knowbe4

Effective Security Awareness Training Really Does Reduce Breaches

By Roger A. Grimes & Dr. Martin Kraemer

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

0359-B 1025

Inside this Report

Mitigating Human Risk

KnowBe4, Inc. has over a decade of data from over 70,000 customer organizations to show that a good security awareness training (SAT) program, including simulated phishing campaigns, significantly reduces human cybersecurity risk. We have data to show that SAT reduces the likelihood that someone appropriately trained will negatively interact with a simulated or real phishing message and that an effective human risk management (HRM) program reduces the likelihood of the organization's real-world compromise.

This paper will discuss the importance of decreasing human risk, particularly using an effective SAT program, with data analysis from real-world customers showing its proven efficacy in significantly reducing human risk factors. Having an effective SAT program is confirmed to reduce the risk of real-world data breaches.

70%–90% of Hacking Is from Social Engineering

Most cybersecurity events involve a human misstep, usually involving social engineering and, more specifically, phishing. This is not new. Since the beginning of computers, social engineering has been the number one way, by far, for bad actors to accomplish malicious hacking.

Social engineering is someone (or a group) often fraudulently posing as someone (e.g., friend, boss, etc.), something (e.g., police, tax authority, etc.) or some well-known brand (e.g., Microsoft, PayPal, your bank, etc.) you might otherwise trust more than if you knew their true identity trying to maliciously trick you into performing an action that would be harmful to your own interests. They want you to provide confidential information like your login details, download a boobytrapped document, run malware, etc.

Difference Between Social Engineering and Phishing?

What is the difference between social engineering and phishing? Although there is no "official" agreed-upon global definitions of social engineering and phishing, most sources categorize phishing (which often involves online digital media) as a subset of social engineering. Social engineering can also be done in person, using physical paper mail services, and other non-digital means. The term phishing came about during the digital age of the internet.

Decades of studies have consistently shown that 70% to 90% of all malicious data breaches involve social engineering and phishing. No other root cause method of malicious hacking (e.g., unpatched software and firmware, eavesdropping, cryptography attacks, physical theft, etc.) comes close. In fact, if you add up all other causes for successful cyberattacks together, they do not come close to equaling the damage done by social engineering and phishing alone.

NOTE

The second most popular reason for successful malicious hacking after social engineering and phishing is the exploitation of vulnerabilities in software and firmware. Google's Mandiant said vulnerability exploitation was responsible for 33% of all data breaches. After social engineering and vulnerability exploitation, all other initial access hacking methods added up altogether do not amount to 10% of the problem.

Depending on the survey done, the taxonomy used, and the sampled population involved, you may see various reports and studies state that social engineering is only involved in a lesser percentage of malicious hacking, say forty percent. However, nearly every study has shown that social engineering and phishing are the most common methods of malicious hacking used by attackers, even if they are listed as having a smaller percentage than 70% - 90%.

KnowBe4's Javvad Malik, Lead Security Awareness Advocate, did a meta-analysis of this by downloading 100 different cybersecurity reports with threat intelligence information from 43 different vendors and sources. Many of these came from what would reasonably be considered household names in the security industry, including Kaspersky, Securelist, ESET, McAfee, and Trend Micro. The result was that almost all of these reports concluded that social engineering and phishing were the top individual cyber threats no matter what individual percentage they attributed to it.

Here are some other relevant claims:

- In August 2023, Comcast reported that 89.46% of attacks on their customers started with phishing. You can read the whole report here.
- Social engineering and phishing are a worldwide problem. The U.K.'s Official Government Statistics Cyber Security Breaches Survey 2022 stated the following, "...the most common threat vector was phishing attempts (83%)."
- InfoBlox's 2022 Global State of Security Report states, "The most successful mode of attack was phishing (58%)."
- In May 2023, Barracuda Networks reported that although spear phishing only accounted for 0.1% of all email-based attacks, it accounted for 66% of successful compromises. That is huge for a single root cause!

This should not be a surprise. Most people and organizations suffering a successful hacker or malware attack will readily admit it involved social engineering and phishing.

