THE IMPACT OF CYBERCRIME

A STATISTICAL SNAPSHOT OF THE LAST YEAR IN CYBERSECURITY ATTACKS, PREPAREDNESS, AND MITIGATION EFFORTS

Cyberattacks have been increasing at an exponential rate from 2020 to 2021, which means proactive preparedness, risk-mitigation, incident-response plans, and a Zero-Trust cybersecurity resiliency model must all be in place. Don’t be a statistic of the ransomware trap and of cyber breach. Assess your cybersecurity preparedness here and then watch the Sterling Cybersecurity Webinar Series.

$350 MILLION
Total amount paid by ransomware victims increased by 311% in 2020 totaling $350M worth of cryptocurrency

Chainalysis 2021 Crypto Crime Report

84% of Federal IT managers agree cybersecurity is a top or high priority within their agency; yet, only 34% say their senior leadership is fully engaged.

FEDERAL CYBERSECURITY IN A CHANGING WORLD

MeriTalk

43% of Feds say legacy infrastructure is preventing them from implementing the ideal cybersecurity system

FEDERAL CYBERSECURITY IN A CHANGING WORLD

MeriTalk

58% of US CEOs and CISOs say cybersecurity is a top priority in their organization

FEDERAL CYBERSECURITY IN A CHANGING WORLD

MeriTalk

88% of US respondents agree that nation-states are more motivated than ever to pursue attacks against organizations

2020 CrowdStrike Global Security Attitude Survey

84% of Federal IT managers agree cybersecurity is a top or high priority within their agency; yet, only 34% say their senior leadership is fully engaged.

FEDERAL CYBERSECURITY IN A CHANGING WORLD

MeriTalk

43% of Feds say legacy infrastructure is preventing them from implementing the ideal cybersecurity system

FEDERAL CYBERSECURITY IN A CHANGING WORLD

MeriTalk

58% of US CEOs and CISOs say cybersecurity is a top priority in their organization

FEDERAL CYBERSECURITY IN A CHANGING WORLD

MeriTalk

88% of US respondents agree that nation-states are more motivated than ever to pursue attacks against organizations

2020 CrowdStrike Global Security Attitude Survey

Has your organization suffered from a ransomware attack in the past 12 months? (87% of US respondents have had or expect to have a ransomware attack)

13% no – and we do not expect to

29% no – but we expect we will

22% yes – more than once

36% yes – but only once

2020 CrowdStrike Global Security Attitude Survey

Average number of hours respondents estimate that it would take their organization to detect a cybersecurity incident

117 HOURS

8 IN 10 executives say they are concerned about their organization falling victim to a nation-state cyber-attack

“Securing a shifting landscape: Corporate perceptions of nation-state cyber-threats” is a report from The Economist Intelligence Unit

61% of respondents’ organizations have spent at least $1M (USD) on digital transformation over the last three years, with the average spend approaching $5M

2020 CrowdStrike Global Security Attitude Survey

Determine your levels of preparedness, response, and resilience capabilities, take the Cybersecurity Preparedness Self-Assessment

www.sterling.com