GuyCarpenter

CYBER'S SLEEPER THREAT:

Business Email Compromise

A business of Marsh McLennan

Key Takeaways

- Business email compromise (or BEC), a sophisticated form of phishing that involves attackers manipulating individuals into unwittingly facilitating fraudulent activities, is considered one of the most financially damaging cyber threats.
- BEC can impact companies regardless of industry or revenue, bringing with it potentially devastating financial impacts.
- Marsh claims data has shown smaller-revenue companies are far more likely to lose a greater percentage of their revenue in a BEC event than a large-revenue company could expect.
- Analysis of the Marsh Cyber Self-Assessment (CSA) data indicates using multifactor authentication (MFA) and cybersecurity awareness programs are the top 2 controls for the prevention of BEC events.
- The cyber (re)insurance industry has a collective interest in monitoring the escalating BEC threat and supporting organizations to improve their resilience against BEC attacks.

Compared to other cyber threats such as ransomware attacks, zero-day vulnerability exploits, and cloud service provider outages, business email compromise (or BEC) is akin to a "sleeper threat" in that it does not dominate news headlines. However, BEC is considered one of the most financially damaging cyber threats by the Federal Bureau of Investigation.[1]

BEC is a sophisticated form of phishing that involves attackers impersonating legitimate entities or individuals to deceive employees into transferring funds, divulging sensitive information or performing actions that compromise the security of the organization. This method exploits human vulnerabilities rather than technical weaknesses, making it exceedingly difficult for traditional security measures to detect and mitigate the risk effectively.

One of the most prevalent and damaging manifestations of BEC is wire fraud. In a BEC wire fraud scenario, cybercriminals leverage social engineering tactics to manipulate employees into initiating unauthorized wire transfers, often resulting in significant financial losses for the targeted organization.

As the frequency and sophistication of BEC attacks continue to rise, businesses must better understand the intricacies of this threat to implement robust defenses and safeguard their assets, reputation and operations. This report provides a comprehensive overview of the BEC threat and investigates whether it only affects specific silos of the economy or if it has a broader effect.

A well-informed approach is crucial for businesses to stay ahead of cyber adversaries and protect themselves against BEC-related wire frauds in an increasingly digital and interconnected environment. The escalating BEC activity also results in an increase of cyber insurance claims. BEC is an important component of the ever-evolving cyber threat environment that the (re)insurance industry should monitor closely. We have a collective interest in supporting organizations to develop a robust risk management framework, in order to stay vigilant and resilient to attacks such as this.

BEC Threat Landscape

Unravelling the Intricacies of Wire Fraud

Unlike traditional cyber threats that exploit technical vulnerabilities, BEC attacks exploit human trust and manipulate individuals into unwittingly facilitating fraudulent activities. BEC attacks typically involve sophisticated impersonation schemes, in which cybercriminals masquerade as trusted entities, such as company executives, vendors or business partners, to deceive employees into divulging sensitive information, authorizing fraudulent transactions or compromising corporate networks.

According to the FBI's Internet Crime Complaint Center (IC3)[2] , every year reported economic losses associated with BEC attacks exceed billions of dollars. Between October 2013 and December 2022, the following statistics were reported in victim complaints to the IC3:

- Total US victims: 137,601.
- Total US exposed dollar loss: USD 17.3 billion.

In 2023 alone, the IC3 received more than 21,000 complaints related to BEC[3], representing a significant increase from previous years. Moreover, the financial

[1] "Business Email Compromise", Federal Bureau of Investigation, https://www.fbi.gov/how-we-can-help-you/scams-and-safety/common-scams-and-crimes/business-email-compromise
[2] "Business Email Compromise: The $50 Billion Scam", Federal Bureau of Investigation, https://www.ic3.gov/Media/Y2023/PSA230609
[3] Federal Bureau of Investigation Internet Crime Complaint Center, "Internet Crime Report 2023"

impact of these attacks continues to escalate, with the average loss per BEC incident now surpassing 6 figures.