Ransomware and Data Breaches Are the Most Damaging Attacks

There are many different types of cyberattacks a company can suffer, including malware attacks, stolen credentials, data exfiltration, denial of service, physical theft, etc. But for nearly a decade now, ransomware attacks have loomed as some of the most feared and damaging attacks. Most CISOs list a ransomware attack as their number one concern, and rightfully so.

Ransomware attacks often cause weeks to months of operational interruption. Many companies do not fully recover for over a year. The average ransom payment, if paid, can cost hundreds of thousands to millions of dollars. Ransomware recovery costs often cost many millions of dollars more. Ransomware can easily cause long-term reputational harm, lawsuits, regulatory fines, and even threaten ongoing business concerns, above and beyond any of the other types of cyberattacks.

Most Ransomware Attacks Are Data Breaches

Most ransomware attacks now involve data exfiltration of confidential data (e.g., data breaches). Early versions of ransomware simply encrypted files and asked for payment to provide the decryption key to unlock the encrypted files. However, starting in November 2019, ransomware attacks started to include a data exfiltration phase, where the involved attacker exfiltrated confidential data before performing the encryption phase.

The attacker then threatens the victim with revealing the confidential stolen data to the world, or at least to other attackers or the victim's competitors, if the ransom is not paid. This new attack method was created to offset victims who had good backups and did not feel the need to pay to get the ransomware decryption key. The exfiltration of unencrypted confidential data by an unauthorized party is a data breach.

Today, according to many cybersecurity firms, most ransomware also does data exfiltration. For example, Arctic Wolf, stated that 91% of ransomware attacks involve data exfiltration. Coveware has the number slightly lower at 75%. So today, if you have a ransomware event that is not also a data breach event, consider yourself lucky.

In their July 30, 2024 Quarterly Report, Coveware states that 43% of ransomware victims who pay the ransom do so purely because of the data exfiltration event () even though the victims did not have their data encrypted during the attack.

Social Engineering Causes Most Ransomware Attacks

Out of all the ways that ransomware can get on a device or network, social engineering is the number one way. KnowBe4 previously released a white paper entitled, The Root Causes of Ransomware, about this fact. Many other sources have come to the same conclusion.

For example, the 2024 Microsoft Digital Defense Report stated "[For ransomware] the most prevalent initial access techniques continue to be social engineering—specifically email phishing, SMS phishing, and voice phishing—identity compromise, and exploiting vulnerabilities in public-facing applications or unpatched operating systems."

Human risk can be mitigated using the best defense-in-depth combination of policies, technical defenses (e.g., content-filtering, file attachment blocking, etc.), and training. After decades of trying, policies and technical defenses alone have proven inadequate at blocking social engineering and phishing. The fact that social engineering and phishing are involved in such a large percentage of attacks demonstrates how easily these types of attacks get past policies and technical defenses.

Subsequently, all users should be trained to recognize social engineering and phishing attacks and learn how to mitigate and appropriately report them. Training and SAT is just one of the ways to reduce human risk, but it is a significant part of the process.

Clearly, reducing human risk, and in particular, social engineering and phishing attacks, is one of the best cybersecurity mitigations any organization can do.

Good SAT Mitigates Human Risk

We have previously shown in a white paper entitled, Data Confirms Value of Security Awareness Training and Simulated Phishing that an effective SAT program including simulated phishing works well to reduce the percentage of people who will inappropriately respond to a simulated phishing exercise (what we call the Phish-prone™ Percentage or PPP), and that the more often SAT and simulated phishing are performed within an organization, the lower the PPP.

We also have data, shown below, that proves that organizations that have a good SAT program (including frequent simulated phishing campaigns) reduce real human risk and have fewer real-world compromises. And the more often you train and conduct simulated phishing campaigns, the lower the real human risk is.

NOTE
KnowBe4 considers a good SAT program to include at least quarterly training and simulated phishing tests, although even more frequent training and simulated phishing are demonstrated to provide even more risk reduction. We consider an effective SAT program to be one where training is done at least monthly with simulated phishing campaigns done at least monthly as well, if not more frequently.

If you are interested in more details of what KnowBe4 recommends for an effective SAT program, read it here.

The Ultimate Question

Ultimately, there is only one question to ask regarding the effectiveness of SAT programs.

