KnowBe4

PHISHING BY INDUSTRY

BENCHMARKING REPORT | 2022 EDITION

Verizon's 2022 Data Breach Investigations Report states that "the human element continues to drive breaches. This year, 82% of breaches involved the human element. Whether it is the use of stolen credentials, phishing, misuse or simply error, people continue to play a very large role in incidents and breaches alike."

INTRODUCTION

The human layer continues to be the most enticing attack vector for cybercriminals. Sadly, most organizations continue to neglect this easily penetrable entry point. Throughout 2021, the world continued to see significant year-over-year increases in phishing attacks. No industry vertical, size of business or geography was immune. The human layer was under attack in both professional settings and personal settings. Cybercriminals do not discriminate when they consider victims, as carefully constructed attacks target humans both at work and play, day or night through various types of social engineering.

The FBI's Internet Crime Complaint Center (IC3), *continued to receive a record number of complaints from the American public: 847,376 reported complaints, which was a 7% increase from 2020, with potential losses exceeding $6.9 billion.* Additionally, business email compromise incidents accounted for *19,954 complaints with an adjusted loss of nearly $2.4 billion.* And these are just the reported incidents.

Industries are grappling with how they can better develop their human defense layer to detect, protect and report suspicious actions before it's too late and their systems are compromised.

Most organizations turn first to technology as the means to combat cybercriminals, not taking into account that investing in human awareness and intervention is equally, if not more, critical. According to the Verizon 2022 Data Breach Investigations Report, *82% of all security incidents involve a human element,* proving how susceptible humans can be.

Security leaders who continue to invest solely in sophisticated technology and security orchestration run the risk of overlooking a best practice proven to reduce their vulnerability: security awareness training coupled with frequent simulated social engineering testing. This approach not only helps raise the readiness level of humans to combat cyber crime, it lays the critical foundation necessary to drive a strong security culture throughout an organization.

As the world finally begins to emerge from the grip of the COVID-19 pandemic, social engineering attacks continue to rise. The use of email, phone calls, texts, social media and other outreach methods all work together to evade an organization's secure infrastructure as workforces and individuals remain more distracted and exposed than ever.

Distraction can easily lead to disaster. With phishing on the rise, an employee's mindset and actions are critical to the security posture of every organization. Security leaders need to know what happens when their employees receive phishing emails: are they likely to click the link? Get tricked into giving away credentials? Download a malware-laced attachment? Will they simply ignore the email or delete it without warning their employer? Or will they report the suspected phish and play an active role in the human defense layer?

Each organization's employee susceptibility to these phishing attacks is known as their Phish-prone™ Percentage (PPP). By translating phishing risk into measurable terms, leaders can quantify their breach likelihood and adopt training that reduces their human attack surface.

Understanding Risk by Industry

An organization's PPP indicates how many of their employees are likely to fall for social engineering or phishing scams. These are the employees who might be tricked into clicking on a link, opening a file infected with malware or transferring company funds to a cybercriminal's bank account. A high PPP indicates greater risk, as it points to a higher number of employees who typically fall for these scams. A low PPP is optimal, as it indicates the staff is security-savvy and understands how to recognize and shut down such attempts.

In short, a low PPP means that an organization's human security layer is providing security strength rather than weakness. The overall PPP offers even more value when placed in context. After seeing their PPP, many leaders ask questions such as "How does my organization compare to others?" and "What can we do to reduce our Phish-prone Percentage and better equip our human layer?"

KnowBe4, the provider of the world's largest security awareness training and simulated phishing platform, has helped tens of thousands of organizations reduce their vulnerability by training their staff to recognize and respond appropriately to common scams.

To help organizations evaluate their PPP and understand the implications of their ranking, KnowBe4 conducts an annual study to provide definitive Phish-prone benchmarking across industries. Categorized by industry vertical and organization size, the study reveals patterns that can light the way to a stronger, safer and more secure future.

2022 GLOBAL PHISHING BY INDUSTRY BENCHMARKING STUDY

Every organization struggles to answer an essential question: "How do I compare with other organizations that look like me?" To provide a nuanced and accurate answer, the 2022 Phishing By Industry Benchmarking Study analyzed a data set of over 9.5 million users, across 30,173 organizations, with over 23.4 million simulated phishing security tests, across 19 different industries.

Methodology For This Year's Study

All organizations were categorized by industry type and size. To calculate each organization's PPP, we measured the number of employees who clicked a simulated phishing email link or opened an infected attachment during a testing campaign using the KnowBe4 platform.

In our 2022 report, we continue to look at the following three benchmark phases:

- **Phase One:** Baseline Phishing Security Test Results
- **Phase Two:** Phishing Security Test Results Within 90 Days of Training
- **Phase Three:** Phishing Security Test Results After One Year-Plus of Ongoing Training

ANALYZING TRAINING IMPACT

To understand the impact of security awareness training, we measured outcomes at these three touchpoints to answer the following questions:

PHASE ONE

1

If you have not trained your users and you send a phishing attack, what is the initial resulting PPP?

To do this, we monitored employee susceptibility to an initial baseline simulated phishing security test. From that established set of users, we look at any time a user has failed a simulated phishing security test prior to having completed any training.

PHASE TWO

2

What is the resulting PPP after your users complete training and receive simulated phishing security tests within 90 days after training?

We answered this question by finding when users completed their first training event and looking for all simulated phishing security events up to 90 days after that training was completed.

PHASE THREE

3

What is the final resulting PPP after your users take ongoing training and monthly simulated phishing tests?

To answer this, we measured security awareness skills after 12 months or more of ongoing training and simulated phishing security tests, looked for users who completed training at least one year ago, and took the performance results on their very last phishing test.

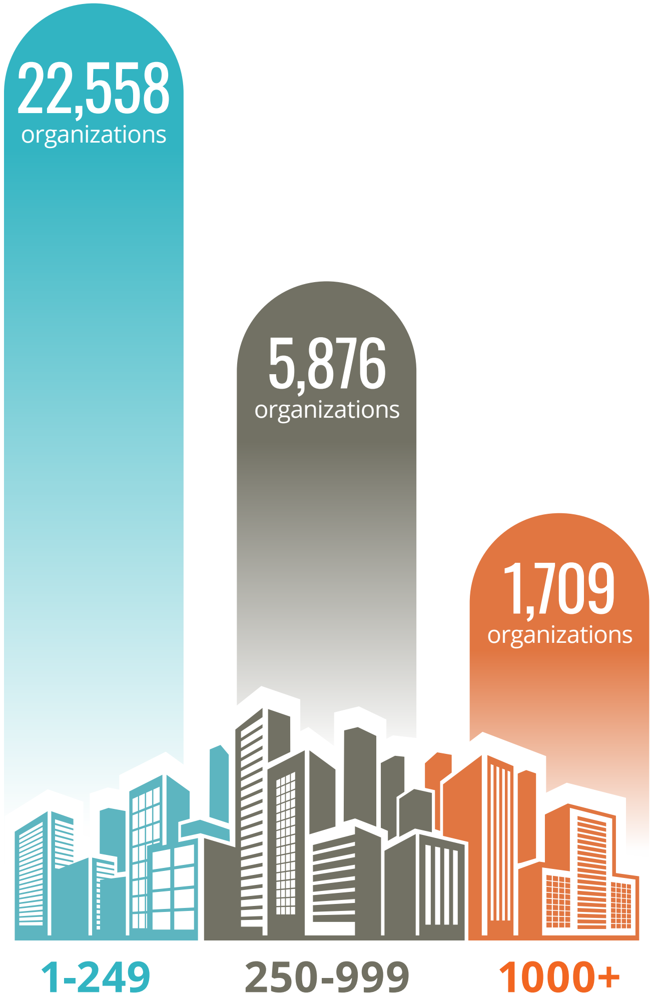
METHODOLOGY AND DATA SET

23.4 million phishing security tests

9.5 million users

30.1 thousand organizations

ORGANIZATION SIZE RANGES



19 INDUSTRIES

- Banking
- Business Services
- Construction
- Consulting
- Consumer Services
- Education
- Energy & Utilities
- Financial Services
- Government
- Healthcare & Pharmaceuticals
- Hospitality
- Insurance
- Legal
- Manufacturing
- Not For Profit
- Other
- Retail & Wholesale
- Technology
- Transportation

