KnowBe4

Cyber Insurance and Security: Meeting the Rising Threat

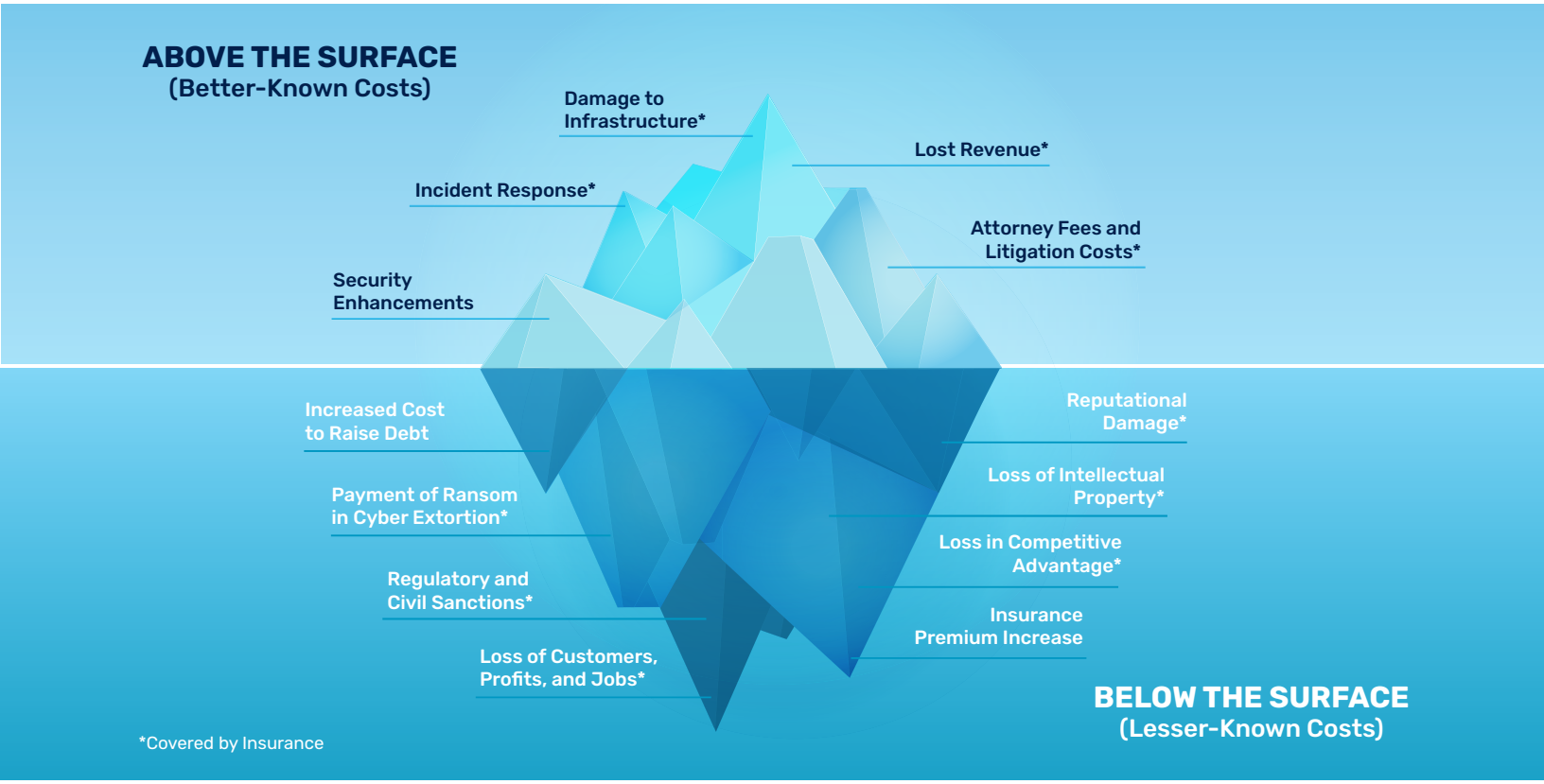
Table of Contents

In an ecosystem that is increasingly reliant on digital systems, a failure to recognize the inherent risks of disruption or infiltration of the IT infrastructure puts any enterprise, large or small, at risk of severe damage and in some cases even collapse. Ignoring the need to manage cyber risk with strengthened security practices, and neglecting the need for insurance to transfer the risk should those safeguards fail, are no longer options.

