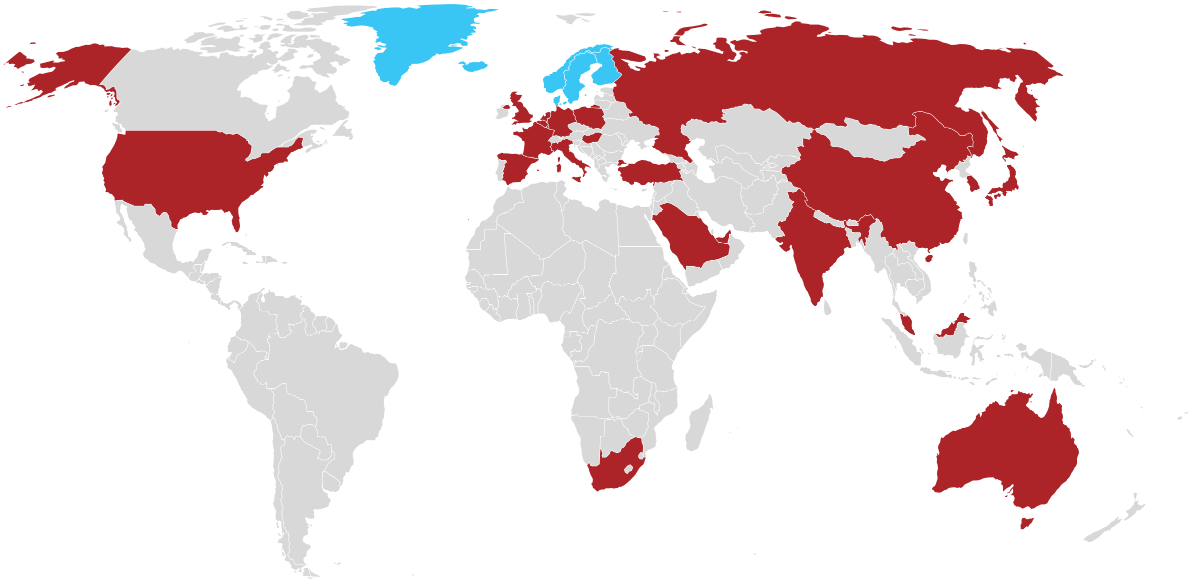
Veritas Ransomware Resiliency Research for the Nordics

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 2,840 IT leaders and professionals in 24 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've 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.



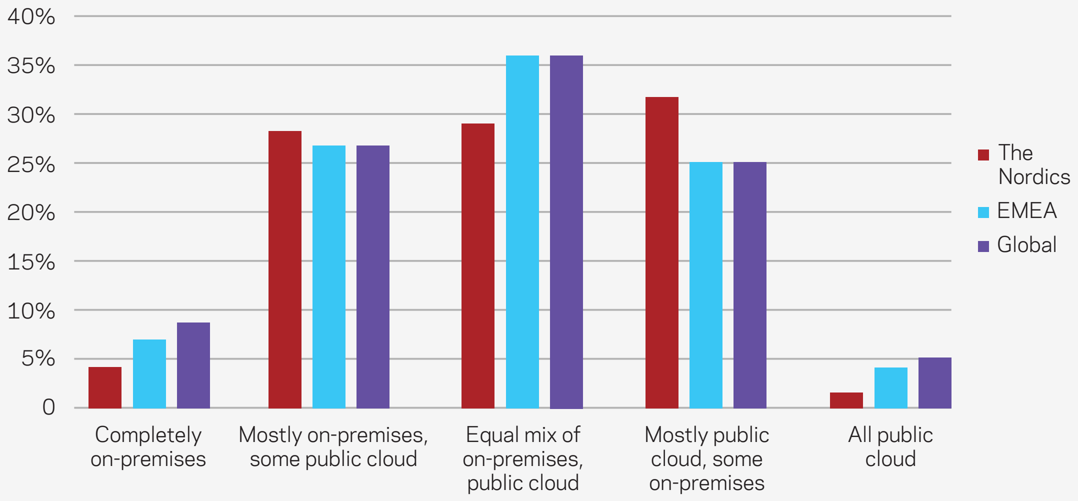
The Nordic Outlook

Many enterprises in the Nordics are facing a significant resiliency gap, leaving their business-critical data vulnerable to ransomware threats. As they've adopted more cloud platforms, creating more IT complexity, their resiliency planning has not kept pace, leaving them at risk. Nearly three in ten of respondents in the Nordics said their company had suffered a ransomware attack. Too many of them face the prospect of lengthy business disruption or lost data if they were to be hit with a ransomware attack.

IT Complexity

- 29% of enterprises in the Nordics are adopting a hybrid multi-cloud strategy, slightly lower than the EMEA average of 36%.
- The average company in the Nordics is using about 12.9 cloud services (IaaS, PaaS and SaaS), just above the EMEA average of 12.

Where does your organization keep most of its data and applications?