WHO'S AT RISK: RANKING INDUSTRY VULNERABILITY

The results across the 9.5 million users highlight an all too familiar truth for organizations: failure to effectively train your users leaves them, and your organization, unprepared and vulnerable to social engineering attacks. The Phish-prone Percentage data, although slightly more favorable than 2021, continues to show that no single industry across all-sized organizations is doing a good job at recognizing the cybercriminals' phishing and social engineering tactics. When users have not been tested or trained, the initial baseline phishing security tests show how likely users in these industries are to fall victim to a phishing scam and put their organizations at risk for potential compromise.

The overall 2022 PPP baseline average across all industries and size organizations was **32.4%**, up one point from 2021. Trends varied across different industries, revealing the bleak truth that untrained users are failing as an organization's last line of defense against phishing attacks.

- Across small organizations (1-249 employees), the **Education Industry**, although slightly better than 2021, enters 2022 with a **PPP of 32.7%**. **Healthcare & Pharmaceuticals** is next with a **PPP of 32.5%**. Unseating Not-for-Profit for the last spot is **Retail & Wholesale** with a **PPP of 31.5%**.
- With mid-sized organizations (250-999 employees), the top three industries from 2021 remained. The **Hospitality industry** was unchanged in 2021 with a PPP of **39.4%**. **Energy & Utilities** and **Healthcare & Pharmaceuticals** swapped positions, with Healthcare & Pharmaceuticals next with a **PPP of 36.6%** and **Energy & Utilities** following with a **PPP of 34%**. It is worth noting that all three industries had stronger PPPs vs. 2021 ratings, although they remained the industries most at risk.

Who's at Risk?

The top three industries by organization size

SMALL 1-249	MEDIUM 250-999	LARGE 1,000+
32.7% Education	39.4% Hospitality	52.3% Insurance
32.5% Healthcare & Pharmaceuticals	36.6% Healthcare & Pharmaceuticals	52.2% Consulting
31.5% Retail & Wholesale	34% Energy & Utilities	50.9% Energy & Utilities

- For large organizations (1,000+ employees), we saw Energy & Utilities fall out of the top spot and be replaced by **Insurance** (second in 2021) with a **PPP of 52.3%**. The **Consulting industry**, new to the ranking, was next with a **PPP of 52.2%**, while **Energy & Utilities** rounded out the group with a **PPP of 50.9%**. Banking fell out of the top three in 2022.
- The winner of the lowest Phish-prone benchmark across small organizations (1-249 employees) was **Banking** with a **PPP of 25.4%**; across mid-sized organizations was **Government** with a **PPP of 26.4%**; and across large organizations was **Hospitality** with a **PPP of 20.4%**. Although the lowest in the findings, these PPP results strongly indicate that an untrained user base is still vulnerable to falling for phishing attacks.

PHASE ONE: BASELINE PHISHING SECURITY TEST RESULTS

The initial baseline phishing security test was administered within organizations that had not conducted any security awareness training from the KnowBe4 platform. Users received no warning, and the tests were administered on untrained people going about their regular job duties. The results continue to indicate high risk levels year-over-year:

- Across all industries and all sizes, the average Phish-prone Percentage was **32.4%**, up 1 point from 2021. **That means one out of three employees was likely to click on a suspicious link or email or comply with a fraudulent request**, about the same outcome as last year.
- The 2022 data showed the most significant improvement was seen with **Large Construction** companies, which positively moved from a PPP of **42.7% to 37%**. Adversely, the most significant decline was visible in **Large Consulting** companies, moving negatively from **28.4% in 2021 to 52.2% in 2022**.
- What is most concerning are the PPPs of the following industries in the Large category, which all have PPPs north of 40%: **Banking 43.5%, Healthcare & Pharmaceuticals 45%, Energy & Utilities 50.9%, Consulting 52.2% and Insurance 52.3%**. This means that employees in these categories are at a high risk of falling for social engineering attacks, some a staggering 50+%.

Thoughts: As cyber threats grow, the communication of these threats is filtering to the masses through social/news media. In some areas, people have more information thrust at them, so their awareness is growing more organically. The question remains if that ground-level awareness will transfer to the workplace and grow with training into something more developed and instinctive. Without training and frequent reinforcement, every organization, regardless of size and vertical, is susceptible to phishing and social engineering. Workforces in every industry represent a possible doorway to attackers, no matter how steep the investment in world-class security technology.

Phase One

32.4% Initial Baseline Phishing Security Test Results

Organization Size	Initial PPP
1-249	28.8%
250-999	30.2%
1000+	35.2%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	25.4%	27.3%	43.5%
Business Services	27.4%	30%	29.2%
Construction	29.6%	32.9%	37%
Consulting	27.5%	30.6%	52.2%
Consumer Services	30.4%	29.1%	24.3%
Education	32.7%	29.3%	28.4%
Energy & Utilities	29.4%	34%	50.9%
Financial Services	26.4%	28.7%	35.9%
Government	28%	26.4%	24.8%
Healthcare & Pharmaceuticals	32.5%	36.6%	45%
Hospitality	28.5%	39.4%	20.4%
Insurance	26.2%	30.3%	52.3%
Legal	27.3%	27.6%	29.2%
Manufacturing	29.5%	29.5%	33.1%
Not-For-Profit	29.6%	30.8%	36.5%
Other	30.5%	31.9%	26.8%
Retail & Wholesale	31.5%	30.6%	38.6%
Technology	26.7%	28.2%	33.2%
Transportation	27%	32%	24.8%

PHASE TWO: PHISHING SECURITY TEST RESULTS WITHIN 90 DAYS OF TRAINING

When organizations implemented a combination of training and simulated phishing security testing after their initial baseline measurement, results changed dramatically. We found that after users complete their first training event, the simulated phishing security test results up to 90 days after that training is completed are more favorable. In those 90 days after completed training events, the average Phish-prone Percentage was cut to almost half at 17.6%, consistent with the studies from the past three years. The dramatic drop in Phish-prone Percentages was not specific to a certain industry or organization size, but here are a few interesting data points:

- The most significant reduction was seen in the following organizations: small (1-249 employees) **Education** experienced a **46% decrease** from 32.7% at baseline to 17.9% within 90 days of training; mid-size (250-999 employees) **Hospitality** experienced a **51% decrease** from 39.4% at baseline to 19.4% within 90 days of training; and large (1000+ employees) **Insurance** experienced a **67% decrease** from 52.3% at baseline to 17.3% within 90 days of training after recording one of the highest initial baseline PPPs.
- The significant drop from **32.4% to 17.6%** for all industries proves that a security awareness training program can pay meaningful dividends in building a strong human defense layer as part of your defense-in-depth IT security posture—even within the first three months.