In the realm of BEC, wire fraud stands out as a sophisticated and prevalent tactic employed by cybercriminals to exploit human vulnerability and carry out financial deception. The consequences of falling victim to BEC wire fraud can be dire, with organizations facing staggering financial losses, damaged reputations and operational disruption. Understanding the nuances of this threat landscape is vital for businesses seeking to safeguard their financial assets and mitigate the risks associated with BEC wire fraud.

1. Impersonation Tactics and Psychological Manipulation

At the heart of BEC wire fraud is the intersection of impersonation tactics and psychological manipulation, orchestrated by cybercriminals to exploit human vulnerabilities and bypass organizational defenses. Leveraging social engineering techniques, attackers craft email communications that impersonate trusted individuals within the organization, such as senior executives, established vendors or business partners. These messages are carefully designed to evoke a sense of urgency, authority or familiarity, compelling targeted employees to comply with fraudulent requests without question.

By exploiting insider knowledge gleaned from reconnaissance efforts and monitoring email communications, cybercriminals tailor their messages to align with established communication patterns and organizational hierarchies, thereby lowering the recipient's guard and increasing the likelihood of successful exploitation. Emotional appeals, such as messages emphasizing loyalty or fear of reprisal, are often deployed to override rational judgment and induce compliance with fraudulent instructions.

2. Fraudulent Wire Transfer Requests

Once trust has been established and employees are primed for compliance, cybercriminals proceed to orchestrate fraudulent wire transfer requests designed to divert funds into accounts controlled by the attackers. These requests often involve convincing pretexts, such as urgent payment for purported business expenses, invoice payments to fictitious suppliers, or instructions to update banking information due to purported security concerns. By exploiting common business processes and workflows, attackers can seamlessly blend their fraudulent requests into legitimate communications, making detection and interception challenging for unsuspecting employees and financial institutions alike.

THE CONSEQUENCES OF A SUCCESSFUL BEC ATTACK CAN BE DEVASTATING, RANGING FROM FINANCIAL LOSSES AND REGULATORY PENALTIES TO IRREPARABLE DAMAGE TO AN ORGANIZATION'S REPUTATION AND CUSTOMER TRUST.

3. Evolving Tactics and Techniques

The landscape of BEC wire fraud is dynamic and constantly evolving, with cybercriminals continually refining their tactics and techniques to evade detection and exploit new vulnerabilities. Attackers employ a diverse array of tools and methods to achieve their objectives:

- Email spoofing: a deceptive tactic used by cybercriminals to forge the sender's email address, making it appear as if the message originated from a trusted source within the recipient's organization. This technique is typically facilitated by readily available spoofing tools and techniques that allow attackers to manipulate email headers and disguise their true identities. By spoofing the sender's address, attackers can bypass email authentication mechanisms and evade detection by traditional email security filters, increasing the likelihood of their fraudulent messages reaching their intended recipients.

- Domain impersonation: involves the creation of fraudulent email domains or the compromise of legitimate domains to lend credibility to BEC wire fraud schemes. Attackers often register domain names that closely resemble those of legitimate organizations or leverage subdomains of compromised domains to create convincing email addresses that mimic trusted entities within the organization. By exploiting the trust associated with familiar domain names, attackers can deceive employees into believing that their fraudulent communications are legitimate, thereby increasing the likelihood of successful exploitation.

- Malware-enabled attacks: a sophisticated variant of BEC wire fraud in which attackers leverage malicious software to compromise email accounts, exfiltrate sensitive information or facilitate fraudulent transactions. These attacks may involve the distribution of malware-laden email attachments or the exploitation of software vulnerabilities to gain unauthorized access to corporate networks. Once installed, malware can enable attackers to monitor email communications, harvest login credentials and manipulate financial transactions, providing them with unprecedented access and control over the targeted organization's digital assets.

The pervasiveness of BEC attacks presents a formidable challenge for organizations across industries, as they navigate the delicate balance between fostering open communication and safeguarding against malicious actors. The consequences of a successful BEC attack can be devastating, ranging from financial losses and regulatory penalties to irreparable damage to an organization's reputation and customer trust.

