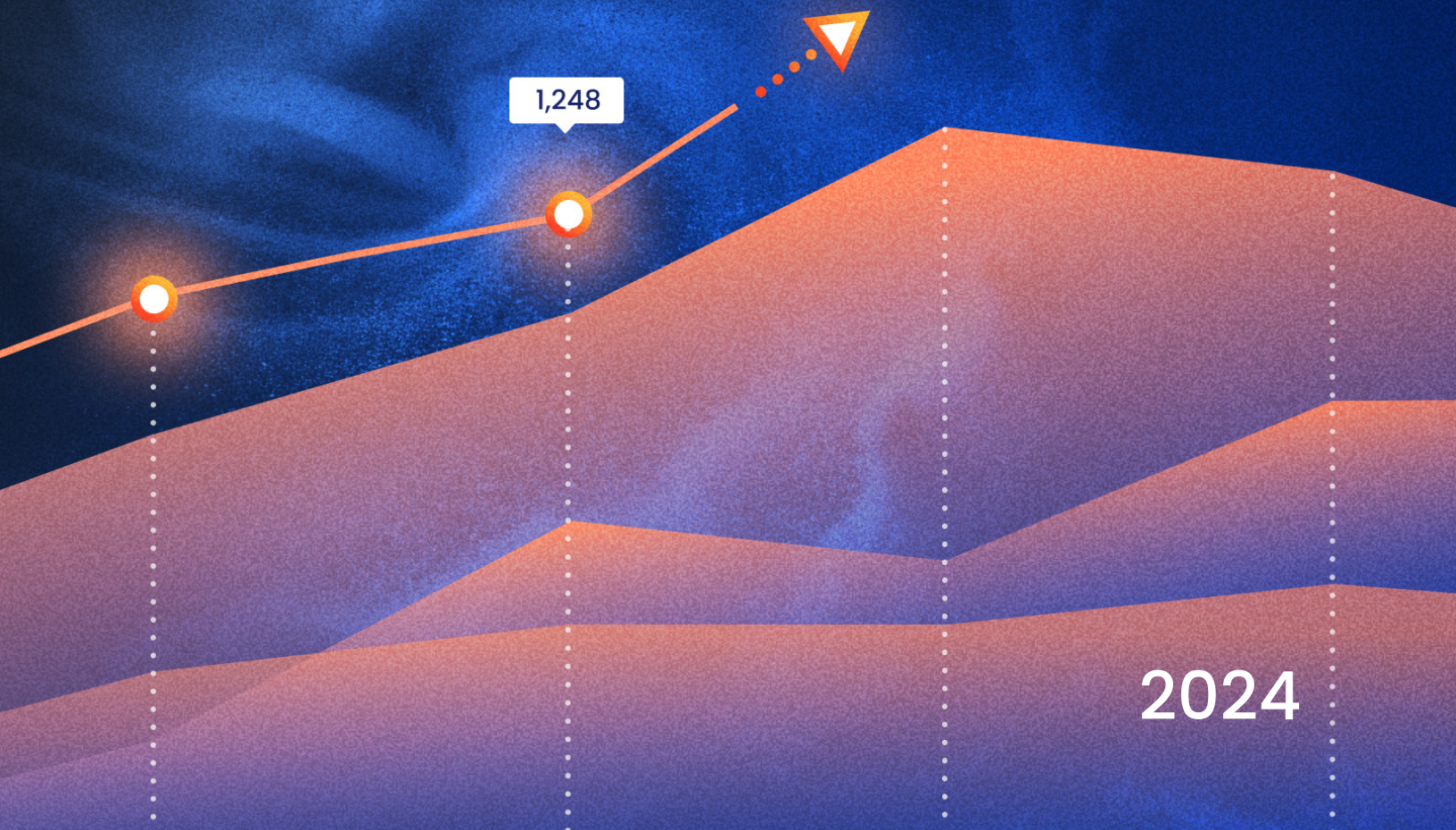
CORVUS
BY TRAVELERS

Q2 CYBER THREAT REPORT

Ransomware Season Arrives Early



2024

Table of Contents

Introduction 3

Global Ransomware Activity 3

Activity Across Ransomware Groups in Q2: LockBit Surges Back 4

Ransomware costs are rising; backups remain a critical tool to avoid the worst outcomes 6