Thoughts: After applying only 90 days of new-school security awareness training, we saw a significant improvement in employees' abilities to detect malicious emails across every industry and size of organization. Think about it in terms of a weight loss plan; it takes at least 90 days to start seeing results. In that same timeframe, your newly 90-day trained employees can cut the potential of your organization experiencing a brand/revenue damaging breach by nearly half. It takes a 90-day investment to raise readiness levels and lower risk. As with any significant change, it takes time to break old habits and create new ones. Once these new habits are formed however, they become the new normal, part of the organizational culture, and influence how others behave, especially new hires who look to others to see what is socially and culturally acceptable in the organization.

Phase Two

17.6% Phishing Security Test Results Within 90 Days of Training

Organization Size	90-Day PPP
1-249	17.5%
250-999	17.9%
1000+	17.4%

Industry	**1-249** Employees	**250-999** Employees	**1000+** Employees
Banking	12.3%	13.6%	15.6%
Business Services	18.3%	18.6%	17.7%
Construction	19.5%	20%	15.8%
Consulting	17.5%	20.1%	21.3%
Consumer Services	18.8%	21%	16.1%
Education	17.9%	18.5%	18.8%
Energy & Utilities	16.8%	17.2%	16.4%
Financial Services	15.1%	16%	19.1%
Government	16%	15.5%	15.2%
Healthcare & Pharmaceuticals	19.7%	19.1%	17.2%
Hospitality	19.7%	19.4%	12.2%
Insurance	17.7%	17.5%	17.3%
Legal	16.5%	15.9%	13%
Manufacturing	17.7%	17%	16.5%
Not-For-Profit	20.3%	20.8%	18.2%
Other	19%	21.4%	20.1%
Retail & Wholesale	18.3%	18.1%	18.1%
Technology	18.9%	18.8%	19.2%
Transportation	18.5%	18.7%	16.5%

PHASE THREE: PHISHING SECURITY TEST RESULTS AFTER ONE YEAR-PLUS OF ONGOING TRAINING

At this stage, we measured security awareness skills after 12 months or more of ongoing training and simulated phishing security tests. We looked for users who completed training at least one year ago and analyzed the performance results on their very last phishing test. The results continue to be dramatic year-over-year, showing that having a consistent, mature awareness training program reduced the average PPP from 32.4% all the way down to **5%. These results were demonstrated significantly across all industry sizes and verticals.**

For a second year, the lowest PPP in small organizations (1-249 employees) was **Banking** at **2.6%**. Also, for a second year, the **Banking** industry scored the lowest PPP in the mid-size organizations category (250-999 employees) at **3.3%**. In the category of large organizations (1000+ employees) and also for a second year, the **Hospitality** industry scored **1.3%**, a favorable decrease from their 2021 score of 4%. With Banking being one of the most attacked and regulated industries, the results are no doubt based on the head start they had with cyber crime and the diligence they have applied to training.

After comparing the data, the industries that showed the greatest holistic improvement were both in the large category (1000+ employees): **Energy & Utilities industry, which went from a benchmark PPP of 50.9% to 3.6% after at least 12 months of security awareness training, a 93% reduction and the Consulting industry which went from a benchmark PPP of 52.2% to 4.9%, a 91% reduction.** The Energy & Utilities industry, which experienced one of the largest cyber attacks on an oil infrastructure target in the history of the United States (Colonial Pipeline), continues to be a high profile and high destruction target for cybercriminals. Also highly targeted is the Consulting industry where in August 2021, one of the largest global consulting groups was hit with a massive $50 million ransomware attack by the group LockBit with help from an internal source (insider threat).

Phase Three

5% Phishing Security Test Results After One Year-Plus of Ongoing Training

Organization Size	12-Month PPP
1-249	3.8%
250-999	5%
1000+	5.8%

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	2.6%	3.3%	3.4%
Business Services	3.8%	5%	6%
Construction	4.1%	4.8%	4.6%
Consulting	3.8%	4.8%	4.9%
Consumer Services	4.7%	4.7%	3.3%
Education	4.1%	5.4%	6.5%
Energy & Utilities	3.4%	5%	3.6%
Financial Services	3.7%	4.9%	5.5%
Government	3.9%	3.9%	7.1%
Healthcare & Pharmaceuticals	4.1%	5.1%	5.9%
Hospitality	4.4%	5.6%	1.3%
Insurance	3.3%	4%	5.3%
Legal	4.1%	5.2%	5.6%
Manufacturing	3.3%	5.3%	6.2%
Not-For-Profit	4.1%	4.9%	4.5%
Other	3.2%	4%	6.2%
Retail & Wholesale	3.6%	5.3%	4.7%
Technology	4.7%	5.9%	7.2%
Transportation	4.1%	9.6%	4.5%

AVERAGE IMPROVEMENT RATES ACROSS ALL INDUSTRIES AND ORGANIZATION SIZES

It is clear that after one year or more of security awareness training combined with frequent simulated phishing tests, **organizations across all sizes and industries drastically improved**. Organizations with 1-249 employees continued to achieve the **best overall improvement with 17 out of 19 industries coming in at 85% or above**.

Across mid-size organizations, improvement rates were good with **17 industries coming in at 80% or better**, two industries fell slightly below 80%. For large organizations, we saw **14 industries with improvement rates above 80%**, with the remaining five ranging from 71% to 79%.

When you look across all industries and sizes, the **85% average improvement rate** from baseline testing to one year-plus of ongoing training and testing is **outstanding proof for gaining buy-in to establish a fully mature security awareness training program**.

KnowBe4 finds that the industry-wide 32.4% of untrained users will fail a phishing test.

Once trained, only 17.6% of users failed within 90 days of completing their first KnowBe4 training. After at least a year on the KnowBe4 platform, only 5% of users failed a phishing test.

Average Improvement

85%

Average Improvement Rate Across All Industries and Sizes

Industry	1-249 Employees	250-999 Employees	1000+ Employees
Banking	90%	88%	92%
Business Services	86%	83%	79%
Construction	86%	85%	88%
Consulting	86%	84%	91%
Consumer Services	85%	84%	86%
Education	87%	82%	77%
Energy & Utilities	88%	85%	93%
Financial Services	86%	83%	85%
Government	86%	85%	71%
Healthcare & Pharmaceuticals	87%	86%	87%
Hospitality	84%	86%	93%
Insurance	87%	87%	90%
Legal	85%	81%	81%
Manufacturing	89%	82%	81%
Not-For-Profit	86%	84%	88%
Other	90%	87%	77%
Retail & Wholesale	89%	83%	88%
Technology	83%	79%	78%
Transportation	85%	70%	82%

2022 INTERNATIONAL PHISHING BENCHMARKS

At the international level, we used a slightly different data set that does not include separate industries to determine phishing benchmarks regionally across small, medium, and large organizations. We included organizations where a definitive country was associated with the customer account so it could be included in the international benchmark analysis. The same benchmarking phases used to measure Phish-prone Percentages across industries were used for the international data set.