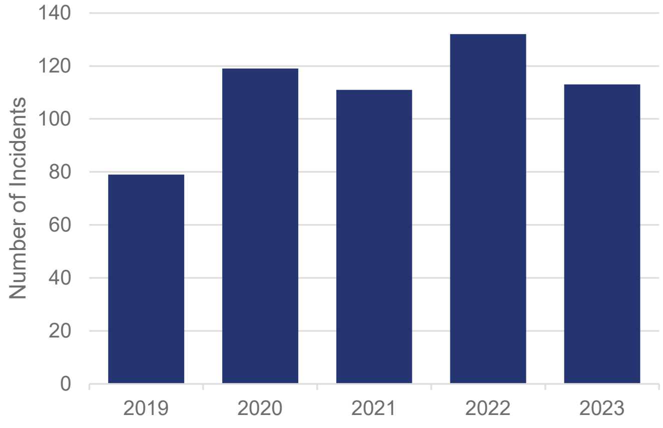
Cyber Model Vendors' View of BEC Risk

Even though BEC has proven to be a considerable financial threat to the economy, commercially available cyber vendor models have mixed reception as to whether it should be accounted for in their catastrophe event catalogue because its impact is perceived to be more attritional and frequency-driven. Cyber catastrophe models, which have historically focused on low-frequency/high-severity events driven by ransomware or cloud outage, are increasingly recognizing the significance of BEC as a critical component of cyber risk assessment. However, at the time of this report, only one of the industry-leading vendors has incorporated BEC as an explicit cyber peril into its models, with loss contribution limited to the attritional component of the model. While BEC's reported loss amounts are staggering, the proliferation of these consistently-used attack techniques creates a grey space between attritional and catastrophe risk.

Financial Impact of BEC

Frequency of BEC Events

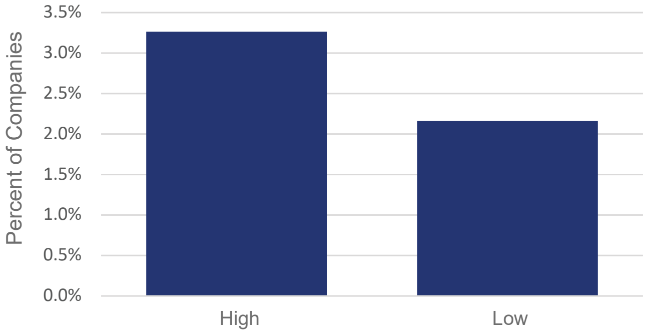
Figure 1: BEC Incidents Each Year



Source: Marsh McLennan Cyber Risk Intelligence Center

BEC is not a new threat vector. That said, like many cyberattack vectors, it is one gaining in popularity due to its relatively low technical lift, making it highly effective and lucrative from the threat actors' perspective. Our team leveraged the Marsh claims database to understand more about the trends in BEC events over time. This database is aggregated and includes more than 800,000 claims and notices of loss across multiple lines of insurance, reported by Marsh clients, beginning in 2004 and continuing through the present day. Of these claims and notices, over 9,000 impact cyber policies, and more than 6,000 impact crime policies. Figure 1 shows the number of BEC events affecting either cyber or crime policies, beginning in 2019. It is worth noting that these are successful BEC attacks, in which the affected organization sent money to a fraudulent account, regardless of whether they were able to recover some or all of the funds transferred.

