State of Ransomware for 2022 and Beyond

A global survey of IT and InfoSec leaders reveals how insider threats are evolving, what impact cyber insurance and the blame culture are having on the cybersecurity industry, and why deep observability is integral to tackle the ransomware crisis.

Data collection: 22 – 29 June 2022
Respondents: 1,020 CIOs/CISOs/CTOs, and other Network and Cloud leaders
Regions: US; UK; France; Germany; Singapore; Australia

RANSOMWARE IS A BOARD-LEVEL PRIORITY

59%

59% of organizations believe ransomware has worsened in Q2 2022

89%

89% of global boardrooms see ransomware as a priority concern

33%

Most boardrooms **(33%)** view ransomware as a **reputational issue**

RANSOMWARE THRIVES IN COMPLEXITY, AND MORE VISIBILITY IS NEEDED

Increasing sophistication of cybercriminals is viewed worldwide **(59%)** as the leading cause behind the worsening crisis

60% agree **the security tools that they're currently using are not as effective without complete visibility**

87% of global respondents agree – or strongly agree – that they **need greater visibility to identify where ransomware may be hiding**

INSIDER THREATS ARE EVOLVING

58%

While phishing remains the most common route for ransomware (**58%** of cases), disgruntled employees complicit in ransomware attacks are a rising threat globally

29%

29% of organizations have suffered ransomware attacks enabled by a malicious insider, almost as commonly as the accidental insider **(35%)**

99%

99% of CISOs/CIOs that recognize insider threat as a cause for ransomware attacks view the malicious insider as a significant risk

29%

29% of organizations **don't have the visibility to distinguish** between the two types of insider threat

CYBER INSURANCE AND BLAME CULTURE ARE EXACERBATING THE RANSOMWARE CRISIS

Cyber insurance:
A solution that security professionals are turning to in the wake of the ransomware crisis, although not as commonly as more proactive measures

One in five organizations admitted that **cyber insurance is their entire cybersecurity strategy** and don't have other processes or tools in place

1 in 5

57% agree that the **cyber insurance market is exacerbating the ransomware crisis**

57%

Blame culture:
an environment within which there is a tendency to single out and hold responsible an individual or team for an incident, irrespective of their actual culpability

1 in 3

One in three **CIOs/CISOs believe the blame culture is heavily prevalent** in cybersecurity

94%

94% of respondents who believe there is a blame culture in the industry feel that this could be **a deterrent to the speed of reporting an incident**

DEEP OBSERVABILITY: INTEGRAL TO CYBERSECURITY

78%

Deep observability is increasingly being discussed in the boardroom for better network and cloud security, **78%** of respondents agree

26%

Over a quarter (26%) of CISOs/CIOs claimed they want more visibility through deep observability, so that they have the right level of insight to detect and respond to threats

89%

89% of global security leaders agree deep observability is an **important element of cloud security**

82%

82% believe that deep observability is **part of a safe migration to the cloud**

80%

80% agree that having access to raw packet data can **unlock deep insight and strengthen a security posture**

89%

89% of global respondents agree that deep observability is **somewhat to strongly connected to Zero Trust**

Discover the insights from your region in the full report:
www.gigamon.com/ransomware-survey

DOWNLOAD NOW

Gigamon

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | gigamon.com