

IBM Report: Compromised Employee Accounts Led to Most Expensive Data Breaches Over Past Year

Customer Personal Data Exposed in 80% of Breaches Analyzed; AI and Automation Significantly Reduce Costs

CAMBRIDGE, Mass., July 29, 2020 /PRNewswire/ -- IBM Security (NYSE: [IBM](#)) announced today the results of a global study examining the financial impact of data breaches, revealing that these incidents cost companies studied \$3.86 million per breach on average, and that compromised employee accounts were the most expensive root cause. Based on in-depth analysis of data breaches experienced by over 500 organizations worldwide, 80% of these incidents resulted in the exposure of customers' personally identifiable information (PII). Out of all types of data exposed in these breaches, customer PII was also the costliest to businesses studied.

As companies are increasingly accessing sensitive data via new remote work and cloud-based business operations, the report sheds light on the financial losses that organizations can suffer if this data is compromised. A separate IBM [study](#) found that over half of surveyed employees new to working from home due to the pandemic have not been provided with new guidelines on how to handle customer PII, despite the changing risk models associated with this shift.

Sponsored by IBM Security and conducted by the Ponemon Institute, the [2020 Cost of a Data Breach Report](#) is based on in-depth interviews with more than 3,200 security professional in organizations that suffered a data breach over the past year.¹ Some of the top findings from this year's report include:

- **Smart Tech Slashes Breach Costs in Half:** Companies studied who had fully deployed security automation technologies (which leverage AI, analytics and automated orchestration to identify and respond to security events) experienced less than half the data breach costs compared to those who didn't have these tools deployed – \$2.45 million vs. \$6.03 million on average.
- **Paying a Premium for Compromised Credentials:** In incidents where attackers accessed corporate networks through the use of stolen or compromised credentials, studied businesses saw nearly \$1 million higher data breach costs compared to the global average – reaching \$4.77 million per data breach. Exploiting third-party vulnerabilities was the second costliest root cause of malicious breaches (\$4.5 million) for this group.
- **Mega Breach² Costs Soar by the Millions:** Breaches wherein over 50 million records were compromised saw costs jump to \$392 million from \$388 million the previous year. Breaches where 40 to 50 million records were exposed cost studied companies \$364 million on average, a cost increase of \$19 million compared to the 2019 report.
- **Nation State Attacks - The Most Damaging Breaches:** Data breaches believed to originate from nation state attacks were the costliest, compared to other threat actors examined in the report. State-sponsored attacks averaged \$4.43 million in data breach costs, surpassing both financially motivated cybercriminals and hacktivists.

"When it comes to businesses' ability to mitigate the impact of a data breach, we're beginning to see a clear advantage held by companies that have invested in automated technologies," said Wendi Whitmore, Vice

President, IBM X-Force Threat Intelligence. "At a time when businesses are expanding their digital footprint at an accelerated pace and the security industry's talent shortage persists, teams can be overwhelmed securing more devices, systems and data. Security automation can help resolve this burden, not only supporting a faster breach response but a more cost-efficient one as well."

Employee Credentials and Misconfigured Clouds - Attackers' Entry Point of Choice

Stolen or compromised credentials and cloud misconfigurations were the most common causes of a malicious breach for companies in the report, representing nearly 40% of malicious incidents. With [over 8.5 billion records](#) exposed in 2019, and attackers using previously exposed emails and passwords in one out of five breaches studied, businesses should rethink their security strategy via the adoption of a zero-trust approach – reexamining how they authenticate users and the extent of access users are granted.

Similarly, companies' struggle with security complexity – a top breach cost factor – is likely contributing to cloud misconfigurations becoming a growing security challenge. The 2020 report revealed that attackers used cloud misconfigurations to breach networks nearly 20% of the time, increasing breach costs by more than half a million dollars to \$4.41 million on average – making it the third most expensive initial infection vector examined in the report.

State Sponsored Attacks Strike Heaviest

Despite representing just 13% of malicious breaches studied, state-sponsored threat actors were the most damaging type of adversary according to the 2020 report, suggesting that financially motivated attacks (53%) don't necessarily translate into higher financial losses for businesses. The highly tactical nature, longevity and stealth maneuvers of state-backed attacks, as well as the high value data targeted, often result in a more extensive compromise of victim environments, increasing breach costs to an average of \$4.43 million.