Does a good security awareness training program with simulated phishing campaigns reduce an organization's risk of being compromised by a real-world attack?

Every other measure does not get at the exact goal of why we need effective SAT programs. If effective SAT programs really do reduce human risk as we expect, we should see evidence of reduced real-world compromises from human risk reduction from organizations that have effective SAT programs.

The best way to objectively answer that question would be to collect global large-scale data on which organizations have or have not suffered a data breach in a given time period and compare those findings with whether they had used or did not use a good SAT program prior to the attack to reduce human risk.

If good SAT did indeed help organizations avoid getting breached (and there was proven correlation and causation), you would expect that organizations that had good SAT programs would be breached less than organizations that did not have good or no SAT programs prior to the incident(s).

NOTE
Solid, scientific correlation and causation would still be ultimately difficult to confirm without a structured experiment involving randomly selected participants who had effective SAT programs and randomly selected other participants who were asked to do no training or testing as the control group.

The Challenge

Unfortunately, a large global dataset showing who has or hasn't been breached AND whether or not they had a good SAT program in place ahead of the breach does not exist.

It is challenging to answer the ultimate question either way using our large global customer dataset because although we do have internal data showing how much our customers do or do not use SAT and simulated phishing, our customers usually do not tell us when they have or have not suffered a data breach, and if that data breach was related to social engineering and phishing. Further, we certainly do not have the data on non-customers and whether they did or did not suffer a data breach in a given time period and whether or not they had a good SAT program and simulated phishing campaigns.

However, we came up with the best representation of that sort of dataset that we could construct with available data.

NOTE
We realize that even what we did to find the best representation of data to answer the ultimate question will not 100% satisfy everyone. But we think we did our best to find the worthiest, largest dataset to answer the question as well as it could be answered.

What We Did

First, we purchased the largest publicly-known list of compromised organizations from the Privacy Rights Clearinghouse. The Privacy Rights Clearinghouse (PRC) breach database contains records for over 17,500 data breaches since 2005 publicly announced by U.S. organizations. Anyone can purchase it for $450.

As a global company with customers around the world, we would rather use a global database including non-U.S. organizations and breaches, but this U.S.-only collection is the single largest public breach database available. Nothing else comes even close, regarding the number of compromises over almost a decade. At the time we purchased it, it had over 35,000 separate public breach notifications (for the 17,500 unique breach events). Many organizations had multiple breach announcements for the same breach and/or suffered multiple publicly-announced breaches.

NOTE
It is very common for a single organization in the PRC database to suffer multiple public breaches from different cybersecurity events. A noteworthy percentage of breached companies suffered multiple breaches. It is not difficult to imagine that a company that has suffered a breach because of weak security controls or practices is breached again as it tries to improve its security posture over time.

We then downloaded our much larger customer list and compared it to the PRC records.

Analysis and Results

The vast majority of our current U.S. customers (97.6%) have not suffered a public data breach (at least since 2005). At the time we ran our analysis query, we had 63,347 current U.S. and international customers.

Type of KnowBe4 Customer	Accounts	%
U.S. Current Customers	50,010	79.94%
Non-U.S. Current Customers	13,337	21.06%
Current Customers Total	63,347	100.00%

NOTE
Today, we have over 70,000 current U.S. and international customers.

The PRC database only includes data on U.S. organizations and data breaches, so we needed to do our analysis using only our 50,010 current U.S.-based customers.

KnowBe4 Current U.S. Customers in the PRC Database

The first analysis was to find out how many of our current U.S. customers appeared in the PRC database. This was one of the toughest parts of the analysis, to ensure we were confidently matching our customers with the exact same organization listed in the PRC database, if they were listed. We often found slight to moderate inconsistencies in the names listed that belonged to the same customer and, conversely, very similar names belonging to different customers. We found numerous variations all over the place in each direction. We had to refine our queries several times and test our results for accuracy. We worked hard to ensure the best matching accuracy possible. Here is what we found (shown below):

Type of KnowBe4 Customer	Accounts
KnowBe4 Current U.S. Customers	50,010
KnowBe4 Current U.S. Customers in PRC Database	1,189
% of KnowBe4 Current US Customers in PRC Database	2.37%

Our Customers Are Less Likely To Be Breached

This compares very favorably to figures routinely reported for decades that the percentage of organizations experiencing a data breach of some type, including ransomware, was, depending on the year and source, around 20% - 69% in a single year.