- All of that cloud usage is creating more IT complexity. 87% of Nordic respondents said their enterprise's security measures lag behind their IT complexity, compared to 67% across EMEA and 64% globally.

- Nordic IT leaders are concerned by the lack of visibility into data and applications, along with external attack threats.

Nordic IT leaders’ top IT overcomplexity concerns:		EMEA IT leaders’ top IT overcomplexity concerns:	
39%	Lack of visibility into increasing levels of data and applications	37%	Increased risks of external attacks, such as data breaches and ransomware
36%	Increased risks of external attacks, such as data breaches and ransomware	36%	Increased risk of internal attacks (leaks, employee error, malfeasance, etc.)
34%	How much more difficult it makes my job	35%	Potential for data loss

- Enterprises in the Nordics are taking action to address their resiliency gap, albeit at a more measured pace compared to their global counterparts. 41% of Nordic respondents said their company has increased their IT security budget since the start of the COVID-19 pandemic, slightly lower than the 42% across EMEA overall.

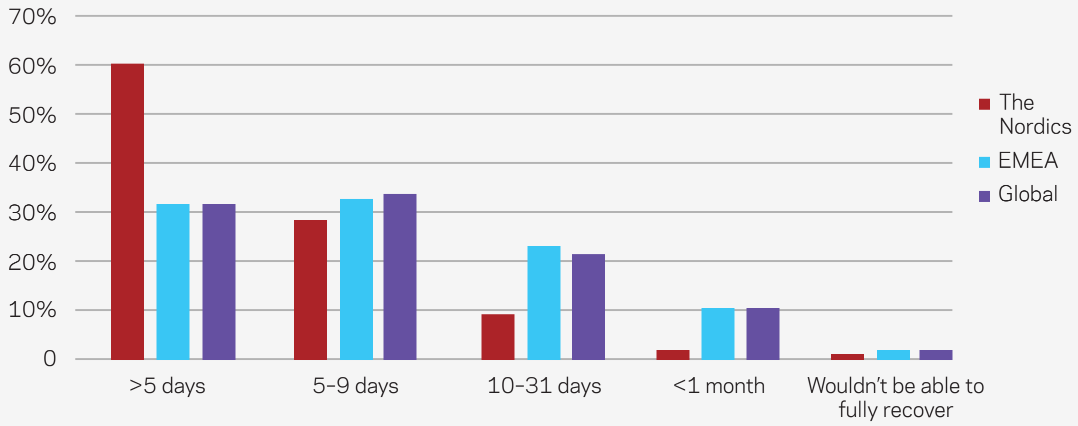
Impact of Ransomware

- Ransomware is a growing threat. 29% of Nordic respondents said they had faced at least one attack, the same as EMEA overall and below the global average of 41%.
- Too many enterprises in the Nordics are paying the price for not being sufficiently resilient. Because their backup and recovery systems aren’t robust enough, when Nordic companies are attacked by ransomware, they often have no choice but to pay the ransom. Among those experiencing a ransomware attack, 86% of Nordic respondents said their company paid all or part of the ransom. This is still significantly higher than EMEA (55%) and globally (60%).

The Resiliency Gap

- Nordic enterprises appear to be more resilient than their EMEA and global counterparts. 40% of Nordic enterprises believe it would take 5 days or longer to fully recover from a ransomware attack, significantly better than the EMEA and global average of 66%.

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



- Too many Nordic enterprises aren't sufficiently backing up their data. Only 8% of Nordic respondents said their company follows the recommended best practice of having three copies of their data, with one copy offsite and offline. This is below the EMEA average of 14% and the global average of 17%. A further 36% of Nordic respondents said their company has three or more copies of their data onsite, the same as the global average.

- Nordic organizations are testing their disaster recovery plan more frequently their EMEA and global counterparts – 90% have tested it in the last three months, well above EMEA (62%) and globally (61%).

The Nordic Recommendation: Threats loom for enterprises in the Nordics. Despite aggressively moving data and workloads to the cloud, 87% of Nordic organizations say their security measures are not keeping pace with their increasingly complex IT infrastructure, and just 44% have three copies of their data. The fact that 86% of Nordic companies that have been attacked by ransomware needed to pay all or part of the ransom indicates that these companies need to focus more on resiliency planning. Companies in the Nordics need to address their resiliency gap as soon as possible so that they can recover their data without paying the ransom. Enterprises in the Nordics should consider adopting more robust methods of ransomware attack mitigation. These include:

- **End-to-end strategy review**: Enterprises in the Nordics should review their resiliency strategy to ensure that it is predictable and based on real-time visibility, monitoring and recovery automation.
- **Protect your backups**: Use tools and processes to make sure your backups are not at risk in the event of a Cyber-attack.
- **Immutable storage**: IT teams should use immutable and indelible storage technology to prevent ransomware from encrypting or deleting backups.
- **Pay close attention to information protection success rate**: 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 are 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.
- **Access management**: Implement role-based access control and limit access to only required functionality for individuals and personas.