THE COSTS OF A CYBERATTACK

The ramifications and costs of a cyberattack can be staggering, going well beyond the easily visible disruption of service or exposure of data. Even after operations are restored, costs frequently continue to balloon as the attack is followed by potential civil litigation, regulatory fines, and the costs of repairing reputational or competitive losses.

Ramifications of a Cyberattack[1]



The 2024 IBM Cost of a Data Breach[2] report puts the average cost of a data breach at $4.88M, up from $4.45M in 2023, and up from $3.86M in 2018. Four countries exceeded the average: The United States ($9.36M), the Middle East ($8.75M), Benelux ($5.90M), and Germany, ($5.31M).

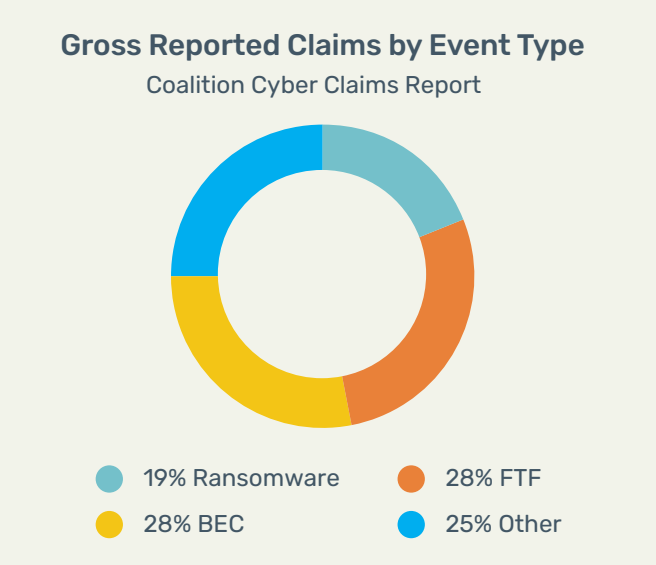
The number of organizations paying regulatory fines of more than $50,000 increased in the 2024 report by 22.7%, and those paying more than $100,000 increased by 19.5%.

1 "Cyber Insurance: What You Need to Consider Before Purchasing a Policy," Chase, J.P. Morgan. Link
2 IBM Cost of a Data Breach Report 2024, Link

THE VIEW FROM THE INSURANCE INDUSTRY

The 2024 Coalition Cyber Claims Report[3] notes that in 2023 in the U.S., the FBI received more than 880,000 complaints of cybercrime with reported losses of $12.5 billion, a 13% increase over the previous year.[4]

Coalition insurance claims for Funds Transfer Fraud (FTF) increased in severity in 2023 by 24%, to an average loss of more than $278,000, as threat actors using AI tools have been able to launch more sophisticated attacks. Phishing emails, it notes, are also becoming more credible and harder to detect, and threat actors are believed to be using AI to parse information faster, communicate more efficiently, and more effectively generate campaigns targeted toward specific companies.



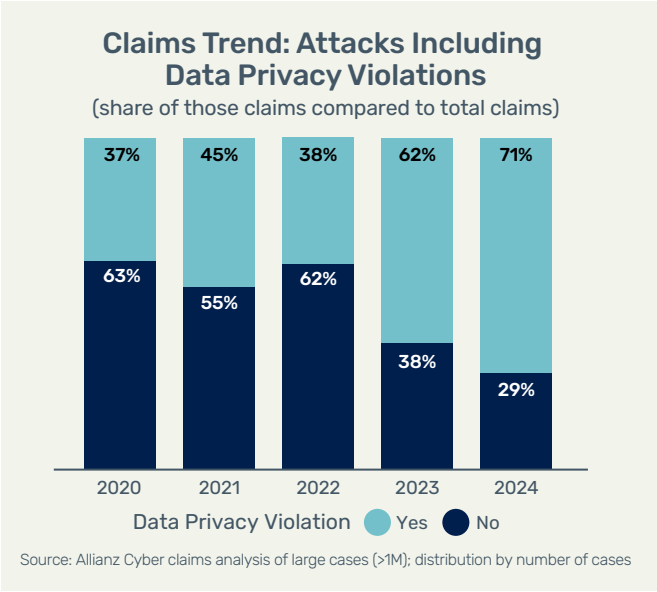
Globally, for their 2024 report,[5] Allianz Commercial surveyed 3069 companies on the most important risks facing their industries. The highest category of risk reported by responding companies was easily cyber incidents, including cybercrime, IT network and service disruptions, malware/ransomware, data breaches, fines, and penalties; at 36% cyber risk was well above supply chain disruptions, regulatory or economic changes, natural catastrophes, and political instability. 59% cited data breaches as the risk exposure that most concerned them.

