Key Findings over the last 12 months

- 70% of the companies expect their business to be harmed by an email-borne attack.
- 64% of email threats rose by 64%.
- 79% experienced a business disruption, financial loss or other setback in 2020 due to a lack of cyber preparedness.
- 3x since the onset of the pandemic, employees are clicking on 3x as many malicious emails as they had before.
- 47% saw an increase in email spoofing activity.
- 8/10 email usage increased this past year at 8 out of 10 companies.
- 70% are concerned about the risks posed by archived conversations from collaboration tools.
- 7/10 organizations believe that employee behaviors are putting their companies at risk.
- 40% of respondents fall short in one or more critical areas of email security systems.
- 13% do not have any email security system in place.
- 61% of organizations were infected with ransomware in 2020.
- 65% never saw their data again despite paying the ransom.
- 52% of ransomware victims paid threat actors' ransom demands.
- 61% of organizations were infected with ransomware.
- 64% of companies impacted lost an average of six working days to downtime.
- 37% said the downtime lasted one week or more.
- 6days companies impacted lost an average of six working days to downtime.
- 35% of ransomware victims paid threat actors' ransom demands.

Ransomware looms large in 2020

Securing the Enterprise in the COVID world
The State of Email Security

GET THE REPORT