

Cost of a Data Breach Report 2020

Key Findings and Best Practices for Public
Sector Organizations

Charles DeBeck
Strategic Cyber Threat
Intelligence Expert
X-Force IRIS

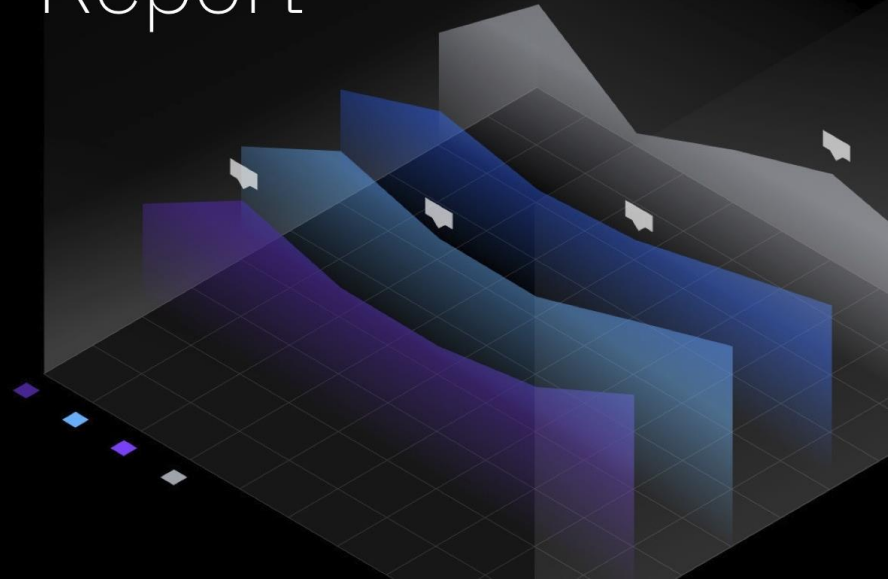


Today's topics

- 2020 Cost of a Data Breach Report: Key findings
- Minimizing data breach costs: Best practices