Industry Insights 8

Conclusion 10

Authors

Jason Rebholz
Chief Information Security Officer
Corvus Insurance

Ryan Bell
Head of Threat Intelligence
Corvus Insurance

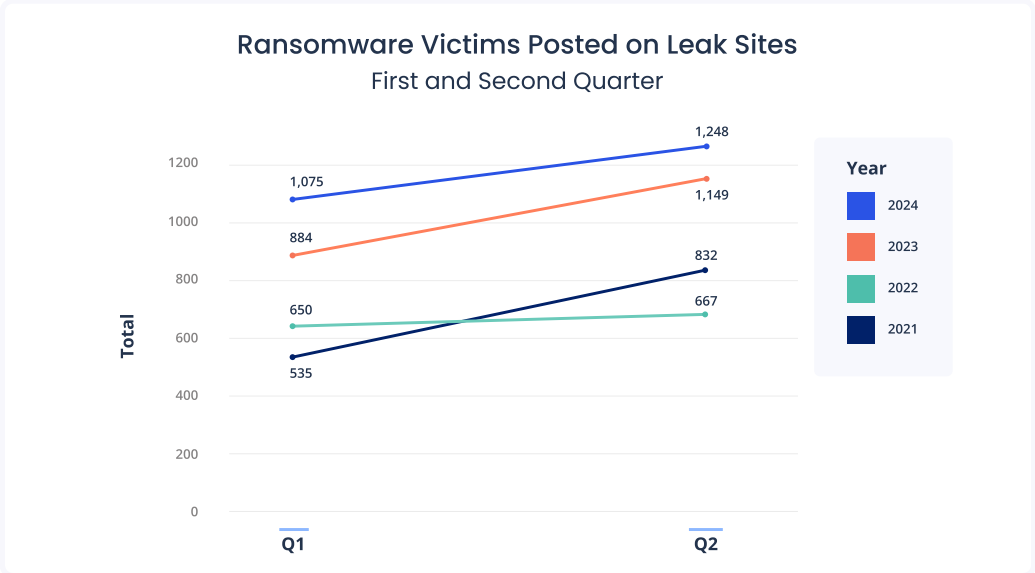
Introduction

In a year marked by shattered records of the unfavorable kind, Hurricane Beryl's early arrival as a Category 5 event in the Atlantic Ocean left scientists astounded. To see a hurricane that early is rare; to see a Cat 5 that early is nearly unprecedented.

This episode parallels the climate within the world of ransomware. The first half of 2024 saw the highest level of ransomware activity we've seen in that portion of the year. In the recent past, the third and fourth quarters have seen the highest ransomware activity in a given year. If those trends were to hold this year, that would mean ransomware attacks will hit new highs once again this year: a foreboding forecast.

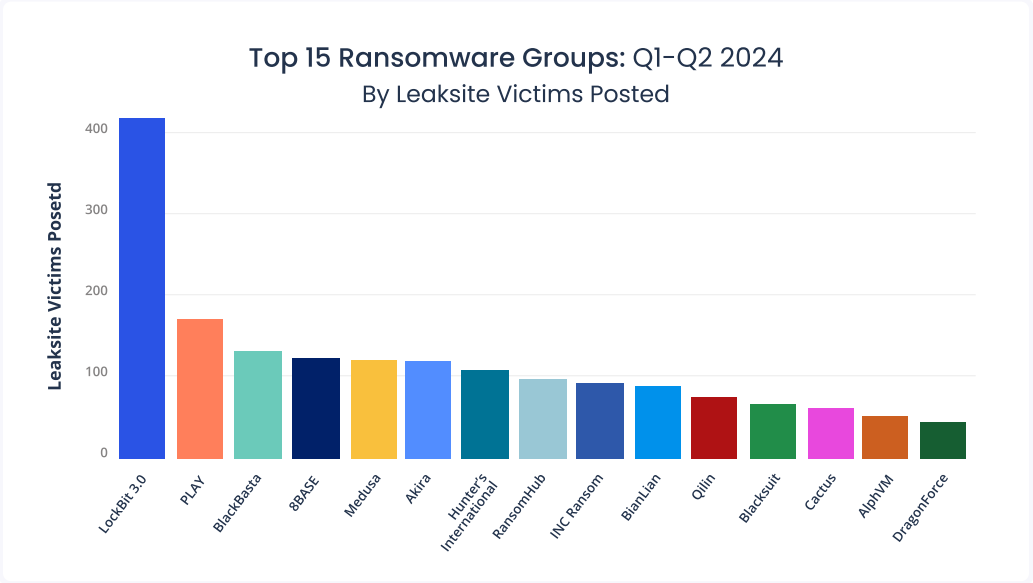
In addition to the continued elevated level of attacks, this quarterly report unpacks several associated trends, including the ever-growing demands in ransom payments and the swell in significant third-party breaches that underscore the acute risk surrounding third parties and supply chains.

