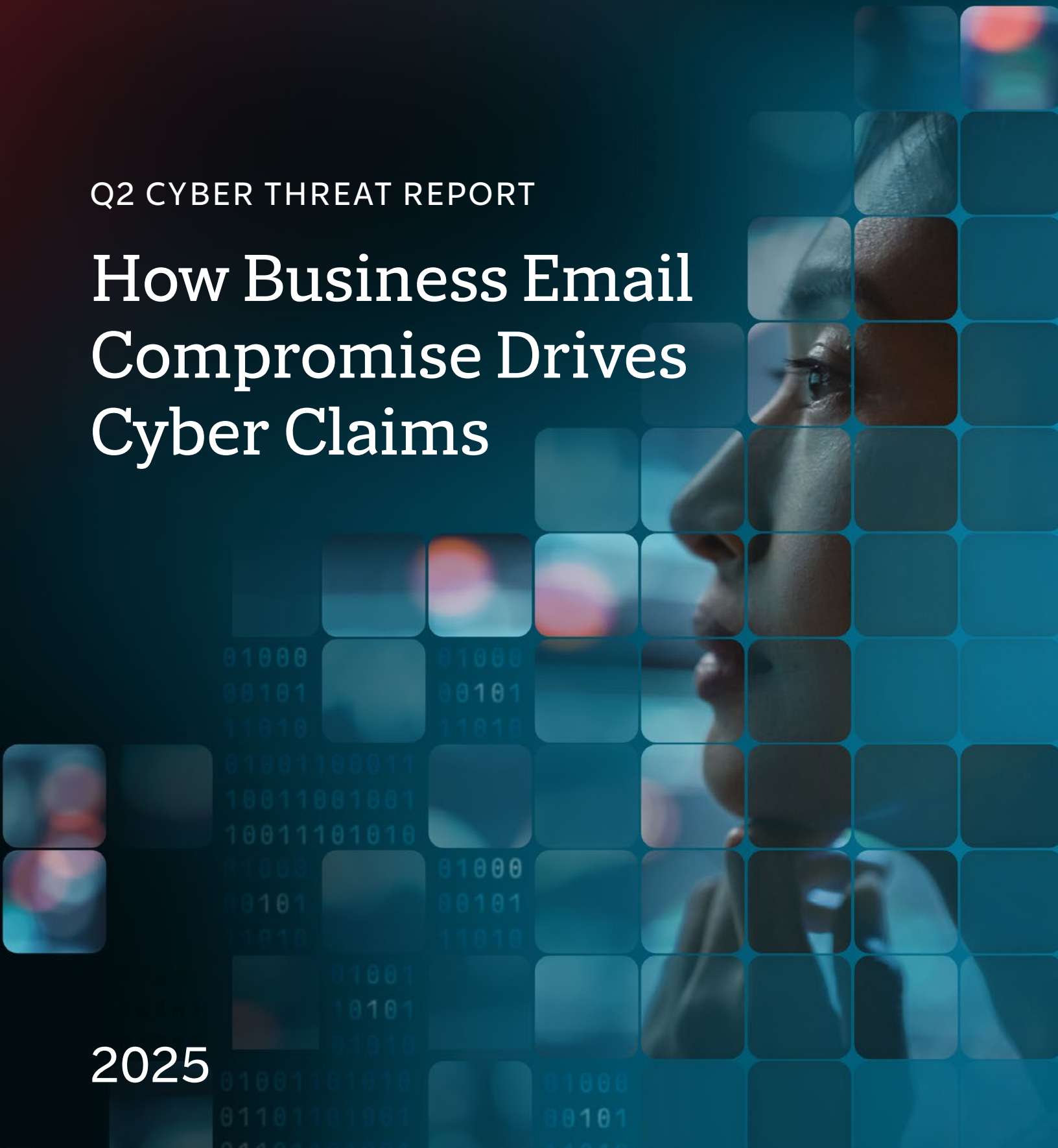
TRAVELERS

Q2 CYBER THREAT REPORT

How Business Email Compromise Drives Cyber Claims



2025

Table of Contents

Published by Travelers with contributions from:

Ryan Bell

Director, Threat Intelligence – Cyber Risk Services, *Travelers*

Nicholas Kelley-Ossey

Sr. Director, Cybersecurity, *Travelers*

Courtney Hassenfeldt

Cybersecurity Technologist, *Travelers*

Alex Pinto

Sr. Director of Product Marketing – Cyber, *Travelers*

Executive Summary

In Q2 2025 activity on ransomware leak sites, our proxy for overall ransomware activity, dialled back slightly – down to levels that put it in line with the long-term rise in activity observed over the past few years. That's not overwhelmingly great news, but it's far better than one possible alternative: that the elevated levels of activity observed in Q1 were only the beginning of an upward change in the trajectory of ransomware activity. It seems, for now, that is not the case.

The ransomware ecosystem is in disarray after law enforcement actions and internal strife led to the dissolution of notable groups of threat actors in the first half of 2025. We cover these happenings in this edition of the Cyber Threat Report, as we always do. But we're also taking some time to focus on a less dramatic – but more consistent – factor in the realm of cyber threats: business email compromise (BEC).

A UK government Cyber Security Breaches survey for 2024 demonstrated that half of all UK businesses experienced a breach or attack, and that phishing was overwhelmingly the most common attack vector for cyber and fraud incidents including BEC. At Travelers, situations involving BEC or social engineering fraud (a frequent outcome of BEC) represented nearly half of all cyber claims in the past five years. Clearly, this area of cyber risk is meaningful yet it consumes a fraction of the attention that software vulnerabilities and ransomware do. We're hoping to change that, just a tiny bit, this quarter.

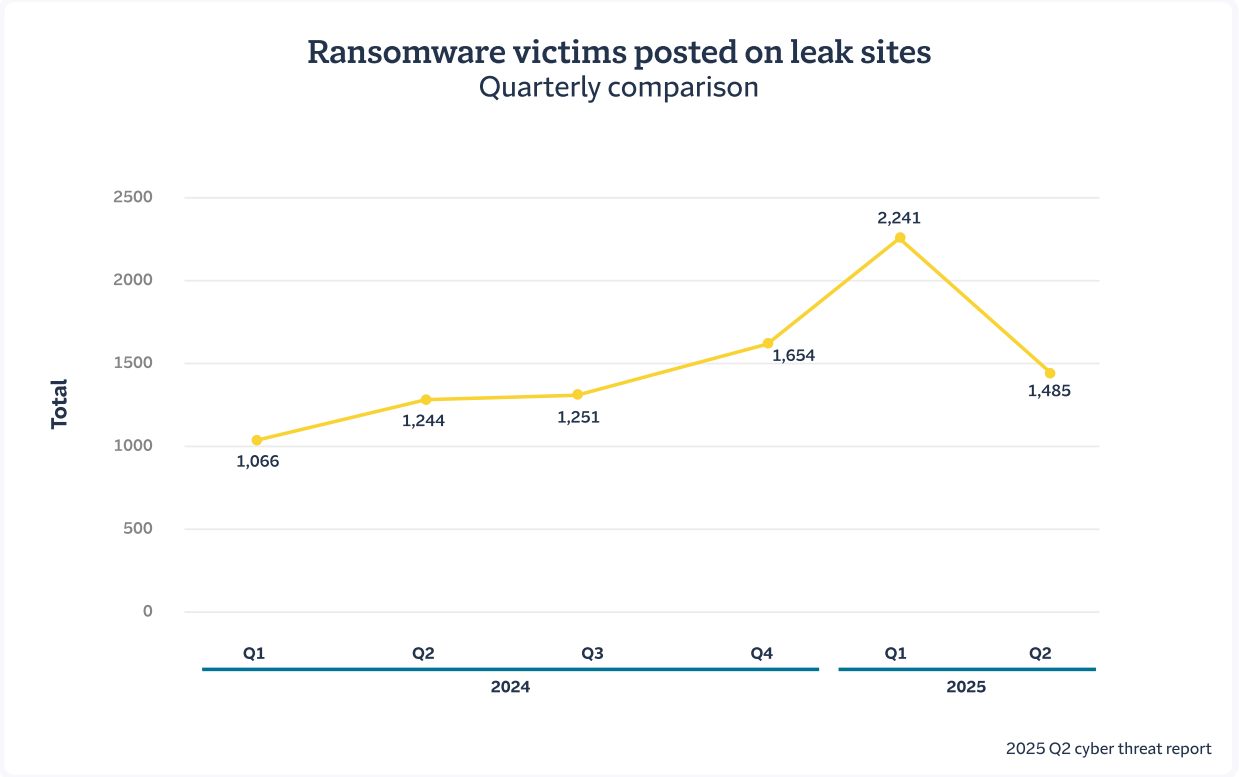
Ransomware activity eases: leak site listings declined to 1,485 incidents in Q2 2025, after reaching 2,241 incidents in Q1.

