IT leaders are over-stressed and under-prepared for ransomware attacks

Submitted by: Maillot Jaune Communications
Thursday, 2 December 2021

Stress levels are rising, investment is too low, IT leaders feel they don't get the executive support they need.

86% of leaders reveal ransomware causes workplace stress, while 53% would rather pay a ransom than invest in defending against it

London, UK – Osirium's 2021 Ransomware Index survey has revealed that 53% of its 1001 UK IT manager respondents don't believe they invest enough to prevent ransomware attacks, whilst a similar number (52%) don't feel supported to do so by their company's board. With less than 10% believing that they can prevent a future ransomware attack, it is little wonder that stress levels are so high for these IT leaders.

The survey findings raise concerns about UK IT teams' ability to properly manage potential ransomware attacks, of which their likelihood of becoming a victim is increasing rapidly. Of those surveyed, only 21% claimed they had never been attacked. Perhaps more surprisingly, 53% of respondents agreed with the statement: "It would be cheaper to pay the ransom demand than continuously invest in preventing ransomware".

More than half of the survey respondents also claimed that they do not have sufficient budget/resources to cope with the constantly evolving threat landscape, which makes the research finding, that many feel the only way to deal with the problem is to pay, even more impactful.

The stress to UK IT managers, caused by the spectre of Ransomware, is an increasingly significant downside to an already difficult job. 86% of the IT managers surveyed said they feel stressed about the prospects of a ransomware attack, with 22% saying it more than doubled their stress levels.

David Guyatt, Founder and CEO of Osirium said: "This situation is unsustainable, and it is likely only a matter of time until many of these ill-prepared businesses fall victim to a ransomware attack. The cost of paying a ransom is merely the tip of the iceberg. Add in the real and virtual costs, such as reputational damage, regulatory fines and lost business through downtime, and it is hard to justify not having robust malware and ransomware protection in place."
Guyatt's comments are further substantiated by the Osirium report finding: 19% considered reputational damage to be a major concern, with 24% concerned about downtime and 28% citing data protection worries.

"Right now, many businesses are deep into the planning process as they prepare for 2022 and beyond," added Guyatt. "This will be a pivotal moment for UK business leaders, and those who neglect to prioritise their ransomware defence and remediation systems may just as well paint a target on their back. Failure to prepare, and the associated stress on the IT department, could easily also result in individuals experiencing major burnout, the impacts of which will only lead to further security challenges."

Access the Executive Summary here: https://www.osirium.com/documents/osirium-ransomware-index-stress

The Osirium Ransomware Index Methodology
The survey was carried out on behalf of Osirium by Atomik Research, an independent creative market research agency that employs MRS-certified researchers and abides to MRS code, and surveyed 1001 IT managers across the UK between 30 July and 5 August 2021.

About Osirium Technologies
Osirium Technologies plc(AIM: OSI) is a leading UK-based cybersecurity software vendor delivering Privileged Access Management (PAM), Privileged Endpoint Management (PEM) and Osirium Automation solutions that are uniquely simple to deploy and maintain.

With privileged credentials involved in over 80% of security breaches, customers rely on Osirium PAM's innovative technology to secure their critical infrastructure by controlling 3rd party access, protecting against insider threats, and demonstrating rigorous compliance. Osirium Automation delivers time and cost savings by automating complex, multi-system processes securely, allowing them to be delegated to Help Desk engineers or end-users and to free up specialist IT resources. The Osirium PEM solution balances security and productivity by removing risky local administrator rights from users, while at the same time allowing escalated privileges for specific applications.

Founded in 2008 and with its headquarters in Reading, UK, the Group was admitted to AIM in April 2016.

For further information please visit www.osirium.com or contact:

Clare Shephard
maillot jaune communications
clare.shephard@maillot-jaune.co.uk