REPORT

The Osirium Ransomware Index: Executive stress and investment

Most IT leaders feel over-stressed and under-resourced to cope with the increasing ransomware threat

OSIRIUM

Introduction

Ransomware has been the fastest rising threat to IT teams over the last few years. As the Ransomware Index has shown, around 80% of businesses admit to already having been attacked.

Previous summaries from the Ransomware Index have focused on how prepared IT leaders are to protect vital systems such as backups and the risks introduced with outsourced IT. In this summary, we focus on the human impacts of not having the resources or support to implement those protections.

Leading IT and security teams is already a stressful position as every change they make could potentially open the business to attack. As this research shows, that stress level is increased by the lack of support from business leaders. The result will not only leave the organisation vulnerable to attack but have a real human cost in terms of increased stress levels leading to lost working hours and, potentially, to staff leaving for easier environments.

The lessons to learn are that investment levels in ransomware protection need urgent review by business leaders. When considering IT budgets, ransomware protection has to be a high priority.

> *The current situation is unsustainable. We are at 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.*

David Guyatt, Co-Founder and CEO, Osirium

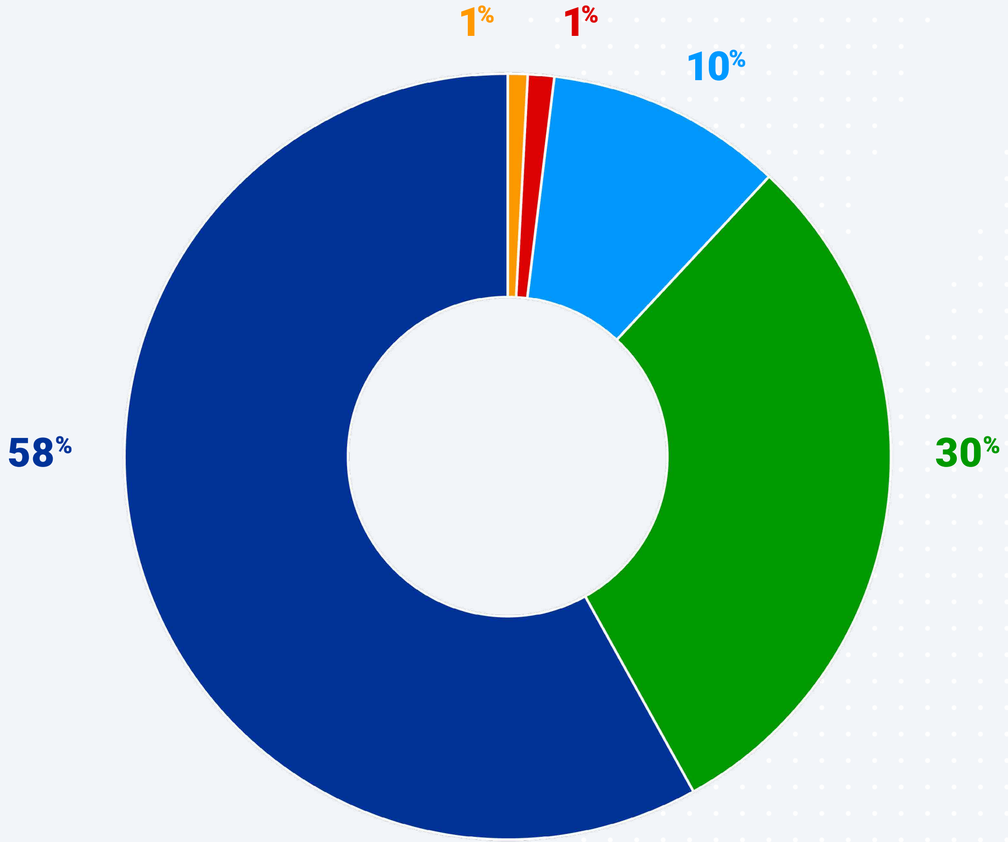
Organisations are not ready for a ransomware attack

Only 30% claim to be “extremely prepared” for an attack.

Just over half (58%) claim to be “somewhat prepared”, but that leaves a lot of opportunities for an attack or extending times for recovery. This lack of preparation is clearly associated with a lack of investment and support by executive leadership.

How prepared are you for a ransomware attack?