Figure 2: Percent of Companies in Revenue Group with BEC Event



Source: Marsh McLennan Cyber Risk Intelligence Center

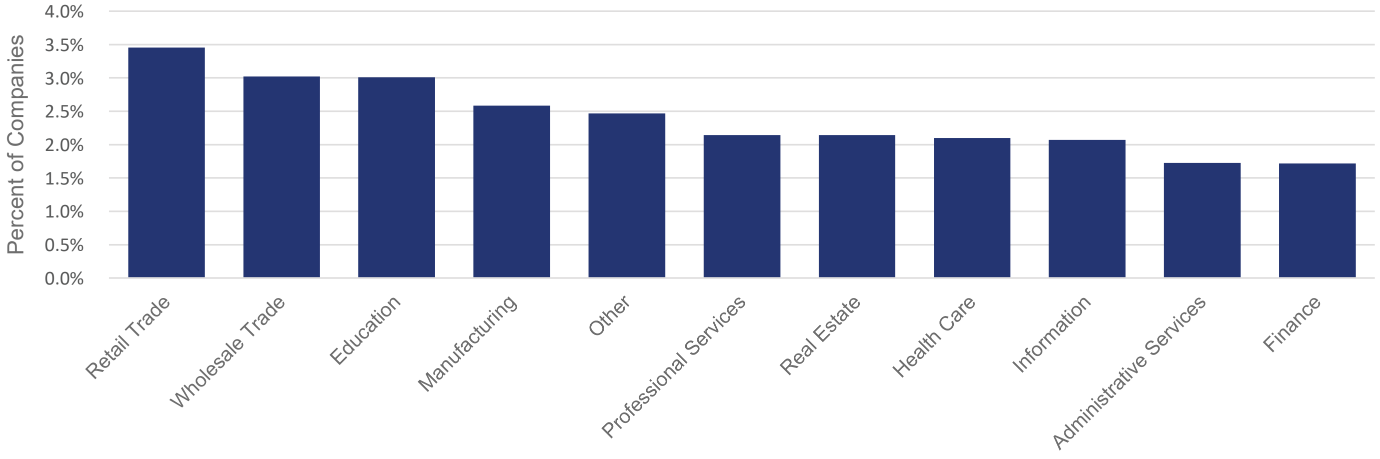
Figure 1 shows that 2019 had the fewest, with a peak of incidents in 2022, and an overall pattern of an increasing number of BEC events. It is also important to note that the 2023 BEC incident count is not yet fully developed, therefore the 2023 number could end at a higher level than displayed above. The data clearly shows that successful BEC attacks are trending upward. The next question is which companies might be at greater risk.

Which Businesses Are Most at Risk?

BEC is a threat vector that can potentially affect any company, regardless of industry or revenue. That said, there are some trends to be gleaned in the firmographics of companies most often affected by BEC events.

Examining the successful BEC events from 2019 onward, we can first break down the prevalence of events by revenue. In Figure 2, companies are divided into high- and low-revenue companies, where high-revenue companies

Figure 3: Percent of Companies in Industry Group with BEC Event



Source: Marsh McLennan Cyber Risk Intelligence Center

are those with an annual revenue of at least USD 1 billion. The figure shows the percentage of companies in each revenue bin each year that were affected by at least one BEC event, averaged across the 5 years of historical data. The companies affected are those from the Marsh claims database, triggering either cyber or crime policies. The total number of companies cited represents those that obtained a cyber or crime policy via Marsh at any time between 2019 and 2023.

Figure 2 shows that a greater percentage of high-revenue companies were affected by a BEC event within the time frame than were low-revenue companies. This is consistent with patterns observed from other cyber events, such as ransomware. One reason for this difference in prevalence could be that higher-revenue companies are more often targeted by threat actors than lower-revenue companies, regardless of attack scenario.

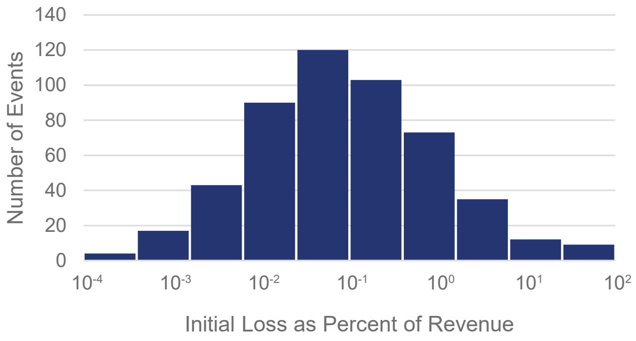
Next, we can break down the prevalence of BEC events by industry. Figure 3 shows the percentage of companies per year in each industry sector affected by a BEC event, averaged across the 5 years of historical event data. This figure was produced utilizing a consistent dataset to the revenue analysis.

Figure 3 shows that the prevalence ranges from a low of 1.7% of companies in the finance sector to a high of almost 3.5% of companies in the retail trade sector. This variation in prevalence could be caused by some sectors being more targeted than others, or due to some industries implementing more robust cyber security controls or cyber training programs than others.

Severity of Business Email Compromise Events

The initial loss from a BEC event can be quite severe. To better comprehend the magnitude of financial impact a company could face as a result of BEC, we first normalize the initial loss by the revenue of the company, and then bin the number of events from our data event set by the normalized initial loss. The results are shown in Figure 4.