Social Engineering Fraud and Business Email Compromise (BEC) continue to drive claims: When combined, these often-overlapping categories are consistently among the top three drivers of claims at Travelers. BEC exploits are evolving to include new tactics, including extortion.

Ransomware Leak Site Activity Declines Quarter-over-Quarter; Remains Elevated Against Long-term Averages

After reaching 2,241 incidents posted on ransomware leak sites in Q1 2025 — the highest quarterly total that Travelers has reported in four years of tracking this metric — listings declined to 1,485 incidents in Q2 2025.

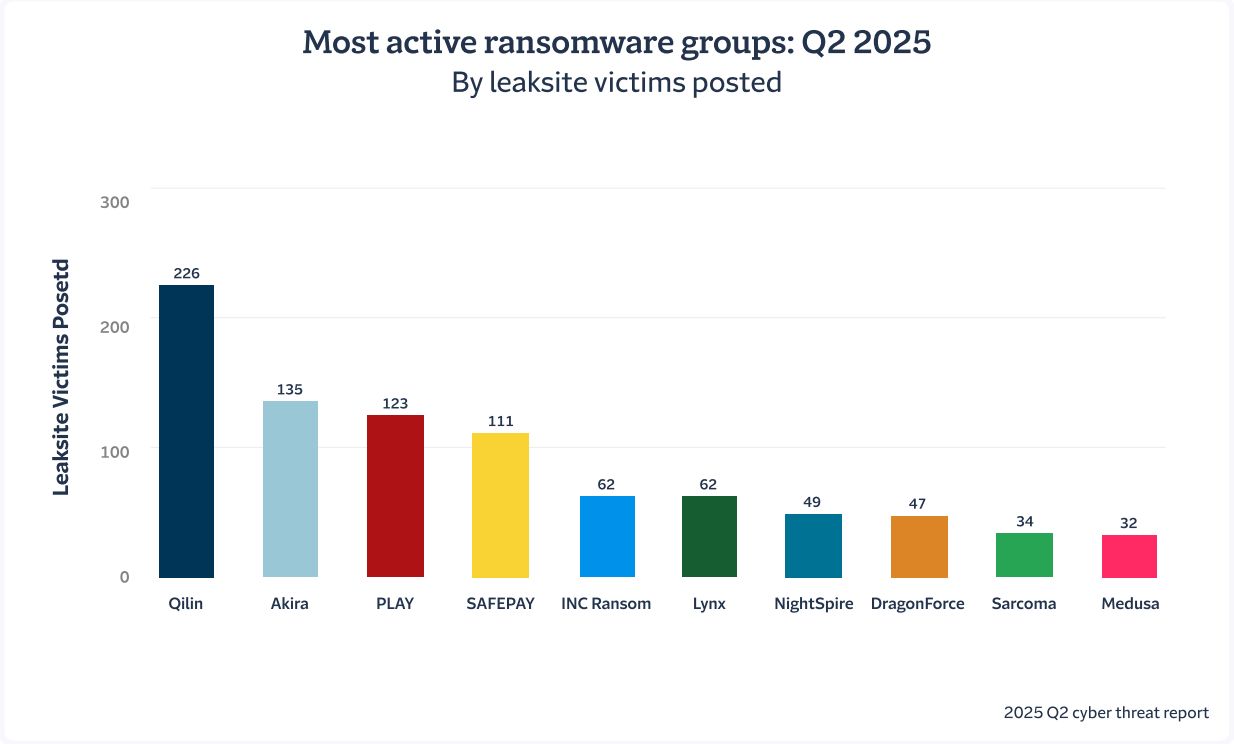
While any decrease in ransomware activity is notable, the activity in Q2 2025 is in line with the general upward trajectory in activity that began in Q1 2024 (at which time there were 1,066 incidents).



