DISASTER RECOVERY 2021: 37 TRENDS AND STATISTICS

Key Insights Impacting Your Business

COVID-19 IMPACT ON SECURITY EFFECTIVENESS (1)

Effectiveness of organizations' IT security posture prior to COVID-19 and due to COVID-19:

71% Effectiveness prior to COVID-19

45% Effectiveness due to COVID-19

BREACHES IMPACTING LARGE AND SMALL BUSINESSES; (2)

external vs internal attackers

Verizon Data Breach Investigations Report 2020

72% of breaches involved large business victims (28% involved small business victims)

70% of breaches perpetrated by external actors

30% involved internal actors

55% of breaches involved organized criminal groups

MOST SMBS FEEL READY FOR DISASTER, YET MANY LACK PLANS (3)

74% of retail/e-commerce and healthcare industry and 73% executives said their top expectation of a disaster recovery solution is to minimize the time until their business is fully operational following a disaster

64% of accounting/finance/banking sector leaders said zero data loss is their top expectation of a disaster recovery solution

63% of telecommunications leaders indicated their top expectation of a disaster recovery solution is to deliver cost savings related to on-call IT technicians

More than half of the survey group said they had faced malware infections, corrupted hard drives, and/or other micro-disasters within the past year

MORE THAN 1 IN 5 SMBS LACKS PROPER DATA PROTECTION (4)

58% of C-level executives at small and medium businesses (SMBs) said their biggest data storage challenge is security vulnerability.

Nearly half (49%) of top leaders at SMBs said cyberattacks are their biggest data protection concern.

SYSTEM ERROR

Micro disasters such as corrupted hard drives and malware infections were the second most commonly indicated concern, garnering a 46% share from the group. System crashes (41%), data leaks (39%), ransomware attacks (38%), and human errors (38%) were next on the list.

About 20% of SMB leaders said they do not currently have a data backup or disaster recovery solution in place.

CLOSE TO HALF OF SMBS HAVE BEEN RANSOMWARE ATTACK TARGETS (5)

Ransomware attacks are not at all unusual in the SMB community, as 46% of these businesses have been victims.

And 73% of those SMBs that have been the targets of ransomware attacks actually have paid a ransom.

Business-to-business (B2B) organizations were more likely to have experienced a ransomware attack. Representatives from more than half (55%) of the B2Bs said they had been hit by ransomware.

PAY FOR UNLOCK

80% of B2B companies are better prepared with a plan in place to mitigate attack vs B2C organizations (62%).

B2C organizations clearly are not immune to the ransomware risk. The research showed that more than a third (36%) of this group said they have been victims of ransomware attacks.

"In Q4 of 2019, average downtime caused by ransomware increased to 16.2 days, from 12.1 days in Q3 of 2019. The increase in downtime was driven by a higher prevalence of attacks against larger enterprises, who often spend weeks fully remediating and restoring their systems. Established enterprises have more complex networks, and restoring data via backups or decryption takes longer than restoring the network of a small business."

HEAVY COSTS OF BUSINESS DOWNTIME (6)

More than a third (37%) of SMBs in the survey group said they have lost customers and 17% have lost revenue due to downtime

46% of B2B SMBs said they have lost customers due to downtime problems

26% of B2C said they have lost customers due to downtime problems

Most common causes of the downtime that creates these business challenges

Software failure **52%**

Cybersecurity issues **53%**

ERROR

A significant but far smaller share of the SMB survey group blamed downtime on hardware failure (38%), human error (36%), natural disaster (30%), and/or hardware theft (24%)

IT DOWNTIME AND ITS IMPACT ON BUSINESSES (7)

96% of global IT decision makers surveyed had experienced at least one outage in the past 3 years.

According to global IT decision makers, 51% of outages are avoidable. **51%**

53% Global IT decision makers also said 53% of brownouts are avoidable.