Figure 4: Distribution of Initial Loss Severity



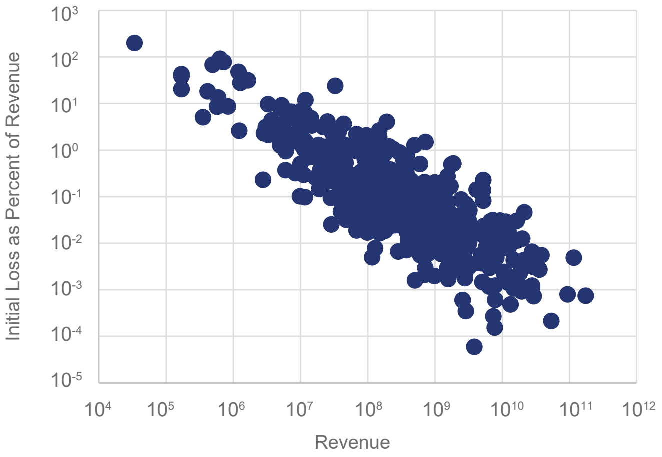
** This figure utilizes scientific notation, a compact way to write very large or small numbers. For example, the number 0.0001 in scientific notation is 10^{-4}. The value 100,000 in scientific notation is 10^{5}.*

Source: Marsh McLennan Cyber Risk Intelligence Center

The initial losses range from only 0.0010% of the company revenue up to 100%. The greatest number of events have a loss around 0.1% of the company revenue. While 0.1% may not seem like much, for a company with a revenue of billions of dollars, that could wind up being quite a large amount.

While the data shows some BEC events where the initial loss is equivalent to a company's revenue, it's worth trying to discern if there is any correlation between that initial loss percentage and the revenue of the affected organization. After all, 100% of USD 500,000 in revenue is a much smaller number than 100% of USD 500 million in revenue. The figure below shows the initial loss percentage plotted against the revenue of the organization.

Figure 5: Initial Loss versus Revenue



** This figure utilizes scientific notation, a compact way to write very large or small numbers. For example, the number 0.0001 in scientific notation is 10^{-4}. The value 100,000 in scientific notation is 10^5..*

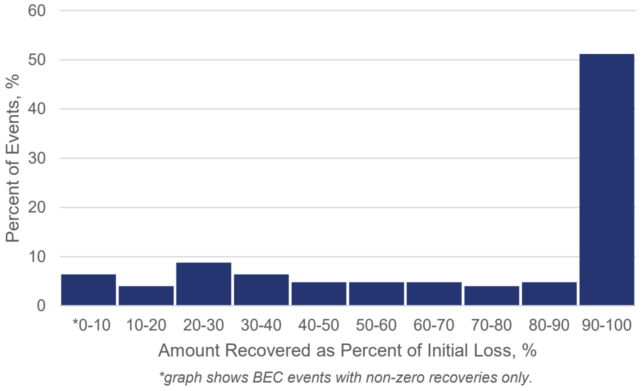
Source: Marsh McLennan Cyber Risk Intelligence Center

Figure 5 demonstrates a strong correlation between the initial loss percentage and the revenue of the company. Smaller-revenue companies are far more likely to lose a greater percentage of their revenue in a BEC event than a large-revenue company. This a very important point to keep in mind—while smaller-revenue companies have fewer BEC events, when they do suffer one, the financial impact could be severe.

When a BEC attack occurs, it's crucial to act quickly. By reaching out to banks and law enforcement, it is possible to recover some or all of the lost funds. Figure 6 shows the percentage recovered for those BEC events where at least some funds were recouped.

Recovery amount is 90-100% of the initial loss in half the cases when funds are recovered. However, less than 25% of the events had *any* funds recovered. This underscores the importance of preventing BEC attacks in the first place.

Figure 6: Distribution of Amount Recovered



Source: Marsh McLennan Cyber Risk Intelligence Center

Preventing Business Email Compromise Events

The historical claims evidence shows BEC events can affect companies of any size or industry, and can potentially have devastating financial impacts. However, companies have multiple options to decrease the likelihood of experiencing a BEC event.