Global Ransomware Activity



Q2 of 2024 witnessed an alarming 1,248 ransomware victims posted to leak sites, positioning it as the second most prolific quarter on record by that measure of activity. That represents a 16% increase from the previous quarter and a sustained 8% year-over-year rise. It's important to remember that ransomware activity can exhibit seasonality; we often see dips in January and during the peak summer months of July and August. Despite last year's anomaly caused by Cl0p's widespread exploitation of file transfer software MOVEit, we expect to see a similar downturn this summer, though threats will persist and we do expect that from September through December activity will be high, based on trends year-to-date.

Activity Across Ransomware Groups in Q2: LockBit Surges Back



As some ransomware groups fade away—like the unexpected departure of the ALPHV(BlackCat) group in Q1, an event we covered in our last report — others quickly emerged in Q2 to fill the void, including PLAY, Medusa, RansomHub, INC Ransom, and Blacksuit, among other lesser-known factions.

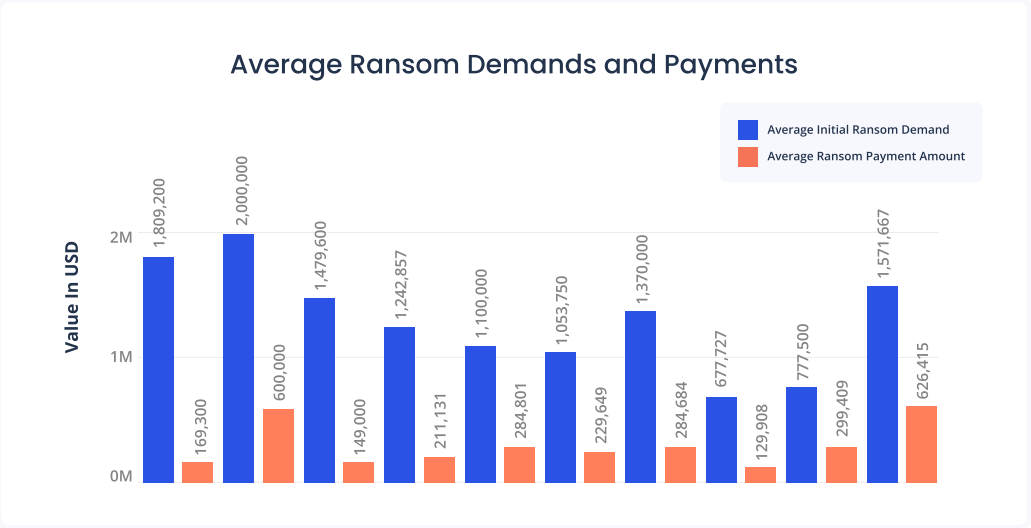
In the case of the LockBit ransomware gang, law enforcement's actions against the group earlier in the year had a significant impact. In an announcement, international law enforcement unmasked the principal orchestrator of LockBit which resulted in the imposition of OFAC sanctions against him. These sanctions further complicate the process of ransom payments and casts further doubt on the group's ability to sustain its operations moving forward. To date there has been no indication of the group reverting to its previous levels of activity.