Phase One

Initial Baseline Phishing Security Test Results

Phase Two

Phishing Security Test Results Within 90 Days of Training

Phase Three

Phishing Security Test Results After One Year-Plus of Ongoing Training

		BASELINE			90 DAYS			1 YEAR		
	Organization Size	1-249	250-999	1000+	1-249	250-999	1000+	1-249	250-999	1000+
REGION	North America	28.7%	30.2%	35.8%	17.4%	17.9%	17.4%	3.5%	4.6%	6%
			TOTAL: 32.4%			TOTAL: 17.5%			TOTAL: 4.7%	
	Africa	30.2%	27.4%	32.4%	24.8%	21%	17.9%	8.1%	12.7%	4%
			TOTAL: 31.4%			TOTAL: 18.8%			TOTAL: 5.4%	
	APAC (Asia, Oceania & Australia)	30.2%	32.6%	36.7%	21.1%	19.2%	15%	4.4%	6.2%	5.2%
			TOTAL: 34.5%			TOTAL: 16.9%			TOTAL: 5.4%	
	Europe	27.8%	28.2%	31.1%	17.9%	18.2%	18.9%	4.2%	6.7%	8%
			TOTAL: 29.9%			TOTAL: 18.5%			TOTAL: 6.3%	
	South America	30.9%	30%	45.6%	24.7%	22.2%	19.3%	1.8%	9.8%	0.8%
			TOTAL: 39.9%			TOTAL: 20.5%			TOTAL: 3.2%	
	United Kingdom & Ireland	26.2%	27.7%	32.7%	16.7%	16.2%	17.5%	3.9%	4.3%	8.3%
			TOTAL: 30%			TOTAL: 17%			TOTAL: 5.5%	

NORTH AMERICA

Most Prevalent Issues

Ransomware clearly stands out as one of the biggest cyber threats to organizations across industries of all sizes. This malware not only stops the operation of the organization, but also puts the information of customers and employees at risk for public exposure on the internet. In addition, for many organizations, this type of breach is quite public, especially when websites are defaced, or services suspended, and offices closed down during the recovery. This public nature of ransomware can have a serious impact on the reputation of an organization.

Things can get really ugly when the ransomware gangs reach out to the customers of the victim organization, using the customer base as a way to increase the pressure to pay the attackers. Unlike early versions of ransomware that were almost completely automated, modern strains of ransomware often involve a significant human interaction, mapping out the most critical systems, creating backdoors and stealing the data that will do the most harm. In some cases, the bad actors have been known to review cyber insurance policies and financial information so they could better determine a ransom that they know the organization can afford to pay. These activities have all driven the ransom demands higher than ever.

In addition to ransomware, Business Email Compromise (BEC), also known as CEO Fraud, continues to run rampant in North America. These attacks take place through email phishing, vishing and smishing, and are very effective. Unlike ransomware, these attacks generally do not use malicious links or malware-infected documents that technical controls can flag. These attacks are almost purely done through social engineering. From requests for gift cards to large wire transfers, these attacks continue to hit organizations of all sizes, and in all industries, right in the pocketbook.

These attacks, even when successful, are far less visible to the general public, as they typically do not impede the day-to-day operations. This makes them hard to detect, unless the organization decides to publicly disclose the loss, something that is rarely done if not required. For organizations in industries that are tightly regulated, successful attacks are often only revealed within the filings of quarterly or annual financial reports.

Specifically in Mexico, their growing economy coupled with rapid digital growth has brought persistent challenges putting cybersecurity culture to test every day. According to the 2021 Internet Crimes Report published by the FBI, Mexico was the 13th most targeted country globally—ranking second in Latin America with a steady increase in the number of reported incidents in recent years. More on Mexico can be found in the South America regional section of this report.

Economic Impact

With ransomware payments averaging $570,000 in 2021, and with BEC losses topping $1.8 billion in 2020 according to the FBI, clearly a cyber attack can be a terminal event for many organizations. While cyber insurance may help a little, in an effort to control the hemorrhaging of funds related to these payouts, many insurers are raising rates significantly, requiring strict compliance to best practices, declining to insure organizations altogether, or working hard to limit the amount of payouts in the event of a successful cyber attack.

With ransom demands reaching $50 million or more, very few organizations can ignore the threat. In addition, once the victim of a malware or ransomware attack, organizations face significant costs related to digital forensics steps needed to find the initial infection vector and to close any back doors left by the attackers. Without finding and resolving any potential way the attackers could reinfect the organization, it is only a matter of time before they are reinfected.

Typical Business Profile

In North America, organizations of all sizes struggle with a lack of resources and funding in the battle against cyber crime. This is especially true of small and medium-sized organizations that may not be able to justify a full-time cybersecurity expert on staff. Many of these smaller organizations believe that they are too small to be a target for cybercriminals. Unfortunately for them, this is simply not true, especially in the modern ransomware age, where access to your own data has a tremendous amount of value for organizations that wish to stay in business. While the cost of hiring a dedicated cybersecurity expert is prohibitive for many smaller organizations, many of them can work with channel partners to manage their security tools and even their awareness and training programs, an approach that can lead to a great deal of value for the money.

Regardless of the specific type of attack, a cyber incident can be a serious problem for organizations involved in Mergers and Acquisitions (M&A) deals. The result of a successful attack can greatly devalue the price of the organization being acquired, trigger issues with regulatory bodies such as the Securities and Exchange Commission (SEC), or empty the coffers of the acquiring organization—all things that can scuttle an acquisition quickly.

Cultural Adoption

Awareness and education programs are maturing, with a focus on changing the behavior of employees and effecting a positive change in the overall security culture of the organization, as opposed to simply providing information. These mature programs often operate in the same ways and emulate marketing campaigns that target new and existing customers.

This means repeated exposure to the material over time, rather than having one big push per year. This approach keeps the material top-of-mind and impacts behaviors in a positive way. To put it in simple terms, in North America, employee education and training has advanced significantly to be utilized as a key method to secure organizations. According to the 2022 KnowBe4 Security Culture Report, the North America region scores more favorably than the rest of the world, with an average score of 74 (out of 100). This security culture score reflects the ideas, customs, and social behaviors that impact an organization's security.

General Attitudes

In North America, many organizations have become aware of the human-level risks employees face and have begun to address this by providing employees the education, training and skills needed to protect themselves and the organization from the attacks used by bad actors.

Key Takeaways

Clearly the problem of cyber crime is one that cannot be ignored and is not going away. The financial and operational impact is simply too great for even the largest of organizations to shrug off. While cyber insurance can soften the blow of a payout a little bit, it is not a reasonable replacement for adequate prevention and recovery methods and can do nothing to resolve the reputational damage caused by a significant attack.

Technology plays an important role in preventing and recovering from an attack; however, the human factor is by far the most common initial network entry point. In other words, it is at the human layer that an attack most often pivots from an attempt to a successful network intrusion. Most North American organizations have begun to recognize this danger and have started putting a significant focus on ways to help employees protect themselves from this constant barrage of attacks from the bad actors. Not only are they seeing the significant reduction of incidents related to email phishing through security awareness education, they are also embracing the training and education to drive a shift in the organization's overall security culture and maturing into long-term educational campaigns focused on this goal.

N. AMERICA	BASELINE	90 DAYS	1 YEAR
1-249	28.7%	17.4%	3.5%
250-999	30.2%	17.9%	4.6%
1000+	35.8%	17.4%	6%
Average PPP Across All Organization Sizes	32.4%	17.5%	4.7%

UNITED KINGDOM & IRELAND (UK&I)

Most Prevalent Issues

In 2021, the global pandemic that dominated our lives and businesses became business as usual. Working from home became the norm, and UK&I businesses adapted to the situation. Additionally, January 2021 officially marked the end of the Brexit transition period, which led to concerns over the loss of threat and data sharing capabilities with the EU.

The region continued to see consistent attacks originating from crime gangs based out of Russia. According to the National Cyber Security Centre (NCSC), China remained a highly sophisticated actor in cyberspace with increasing ambition to project its influence beyond its borders and a proven interest in the UK's commercial secrets. How China evolves in the next decade will probably be the single biggest driver of UK&I's future cybersecurity.

Ransomware continued to be the biggest public threat in 2021. In May 2021, a ransomware attack against the Irish Health Service Executive (HSE) disrupted Irish healthcare IT networks and hospitals. The organization took four months to completely recover from the attack, which caused significant real-life consequences to patients and their families.

The compromise of the software company SolarWinds and the exploitation of Microsoft Exchange Servers highlighted the threat from supply chain attacks, with many organizations in UK&I being adversely impacted.

