PULSE | Hitachi ID

THE RISING CYBER THREAT: Hackers Have Approached 65% of Executives or Their Employees To Assist in Ransomware Attacks

Ransomware attacks regularly generated prominent news coverage in 2021, and they are continuing to grow in frequency, complexity and sophistication. Yet, there is another facet of ransomware attacks that has not received the same attention in the media: insider threats.

Since our last survey conducted in November, there has been a 17% increase in the number of employees and executives who have been approached by hackers to assist in ransomware attacks. To combat this rising threat, businesses must take a proactive defense approach to cybersecurity to face financial and reputational damage.

To gain a better understanding of the different types of ransomware threats, Pulse and Hitachi ID surveyed 500 IT and security executives on how hackers are approaching employees, how ransomware is impacting an organization's cybersecurity approach, and how prepared businesses really are to combat these attacks.

Data collected from November 7, 2021 - January 4, 2022 | Respondents: 500 IT and security executives

EMPLOYEES AND EXECUTIVES CONTINUE TO BE TARGETED TO ASSIST IN RANSOMWARE ATTACKS—PRIMARILY THROUGH EMAIL

Over half (65%) of respondents say they or their employees have been approached by a hacker to assist in ransomware attacks. Interestingly, this is a 17% increase in comparison to a similar survey run in the Fall of 2021.

ALTHOUGH MANY CONSIDER THEMSELVES PREPARED TO DEFEND AGAINST RANSOMWARE, RELIANCE ON PERIMETER DEFENSE MAY PRESENT A WEAK LINK

Roughly half (51%) of executives feel moderately prepared to prevent a ransomware attack, with 4% saying they feel most prepared.

Similarly, in the event that a hacker breaches their system, 50% of leaders say their organization is moderately or most prepared to reduce the damage or stop the attack.

However, most decision-makers stated that they mostly rely on perimeter defense (65%), with 6% exclusively using perimeter defense.

CYBERSECURITY MEASURES MULT ACCOUNT FOR INTERNAL AND EXTERNAL THREATS

While 36% are more concerned about external threats than internal ones, more than half (53%) are equally concerned about both.

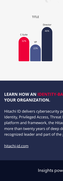
Of those who were approached to assist in a ransomware attack (n = 65), 49% opposed the invitation to follow an enforcement with only 18% who reported both internally and externally.

Overall, 57% of respondents reported that they or their employees were offered cash or Bitcoins worth less than $500,000 USD.

EXECUTIVES CONTINUE TO INVEST IN CYBERSECURITY MEASURES EVEN WHEN THEY HAVE INSURANCE COVERAGE FOR RANSOMWARE

Most companies (63%) have an insurance policy that covers ransomware attacks.

53% note that their insurance policy did not impact their cybersecurity investments.



Still, most (66%) have added or plan to add new security measures to curb ransomware attacks.

Three of the top recurring themes for new security features were tools, employee skills, and better compliance and security policies.

RANSOMWARE ATTACKS ARE BOTH NOTICEABLE, BUT HOW MANY BUSINESSES HAVE BEEN HIT? WHAT ARE THEY DOING ONCE ATTACKED?

38% of respondents say their company has been a victim of a ransomware attack.

Of those who said they had been approached to assist in a ransomware attack (n = 65), 49% ended up a victim to a ransomware attack.

Most consulted an external party before taking action and were advised not to pay ransom.

20% paid the ransom while 29% did not, although 32% chose not to disclose this information.

Most ransomware requests were between $300,001 and $600,000.

RESPONDENT BREAKDOWN

LEARN HOW AN IDENTITY-BASED SECURITY MODEL CAN PROTECT YOUR ORGANIZATION.

Hitachi ID delivers a cybersecurity platform connected with the industry's only single identity, Privileged Access, Threat Detection, and Password Management platform and framework, the Hitachi ID Resource Security Fabric. Building on more than twenty years of deep identity expertise, Hitachi ID is an analyst recognized leader and part of the global "One Hitachi" portfolio.

Hitachi-id.com