Contributing Factors to Activity in Q2 2025

Several factors appear to have contributed to the quarter-over-quarter reduction in ransomware activity. First, there has been significant upheaval within the ransomware criminal ecosystem over the past year. Early in the quarter, a well-known ransomware group called RansomHub suddenly went offline. RansomHub's affiliates were thrust into confusion when their negotiation platforms became inaccessible. Subsequent investigations by threat intelligence firms revealed that the group's administrators were dealing with disagreements with an unknown number of affiliates.

While affiliates working with RansomHub ultimately moved to other groups, this took some time. Meanwhile, several other groups took advantage of the void left by RansomHub, including Qilin, Akira and Dragonforce, the last group being a newcomer in Q2.

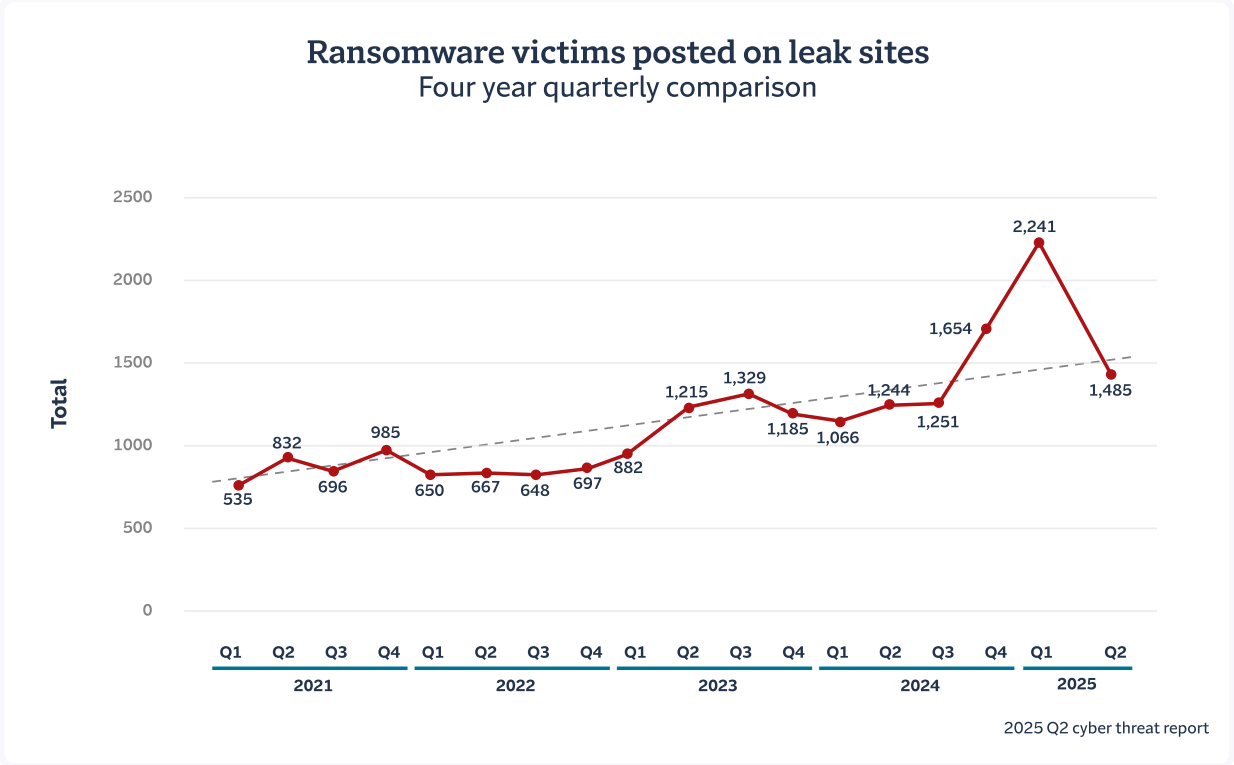


Another factor likely contributing to the decreased leak site activity was the takedown of LummaStealer, a popular type of malware used to gain initial access to networks. The takedown came on the heels of RansomHub's strife and resulted in the seizure of over 2,000 domains in May 2025. Given LummaStealer's widespread use by cybercriminals, this takedown likely interrupted a number of attempts at gaining initial access to victim systems.