Allianz's analysis of their claims for the period showed that their concerns are not unfounded. In the 2024 report, severity of claims received for cybercrime had increased by 17%; by comparison, in 2023 severity had increased just 1%. Large cyber claims — those in excess of 1 million euros ($1.1 million) — were more frequent, increasing by 14% in the first six months of 2024. The U.S. accounted for 72% of large claims.

Key contributors were the rise in ransomware attacks (ransomware accounted for 58% of the value of large cyber claims in the first six months of 2024). The exfiltration of sensitive personal information increases the scope of the attack and often adds the expense of regulatory fines to the cost. It increases ransom demands and allows hackers to make additional income from the sale of the data, making exfiltration of private data an increasing target for attackers.

The increases in data exfiltration have also created a surge in class action litigation for alleged privacy violations. This was particularly strong in the U.S., where the number of states with comprehensive data privacy laws rose from five to 13 since the beginning of 2023. The Asia-Pacific region has also seen significant developments in data privacy laws, opening the door to litigation, particularly in Japan, South Korea, India and China.

3 Coalition 2024 Cyber Claims Report
4 Federal Bureau of Investigation, 2023 Internet Crime Report
5 Cyber security resilience 2024 webinar, Alliance Commercial. Link



The Allianz report notes that data breach class actions have surged in the U.S., emerging as one of the fastest growing areas of U.S. class action litigation, and creating additional costs and reputational risks for both U.S. and multinational companies. Over 1,300 data privacy related class action lawsuits were filed in the U.S. in 2023. This was more than double the number filed in 2022, and four times the number filed in 2021. The report notes that "a complex regulatory and legal landscape around data privacy has created a grey area ripe for class action lawsuits." The potential for a similar rise in Europe as awareness of data protection rights is increasing and third-party litigation funding contributes to a more consumer-friendly litigation environment.

Incident Costs

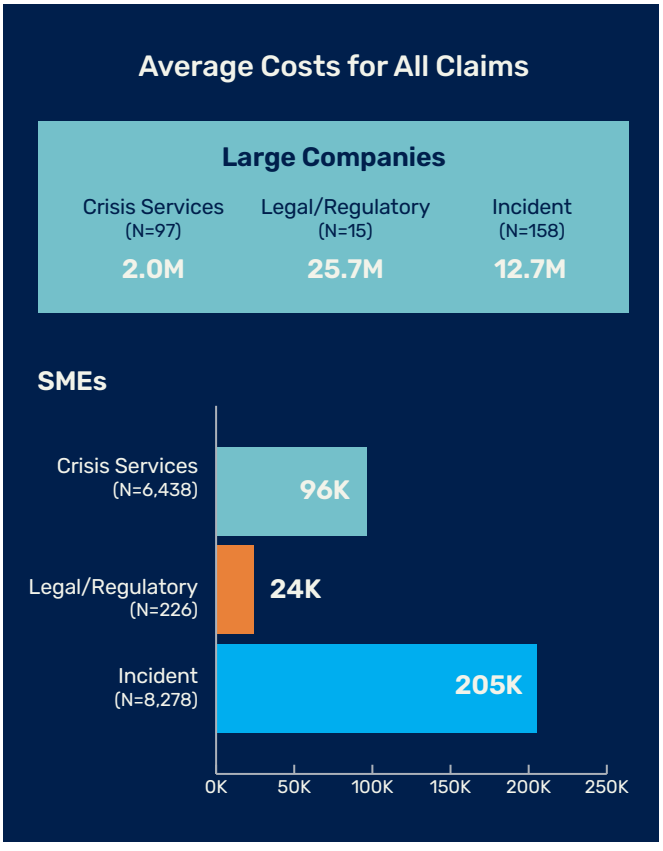
The 2024 NetDiligence Cyber Claims Study[6] analyzes over 10,000 cyber claims for incidents that occurred during the five-year period 2019–2023. 98% of the claims ($1.9B in total) were from small to medium enterprises (SMEs) with less than $2 billion in annual revenue. 2% of claims ($2.0B in total) were from large companies with more than $2 billion in annual revenue. Claims ranged from less than $1,000 to over $500M. The number of records exposed in data breaches ranged from 1 to over 140M.