Overall, the tactics of criminals remained broadly similar to what we have observed in previous years. Social engineering, exploiting unpatched vulnerable software and compromising weak credentials remained the prevalent attack vectors. With home-based and hybrid working, the social engineering attack surface increased, with many attacks coming via home landlines, SMS, social media or emails to both personal and corporate accounts.

Economic Impact

The economic impact of cyber crime is always difficult to estimate due to the lack of consistency in how the economic impact is measured and the inconsistency in incident reporting.

The National Fraud Intelligence Bureau receives all cyber crime reports that are submitted to Action Fraud. According to its stats, nearly half a million reports were filed, which amounted to losses of £2.6 billion.

Approximately 86,000 of the reported incidents in 2021 were related to online shopping and auctions. Additionally, with regards to cyber crime, there were nearly 14,000 reports of email and social media hacking.

In reality, this figure likely is not even the tip of the iceberg and the true economic impact of cyber crime. It likely runs into tens of billions of pounds every year for the UK&I economy.

Typical Business Profile

According to official UK government figures, 75% of UK businesses had zero employees and did not employ anyone aside from the owner(s) in 2021, while over 99% of businesses were small or medium size employing 0-249 people.

The service industries accounted for 76% of businesses, and 16% of SME (small-to-medium enterprise) employers were led by women. There were no all-male boards in the FTSE100.

Cultural Adoption

According to the 2022 KnowBe4 Security Culture Report, the UK&I region scores comparatively well with the UK security culture index score of 74 (out of 100) and Ireland at 78 (out of 100). This security culture score reflects the ideas, customs and social behaviors that impact an organization's security.

General Attitudes

The department for Digital, Culture, Media & Sport (DCMS) conducts an annual survey on cybersecurity awareness and attitudes. According to the results, three-quarters of businesses (77%) and seven in 10 charities (68%) say that cybersecurity is a high priority for their senior management. Both groups are relatively equally split between saying it is a “very” or “fairly high” priority.

According to the Cyber Security Breaches Survey 2021 conducted by the UK government, it is more common for larger businesses to say that cybersecurity is a high priority (95% of medium businesses and 93% of large businesses vs. 77% overall). The same is true for high-income charities (96% of those with £500,000 or more vs. 68% of charities overall).

The business sectors that attach a higher priority to cybersecurity are:

- Finance and insurance (72% say it is a very high priority vs. 37% of all businesses)
- Information and communications (62%)
- Health, social work and social care (56%)

These three sectors have consistently treated cybersecurity as a higher priority. By contrast, but also in line with last year, the food and hospitality sector and construction sector both tend to treat cybersecurity as a lesser business priority (only 62% and 64% say it is a high priority vs. 77% of businesses overall).

Key Takeaways

COVID-19 has been the great catalyst that has accelerated digital transformation at perhaps a faster rate than organizations and society as a whole were ready for. While this has brought about many benefits, there has been much technical debt accrued.

While ransomware has dominated the headlines, NCSC highlighted the growing cybersecurity threats in intensity, complexity and severity. The growing dependence on digital infrastructure and technologies, particularly during the time of remote or hybrid working, has also increased the exposure to risk.

Social engineering remains one of the biggest threats both in cyber crime and broader fraud. According to Gov.UK, of the 39% of UK businesses who identified an attack, the most common threat vector was phishing attempts (83%). There is also a growing challenge of maintaining software and systems to ensure they are up to date and protected. Supply chain risks are also a major concern, both for commercial software and open source.

As part of its plan to tackle these, the government is proposing the forthcoming National Resilience Strategy and a Digital Strategy to set out clear visions of the nation’s ambitions to build a more inclusive, competitive and innovative digital economy for the future.

With one eye on the future, it is important though for the UK&I region to keep the other eye firmly on the present and to strengthen organizations and individuals against the common forms of attacks that have proven successful time and time again. If credentials cannot be protected, systems not patched or individuals not provided security awareness training, the path to an innovative digital economy could very well be a bumpy one.

UK & IRELAND	BASELINE	90 DAYS	1 YEAR
1-249	26.2%	16.7%	3.9%
250-999	27.7%	16.2%	4.3%
1000+	32.7%	17.5%	8.3%
Average PPP Across All Organization Sizes	30%	17%	5.5%

EUROPE

Most Prevalent Issues

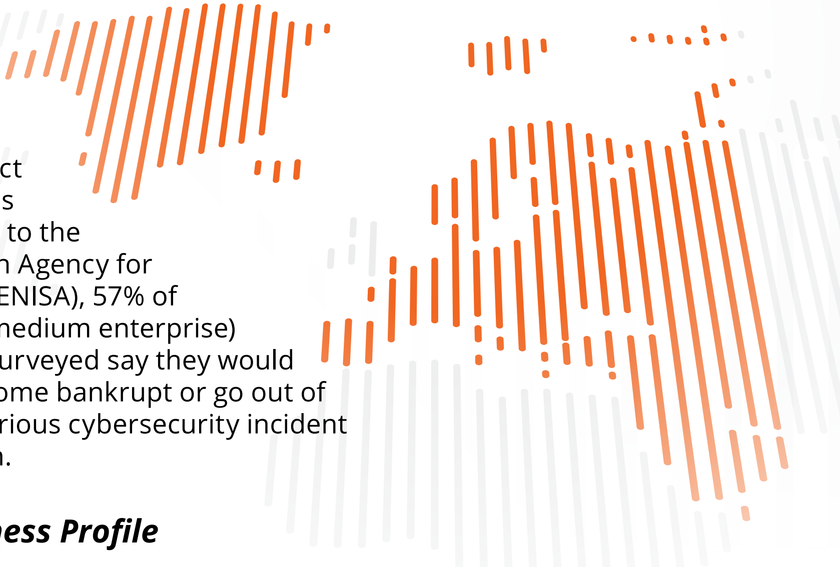
The COVID-19 crisis pushed the reliance on information and communication technology to an all-time high. To stay in business, organizations had to resort to alternative business continuity measures including adoption of new cloud services, creating direct-to-consumer services, introducing new forms of digital payment and enabling staff to work remotely. These changes had to be done at an accelerated pace, often opening up critical security gaps.

Large enterprises, in general, have the capabilities and resources at hand to withstand the impact of such a major crisis, while small and medium-sized organizations suffer most. Next to making up the vast majority of organizations in the EU, these small and medium-sized organizations are also the most vulnerable group, with cybersecurity budgets often limited and resilience to major catastrophes low.

Major incidents threatening Europe have shown to have far reaching consequences. With the reliance on the internet in Europe only increasing, crises like the COVID-19 pandemic, the war in Ukraine, and the increase in cyber crime overall can have a devastating impact on organizations. Prevalent cybersecurity issues, according to Europol, are caused by phishing and social engineering attacks. Given that the EU represents the largest economy in the world, it is crucial to decrease the risk of falling victim to such attacks by increasing security awareness in people.

Economic Impact

The economic impact of cyber crime in Europe is hard to accurately determine. Unclear metrics, undisclosed incidents and a general lack of financial data make it close to impossible to provide an accurate accounting.



Though no clear data is available, it is clear that the economic impact of cyber crime is high. According to the European Union Agency for Cybersecurity (ENISA), 57% of SME (small-to-medium enterprise) organizations surveyed say they would most likely become bankrupt or go out of business if a serious cybersecurity incident were to happen.

