Cyber risk is still ranked as the most significant risk facing directors and officers, but this year, we asked people also to comment on cyber extortion and it has immediately been ranked in the top four risks across all regions, company revenue sizes and industries.

The concerns around cyber extortion are undoubtedly driven by the surge in ransomware attacks over the last 24 months, the majority of which have included the demand for an extortion payment. Ransomware has become a low investment, low risk and high reward method of cybercrime which organisations cannot ignore. Looking at our WTW Claims Insight Data – where we have reviewed more than 2,000 claims’ across our portfolio – we have seen a 200% increase in ransomware claims notifications under cyberinsurance policies since 2019.

From an industry sector perspective, our data shows the top three industry sectors impacted by ransomware attacks are healthcare, manufacturing and education. In 2021, we also saw a shift in tactics from the cybercriminals, including one of the first major attacks against critical infrastructure, the highly publicized Colonial Pipeline attack. As a result, governments and regulators have been alerted to ransomware and extortion activity.
From a cost perspective, our claims data shows the top two cost components following ransomware attack are business interruption (33%) and ransomware payments (22%), with an average ransom demand of $5.5m.

The top two cost components following ransomware attack

<table>
<thead>
<tr>
<th>Business interruption</th>
<th>32%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ransomware payments</td>
<td>22%</td>
</tr>
</tbody>
</table>

with an average ransom demand of $5.5m

To pay or not to pay?
When faced with an extortion demand, one of the key considerations for directors and officers is whether or not to pay the demand. In our experience, the discussion around whether to pay is not always straightforward. The board will usually need to consider several factors including:

- **If we don’t pay, will we be able to recover our systems and data?** And even if we do pay, does this guarantee we will recover everything?

- **Are we allowed to pay?** Putting aside the question of whether or not to pay, the legality of extortion payments requires careful consideration. The position on legality varies across jurisdictions and there are several financial sanctions and legislative requirements that potentially come into play.

- **If we can pay, how would we pay an extortion demand?** Ransomware attackers often demand ransom payments in cryptocurrency. Therefore, if the decision is taken to pay, it’s important to plan how you would access cryptocurrency.

- **Do we have insurance in place and what does it cover?** For companies purchasing specific cyberinsurance, coverage will usually be provided for the financial impacts of a cyber extortion event, including extortion payments, incident response costs, business interruption and regulatory costs and liabilities. Coverage will also usually include access to specialist extortion advisors to support with the investigation and recovery.

The risk of cyber extortion is real, and we have outlined above, the considerations for directors and officers can be complicated. If nothing else, this highlights the need for directors and officers to be aware the exposure and to ensure that their organisation takes a proactive approach to cyber risk identification, quantification, and mitigation.
About WTW

At WTW (NASDAQ: WTW), we provide data-driven, insight-led solutions in the areas of people, risk and capital. Leveraging the global view and local expertise of our colleagues serving 140 countries and markets, we help you sharpen your strategy, enhance organizational resilience, motivate your workforce and maximize performance. Working shoulder to shoulder with you, we uncover opportunities for sustainable success — and provide perspective that moves you. Learn more at wtwco.com.