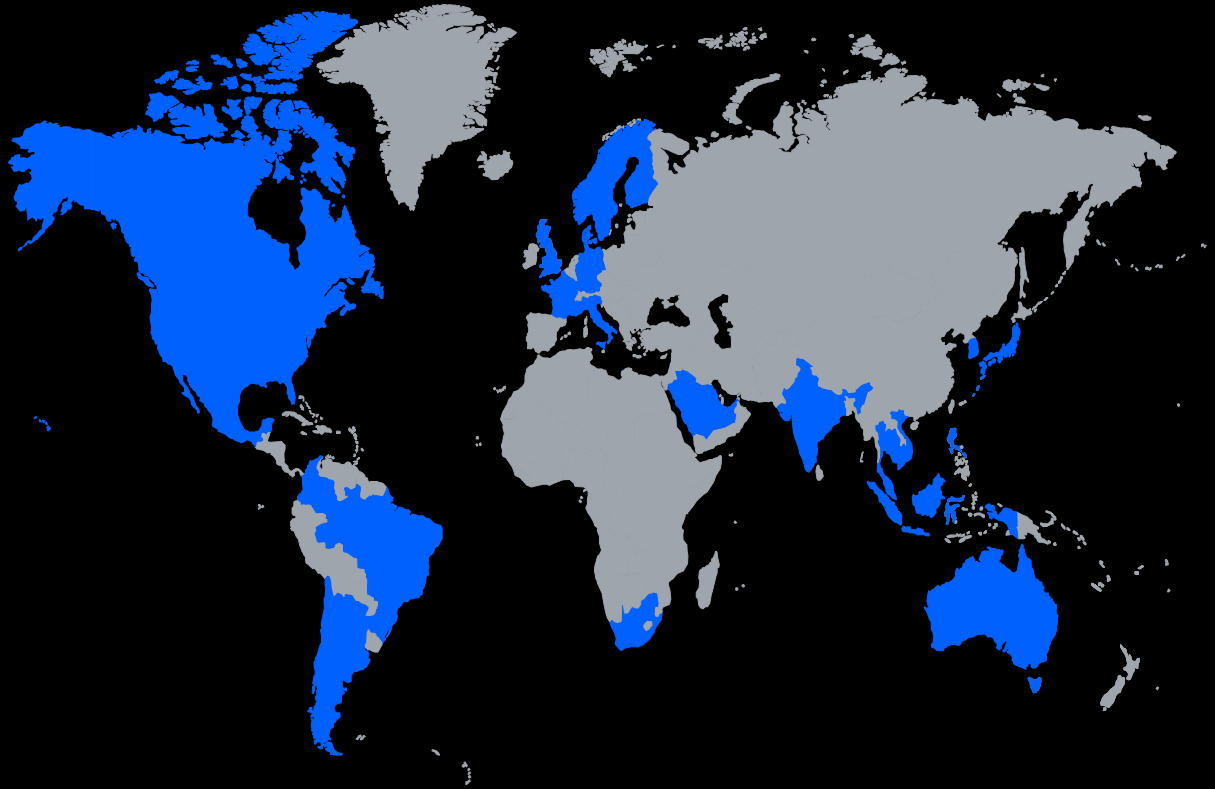


Cost of a Data Breach Report²⁰²⁰



Cost of a Data Breach Report

- 524 breaches studied
- 550+ costs factors analyzed
- 17 countries/regions
- 17 industries
- 15th year



Public Sector highlights

\$1.08M

324 days

Breach lifecycle

231 + 93

days to identify and contain

Global Average: 280 days

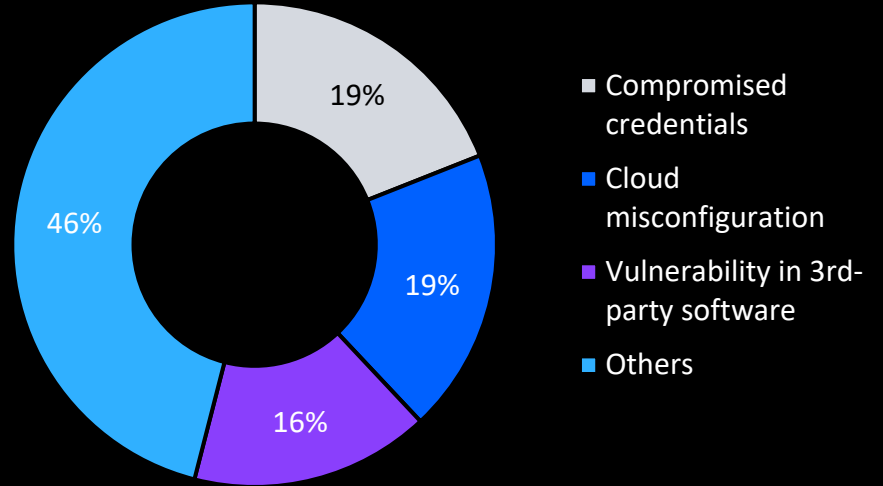
Attack vectors

52%

breaches caused by malicious attacks
(criminal attacker or insider)

80% of breaches contained customer PII,
costliest per compromised record at **\$175**

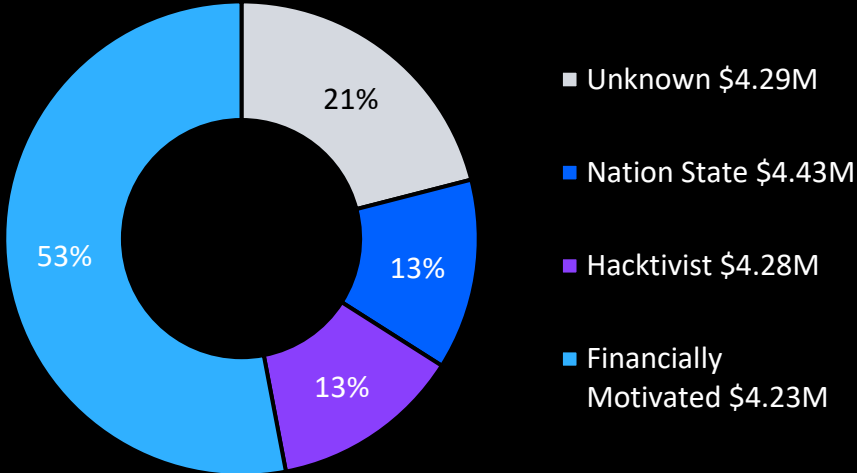
Top 3 most common initial attack vectors were also the most expensive avg >\$4.6M