This means only 2.4% of our current U.S. customers have suffered a public data breach (at least since 2005).

Some supporting statements from other cybersecurity firms as examples:

- GetApp's 2024 Data Security Report states that 44% of U.S. organizations and 51% of global organizations experienced a ransomware attack in the last 12 months.
- Ponemon Institute's A Crisis in Third-Party Remote Access Security report stated 52% of respondents have experienced a data breach...in the last 12 months
- Research suggests 40% of Fortune 1000 companies will suffer a breach every year
- The 2022 Cymulate survey stated that 40% of respondents admitted to being breached over the past 12 months. After being breached once, 66% of breached respondents said they suffered additional attacks. Attacks primarily (56%) occurred via end-user phishing.

NOTE
It is widely assumed that the total collective incidents of data breaches are much higher than those that are publicly reported. Many data breaches are not publicly reported, either because they are not required or because the involved organizations simply decided not to or neglected to report. For this report and subsequent involved comparison, we assume that the percentage of non-reporting entities globally would be somewhat equivalent in our customer base as well.

This can be due to many reasons and may or may not be correlated or caused by our services. But for whatever reason, our current U.S. customers are far less likely to be publicly compromised than the average U.S. organization.

It could be that customers using any SAT service are better at mitigating human risk and, consequently, all cyberattacks than companies that do not. It would be better to ask which customers became a customer with an already existing excellent human risk mitigation record before becoming a customer and which improved their HRM record during or after becoming our customer. There is no available data to measure the answer to this question. But based on the previous analysis, for whatever reason, our customers seem less likely to appear on public data breach lists.

If we take the lowest figure of 20% of organizations compromised in a single year, this means our current U.S. customers are 8.3 times less likely to be on the public data breach list any year.

Confidence Interval Calculation

Only 2.4% of our U.S. customers appear on the public breach database list. That is a pretty amazing statistic! Some readers may wonder if our U.S. customer list is representative of all U.S. businesses that could appear on the U.S. public breach list or if our customer list is so few that they do not appear on the public breach list just by chance. For example, a company with only 10 customers might be able to accurately say that 100% of their customers do not appear on the public data breach list either. However, that result is probably more likely because they only had 10 customers and not for any other reason. How accurately does our list of 55,010 U.S. customers reflect all U.S. businesses that might appear on the public breach list? Finding out that answer in statistics is known as a confidence interval. So, we calculated the confidence interval for our U.S. customer list to represent all U.S. businesses that could appear on the U.S. public breach list.

We can compare our U.S. customer list of 50,010 (i.e., the sample size) against all U.S. 32.3M businesses (i.e., the population). We could also compare our customer list against the number of U.S. businesses with over 500 employees, 33,200, because those businesses and our customers are more likely to also have data breach reporting requirements. When our 50,010 U.S. customer list is compared against all 32.2M U.S. businesses with a confidence interval of 95% (meaning our customer list is likely to accurately represent the largest list 95% of the time), the margin of error is less than 1%. For the smaller population of just 33,200 U.S. businesses, the margin of error is one-tenth of that result. Thus, our customer list would be expected to accurately reflect U.S. businesses and their chances of being on the U.S. public breach list with high confidence.

Breached Organization Analysis

To help get a better sense of correlation with the services that KnowBe4 provides, we decided to look at organizations that suffered one or more data breaches before becoming a KnowBe4 customer and compare it to the number of breaches suffered by the same customers after becoming a KnowBe4 customer. If a current KnowBe4 customer suffered fewer breaches while they were an existing customer than before they were our customer, that result would support the idea that a good SAT program reduces human risk.

Now that we had the list of 1,189 current U.S. customers who were also breached, we needed to determine if they were breached before they became customers or while they were customers.

Cybersecurity Is About Risk Management

Keep in mind, even though a good SAT program does reduce the risk of breaches, some of our current customers do still sometimes suffer data breaches (from all breach causes, including social engineering).

