Organizations Revising and Ramping Up Prevention and Response Strategies to be Ransomware-Ready

Boosted investments, upgrades in technology, ransomware insurance and increased IT and security training amongst tactics to mitigate risks of potential attack

NEW YORK, NY, UNITED STATES, November 22, 2022 / EINPresswire.com/ -- The clear and present danger of a ransomware attack looms large among all organizations and in the minds of infosec professionals as the number of vulnerabilities increases daily. Many believe the worst is yet to come. According to recent research conducted by CRA Business Intelligence, the research and content arm of the cybersecurity data and insights company CyberRisk Alliance, respondents indicated that their organizations' readiness to respond to a ransomware attack is moderate, at best. Highly targeted sectors such as education, healthcare, and financial services particularly fear they will be the next ransomware victim and are on elevated alert.

Our examination of the market included responses from over 200 security and IT executives and leaders, security administrators, and compliance professionals from the United States. The report indicated that respondents have remained vigilant over the past two years, indicating their organizations have developed or revised their ransomware prevention and response strategies, updated related policies and standards, improved processes, boosted investments in new or upgraded technology, purchased ransomware insurance, started, or increased employee training, and hired additional IT or security staff. The report was underwritten by Crowdstrike.

Key security measures, such as backup and recovery and anti-malware/anti-virus solutions, are included in virtually all organizations' ransomware prevention/mitigation strategies. However, companies and cybersecurity leaders are discovering that's not enough. Many have subsequently added or plan to add additional capabilities, such as endpoint security, vulnerability management, active directory monitoring, credential protection, DNS security tools, security information and event management (SIEM), data loss prevention (DLP) and encryption, and cloud security software.

Organizations that have adopted more advanced ransomware tools and processes have the IT resources to support them are the most "ransomware-ready." Those least prepared have fewer tools and few or no IT/security resources. Unfortunately for many of these organizations, funding has been difficult and some fear their constant pressure to do more with less may have dire consequences.

Key takeaways from the survey:

• Respondents said their organizations have implemented a variety of approaches to respond to or mitigate the risks of ransomware attacks. A majority have embraced well-established methods, such as employee security awareness training (83%), formal policies and procedures (66%), network segmentation (60%), and ransomware incident response plans (54%). At least 4 in 10 respondents have purchased ransomware insurance or follow a standardized framework such as NIST.

• Nearly one in four (23%) respondents reported their organization experienced one or more ransomware attacks in the past 12 months. Almost one out of three (31%) said attackers succeeded in gaining access to their systems, encrypting files, and demanding a ransom — of which 2% paid the ransom.

• The hard lessons from a prior ransomware attack sparked a variety of responses, but most developed a new or revised strategy for ransomware incident response (69%) and started or increased employee training (67%). About one-third (35%) of the victims also purchased or upgraded their ransomware protection software, and 29% hired more IT or security staff following their attacks.

• Only about one in three respondents (35%) think their organization is unlikely to suffer from a ransomware attack in the next 12 months. Their confidence stems from tightened security policies, more effective tools, and increased user education and monitoring. However, 47% believe their organization is likely to suffer a ransomware attack in the next 12 months and that ransomware attacks are a "trend."

• Respondents believe their current defenses are not enough. Their average Ransomware Readiness self-assessment score is 7.2 out of 10. Highly prepared organizations (those with readiness scores of 7.8 or higher) are more likely to have already adopted advanced or specialized ransomware prevention/mitigation solutions.

Looking ahead, most respondents said they are likely to do more to prepare for a ransomware attack in the next 12 months, with (68%) stating that they would develop or revise their ransomware incident response strategy to prepare for a future ransomware attack and put more effort into employee training.

The full research report is available for download here.

About CyberRisk Alliance
CyberRisk Alliance (CRA) is a business intelligence company serving the high growth, rapidly evolving cybersecurity community with a diversified portfolio of services that inform, educate, build community, and inspire an efficient marketplace. Our trusted information leverages a unique network of journalists, analysts and influencers, policymakers, and practitioners. CRA's brands include SC Media, Security Weekly, ChannelE2E, MSSP Alert, InfoSec World, Identiverse, Cybersecurity Collaboration Forum, its research unit CRA Business Intelligence, the peer-to-peer CISO membership network, Cybersecurity Collaborative, and now, the Official Cyber Security Summit and TECHEXPO Top Secret. Click here to learn more.

About Crowdstrike
CrowdStrike has redefined security with the world's most advanced cloud-native platform that protects and enables the people, processes and technologies that drive modern enterprise. CrowdStrike secures the most critical areas of enterprise risk — endpoints and cloud workloads, identity, and data — to keep customers ahead of today's adversaries and stop breaches.

Powered by the CrowdStrike Security Cloud, the CrowdStrike Falcon Platform leverages real-time indicators of attack, threat intelligence on evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities — all through a single, lightweight agent. With CrowdStrike, customers benefit from superior protection, better performance, reduced complexity and immediate time-to-value.

Jenn Jones
CyberRisk Alliance
+1 857-328-0173
email us here