In fact, the respondents in the Middle East, a region that historically experiences a higher proportion of state-sponsored attacks compared to other parts of the world³, saw over 9% yearly rise in their average breach cost, incurring the second highest average breach cost (\$6.52 million) amongst the 17 regions studied. Similarly, businesses studied in the energy sector, one of the most frequently targeted industries by nation states, experienced a 14% increase in breach costs year over year, averaging \$6.39 million.

Advanced Security Technologies Prove Smart for Business

The report highlights the growing divide in breach costs between businesses implementing advanced security technologies and those lagging behind, revealing a cost-saving difference of \$3.58 million for studied companies with fully deployed security automation versus those that have yet to deploy this type of technology. The cost gap has grown by \$2 million, from a difference of \$1.55 million in 2018.

Companies in the study with fully deployed security automation also reported a significantly shorter response time to breaches, another key factor shown to reduce breach costs in the analysis. The report found that AI, machine learning, analytics and other forms of security automation enabled companies to respond to breaches over 27% faster on average, than companies that have yet to deploy security automation – the latter of which require on average 74 additional days to identify and contain a breach.

Incident response (IR) preparedness also continues to heavily influence the financial aftermath of a breach. According to the report, companies with neither an IR team nor testing of IR plans experience \$5.29 million in

average breach costs, whereas companies that have both an IR team and use tabletop exercises or simulations to test IR plans experience \$2 million less in breach costs – reaffirming that preparedness and readiness yield a significant ROI in cybersecurity.

Some additional findings from this year's report include:

- **Remote Work Risk Will Have a Cost:** With hybrid work models creating less controlled environments, the report found that 70% of companies studied that adopted telework amid the pandemic expect it will exacerbate data breach costs.
- **CISOs Faulted for Breaches, Despite Limited Decision-Making Power :** Forty-six percent of respondents said the CISO/CSO is ultimately held responsible for the breach, despite only 27% stating the CISO/CSO is the security policy and technology decision-maker. The report found that appointing a CISO was associated with \$145,000 cost savings versus the average cost of a breach.
- **Majority of Cyber Insured Businesses Use Claims for Third Party Fees:** The report found that breaches at studied organizations with cyber insurance cost on average nearly \$200,000 less than the global average of \$3.86 million. In fact, of these organizations that used their cyber insurance, 51% applied it to cover third-party consulting fees and legal services, while 36% of organizations used it for victim restitution costs. Only 10% used claims to cover the cost of ransomware or extortion.
- **Regional & Industry Insights:** While studied companies in the U.S. continued to experience the highest data breach costs in the world, at \$8.64 million on average, those studied in Scandinavia experienced the biggest year over year increase in breach costs, observing a nearly 13% rise. Responding healthcare companies continued to incur the highest average breach costs at \$7.13 million — an over 10% increase compared to the 2019 study.

About the Study

The annual Cost of a Data Breach Report is based on in-depth analysis of real-world data breaches experienced by over 500 organizations worldwide taking place between August 2019 and April 2020, taking into account hundreds of cost factors including legal, regulatory and technical activities to loss of brand equity, customers, and employee productivity.

To download a copy of the **2020 Cost of a Data Breach Report** , please visit: ibm.com/databreach

Sign up for the 2020 Cost of a Data Breach Report webinar on Wednesday, August 12, 2020 at 11:00 a.m. ET here: <https://ibm.biz/BdqhMf>

About IBM Security

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 70 billion security events per day in more than 130 countries, and has been granted more than 10,000 security patents worldwide. For more information, please check www.ibm.com/security, follow @IBMSecurity on Twitter or visit the [IBM Security Intelligence blog](#).

¹ Report analyzes data breaches occurring between August 2019 and April 2020. Limitations of the report's methodology can be found in the report.

² The 2020 Cost of a Data Breach Report examines the cost of a mega breach, namely breaches involving the loss or theft of one million records or more, based on a separate analysis of a specific sample.

³ According to the IBM 2020 X-Force Threat Intelligence Index: <https://ibm.biz/downloadxforcethreatindex>

Press Contact:



IBM Security Media Relations

Georgia Prassinis

gprassinis@ibm.com

(571) 365-6065

SOURCE IBM

Additional assets available online:  [Photos](#) 

https://newsroom.ibm.com/2020-07-29-IBM-Report-Compromised-Employee-Accounts-Led-to-Most-Expensive-Data-Breaches-Over-Past-Year?utm_source=bi.zone&utm_medium=referral&utm_campaign=news_CP_06-08-20