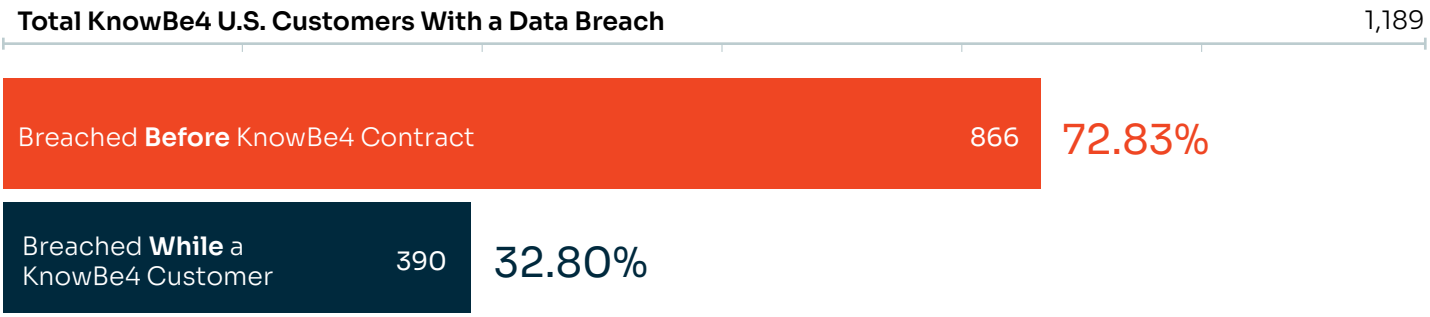
There is no way to completely eradicate risk to zero percent (0%) for any type of cyberattack while still maintaining an operational and responsive business. Few of us would want to work in a world and environment with zero risk. The goal of most cybersecurity is to reduce the most critical and expensive risks and the occurrence and impact of those risks to an acceptable level. Just because you cannot completely eliminate all risk of a cyberattack does not mean you do not recommend or do the mitigation.

For example, according to Google's Mandiant, unpatched software and firmware vulnerabilities are involved in about 33% of successful data breaches. Every organization and person knows they should apply all critical patches in a timely manner. Just because most companies do not do perfect patching does not mean you do not recommend better patching to reduce cybersecurity risk. The name of the game is risk reduction. Companies that do better patching will be at less risk from a successful compromise involving unpatched software or firmware than companies that do not.

Analysis of KnowBe4 Breached Customers

If our current customers are breached less now than before they were our customers, this would support the possible correlation of our services being involved; and vice versa.

Here is what we found:



NOTE
Breached figures are over 100% because some breached customers suffered one or more breaches before becoming our customers and/or one or more breaches after becoming our customers.

The data shows that most data breaches involving our U.S. customers occurred before they were our customers. Keep in mind that most of our current U.S. customers (97.6%) are not reporting any breaches. But if they have been breached, 73% were breached before they were our customer.

Breached U.S. current customers appear 54.9% (72.83%-32.8%)/72.83%) less likely to suffer one or more breaches while being our customer.

This gives additional support that our customers, using good SAT programs, are less prone to breaches. It could also be customers coming to us to implement an SAT program (or improved SAT program) after suffering data breaches due to social engineering and other human risk events. Either way, we did not see data conflicting with the possibility that a good SAT program could have resulted in fewer breaches.

Only 33% of the breaches to the 2.4% of our current U.S. customers who suffered a breach happened while they were using our products and services. In summary, our customers were less likely to suffer a public data breach after becoming our customers than prior to becoming our customers. In general, our customers are far less likely to suffer a public data breach.

Our Breached Customers Have Fewer Breaches

It is not unusual for a previously breached organization to get breached one or more times again. Even in this case, our breached customers also suffered fewer data breaches if they did suffer a public data breach than before they were our customer, as the table below shows.

Type of KnowBe4 Customer	Number of Customer Breaches		Before Freq	During Freq
	Before Contract	During Contract		
Active	2553	752	2.95	1.93

Our breached U.S. customers who were breached before they were our customers were breached an average of almost three times. Our current U.S. customers who suffer breaches while they are our customers are breached less than two times on average, for an overall improvement of 37% [(2.97-1.88)/2.97]. Or looking at it in reverse, our breached customers are 58% [(2.97-1.88)/1.88] less likely to suffer a data breach than before they were our customers, also keeping in mind that 97.6% of our customers did not suffer any breach.