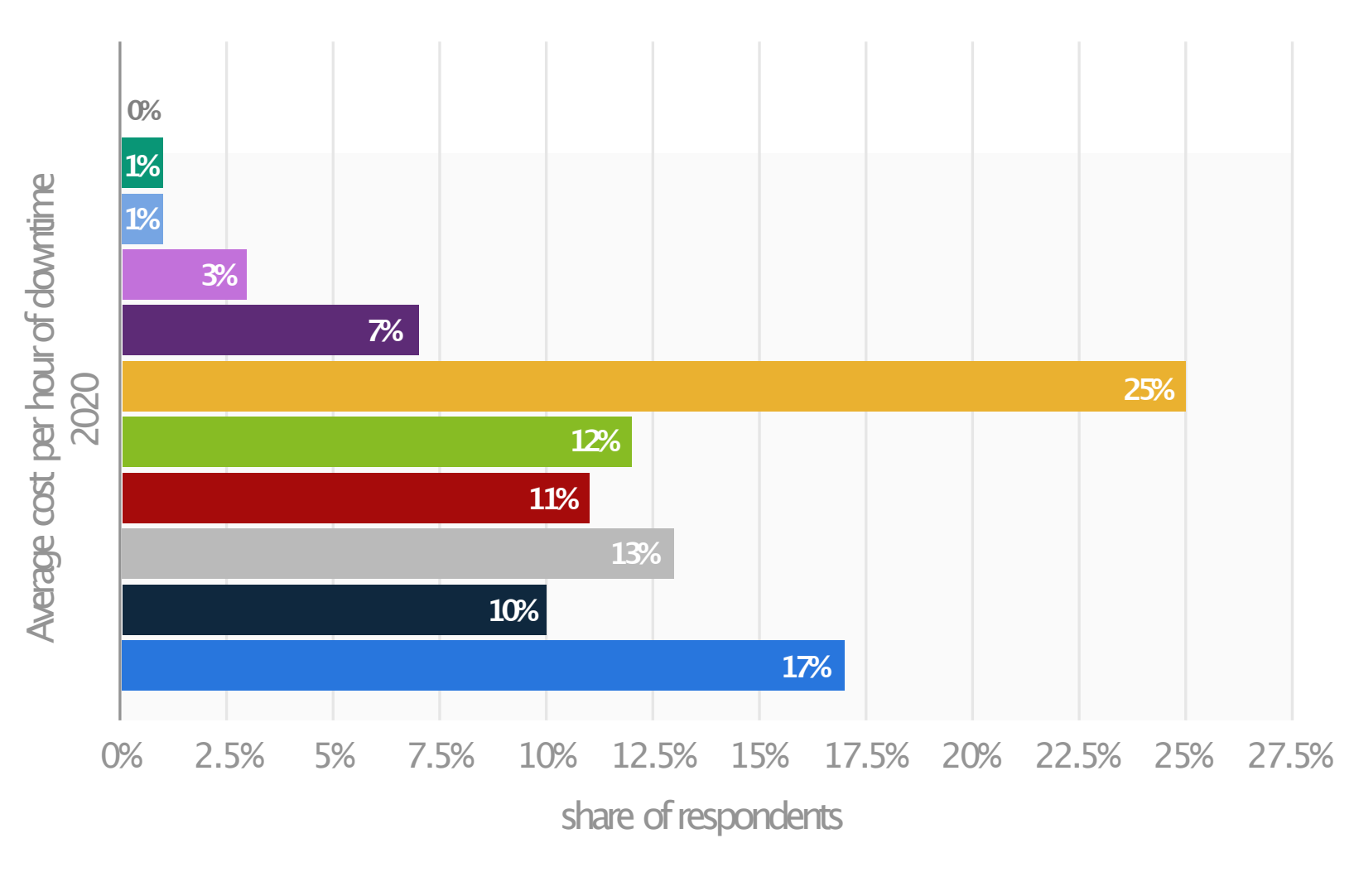
of global IT decision makers think it's likely their company will experience a brownout or outage so severe that it makes national media headlines. **53%**

52% The same percentage (53%) of global IT decision makers think it's likely their company will experience a brownout or outage so severe that someone loses their job as a result.

Companies that have frequent outages and brownouts experience up to 16x higher costs than companies who have fewer instances of downtime. **52%**

AVERAGE COST PER HOUR OF SERVER DOWNTIME (8)

2020	
Up to $10,000	0%
$10,000 to $50,000	1%
$50,000 to $100,000	1%
$101,000 to $200,000	3%
$201,000 to $300,000	7%
$301,000 to $400,000	25%
$401,000 to $500,000	12%
$501,000 to $1M	11%
$1M to $2M	13%
$2M to $5M	10%
> $5M	17%



COST OF DATABREACHES (9)

80% of breaches with customer PII

"Customers' personally identifiable information (PII) was the most frequently compromised type of record, and the costliest, in the data breaches studied. 80% of breached organizations stated that customer PII was compromised during the breach, far more than any other type of record. While the average cost per lost or stolen record was $146 across all data breaches, those containing customer PII cost businesses $150 per compromised record. The cost per record of customer PII increased to $175 in breaches caused by a malicious attack."

"Remote work during COVID-19 was expected to increase data breach costs and incident response times. Of organizations that required remote work as a result of COVID-19, 70% said remote work would increase the cost of a data breach and 76% said it would increase the time to identify and contain a potential data breach. Having a remote workforce was found to increase the average total cost of a data breach of $3.86 million by nearly $137,000, for an adjusted average total cost of $4 million."

"Lost business continued to be the largest contributing cost factor. Lost business costs accounted for nearly 40% of the average total cost of a data breach, increasing from $1.42 million in the 2019 study to $1.52 million in the 2020 study. Lost business costs included increased customer turnover, lost revenue due to system downtime and the increasing cost of acquiring new business due to diminished reputation."

"$5.52 million – Average total cost of a breach at enterprises of more than 25,000 employees, compared to $2.64 million for organizations under 500 employees."

SOURCE

1. https://www.keepersecurity.com/ponemon2020.html
   https://www.keeper.io/hubfs/PDF/Cybersecurity%20in%20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf
2. https://enterprise.verizon.com/resources/reports/dbir/2020/summary-of-findings/
   https://enterprise.verizon.com/resources/reports/dbir/2020/smb-data-breaches-deep-dive/
3. https://www.infrascale.com/press-release/infrascale-survey-shows-that-most-smbs-feel-ready-yet-many-lack-plans-for-disaster/
4. https://www.infrascale.com/press-release/new-infrascale-research-indicates-more-than-1-in-5-smbs-lacks-proper-data-protection/
5. https://www.infrascale.com/press-release/infrascale-survey-reveals-close-to-half-of-smbs-have-been-ransomware-attack-targets/
   https://www.coveware.com/blog/2020/1/22/ransomware-costs-double-in-q4-as-ryuk-sodinokibi-proliferate
6. https://www.infrascale.com/press-release/infrascale-survey-highlights-the-heavy-costs-of-business-downtime/
7. https://www.logicmonitor.com/resource/outage-impact-survey
8. https://www.statista.com/statistics/753938/worldwide-enterprise-server-hourly-downtime-cost/
9. https://www.ibm.com/downloads/cas/RZAX14GX