While we can't precisely determine the impact of these disruptive events in Q2 2025, we can surmise that many threat actors were forced to quickly adapt their approach to gaining initial access to victims and carrying out extortion threats, and this likely degraded their ability to carry out attacks during the quarter.

Looking Forward: Long-term Trends Remain in Place

While the quarter-over-quarter decline in ransomware incidents in Q2 2025 is a positive signal, we caution against any organisation relaxing their approach to risk mitigation. It's worth noting that the heightened Q1 2025 numbers may prove to be an outlier, with the number of Q2 2025 incidents continuing to follow the upward trendline we've documented since Q1 2021 when we began gathering this data. Ransomware remains a viable threat vector.



While the quarter-over-quarter decline in ransomware incidents in Q2 2025 is a positive signal, we caution against any organisation relaxing their approach to risk mitigation.

When undertaking a longer review of the data, what is clear is a consistent rise in activity from leak site data over time. This suggests that while law enforcement actions and improvements to cybersecurity controls can have a real impact on limiting the growth rate of the ransomware ecosystem, and even reduce activity in the short term, when we project across years rather than quarters our assumption remains that activity will continue to grow.

Social Engineering and Business Email Compromise: Key Drivers Behind Cyber Crime

As we reviewed in the previous section, the level of ransomware activity has a propensity to ebb and flow from quarter to quarter. Meanwhile, the threats of Social Engineering and BEC represent a quieter, but also more consistent threat – and one that has equally real financial consequences. In this section we'll cover the basics of BEC, how it impacts organisations, and a couple of the ways that Travelers has observed BEC tactics evolving in recent months. We'll also share some of the guidance we provide policyholders around security and operational controls to help defend against BEC.

Business Email Compromise: A Primer

BEC describes situations in which attackers impersonate executives, vendors or individual employees after compromising a worker's business account (often, but not always, an email account). These attacks frequently begin with a social engineering exploit, as attackers use phishing or spear phishing to gain access to the business account by tricking a victim into downloading malware, or by stealing their credentials through an adversary-in-the-middle (AiTM) attack.

What makes a BEC situation distinct from a garden-variety phishing exploit is that the social engineering efforts don't end with malware being deployed: they continue, only made more realistic and devious by the attacker's ability to review internal company files and communications. In some cases, the attacker may send messages directly through the compromised account to instruct someone to send money to an account under their control; in others, they will use the intelligence gained by reviewing past communications to develop a realistic spoof of a partner or vendor account to achieve the same result.

Through this highly informed and highly targeted style of social engineering, attackers are able to trick employees into transferring company funds to the attackers. The UK economy has an estimated total annual cost of cybercrime of £27 billion, and while BEC costs are not publicly broken down, with BEC being a major component of this, it is realistically estimated to run into the billions of pounds.

Case Study: Business Email Compromise at Manufacturing Firm

The Chief Financial Officer (CFO) at a manufacturing firm fell victim to a spear phishing attack that compromised their corporate digital identity. With access to the executive's email and administrative privileges in the company's cloud environment, the threat actor expanded their reach by compromising additional employee accounts. Using fake forwarded email threads and spoofed contact details, the attacker posed as internal personnel to trick staff into sending fraudulent wire transfers totaling £150,000, authorised via emails sent from the CFO's compromised account.

Upon discovery, the company filed a claim. Travelers initiated a multi-pronged response, including engaging a legal team to lead a forensic and data mining investigation to determine if any notice obligation was triggered. This investigation confirmed that no regulated data had been exfiltrated, but did reveal weaknesses in two areas:

Technical Authentication: While this company required multifactor authentication (MFA) for all accounts, the way that the MFA was configured allowed for SMS (text message) authentication. A threat actor exploited this weakness to perform an AiTM attack and captured an employee's credentials.