- I don’t know **1%**
- Extremely underprepared **1%**
- Somewhat underprepared **10%**
- Extremely prepared **30%**
- Somewhat prepared **58%**

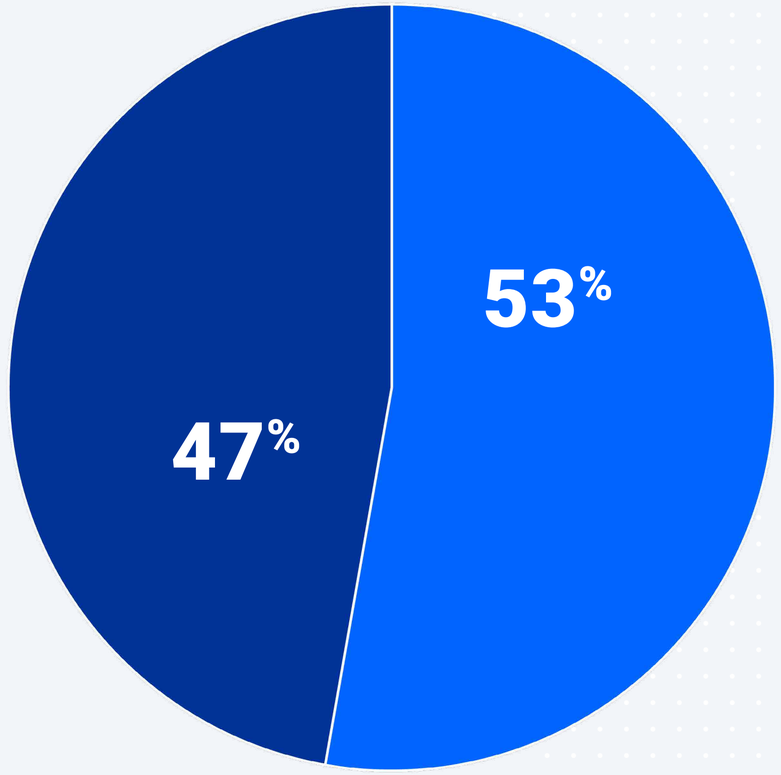


Investment levels do not match the threat

Only 47% believe they invest sufficiently to protect against the threat of ransomware.

Of the 1001 UK IT Leaders surveyed, a majority (53%) don't think they invest enough in ransomware protection. Around 6% said they don't invest at all, or not enough to make a difference and 46% thought they invest, but not enough.

Where IT is outsourced, the lack of investment is even more striking. In that situation, only 40% said they invest sufficiently.



Do you invest enough in ransomware protection?

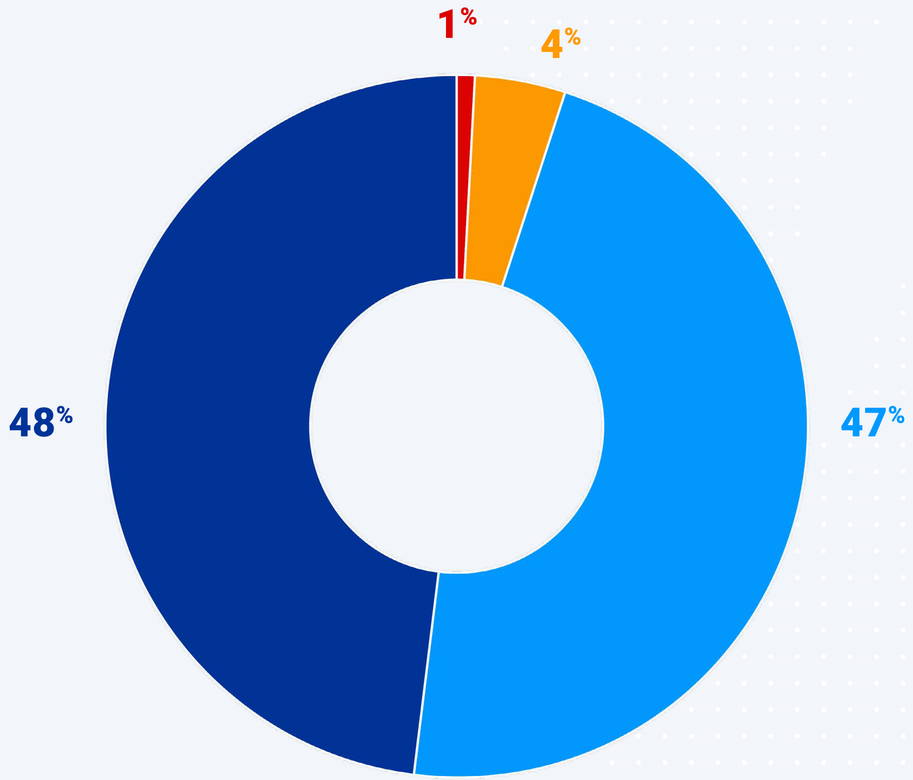
- We invest sufficiently to tackle these problems **47%**
- We don't invest enough **53%**

Lack of support matches lack of investment

52% of IT teams don’t get the executive level support they need.