However, it's worth noting that LockBit did experience a sudden resurgence in May that came as a surprise, before activity dropped back down. After examining the daily activity on the Lockbit leak site, it seems that the abrupt surge in listed victims coincided with that announcement. The leader of the LockBit gang has a history of seeking attention through publicity stunts. For example, they offered $1,000 to anyone who would get a tattoo of "LockBit" on their body, and also put out a $1 million reward for anyone who could uncover the leader's true identity. This sudden burst of activity may have been in response to or in anticipation of law enforcement actions.

Following the unexpected surge, LockBit's operations have persisted but at a significantly reduced capacity compared to their activity before the Q1 law enforcement interventions.

Ransomware costs are rising; backups remain a critical tool to avoid the worst outcomes

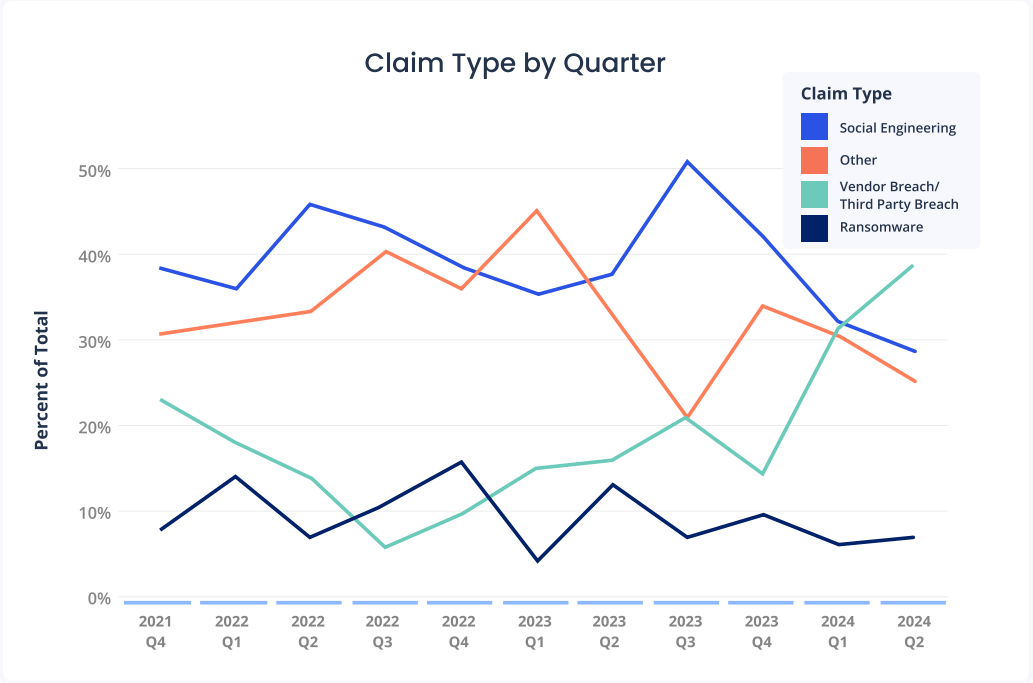
We're witnessing an increase in the frequency and severity of ransomware attacks based on claims occurring within the Corvus book of business. Even more concerning is that ransom demands are starting a significant upward trend and in Q2 hit a near two year high, with average payments even exceeding the highs from 2022.



