IBM Newsroom

IBM Report: Consumers Pay the Price as Data Breach Costs Reach All-Time High

60% of breached businesses raised product prices post-breach; vast majority of critical infrastructure lagging in zero trust adoption; $550,000 in extra costs for insufficiently staffed businesses

CAMBRIDGE, Mass., July 27, 2022 /PRNewswire/ -- IBM (NYSE: IBM) Security today released the annual Cost of a Data Breach Report,[1] revealing costlier and higher-impact data breaches than ever before, with the global average cost of a data breach reaching an all-time high of $4.35 million for studied organizations. With breach costs increasing nearly 13% over the last two years of the report, the findings suggest these incidents may also be contributing to rising costs of goods and services. In fact, 60% of studied organizations raised their product or services prices due to the breach, when the cost of goods is already soaring worldwide amid inflation and supply chain issues.

The perpetuality of cyberattacks is also shedding light on the "haunting effect" data breaches are having on businesses, with the IBM report finding 83% of studied organizations have experienced more than one data breach in their lifetime. Another factor rising over time is the after-effects of breaches on these organizations, which linger long after they occur, as nearly 50% of breach costs are incurred more than a year after the breach.

The 2022 Cost of a Data Breach Report is based on in-depth analysis of real-world data breaches experienced by 550 organizations globally between March 2021 and March 2022. The research, which was sponsored and analyzed by IBM Security, was conducted by the Ponemon Institute.

Some of the key findings in the 2022 IBM report include:

- **Critical Infrastructure Lags in Zero Trust –** Almost 80% of critical infrastructure organizations studied don't adopt zero trust strategies, seeing average breach costs rise to $5.4 million – a $1.17 million increase compared to those that do. All while 28% of breaches amongst these organizations were ransomware or destructive attacks.
- **It Doesn't Pay to Pay –** Ransomware victims in the study that opted to pay threat actors' ransom demands saw only $630,000 less in average breach costs compared to those that chose not to pay – not including the cost of the ransom. Factoring in the high cost of ransom payments, the financial toll may rise even higher, suggesting that simply paying the ransom may not be an effective strategy.
- **Security Immaturity in Clouds –** Forty-three percent of studied organizations are in the early stages or have not started applying security practices across their cloud environments, observing over $660,000 on average in higher breach costs than studied organizations with mature security across their cloud environments.
- **Security AI and Automation Leads as Multi-Million Dollar Cost Saver** – Participating organizations fully deploying security AI and automation incurred $3.05 million less on average in breach costs compared to studied organizations that have not deployed the technology – the biggest cost saver observed in the study.

"Businesses need to put their security defenses on the offense and beat attackers to the punch. It's time to stop the adversary from achieving their objectives and start to minimize the impact of attacks. The more businesses try to perfect their perimeter instead of investing in detection and response, the more breaches can fuel cost of living increases." said Charles Henderson, Global Head of IBM Security X-Force. "This report shows that the right strategies coupled with the right technologies can help make all the difference when businesses are attacked."

Over-trusting Critical Infrastructure Organizations

Concerns over critical infrastructure targeting appear to be increasing globally over the past year, with many governments' cybersecurity agencies urging vigilance against disruptive attacks. In fact, IBM's report reveals that ransomware and destructive attacks represented 28% of breaches amongst critical infrastructure

organizations studied, highlighting how threat actors are seeking to fracture the global supply chains that rely on these organizations. This includes financial services, industrial, transportation and healthcare companies amongst others.

Despite the call for caution, and a year after the Biden Administration issued a cybersecurity executive order that centers around the importance of adopting a zero trust approach to strengthen the nation's cybersecurity, only 21% of critical infrastructure organizations studied adopt a zero trust security model, according to the report. Add to that, 17% of breaches at critical infrastructure organizations were caused due to a business partner being initially compromised, highlighting the security risks that over-trusting environments pose.

Businesses that Pay the Ransom Aren't Getting a "Bargain"
According to the 2022 IBM report, businesses that paid threat actors' ransom demands saw $630,000 less in average breach costs compared to those that chose not to pay – not including the ransom amount paid. However, when accounting for the average ransom payment, which according to Sophos reached $812,000 in 2021, businesses that opt to pay the ransom could net higher total costs - all while inadvertently funding future ransomware attacks with capital that could be allocated to remediation and recovery efforts and looking at potential federal offenses.

The persistence of ransomware, despite significant global efforts to impede it, is fueled by the industrialization of cybercrime. IBM Security X-Force discovered the duration of studied enterprise ransomware attacks shows a drop of 94% over the past three years – from over two months to just under four days. These exponentially shorter attack lifecycles can prompt higher impact attacks, as cybersecurity incident responders are left with very short windows of opportunity to detect and contain attacks. With "time to ransom" dropping to a matter of hours, it's essential that businesses prioritize rigorous testing of incident response (IR) playbooks ahead of time. But the report states that as many as 37% of organizations studied that have incident response plans don't test them regularly.

Hybrid Cloud Advantage
The report also showcased hybrid cloud environments as the most prevalent (45%) infrastructure amongst organizations studied. Averaging $3.8 million in breach costs, businesses that adopted a hybrid cloud model observed lower breach costs compared to businesses with a solely public or private cloud model, which experienced $5.02 million and $4.24 million on average respectively. In fact, hybrid cloud adopters studied were able to identify and contain data breaches 15 days faster on average than the global average of 277 days for participants.

The report highlights that 45% of studied breaches occurred in the cloud, emphasizing the importance of cloud security. However, a significant 43% of reporting organizations stated they are just in the early stages or have not started implementing security practices to protect their cloud environments, observing higher breach costs[2]. Businesses studied that did not implement security practices across their cloud environments required an average 108 more days to identify and contain a data breach than those consistently applying security practices across all their domains.

Additional findings in the 2022 IBM report include:

- **Phishing Becomes Costliest Breach Cause –** While compromised credentials continued to reign as the

most common cause of a breach (19%), phishing was the second (16%) and the costliest cause, leading to $4.91 million in average breach costs for responding organizations.

- **Healthcare Breach Costs Hit Double Digits for First Time Ever** – For the 12th year in a row, healthcare participants saw the costliest breaches amongst industries with average breach costs in healthcare increasing by nearly $1 million to reach a record high of $10.1 million.
- **Insufficient Security Staffing** – Sixty-two percent of studied organizations stated they are not sufficiently staffed to meet their security needs, averaging $550,000 more in breach costs than those that state they are sufficiently staffed.

Additional Sources

- To download a copy of the 2022 Cost of a Data Breach Report, please visit: https://www.ibm.com/security/data-breach.
- Read more about the report's top findings in this IBM Security Intelligence blog.
- Sign up for the 2022 IBM Security Cost of a Data Breach webinar on Wednesday, August 3, 2022, at 11:00 a.m. ET here.
- Connect with the IBM Security X-Force team for a personalized review of the findings: https://ibm.biz/book-a-consult.

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 Security 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 150 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.

Press Contact:

IBM Security Communications
Georgia Prassinos
gprassinos@ibm.com

[1] Cost of a Data Breach Report 2022, conducted by Ponemon Institute, sponsored, and analyzed by IBM

[2] Average cost of $4.53M, compared to average cost $3.87 million at participating organizations with mature-stage cloud security practices

SOURCE IBM

Additional assets available online: Photos (

https://newsroom.ibm.com/2022-07-27-IBM-Report-Consumers-Pay-the-Price-as-Data-Breach-Costs-Reach-All-

Time-High?ref=tresorit.com