Typical Business Profile

Small and medium-sized enterprises represent 99% of all businesses in the EU. According to Statista, as of 2020, approximately 93.3% of enterprises in the non-financial business economy of Europe were micro-sized and employed up to nine people. In the same year, approximately 5.7% were defined as small businesses (10-49 employees), 0.9% were medium-sized (50-249) and 0.2% were large businesses that employed 250 or more people.

Cultural Adoption

According to the 2022 KnowBe4 Security Culture Report, Europe does fairly well with an overall security culture index score of 73 (out of 100). This security culture score reflects the ideas, customs and social behaviors that impact an organization's security and the adoption of security by the employees of an organization.

Various countries in the EU are actively developing awareness of cybersecurity among their citizens and organizations. Ranging from awareness campaigns aimed at consumers, to actively providing open-source intelligence and information on indicators of compromise (IOC) to organizations. These efforts, and the increase of attention to cyber crime by national and local media, has led to an increased realization of the need to adopt security as a basic hygiene factor.

General Attitudes

Digital transformation is one of the major developments that drive European organizations forward. While this development is a positive thing, it also increases the need for a higher resilience against cyber crime. Two key technologies of digitization, the adoption of the Internet of Things technologies and the introduction of Artificial Intelligence, are also being criminally exploited.

Most interesting is the changing expertise landscape. Organizations are increasingly looking for skills associated with overall security management, such as Risk Management and Service Management, while skills like manual penetration testing and technology management are becoming less important due to advances in automation and artificial intelligence.

Overall, the adoption of cybersecurity in organizations is being characterized by the need for cybersecurity to prove its value as a business enabler.

Key Takeaways

The reliance on information and communication technology driven by the COVID-19 pandemic leads to the challenge surrounding cybersecurity. This reliance on communication technologies is being criminally exploited in the form of cyber attacks. Social engineering, ransomware and supply chain attacks are specially designed to cripple businesses. Phishing remains the primary attack vector, making people a critical part of any organization's security posture.

Due to the shortage of skilled labor and the increasing number of cyber crime incidents in Europe, organizations need to focus on employees as a critical security layer. Employees are viewed as an asset they need to protect, but also as one they can enable as a part of their overall security posture and firewall. With the average Phish-prone Percentage for Europe at 29.9%, it is imperative for organizations to invest in security awareness programs to enable people to make better security decisions.

EUROPE	BASELINE	90 DAYS	1 YEAR
1-249	27.8%	17.9%	4.2%
250-999	28.2%	18.2%	6.7%
1000+	31.1%	18.9%	8%
Average PPP Across All Organization Sizes	29.9%	18.5%	6.3%

AFRICA

Most Prevalent Issues

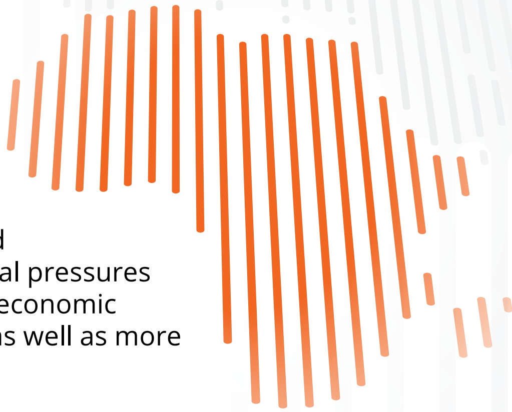
As reported by the Africa Center for Strategic Studies, Africa faces a growing array of cyber threats from espionage, critical infrastructure sabotage and organized crime. Still, only about a third (17) of Africa's 54 countries have completed a national cybersecurity strategy. Additionally, the countries with strategies fall short as their plans do not include key stakeholders, adequately address capacity building and are not frequently enough adapted to the evolving threats. Previous efforts to improve cross-border cyber cooperation in Africa, most notably the AU-sponsored Convention on Cyber Security and Personal Data Protection (the Malabo Convention), have not yet achieved adequate national-level support.

One of Africa's biggest cybersecurity issues is the skills shortage. The continent faces a growing 100,000-person gap in certified cybersecurity professionals. Many businesses, agencies and consumers lack cyber awareness and businesses fail to implement basic cybersecurity controls.

Governments frequently do not adequately monitor threats, collect digital forensic evidence and do not prosecute computer-based crime.

Economic Impact

As incidents and financial impact are not officially disclosed, it is difficult to know how much cyber crime really impacts the African economy. A staggering 96% of cybersecurity incidents go unreported or unresolved, meaning that cyber threats in Africa are likely much worse than formally recognized.



Data published in the 2020 Annual Report of the South African INSURANCE CRIME BUREAU shows that the rapid growth in Africa's digital economy has outpaced developments in providing adequate cybersecurity, and combined economic, political and social pressures are causing an increase in “desperate economic crime,” including both physical crime as well as more sophisticated fraud and cyber crime.

The 2021 ITWeb and KnowBe4 Ransomware Survey in South Africa showed that 32% of the respondents had been subject to a cyber extortion attack. And 4% of those who fell victim paid the ransom demand—making this a lucrative region for ransomware gangs.

Apart from the direct losses experienced from cyber extortion attacks and cyber fraud, the lack of adequate cybersecurity and protections result in many countries and organizations not being able to benefit from the opportunities of the Fourth Industrial Revolution. The majority of African nations are underprepared to deal with the advances in AI, wireless communications, quantum computing and automation that are likely to characterize the coming decade. This means that African organizations will not be able to benefit economically from these technologies if they are not adequately prepared to face the cyber threats.

Typical Business Profile

Africa's 54 countries are diverse in terms of population, development levels, growth rates and stability. While Nigeria has nearly 190 million people and Ethiopia and Egypt have over 90 million people each, most African nations have populations below 20 million. Africa's potential as a growth market for business remains underestimated and misunderstood. More than 400 companies in Africa earn annual revenues of $1 billion or more; and they are, on average, faster growing and more profitable than their global peers.

KnowBe4's Phishing by Industry Benchmark Report is based on a total of 7,490 phishing simulation tests across 300 African organizations. Of these, 58% of the organizations are SMEs (small-to-medium enterprise) with 1-249 users, 28% are medium with 250-999 employees and 14% of the organizations have 1000+ users.

The majority of the data set is derived from organizations in South Africa, followed by Kenya, Nigeria and Botswana.

Cultural Adoption

Africa's current population of around 1.2 billion people is projected to reach 1.7 billion by 2030. African innovators are often driven by a deeper purpose. They look at Africa's high levels of poverty and its gaps in infrastructure, education and healthcare, and they see human issues they feel responsible for solving. In considering risks, instability, access to capital, corruption and cybersecurity are of greatest concern to potential investors and entrepreneurs. The growing rate of mobile device consumers, many of which are first time internet users, lack basic cyber literacy skills.

KnowBe4's African Cybersecurity and Awareness Report 2021 uncovered that the pandemic still plays a major role in influencing working behaviors and patterns amongst the 800 respondents from eight African countries. Only 38% of respondents have returned to their offices or are accessing the internet from their office network, while 55% continue to work from home.

Of the respondents, 72% said they were concerned about cyber crime but also lacked the very basic understanding of what type of threats they are actually exposed to. Also, 54% of respondents did not know what a ransomware attack was, 26% have experienced a social engineering attack over the phone (vishing) and 34% have lost money because they fell victim to a scam. The pandemic's effects continue to influence employee behavior, with 55% of respondents planning to continue to work from home.