Most of our current U.S. customers did not suffer a public data breach (97.4%) and if they did suffer a breach while being our customer, suffered fewer breaches on average Cyber Insurance Policies Often Require SAT Programs

The cyber insurance industry and their actuaries independently support our results, as almost all cyber insurance policies require that a covered policyholder have an existing, effective SAT program. You will find it hard to get a cyber insurance policy without an effective SAT program in place; and even if you could, the resulting policy will be more expensive in most instances.

Here are some related supporting links:

- "Every cyber insurance policy requires a security awareness program."
- "Cybersecurity insurance providers will often expect your employees to have completed Security Awareness Training before offering to cover you."
- 5 Requirements to Get Cyber Insurance
- 7 Cyber Insurance Requirements (And How to Meet Them)
- AIG Cybersecurity Checklist

The cyber insurance industry has done the number crunching, and an effective SAT program is most often a critical requirement for getting cyber insurance coverage.

Report Caveats

We are well aware that our best dataset representation and analysis does not conclusively prove that an effective SAT program prevents actual data breaches, with confirmed correlation and proven causation. It is impossible to prove or disprove that thesis without designing several experiments where some randomly chosen large organizations are instructed to perform effective SAT and other randomly selected large organizations are told to do no SAT (to represent the control group). Very few large organizations, if any, would agree to do zero training and simulated phishing in a given year, with no other varying risk factors involved, to participate in an experiment. And that experiment would need to be performed by several different researchers across disparate populations over long periods of time in order to gauge true effectiveness.

With that admitted, we tried our best to create a representative dataset that might add or remove support for correlation and causation of a good SAT program, decreasing the risk of real data breaches. We accept our conclusions may be different if we had a wider variety of data and more definitive experimentation.

However, our previous studies on Phish-prone™ Percentages involving simulated phishing does also support that effective SAT programs do reduce the chances that a well-trained and tested employee will negatively interact with a simulated phishing test, and this new data about real world consequences supports that prior finding (versus contradicting it).

Other Caveats and Considerations

We cannot conclusively prove causation that an effective SAT program alone provides these results. We have to assume that an organization doing an effective SAT program is likely also doing other things (e.g., policies, technical controls, etc.) that all collectively bear responsibility to reduce the risk of real-world data breaches. We can only say that our current customers are breached less often than the average organization and, if breached, suffer fewer breaches.

Lastly, it must be noted that the data breaches in the PRC database are due to all sorts of root causes, including human mistakes and physical thievery. A large percentage of the data breaches in the PRC database are reported as “unknown”. Many others are misclassified with incorrect taxonomy (a subject for another day).

What we can conclusively state, as discussed above, is that almost all the independent data for many decades has consistently shown social engineering and phishing are the top hacking causes for data breaches by far above all others. The breaches listed in the PRC database would not be expected to substantially deviate from every other trusted source’s findings.

Summary

We have over 50,010 active U.S. customers. The vast majority (97.6%) have not suffered a public data breach. Even our breached U.S. customers appear 65% less likely to suffer one or more breaches while being our customer.

Based on the data analyzed for this report and other supporting analyses, it is likely that an effective SAT program significantly reduces human risk and the chances of a real-world compromise.

More 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 workforces to make smarter security decisions every day. Trusted by over 70,000 organizations worldwide, KnowBe4 helps to strengthen security culture and manage human risk. KnowBe4 offers a comprehensive AI-driven "best-of-suite" platform for Human Risk Management, creating an adaptive defense layer that fortifies user behavior against the latest cybersecurity threats. The HRM+ platform includes modules for awareness and compliance training, cloud email security, real-time coaching, crowdsourced anti-phishing, AI Defense Agents and more. As the only global security platform of its kind, KnowBe4 utilizes personalized and relevant cybersecurity protection content, tools and techniques to mobilize workforces to transform from the largest attack surface to an organization's biggest asset. For more information, please visit www.KnowBe4.com

knowbe4

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