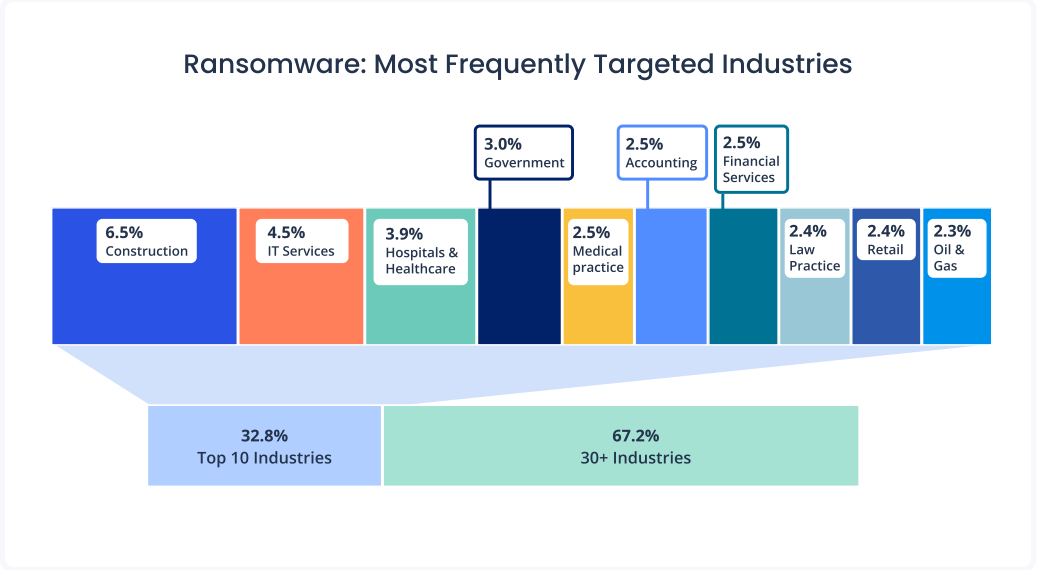
Although threat actors control how much is demanded for ransom, certain measures can impact the propensity of an organization to pay that ransom. The presence of backups is a significant factor. Given that ransomware's primary goal is to render data inaccessible through encryption, those without robust backups are more likely to have their hand forced in a ransom situation — 2.38 times more likely to pay a ransom, to be exact, according to recent Corvus claims data.

Moreover, organizations with effective backup strategies, including immutable backups and what we refer to as a "3-2-1" strategy, wherein multiple copies of data are stored in locations that are segregated from the primary network, tend to fare better financially even if they do end up having some costs associated with an incident. Among Corvus policyholders who reported ransomware incidents, the median claim costs for those with backup strategies in place was 72% lower than for their less-prepared counterparts. This is mainly because those organizations are able to skip the costly process of decryption, which requires hiring third-party experts: they instead recover all or most of their critical data from backups.

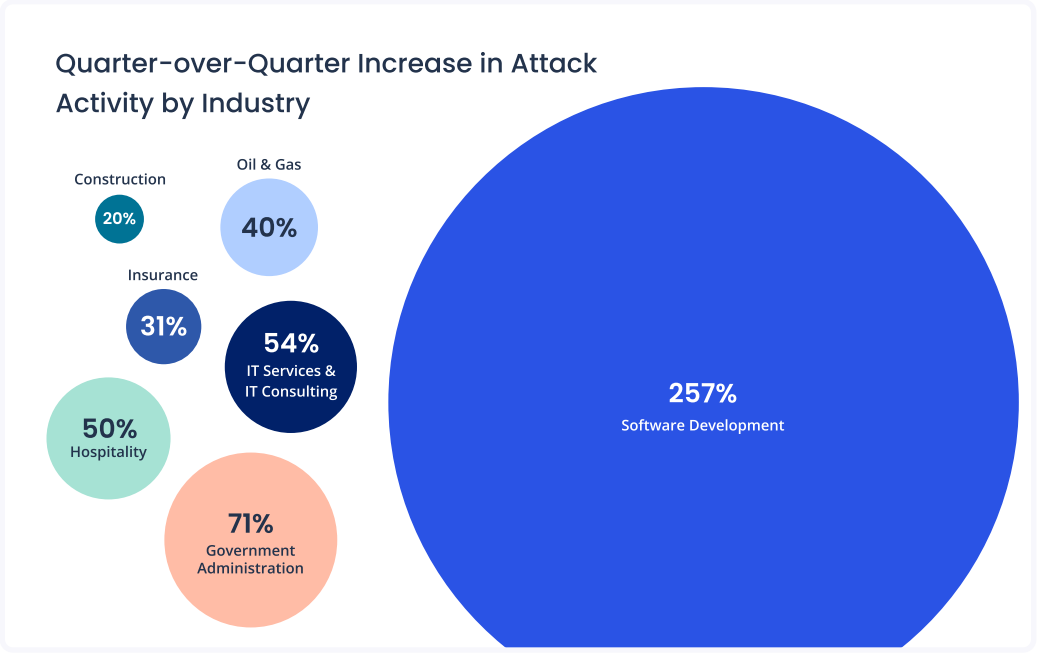
Unfortunately, backups aren't a silver bullet. While they do reduce the chances of a ransom being paid and reduce the cost of claims overall, they don't completely eliminate risk. Ransomware operators have evolved their tactics, recognizing that many organizations possess valuable and sensitive information. They exploit this by engaging in double-extortion schemes — they not only encrypt the data, but they also exfiltrate (steal) it, threatening to release it on the dark web. In 2024, data theft was involved in 93% of ransomware incidents among Corvus policyholders, a dramatic increase from a rate of less than 50% as recently as 2022. Consequently, even entities with secure backups may find themselves paying ransoms to prevent the exposure of stolen data. And if we learned anything from the LockBit saga, it's that threat actors often don't delete data even when they say they do.