General Attitudes

With a median age of just 19.7 years, Africa is the youngest population in the world. And Africa's growing youth is demanding access to global connectivity and is driving technology adoption and digitalization: mobile smart device ownership is growing exponentially, social media use is increasing and the Internet of Things (IoT) is becoming a reality. According to the IMF (International Monetary Fund), sub-Saharan Africa is the only region in the world where nearly 10% of its gross domestic product is generated through mobile money. People use their mobile devices for salaries, payments, bills and shopping. KnowBe4's African Cybersecurity and Awareness Report 2021 uncovered that 71% of the respondents from eight African countries use their mobile data to access the internet, while 63% use their mobile phone for mobile banking and payments. WhatsApp remains the popular app of choice at 91%, with email at 75% and Telegram at 52%.

With this growing prosperity and digitization, however, comes new risks and vulnerabilities that could undermine the progress. More work needs to be done by both companies and governments alike to address Africa's users "unconscious incompetence" with regards to cybersecurity and protect its citizens from cyber crime.

Key Takeaways

The KnowBe4 African Cybersecurity and Awareness Report 2021 reveals a security threat landscape that has modified and adapted to changing working conditions and security concerns over the past year. Only 40% of the respondents believe they fully understand their security roles and responsibilities and only 28% believe that their employers have adequately trained them in cybersecurity. Attacks against African organizations are consistent with attacks in other countries, such as cyber extortion, banking Trojans, investment scams (including crypto scams), business email compromise (BEC) and social engineering for financial fraud. However, the threat is amplified, as Africans are inherently less aware of cyber threats than other countries. Relatively basic scams like BEC, phishing, vishing and smishing are successful, especially amongst small, underequipped businesses. Ransomware has increased in popularity. With more pressing issues to solve, such as youth unemployment, poverty, inequality and violent crime, there is a lack of prioritization and investment for cybersecurity amongst both businesses and governments.

Businesses in this region often cannot afford even the most basic security controls. Those that can invest struggle to find those who have cybersecurity skills. Public-private partnerships are needed to assist Africa in its cybersecurity challenges. The private sector, particularly financial services sectors, possess human capital, infrastructure, capabilities and expertise in cybersecurity that governments lack. It remains critical that organizations train employees and their customers around security best practices. Governments and education institutions need to invest in expanding the much-needed security professional capacity as well as making cybersecurity awareness a life skill for every youth entering the workforce.

AFRICA	BASELINE	90 DAYS	1 YEAR
1-249	30.2%	24.8%	8.1%
250-999	27.4%	21%	12.7%
1000+	32.4%	17.9%	4%
Average PPP Across All Organization Sizes	31.4%	18.8%	5.4%

SOUTH AMERICA

Most Prevalent Issues

Cyber attacks come in all shapes and sizes in Latin America. Most notably worms, trojans, spyware, ransomware and especially phishing, are part of the extensive list.

The global COVID-19 pandemic caused profound changes in society, affecting all companies and people in different aspects. Due to the spread of the virus, numerous organizations have shifted to remote working, which has had a strong technological impact, especially with regard to cybersecurity.

With interconnectivity more present than ever and with the expansion of remote work, new challenges in information security have arisen, increasing risks to exponential levels. Once the corporate environment is changed to a remote working structure, it needs to have its security well designed and configured to avoid malicious actors causing business damage.

On the global stage, two Latin American countries appear among the 10 nations most affected by phishing attacks. Brazil appears at the top of the ranking with 12.4% and Ecuador occupies the 10th position on the list with 10.7%. In other words, the sum of attacks in these two South American countries represents 23.1% of phishing attacks worldwide.

Phish-prone Percentage

In 2021, we identified that the Phish-prone Percentage in Latin America was 39.9%. The numbers point to an increase of 6.1% compared to the 33.7% recorded in the year 2020 and published in the 2021 Phishing By Industry Benchmarking Report.

It is notable that South America is the global region most susceptible to phishing attacks, compared to other regions such as North America (32.4%), Asia (34.6%), Europe (29.9%) and Oceania/Australia/Asia (34.5%).

When companies with employees above 1,000 are evaluated, Peru appears at the top of the Phish-prone Percentage ranking with 72.7%, followed by Brazil (65.1%) and Colombia (46.6%).

Economic Impact

The hyper-connectivity of the last few decades has broadened the landscape of cyber activities and also the crosshairs of cyber attackers. Every user, company and government is a target, and therefore, security must be seen as an important and highly prioritized investment of resources.

Due to several technical and financial factors, cyber attacks often go unnoticed, but certain offensive actions can pose serious threats and generate significant economic losses.

Estimates of the financial losses caused by cyber attacks increase year after year. According to the Cybersecurity in Latin America Report by Statista, the cybersecurity market in Latin America was valued at almost $12.9 billion in 2019. This amount is expected to exceed 25 billion dollars by 2025. Brazil, Mexico and Colombia appear as the countries most targeted by cybercriminals. Together, these three nations account for almost 9 out of 10 attacks recorded in Latin America.

Ransomware is one of the most common types of attacks carried out by cybercriminals in Latin America. In the 2020 survey, 65% of respondents in Brazil said that the organization they worked for had been attacked by ransomware, while 44% of respondents in Mexico and Colombia said their organization had been hit by ransomware.

Typical Business Profile

Companies from all market segments have been targets of cyber attacks in Latin America. In Brazil, for example, cases of ransomware attacks were reported against companies in sectors such as health, retail, finance and government institutions.

Even smaller companies that had no tradition of directing investments to the information security area are already dedicating large portions of financial resources in order to contain possible cyber attacks.

In just one case recorded in 2021, an e-commerce company recorded losses of more than R$3.4 billion (Brazilian Real) after the company had its websites hijacked in a ransomware attack.

Cultural Adoption & General Attitudes

Governments in several Latin American countries are working to create well defined information security strategies. Companies and organizations are also creating and implementing new security measures aimed at mitigating all types of future cyber attacks.

As they are among the most focused targets by cybercriminals, the security teams of companies in Brazil, Mexico and Colombia dedicate more than half of their working hours to preventing cyber threats. When it comes to efforts to respond to attacks, these three countries spend on average one-third of their efforts.

For example, in 2020, Brazil stood out as the country in Latin America where there was the highest percentage of phishing attacks. Following this alarming data, the volume of investments in the security area has grown exponentially in medium and large companies. There is a growing demand in the market for professionals who work on implementing security awareness.

In addition to the incidents themselves, security awareness professionals have reported greater adherence to the treatments proposed, ranging from phishing, ransomware, money laundering and other threats.

Key Takeaways

Zero trust assists in decreasing risk: Principles related to a zero trust approach, to include implementation of multi-factor authentication (MFA) or hardware tokens and the principle of least privilege, have the potential to decrease organizations' susceptibility to the top attack types, particularly ransomware and BEC.

Develop a response plan for ransomware: All industries and companies could be at risk for a possible ransomware attack. The key is how quickly teams respond with the information necessary in the first critical moments. This will make all the difference in the amount of time and money lost during a response.

Adopt new-school security awareness training: It is critical to implement a robust plan, including phishing simulations leveraging real-world examples. Additionally, it has never been more critical to train employees using a new-school security awareness program to leverage the detection of social engineering and phishing attacks.

S. AMERICA	BASELINE	90 DAYS	1 YEAR
1-249	30.9%	24.7%	1.8%
250-999	30%	22.2%	9.8%
1000+	45.6%	19.3%	0.8%
Average PPP Across All Organization Sizes	39.9%	20.5%	3.2%

APAC, AUSTRALIA AND NEW ZEALAND

Most Prevalent Issues

APAC

Throughout the APAC region, including Australia and New Zealand, ransomware, supply chains, BEC, online shopping scams, fraud, online banking, identity theft and romance scams are consistent threats, with phishing the most successful attack vector.