The NetDiligence report tracks the costs of responding to a cyber incident in three primary categories:

- Crisis Services, which include legal counsel, forensics, notification, credit/ID monitoring, and public relations.
- Legal/Regulatory, which includes lawsuit defense, lawsuit settlement, regulatory action defense, and regulatory fine.
- Incident Cost, which in this report means the aggregate total of all types of costs/ expenses associated with the incident.

On average, the incidents experienced by large companies were more than 62 times more costly than those at SMEs ($12.7M average cost vs. $205K).

Despite the smaller average, SMEs experienced large losses as well, with perhaps greater organizational impact. There were 327 SME claims with total incident costs greater than $1M, including two SME claims that were greater than $100M.



6 NetDiligence Cyber Claims Study Report 2024. Link

Crisis Services

Across all organization sizes, crisis services costs ranged from less than $100 to almost $26M. At SMEs, crisis services account for 62% of the total incident cost, with an average of $146K per incident. Large companies also paid an average of 62% of the total incident costs for crisis services, with an average crisis services cost of $1.9M per incident. The bulk of these costs, more than 60%, were for forensics and notification.

Causes of Loss

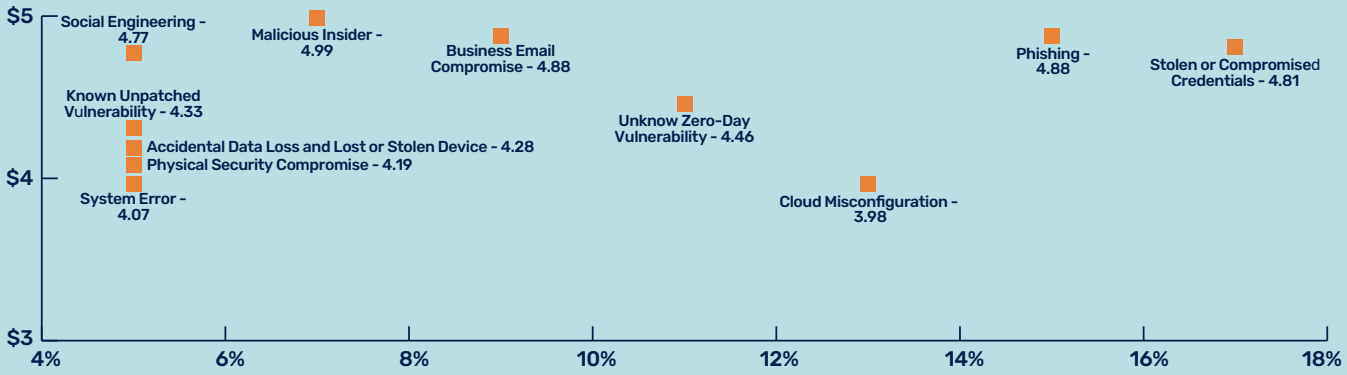
In the five-year period of the NetDiligence report, 97% of cyber insurance claims by SMEs were the result of criminal activities: hacking, ransomware, social engineering, business email compromise (BEC), phishing, theft of money or devices, banking/ACH fraud, and distributed denial of service (DDoS) attacks. In large companies in the same period, criminal activities accounted for 86% of cyber claims.

Ransomware and business email compromise were the two leading causes of loss, accounting for 53% of claims larger than $1,000 in the five-year period 2019–2023. The report says that ransoms "continue to be off the charts, with initial demands as high as $80M and ransoms paid as high as $50M." There were 15 ransoms paid that were larger than $10M.