Preventing Business Email Compromise Incidents

A successful BEC event depends on the threat actor convincing an employee to transfer money to a fraudulent account, against the employee's better judgement. This attack vector requires the bad actor to send an email either from a look-alike email address or from a compromised email account of a vendor or higher-up employee and then convince the receiver to transfer the funds. Therefore, there are 3 main tactics to averting a successful BEC attack:

1. Preventing threat actors from getting access to organization email accounts.
2. Preventing fraudulent emails from reaching employees.
3. Helping employees identify fraudulent emails so that they don't engage the threat actor.

To understand more about the different tactics for preventing BEC events, and the specific controls that can be brought to bear, we can utilize the Marsh Cyber Self-Assessment, in conjunction with the Marsh claims data. The Marsh Cyber Self-Assessment (CSA) is a questionnaire filled out by Marsh clients, which assesses the cyber posture of the client. The questions cover a broad range of cyber-security related topics, including multifactor authentication (MFA), cyber security training, data protection, and more.

To assess which of the cyber controls in the Marsh CSA have the greatest impact on preventing a BEC event, we

Table 1: Top 4 controls from the CSA by signal strength

Tactic	Control	Signal Strength
Prevent threat actors from gaining access to organization email accounts.	Our organization uses an authenticator application as a secondary method for MFA.	2.85
Helping employees identify fraudulent emails.	Our cybersecurity awareness program materials train users to avoid common cyber-risks and threats, such as social engineering and phishing.	2.45
Prevent malicious emails from reaching employees.	The endpoint security tool(s) are configured to block (as opposed to solely notify of) suspected malicious processes and files.	2.36
Prevent threat actors from gaining access to organization email accounts.	Our organization's technical controls detect known compromised/breached passwords on the darkweb or other sources and enforces a password reset.	2.29

Source: Marsh McLennan Cyber Risk Intelligence Center

calculate a “signal strength” for each CSA question. This signal strength is simply:

$$\textit{Signal Strength} = \frac{\textit{Conditional Probability of Event Given Control is NOT Implemented}}{\textit{Conditional Probability of Event Given Control is Implemented}}$$

where

Conditional Probability of Event Given Control is NOT Implemented

$$= \frac{\textit{Number of companies that did not implement control and had an event}}{\textit{Number of companies that did not implement control}}$$

and

Conditional Probability of Event Given Control is Implemented

$$= \frac{\textit{Number of companies that implemented control and had an event}}{\textit{Number of companies that implemented control}}$$

Any CSA with a signal strength greater than 1 has a positive correlation between companies having implemented the control in question and a lower frequency of BEC events. For this analysis, we used the 2023 Cyber Self-Assessment results and the 2023 BEC Marsh claims data. Table 1 shows the top 4 controls from the CSA by signal strength.

To which of the above-mentioned tactics do these controls map?

The first tactic focuses on preventing threat actors from gaining access to employee email accounts, and two of the controls in our list highlight ways to do that. The first control in our list, utilizing MFA, can stop threat actors from accessing and utilizing email accounts, even if they have the account password. The last control in our list, proactively detecting compromised passwords and accounts and enforcing a password reset, is another effective way of preventing threat actors from accessing employee accounts, and thereby helping to prevent BEC events.

The second tactic focuses on preventing malicious emails from reaching employees. The third control in our list, configuring your endpoint security tool to block suspected malicious files, as opposed to simply flagging potentially malicious files, is an effective way to implement this second tactic. Oftentimes, organizations will not actually block suspected malicious files, due to the concern around false positives, where legitimate files and emails are also blocked. However, given how strongly blocking these suspected malicious files correlates with preventing BEC events, it is worth considering implementing this control.

The third tactic focuses on teaching employees to spot social engineering and phishing threats via a cybersecurity training program. The second control in our list, training employees to spot BEC events, is the second-most-important control in our analysis, underscoring the importance of having a robust cybersecurity training program.

Overall, there are many tools available to companies to prevent BEC events. While we know that companies can recover a substantial proportion of their lost funds should they move quickly to report the event to the proper authorities, preventing BEC events in the first place is a much more effective strategy to minimize losses.