Threat actors

Nation state attacks
Less common, but costliest

Share of malicious breaches per threat actor type and average cost



Average amount the presence of these factors either decrease (-\$) or increase (+\$) the average total cost of \$1.08M.**

Top 3 cost amplifiers

Cost factor	Cost adjustment from avg.
Cloud migration	+\$243,251
Security skills shortage	+\$201,077
Complex security systems	+\$200,363

Top 3 cost mitigators

Cost factor	Cost adjustment from avg.
Incident response testing	-\$311,571
Formation of IR team	-\$274,239
Business continuity	-\$262,261

Recommendations

- Adhere to a risk management framework such as NIST.
- Deploy risk-based identity and access management controls and enforce principle of least privilege. Consider continuous authentication mechanisms.
- Document, communicate and practice an organization-wide incident response plan, including participants from security, IT, legal, HR, PR and C-level.

*Unless otherwise indicated, stats shown include breaches up to 100,000 records between August 2019 and April 2020.

** Cost factors cannot be combined and only one cost factor can be added/subtracted from average at a time.

Access the report and cost calculator at ibm.com/databreach



Security automation savings

\$3.58M

Average data breach cost savings for organizations with full deployed security automation vs. those without.

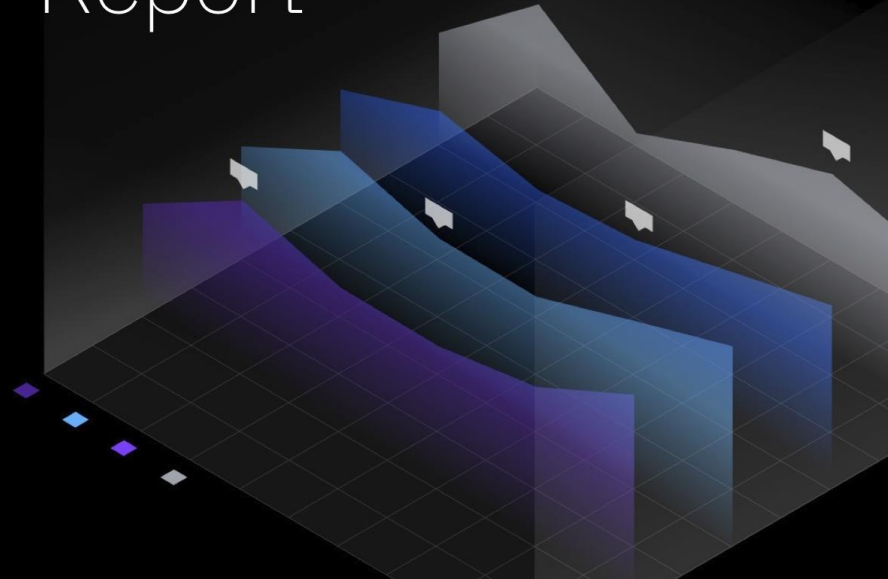
74 days

Faster to identify and contain a threat with fully deployed security automation vs. those without.

Discussion



Cost of a Data Breach Report ²⁰²⁰



Resources

- Download the full report: ibm.com/databreach
- Learn more about IBM Security Incident Response and Intelligence Services ibm.biz/iris-data-breach
- Learn more about IBM Security ibm.com/security
- If you are experiencing an incident, contact X-Force IRIS to help:
[US hotline 1-888-241-9812](tel:1-888-241-9812)
[Global hotline \(+001\) 312-212-8034](tel:+001-312-212-8034)

Thank you

Follow us on:

ibm.com/security

securityintelligence.com

ibm.com/security/community

xforce.ibmcloud.com

[@ibmsecurity](https://twitter.com/ibmsecurity)

youtube.com/ibmsecurity

© Copyright IBM Corporation 2020. 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. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. 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 image features the classic IBM logo, which consists of the letters 'IBM' in a bold, sans-serif font. Each letter is formed by eight horizontal white stripes of equal thickness and height, set against a dark blue background. The stripes are evenly spaced and extend across the width of each letter, creating a distinctive striped pattern. The logo is centered horizontally and vertically in the frame.