For four consecutive years, ransomware has remained SMEs' top financial threat, and continues to increase year over year. In 2024, the average ransomware cost was $432K, up from $334K in last year's report.

The IBM Cost of a Data Breach report also puts phishing, stolen credentials and business email compromise (BEC) among the top initial vectors and the most costly attacks:

Cost and Frequency of a Data Breach by Initial Attack Vector[7]



7 "Cost of a Data Breach 2024," IBM. Link

According to IBM's figures, social engineering and phishing together comprise the largest attack vector method used (44%), by far, to accomplish data breaches. Adding in other human risk factors not involving social engineering, such as malicious insiders (7%), physical security compromise (6%), accidental data loss and lost or stolen devices (6%), and cloud misconfiguration (12%), human risk comprises 75% of all causes of data breaches.

THE MOST EFFECTIVE INSURERS ARE THERE BEFORE THE ATTACK

Insurers of cyber risk have shared interests with their customers: both benefit by reducing risk and mitigating damage from cyberattacks. When there are joint efforts and attention to closing the door to attacks before they occur, their client companies enjoy stability and improved financial health, possibly reduced premiums and access to better coverage, and certainly reduced risk of insurance premium increases resulting from claims. The minimum framework for effective partnership in prevention should include:

Concentrating on the Right Threats[8]

70-90%

of successful hacking involves **Social Engineering**

33%

involves **Unpatched Software/Firmware**

30%

involves **Weak/Compromised Logins**

79% | of compromised logins are stolen using **Social Engineering**

Mitigating Social Engineering Risks

At a minimum, insurers should look for:

- The use of phishing-resistant Multifactor Authentication (MFA) when possible. If it can be spoofed by a Man-in-the-Middle (MitM) the MFA is weak. If the MFA sends a code to be typed in, or a prompt to approve, it is similarly weak. One Factor Authentication (1FA) should not be allowed.
- Use phishing-resistant MFA whenever possible for logins.
- When phishing-resistant MFA is not possible, use any MFA method.

