Chairman and Founder
Ponemon Institute
Larry@Ponemon.org

Amy Glasscock
Senior Policy Analyst
NASCIO
aglasscock@NASCIO.org

Megan Powell
Product Marketing Manager
IBM Security
megan.powell@ibm.com
linkedin.com/in/meganmitchellpowell/

Meredith Ward
Senior Policy Analyst
NASCIO
mward@NASCIO.org