For the original Marsh report exploring how cyber control signal strength impacts the probability of experiencing a cyber event, please see *Using Data to Prioritize Cybersecurity Investments*

Conclusions

Business Email Compromise (BEC) may not always capture sensational headlines like ransomware attacks or cloud outages, but it undeniably poses a significant cyber threat to companies worldwide. Its insidious nature lies in its ability to exploit human vulnerabilities, leveraging social engineering tactics to deceive employees and manipulate financial transactions. Unlike some cyber threats that target specific vulnerabilities or systems, BEC's impact is wide-ranging, affecting companies of all sizes and across all major industry sectors.

While conventional wisdom may categorize BEC as a more attritional and frequency-driven threat, an analysis of the Marsh claims database reveals the severe financial implications that BEC events can entail. BEC events have resulted in significant losses for organizations, highlighting the need for heightened vigilance and proactive cybersecurity measures. With proper cybersecurity tools, controls and employee training in place, BEC is a preventable risk.

By implementing controls that help prevent threat actors from gaining access to organization email accounts, prevent fraudulent emails from reaching employees, and help employees recognize fraudulent emails when they do receive them, organizations can significantly reduce their susceptibility to BEC and safeguard their financial assets from malicious exploitation. BEC may lurk in the shadows of more prominent cyber threats, but its potential impact underscores the imperative for organizations to remain attentive and proactive in defending against this ever-present menace. This is to the mutual benefit of both the policyholder community and the (re)insurance industry, as we collectively strive to improve the resilience of organizations against BEC threat and mitigate its impact on cyber (re)insurance's underwriting profitability.

Authors: Jess Fung, Shu Iida, Carol Aplin

About Guy Carpenter

Guy Carpenter & Company, LLC is a leading global risk and reinsurance specialist with 3,500 professionals in over 60 offices around the world. Guy Carpenter delivers a powerful combination of broking expertise, trusted strategic advisory services and industry-leading analytics to help clients adapt to emerging opportunities and achieve profitable growth. Guy Carpenter is a business of Marsh McLennan (NYSE: MMC), the world's leading professional services firm in the areas of risk, strategy and people. The company's more than 85,000 colleagues advise clients in over 130 countries. With annual revenue of $23 billion, Marsh McLennan helps clients navigate an increasingly dynamic and complex environment through four market-leading businesses including Marsh, Mercer and Oliver Wyman. For more information, visit www.guycarp.com and follow us on LinkedIn and X.

About the Marsh McLennan Cyber Risk Intelligence Center

The Marsh McLennan Cyber Risk Intelligence Center (Center) is Marsh McLennan's enterprise-wide cyber data, analytics, and modelling center of excellence. The Center was founded in 2021 with a mission to advance how businesses and their communities quantitatively and economically anticipate, measure, and manage cyber risk. By leveraging advanced analytical and modeling techniques, the Center brings together Marsh McLennan's expansive proprietary data and models across its Marsh, Guy Carpenter, and Oliver Wyman businesses with complementary leading external sources, to develop a robust suite of cyber quantification tools. The Center's tools power cyber modeling exercises, cyber analytics, and thought leadership insights for Marsh McLennan clients around the world, including cybersecurity technology organizations, insurance and reinsurance providers, and others.

Guy Carpenter & Company, LLC provides this report for general information only. The information contained herein is based on sources we believe reliable, but we do not guarantee its accuracy, and it should be understood to be general insurance/reinsurance information only. Guy Carpenter & Company, LLC makes no representations or warranties, express or implied. The information is not intended to be taken as advice with respect to any individual situation and cannot be relied upon as such. Statements concerning tax, accounting, legal or regulatory matters should be understood to be general observations based solely on our experience as reinsurance brokers and risk consultants, and may not be relied upon as tax, accounting, legal or regulatory advice, which we are not authorized to provide. All such matters should be reviewed with your own qualified advisors in these areas.

Readers are cautioned not to place undue reliance on any historical, current or forward-looking statements. Guy Carpenter & Company, LLC undertakes no obligation to update or revise publicly any historical, current or forward-looking statements, whether as a result of new information, research, future events or otherwise. The trademarks and service marks contained herein are the property of their respective owners.