Investment decisions need support from the highest levels in the business when allocating budgets. Clearly, all spending needs careful review and justification, but the Ransomware Index data suggests ransomware protection is not getting the attention it needs.

Less than half (48%) of IT leaders say they get all the support they need from their boards. 47% say they feel somewhat supported but often not enough.



Do you feel supported?

- Don’t feel supported at all - management is ignoring the risk **1%**
- Don’t feel very supported - I often struggle **4%**
- Get some resources but often not enough **47%**
- Get everything I need **48%**

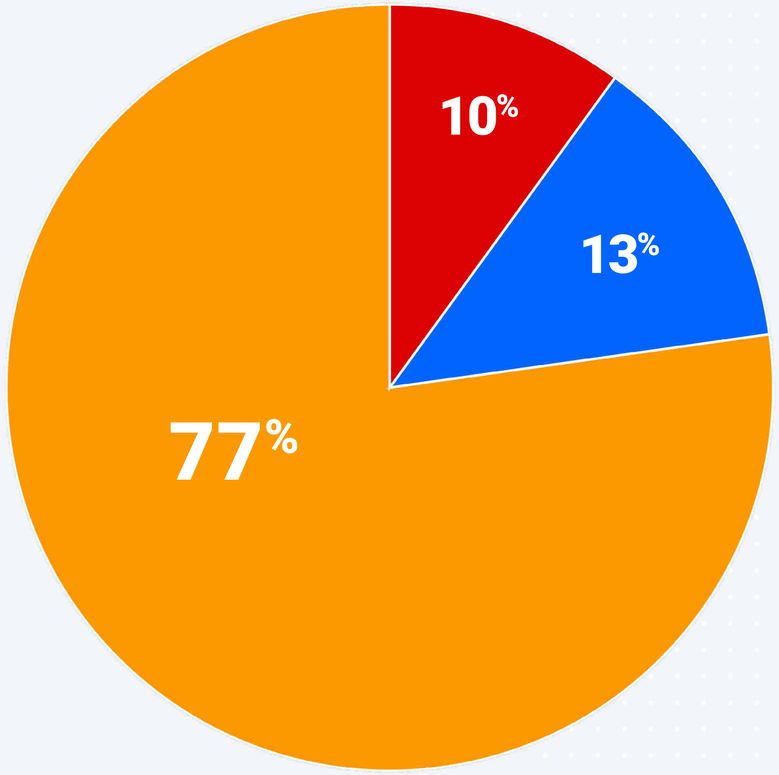
Stress levels are increased by lack of investment and support

22% say their stress levels have more than doubled by concerns about ransomware attacks.

Only 13% of IT Leader said they don’t feel stressed. Unfortunately, that means the majority (77%) feel stressed by potential ransomware attacks. 37% say it affects them most of the time with 22% reporting at least a doubling of stress levels.

How does the thought of ransomware affect your stress levels?

- Increased stress **77%**
- I don’t feel stressed **13%**
- Don’t know **10%**



In Summary

The Ransomware Index reveals a worrying picture of IT organisations in the UK. Teams are over-worked, over-stressed, under-funded and not ready for the ransomware attack which will inevitably come.

This lack of investment and support leaves businesses open for attack and causes more stress for already over-worked IT teams.

Although 53% of respondents say they think it is cheaper to pay a ransom demand than invest in protection (see **the previous Ransomware Index report**), that's a short-sighted view. Paying a ransom is no guarantee of success. The data encrypted by attack may already have been released or sold on the dark web and the decryption keys provided by the attackers aren't guaranteed to work. Even if the recovery is successful, the business downtime and reputational risk may already endanger the future of the business.

The human cost should not be underestimated. When IT experts are over-stressed, they can't perform to their best, they may need more time away from work, and they're more likely to be looking to move to a better supported position with another company. With the lack of expertise generally available in the IT market, replacing an experienced expert is expensive and time-consuming.

The warnings are clear: when considering future investment rounds, executives and board members must fully appreciate the potential impact of ransomware attacks and the need to properly fund and support prevention and recovery investments.

About the Research

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. Atomik 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**.