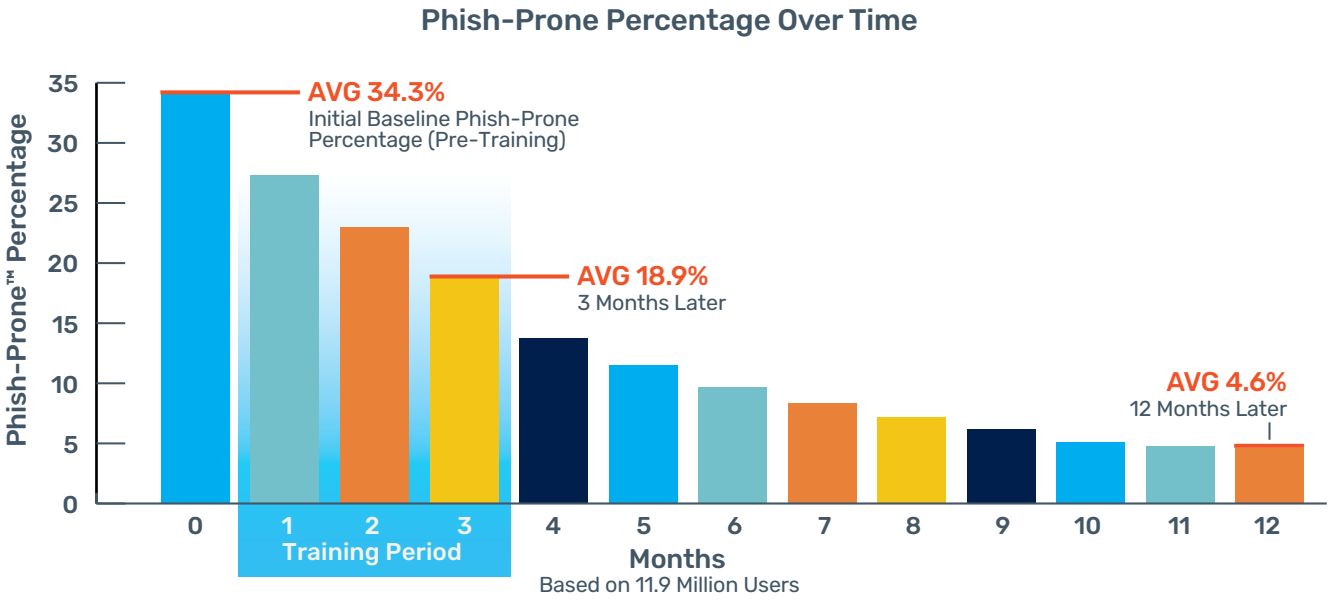
8 Roger Grimes KnowBe4 Presentation

- When MFA is not possible, insist on different, non-guessable/non-crackable passwords for every website and service (12-character random passwords defeat all known guessing/cracking attacks).
- Consider using a password manager for all passwords. Password managers create and allow for people to easily use strong, unique passwords for every site and service.
- If using a password manager, if possible, the password manager should be protected by MFA and/or long passwords.
- All passwords should be changed at least annually.
- Accurate vulnerability assessments.
- Incorproate a human risk management program that includes effective, frequent security awareness training and simulated phishing campaigns.

While insurers have at times treated security awareness training as a yes/no box to be checked in initial assessments, upon closer review, a lack of awareness and training can be one of the most dangerous and least visible security liabilities for any company or organization. It is also an area where diligence can produce the highest rewards.

A Phishing Security Test (PST) is a tool provided by KnowBe4 that can help both insurers and the insured determine how many users in an organization may be susceptible to a phishing attack. The PST works by sending an email to users that includes text to trick users into clicking an embedded link. We offer several different types of PSTs based on your organization's needs, producing an initial assessment of the organization's "Phish-prone™ Percentage." It is not unusual to find an initial 30-35% Phish-prone Percentage in initial testing – in other words, roughly one out of three employees are likely to being tricked into clicking on a hacker or scammer's link in an email.

These percentages drop dramatically after one year or more of ongoing cybersecurity awareness training and testing. Results from the 2024 KnowBe4 Phishing by Industry Benchmarking Report showed that across all industries and sizes, baseline testing to one year or more of ongoing training and testing decreased the average number of "Phish-prone" employees from 34.3% to 4.6%:



Partnering Together

Cybersecurity vendors and insurers can partner together to create a stronger, more comprehensive cybersecurity insurance landscape. Insurers can look for strong security practices within an organization as evidenced by an analysis such as a Risk Score. They can then provide financial incentives to organizations that demonstrate these practices (such as premium credits).

Conclusions and Key Takeaways

The rapidly evolving cyber threat landscape poses an unprecedented challenge to all types of organizations around the world. As the digital ecosystem becomes increasingly complex, the potential for devastating cyberattacks grows exponentially. The staggering costs associated with data breaches, ransomware attacks, and other cyber incidents underscore the critical importance of a comprehensive approach to cybersecurity and more specifically human risk management.

Key Takeaways From This Paper Include:

- The financial impact of cyberattacks is escalating, with average costs reaching $4.88M in 2024 and significantly higher in countries like the U.S.
- Cyber incidents are now considered the top risk by businesses globally, surpassing traditional concerns like supply chain disruptions and natural disasters.
- Social engineering and phishing remain the most prevalent attack vectors, accounting for a significant portion of successful breaches.
- The legal and regulatory landscape is becoming more complex, with an increase in data privacy laws leading to a surge in class action lawsuits.
- Small and medium enterprises (SMEs) are particularly vulnerable, facing potentially catastrophic losses from cyber incidents.
- Human factors continue to be the weakest link in cybersecurity, with 75% of data breaches attributed to human risk.

While insurers have at times treated security awareness training as a yes/no box to be checked in initial assessments, upon closer review, a lack of awareness and training can be one of the most dangerous and least visible security liabilities for any company or organization. It is also an area where diligence can produce the highest rewards.

To Address These Challenges, a Multi-Faceted Approach is Necessary:

- Invest in robust cybersecurity measures, including phishing-resistant multifactor authentication and regular software updates.
- Implement comprehensive and ongoing security awareness training programs for all employees.

- Conduct regular vulnerability assessments and penetration testing.
- Partner with cyber insurance providers who offer proactive risk management services.
- Stay informed about evolving cyber threats and adapt security strategies accordingly.
- Develop and regularly test incident response plans to minimize damage when attacks occur.