Operational Procedure: The employees who were tricked into wiring money had, in fact, followed all of the company's stated procedures for verifying transfers by getting confirmation from the CFO. The issue was that the procedures did not include a requirement to perform an out-of-band authentication. If the individuals had located the CFO's phone number (from a source other than the compromised email account) and called to confirm the order, the fraud would been stopped in its tracks.

Thanks to coordinated efforts with law enforcement authorities, **nearly two-thirds of the stolen funds were recovered**. After the incident, Travelers Cyber Risk Services worked with the firm to strengthen its MFA implementations and reinforce policies around wire transfer authentication. This incident underscores the critical importance of layered security, employee awareness and procedural rigor in defending against sophisticated social engineering threats.

The Cost of Fraud

Historically, BEC has not set off industry-wide alarms, as often happens when a ransomware group targets a string of similar businesses. While we're starting to see more exceptions to this rule – as we'll discuss below regarding the Scattered Spider group – these are attacks that don't feature the spectacle of encrypted networks and ransom demands. As a result, they are less widely reported and less discussed in business media relative to ransomware.

Yet according to the FBI's Internet Crime Complaint Center (IC3), U.S. businesses reported more than £2 billion in losses from BEC scams in 2024. The FBI also found that over the past decade, global reported losses from BEC have exceeded £37 billion, making it one of the most financially damaging forms of cybercrime.

The two related claim categories, BEC and social engineering fraud (a frequent outcome of a successful BEC attack), combine to be consistently in the top three types of claims at Travelers and represent roughly half of all cyber claims in the past five years. Third party sources, like the Verizon Business 2025 Data Breach Investigations Report, also report consistent numbers of incidents from year to year – around 19,000 per year in recent years, with a median loss of £37,000.

At baseline, BEC is already a large component of the overall cyber threat landscape. But the style and tactics of social engineering and BEC are evolving and being used in new ways.

Tactics Converge: Social Engineering Meets Extortion

As we noted in our last two quarterly reports (Q1 2025 and Q4 2024), the "classic" ransomware strategy of exploiting software vulnerabilities has been on the decline. Our team has found that years of increasing ransomware activity has led to more widespread implementation of security controls and improved patch management practices by organisations of all shapes and sizes, making most software vulnerabilities less-effective targets.

With a few exceptions, such as the Cl0p group's rash of attacks in early 2025 that targeted a software vulnerability, most of the currently active ransomware groups have been looking to other opportunities to gain initial access, like brute-forcing passwords. Another emerging trend in this category is threat actors leveraging the kind of sophisticated social engineering tactics often seen in cases of BEC, like those described above, but combining them with extortion. This combined approach isn't entirely new, but it's now being deployed as a central pillar of some groups' strategies in a way that represents a break from the past.

Scattered Spider: A Case Study in Modern Social Engineering

A prominent example of a group combining social engineering, extortion and other tactics in a single attack is Scattered Spider, a loosely affiliated threat group believed to include members in both the U.S. and U.K. Known for its social engineering expertise, the group has been linked to several high-profile breaches, including incidents involving leading retailers and airlines in the U.K. and Australia. These attacks combined elements of BEC and social engineering, such as impersonating company employees to gain unauthorised access to internal systems, but the results of these efforts have gone far beyond the typical fraudulent transfers of funds.

These attacks combined elements of BEC and social engineering, but the results of these efforts have gone far beyond the typical fraudulent transfers of funds.

In one of the more costly events, attackers tied to Scattered Spider used social engineering tactics to deceive IT helpdesk employees who were contracted by an international consumer packaged goods company. Reports indicate that attackers gained access by calling service desks and convincing the employee to reset an account password on their behalf. Once the group gained access, they deployed malware in the manner of a ransomware attack, causing major disruptions in the production and distribution of the company's goods. The scale of the damage was outlined in a lawsuit filed by the company against the IT service provider, which sought £282 million in damages.

While this attack example dates to 2023, Scattered Spider continues to be active. In June 2025, the group reportedly targeted American businesses in a similar manner. Some alleged members of the group were arrested in the aftermath of the recent attacks.

