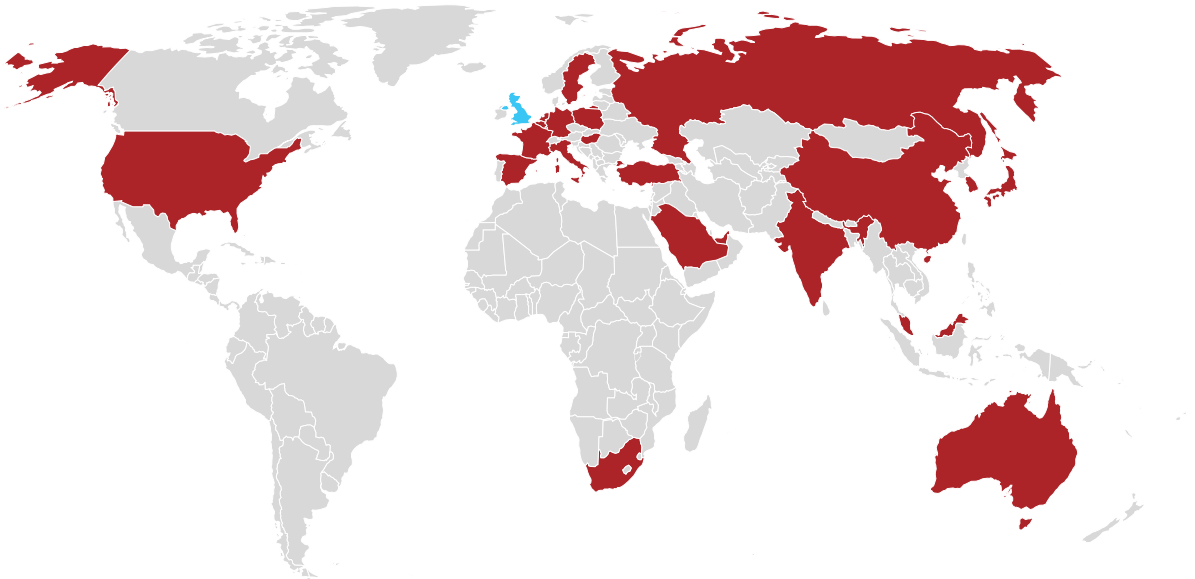
Veritas Ransomware Resiliency Research for EMEA

Global Summary

Digital transformation, and especially cloud adoption, has accelerated due to the global pandemic. Needing to support widespread remote working, enterprises are creating more data and facing a business imperative to move their applications out of their own data centers to the cloud. A new global survey of nearly 2,700 IT leaders and professionals in 21 countries, conducted by Wakefield Research and commissioned by Veritas Technologies, has determined that as this shift accelerates, resiliency planning has not kept pace, creating a significant resiliency gap. There are numerous reasons, but the key is that while enterprises have found the cloud to be an easy-to-adopt platform for running applications and information storage, they have found it much more difficult to implement a platform for resiliency. There is an urgent need for enterprises to close this resiliency gap by accelerating their resiliency planning to keep pace with today's speed and increasing complexity of IT.



VERITAS

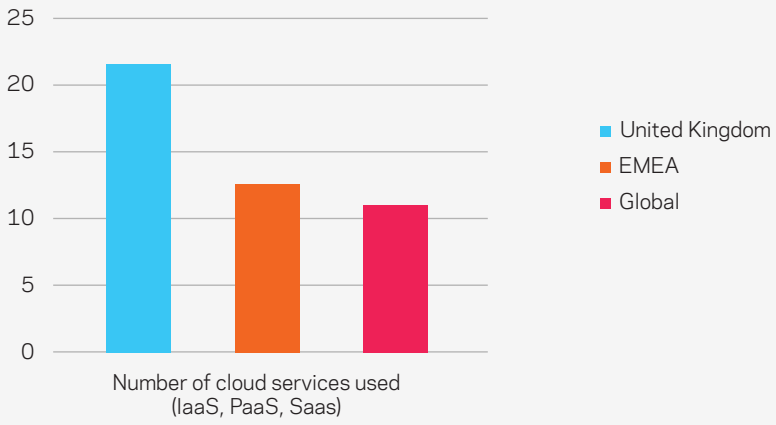
United Kingdom Outlook

Many enterprises in the United Kingdom are facing a significant resiliency gap, leaving their business-critical data vulnerable to ransomware threats. As companies have adopted more cloud platforms, creating more IT complexity, their resiliency planning has not kept pace. Though UK businesses haven't experienced as frequent ransomware attacks as businesses elsewhere in EMEA and globally, too many of them face the prospect of lengthy business disruption or lost data if they were hit with a ransomware attack.