In conclusion, the cyber threat landscape demands a proactive, collaborative approach between businesses, insurers and cybersecurity experts. By focusing on prevention, education and risk transfer through insurance, organizations can better position themselves to withstand the rising influx of cyber threats and protect their assets, reputation and customers in an increasingly digital world.

Download the CISO Security Resource Kit for more the definitive guide on how security awareness training addresses regulatory compliance, cyber insurance and security frameworks.

How KnowBe4 Can Help With Cyber Insurance Premiums

KnowBe4's platform can help with reducing cyber insurance premiums as evidenced as follows by our customers.

"We were able to show our insurance company that we use KSAT and as a result, our cyber-insurance premium was reduced by 20%."
– IT Security Analyst, Customer A

"We had competing bids for cyber-insurance. Many of the bids were from companies which in the past refused to cover us but now, because we are working with KnowBe4, our premiums have gone down."
– Security Analyst, Customer F

"We got cyber insurance last month for the first time because we are using KSAT. The insurers wouldn't look at us before."
– Associate Director, Cybersecurity, Customer K

Additional Resources

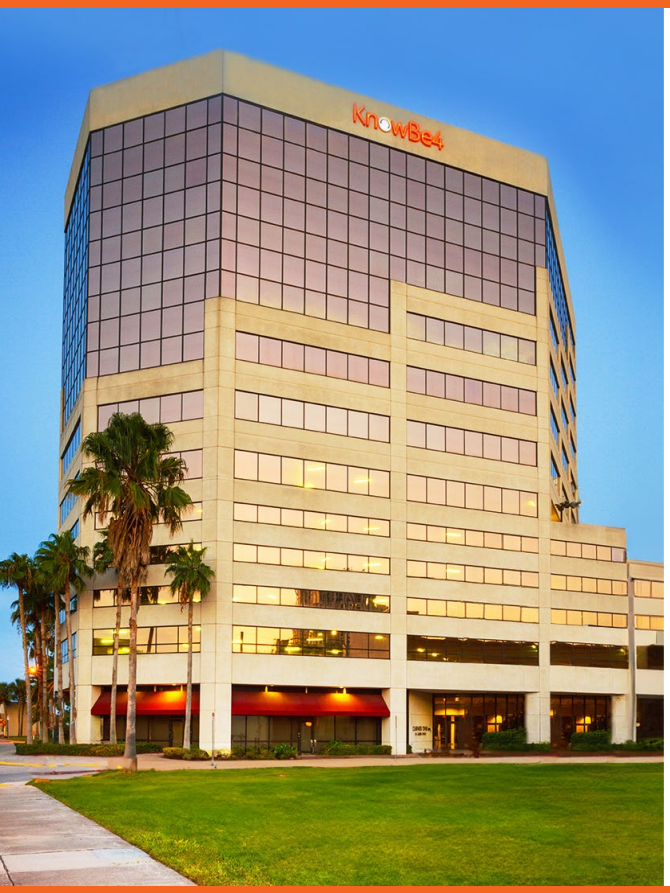
Free Phishing Security Test
Find out what percentage of your employees are Phish-prone with your free Phishing Security Test

Free Automated Security Awareness Program
Create a customized Security Awareness Program for your organization

Free Phish Alert Button
Your employees now have a safe way to report phishing attacks with one click

Free Email Exposure Check
Find out which of your users emails are exposed before the bad guys do

Free Domain Spoof Test
Find out if hackers can spoof an email address of your own domain



About KnowBe4

KnowBe4 empowers your workforce to make smarter security decisions every day. Tens of thousands of organizations worldwide trust the KnowBe4 platform to strengthen their security culture and reduce human risk. KnowBe4 builds a human layer of defense so organizations can fortify user behavior with new-school security awareness and compliance training.

Deploying KnowBe4 results in users that are alert and care about the damage that phishing, ransomware and other social engineering threats pose. The platform includes a comprehensive suite of awareness and compliance training, real-time user coaching, AI-powered simulated social engineering, and crowdsourced anti-phishing defense.

With content in 35+ languages, KnowBe4 provides the world's largest, always-fresh library of engaging content to strengthen your human firewall.

For more information, please visit www.KnowBe4.com

KnowBe4

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | www.KnowBe4.com | Email: Sales@KnowBe4.com

01E10K01