Notwithstanding the arrests, the apparent effectiveness of Scattered Spider's attacks is one reason why we believe that operational controls such as out-of-band authentication could become a topic of renewed interest. No company wants to be defrauded, but reports of attacks that cause major disruption to core business operations have a way of attracting board-level attention, and spurring action. If threat actors continue to use social engineering and BEC tactics as a prelude to encryption, data theft and extortion, it's likely that businesses will focus on the controls that can prevent individuals from being tricked.

Accounts Compromised: Not Just Email

Business Email Compromise is so named because the compromise is typically an email account – but it is not always. In our last two quarterly reports (Q1 2025 and Q4 2024), we discussed examples in which threat actors had compromised business collaboration platforms to perform BEC-like social engineering exploits. In Q2 2025, we continued to see this trend progress with more examples, so it bears mentioning again in any discussion of BEC.

These tools make a tempting target for misuse because they have become a common and expected method of internal communications within customer environments. Most employees have been trained to look out for suspicious emails, but since collaboration tools are typically restricted to individuals directly employed by the organisation, many would rarely think twice about a message sent on the platform. This approach has led to both BEC claims as well as the initial vector for broader ransomware attack campaigns.
Once the account takeover takes place, threat actors easily pivot to shared online repositories scanning for sensitive (PII/PHI) and proprietary data (customer info, blueprints, engineering documents, etc.).

Defending against BEC: Controls, Remediation and the Role of Out-of-Band Authentication

Since BEC relies more on procedural gaps and human error than malware or software exploits, defence requires a combination of technical safeguards and strict operational discipline. One of the most effective controls is out-of-band authentication (OOBA) – verifying sensitive requests like payment changes or updates to contact information via an independent communication channel.

Organisations should never rely solely on email for confirming high-risk actions. Effective controls include:

- Verifying requests using a known phone number, not one provided in the message.
- Initiating a test transaction to confirm new banking details before updating records.
- Reenforcing that procedures must always be followed, no exceptions – even (and particularly) if the request is made with a high degree of urgency.

OOBA should be more than a guideline – it must be a formal requirement, embedded into financial operations and reinforced through regular training. Organisations should retrain staff handling payments at least yearly and should revisit possible procedure changes after experiencing leadership changes, system upgrades or periods of increased phishing activity.

On the technical front, layered defences remain essential. These include:

- **Multifactor Authentication (MFA)** for all access to email and financial systems, ideally using phishing-resistant methods (e.g., hardware tokens or app-based authenticators).
- **Email authentication protocols** (SPF, DKIM, DMARC) to reduce spoofing.
- **Behavioural anomaly detection** to flag suspicious login activity or deviations in financial behaviour.

Regular employee training in procedures like those outlined above remains the cornerstone of BEC defence. Recent studies have shown that, while phishing training does make an impact, especially when it's been conducted recently, there may be a ceiling to its effects. In other words, no amount of additional training is likely to reduce any organisation's risk of a social engineering exploit to zero. That means organisations need to look to the next layer down – how employees respond in the face of certain types of requests, even from fellow employees – to add layers of defence.

OOBA should be more than a guideline – it must be a formal requirement, embedded into financial operations and reinforced through regular training.

Conclusion

In the second quarter of 2025 ransomware activity fell from Q1's elevated level, though the level of activity continues to follow the general upward trendline that Travelers has observed over the past four years. Meanwhile, business email compromise and social engineering remain consistent, costly threats: in some cases, they are now being combined with extortion tactics. The persistence and evolution of these attacks only further reinforces the need for strong procedural controls and a layered approach to defence.

Recommendations from the Travelers Cyber Risk Services Team

To mitigate these risks, organisations should adopt a strong cyber prevention programme, including the following recommendations detailing the top security investments with the greatest return on investment.

These recommendations will help increase the bar required for ransomware actors to successfully carry out an attack on an organisation.

They include:

- Implement phishing-resistant MFA for all remote access and email.
- Run an effective vulnerability management programme to quickly patch critical vulnerabilities in edge devices, such as virtual private networks (VPNs).
- Ensure you have reliable backups and have a resilient disaster recovery and business continuity plan.
- Run endpoint detection and response (EDR) solutions with 24x7 active monitoring.

TRV5492MD 09/25