Increasing IT Complexity

- UK enterprises are aggressively moving to the cloud. 31% of enterprises have either moved all or most of their data to the public cloud and a further 33% have adopted a multi-cloud hybrid strategy.
- The average UK business is using 21 cloud services (IaaS, PaaS and SaaS), more than any other country surveyed in EMEA; the average for EMEA being 13 cloud services and 10 in Asia-Pacific.

How many cloud services does your company use?



- All of that cloud usage is creating more IT complexity. 55% of UK respondents said their enterprise's security measures lag behind their IT complexity.

VERITAS

- UK IT leaders' top concerns around IT overcomplexity run the gamut and differ from their EMEA counterparts:

UK IT leaders' top IT overcomplexity concerns:

39% Increased risks of external attacks, such as data breaches and ransomware

37% Employees having access to files they shouldn't

34% The amount of time it takes IT staff to manage data and applications

EMEA's IT leaders' top IT overcomplexity concerns

37% Increased risks of external attacks, such as data breaches and ransomware

36% Increased risk of internal attacks (leaks, employee error, malfeasance, etc.)

35% Potential for data loss

- UK enterprises are taking action to fix their resiliency gap. 51% of UK respondents said their company had either increased their IT security budgets or kept them flat since the start of the COVID-19 pandemic.

Impact of Ransomware

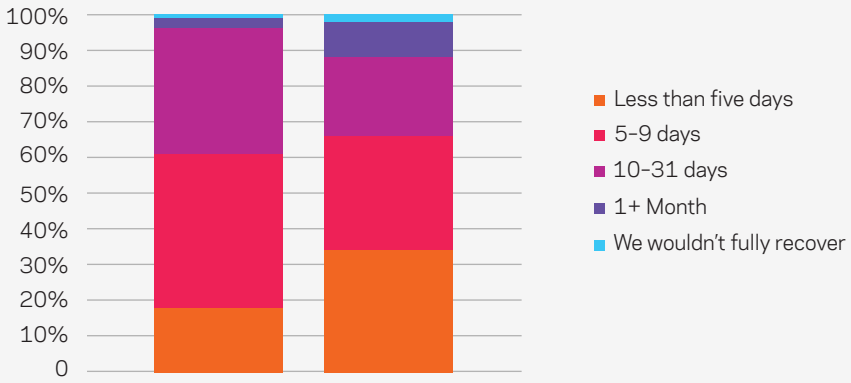
- The UK has been more effective mitigating the ransomware threat compared to their counterparts in EMEA. 29% of UK respondents said they had faced at least one attack, versus 38% in EMEA.
- UK companies, though, are paying the price for not being sufficiently resilient. Because their backup and recovery systems aren't robust enough, when UK companies are attacked by ransomware, they often have no choice but to pay the ransom. Among those experiencing a ransomware attack, 86% of UK respondents said their company paid all or part of the ransom, compared to 49% across EMEA.

VERITAS

Resiliency Gap

- An overwhelming number of UK enterprises – 81% – believe it would take 5 days or longer to fully recover from a ransomware attack. This was the highest percentage of any country surveyed, by far. By comparison, 65% of EMEA respondents said it would take five days or longer for them to fully recover from a ransomware attack.

How long would it take to fully recover from a ransomware attack (if you didn't pay the ransom)?



- Only 5% of UK companies follow the recommended best practice of having three copies of their data, with one copy offsite and offline, which is well below the 14% across EMEA who said so. 35% of UK enterprises have three or more copies of their data
- UK organizations are testing their disaster recovery (DR) plan more regularly than their EMEA counterparts – 87% have tested it in the last three months, compared to 56% in EMEA and 60% worldwide

United Kingdom Recommendation: UK enterprises are among the least capable across EMEA of recovering quickly from a ransomware attack, creating urgency to address their resiliency gap as soon as possible so that they can recover their data without paying the ransom. UK enterprises should consider adopting more robust methods of ransomware attack mitigation. These include:

- **End-to-end strategy review**: UK enterprises should review their resiliency strategy to ensure that it is predictable and based on real-time visibility, monitoring and recovery automation
- **More robust backup**: Companies should follow a "3-2-1" backup approach: a minimum of three copies of their data, in two disparate locations, with at least one offsite.
- **More frequent disaster recovery rehearsals**: Ideally, enterprises should test their DR plan once per month. Their data and applications landscape is changing so quickly that less frequent rehearsals risk having a DR site fail when needed.
- **Frequent security updates**: IT teams should stay current with security patches and new releases with security updates
- **Data encryption**: Enterprises should implement in-transit encryption to protect data from being compromised on the network
- **Immutable storage**: IT teams should use immutable and indelible storage technology to prevent ransomware from encrypting or deleting backups
- **Access management**: Implement role-based access control and limit access to only required functionality for individuals and personas