Industry Insights



Unlike the many of the developments we've discussed above, the top industries found on ransomware leak sites remained mostly stable between Q1 and Q2, though there was some movement among them. For example, construction moved from 2nd to 1st in Q2, and government and oil and gas joined the list. In addition to the top industries, there were a number of industries that showed substantial quarter-over-quarter increases in attack activity.



After observing the typical downturn in ransomware activity during Q1, a rebound in Q2 that would lead to quarter-over-quarter increases across various industries was anticipated. While this uptick wasn't necessarily due to targeted attacks on specific sectors, the overall prevalence of ransomware was higher this quarter. Notably, the IT Services and Software Development sectors experienced significant increases in incidents. While attacks did not reach record levels for these particular industries, the increase is noteworthy.

Notably, the IT Services and Software Development sectors experienced significant increases in ransomware incidents. While attacks did not reach record levels for these particular industries, the increase is noteworthy. Those sectors are particularly vulnerable as they represent a form of "systemic risk" since any issues they encounter can have extensive ripple effects that disrupt operations for numerous downstream clients. Even smaller IT firms can trigger widespread outages among their clientele if their systems are compromised or if attackers leverage their networks to target connected entities.

During Q2, at least three cybercriminal groups appeared to show a disproportionate interest in these technology sectors. This includes RansomHub, which was responsible for 16% of the reported victims within the IT Services industry. Following closely were PLAY and Blacksuit which accounted for an additional 18%.

Out of the 23 ransomware gangs that claimed at least one victim in the IT sector, these three groups alone were linked to 35% of the incidents. It's not definitively clear whether affiliates of RansomHub, PLAY, and Blacksuit are deliberately targeting IT companies. However the patterns suggest that these organizations should be monitored closely because they stand out as potential candidates for orchestrating the next significant vendor or third-party attack.

Conclusion

As we close the chapter on Q2 of 2024, it's evident that the ransomware landscape is developing a knack for disruption. The parallels drawn between the unpredictability of natural disasters and the volatile nature of cyber threats have never been more apt. Just as Hurricane Beryl set a new precedent in meteorological history, the digital storms of ransomware are charting their own destructive course, leaving indelible marks on the fabric of disparate industries.

The data presented in this report paints a stark picture: a relentless increase in ransomware incidents, soaring payment demands, and a burgeoning wave of third-party breaches.

These challenges are exacerbated by threat actors like RansomHub, PLAY, and Blacksuit which are carving out their niches in the IT sector. Add it up and the message is clear—no entity is an island in this digital ecosystem and rthe systemic risks posed by these industries demand heightened vigilance.

These trends also serve as a clarion call to organizations across all sectors: the need for robust, multi-layered security strategies has never been greater. As we navigate through the rest of 2024, businesses must take a proactive stance toward better security and to prepare for the inevitable squalls ahead. This includes taking the insights from this tumultuous period and transforming them into actionable intelligence, fortifying our defenses and fostering resilience against the ever-present threat of cyber disaster.

Corvus analysis was made possible with supporting data from eCrime.ch. This report is intended for general guidance and informational purposes only. This report is under no circumstances intended to be used or considered as specific insurance or information security advice. This report is not to be considered an objective or independent explanation of the matters contained herein.