According to the IBM Security X-Force Threat Intelligence Index 2022 which includes data for 2021, Japan, Australia and India were the most-attacked countries in Asia. This was consistent with the findings reported in the 2021 Verizon Data Breach Investigations Report. The most common type of breaches that took place in APAC were caused by financially-motivated attackers who were phishing employees for credentials, and then using those stolen credentials to gain access to email accounts and web application servers. Verizon also reported that 70% of attacks in APAC contained a social engineering action.

Australia

Over the 2020–21 financial year, the Australian Cyber Security Centre (ACSC), received over 67,500 cyber crime reports, an increase of nearly 13% from the previous financial year. A cyber incident is reported every eight minutes in this region. The global COVID-19 pandemic has been, and continues to be, a trending topic in phishing and spear phishing campaigns designed to obtain valuable information and financial gain in addition to the usual cybercriminal playbook.

According to the Office of the Australian Information Commissioner, health service providers were the most targeted sector followed by Finance, Legal, Accounting and Management Services, Personal Services and finally Education and Insurance. In addition, approximately one quarter of reported cyber incidents were associated with critical infrastructure or essential services.

Economic Impact

According to the Global State of Industrial Cybersecurity 2021: Resilience Amid Disruption Report released by Claroty, 80% of organizations in the APAC region were affected by ransomware attacks in 2021, with 51% paying the ransom.

According to the ACCC (Australian Competition and Consumer Commission), Australians lost a record AU$323 million to scams in 2021 (up a staggering 84% from the previous year). Meanwhile, 790 Singaporean victims fell prey to the recent OCBC Bank smishing scam, with a total loss amount of SGD$13.7 million, illustrating that the potential cost to APAC business is huge.

Typical Business Profile

APAC

The Asia-Pacific region has a population of 4.2 billion. With over 38 countries, it is one of the world's most diverse regions and home to economies that are at the top of digital and societal developments worldwide. This region is also seen as global leaders in high-speed internet access and usage.

Australia

In 2021, there were 2,447,026 actively trading businesses in the Australian economy.

New Zealand

In 2021, there were 562,521 actively trading businesses in the New Zealand economy.

Cultural Adoption

The Adobe 2022 APAC Digital Trends Report predicted that by 2025, an additional 333 million people will be expected to start using mobile internet in APAC for the first time—and they are likely to behave differently than existing internet users.

As remote and hybrid working arrangements continue, there is an ongoing need to address human error as it accounts for the majority of successful cyber attacks through all forms of technology.

General Attitudes

In the 2021 Norton Cyber Safety Insights Report, 79% of Australians, 77% of New Zealanders and 73% of Japanese respondents agreed that “remote work has made it much easier for hackers and cybercriminals take advantage of people” and more than half of adults are more worried than ever about being the victim of cyber crime, but a similar proportion do not know how to protect themselves from it.

Across the APAC region, people are actively seeking out guidance and information on how to increase their online safety and protect their privacy. Unfortunately, they often do not know where to go or how to do it.

The reality is that cyber threats are so pervasive, that keeping individuals and businesses safe requires a combined effort from the government, business leaders, IT departments and employees alike. There is no panacea or magic technology solution that will protect your business. Everyone needs to be educated about potential threats and how to avoid them.

According to KnowBe4’s annual 2021 APAC survey, fewer than half (45%) of APAC IT decision-makers believe that it is everyone’s responsibility to protect the organization from cyber attacks.

APAC	BASELINE	90 DAYS	1 YEAR
1-249	30.2%	21.1%	4.4%
250-999	32.6%	19.2%	6.2%
1000+	36.7%	15%	5.2%
Average PPP Across All Organization Sizes	34.5%	16.9%	5.4%

Given the IT department’s lack of clarity, it is unsurprising that employees are also unaware of who is responsible for cybersecurity:

- Almost a quarter (24%) say technology should be protecting the organization from cyber attacks.
- 21% believe it is the IT department’s responsibility.
- 11% believe it is the government’s responsibility.

Training regarding cybersecurity impacts employees’ views and makes them more likely to take responsibility for their own role in keeping the organization safe. Those who have received training are more likely to believe it is the employee’s responsibility (16%) compared to those who have not received training (11%).

In contrast, those who have never received training are more likely to believe it is the IT department’s responsibility (29% compared to 17%).

Key Takeaways

Our annual 2021 APAC Survey found seven in ten (70%) of IT decision-makers feel the Australian and Singaporean governments should be doing more to protect businesses from cyber attacks. Also, only 52% of these IT decision-makers say they are confident they understand their organization’s responsibilities regarding government reporting of cyber incidents and data breaches.

IT leaders and businesses across APAC are not feeling supported by the government when it comes to security issues and believe the government should be doing more including:

- Providing more education and awareness to all our citizens about the cyber risks and how to stay safe online (45%)
- Providing more training for businesses on cyber risks (42%)
- Providing more funding for businesses for cyber protection (38%)

The education required for those in IT about their obligations and commitments also needs to be provided for the general public regarding how to stay safe online both at home and at work.

KEY TAKEAWAYS: THE VALUE OF NEW-SCHOOL SECURITY AWARENESS TRAINING

The results from all three phases of the study reveal several conclusions:

- **Every organization is at serious risk without new-school security awareness training.** With an average industry baseline PPP of 32.4%, organizations could be exposed to social engineering and phishing scams by a third of their workforce at any given time.
- **Any organization can strengthen security through end-user training in as little as three months.** The power of a good training program is to set up a consistent cadence of simulated phishing and social engineering education in a rapid timeframe.
- **An effective security awareness training strategy can help accelerate results for all organizations.** The struggle of some enterprise leaders to successfully implement security training effectively across the organization is not surprising. Leaders can set themselves up for success by assessing their goals and plotting an organizational strategy before rolling out training.

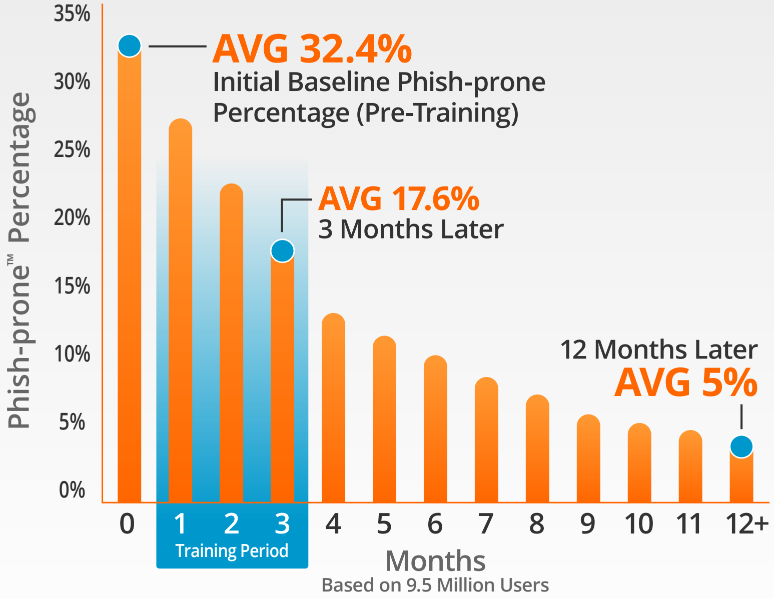
EXECUTIVE TAKEAWAYS

Security and risk management leaders need to understand that in order to favorably change overall security behaviors within their organizations, their programs must have:

- A clearly defined and communicated mandate
- A strong alignment with organizational security policies
- An active connection to overall security culture and human layer of security
- The full support of executives

Without consistent and enthusiastic executive support, raising security awareness within an organization is certain to fail.

The KnowBe4 System Really Works



Source: 2022 KnowBe4 Phishing by Industry Benchmarking Report

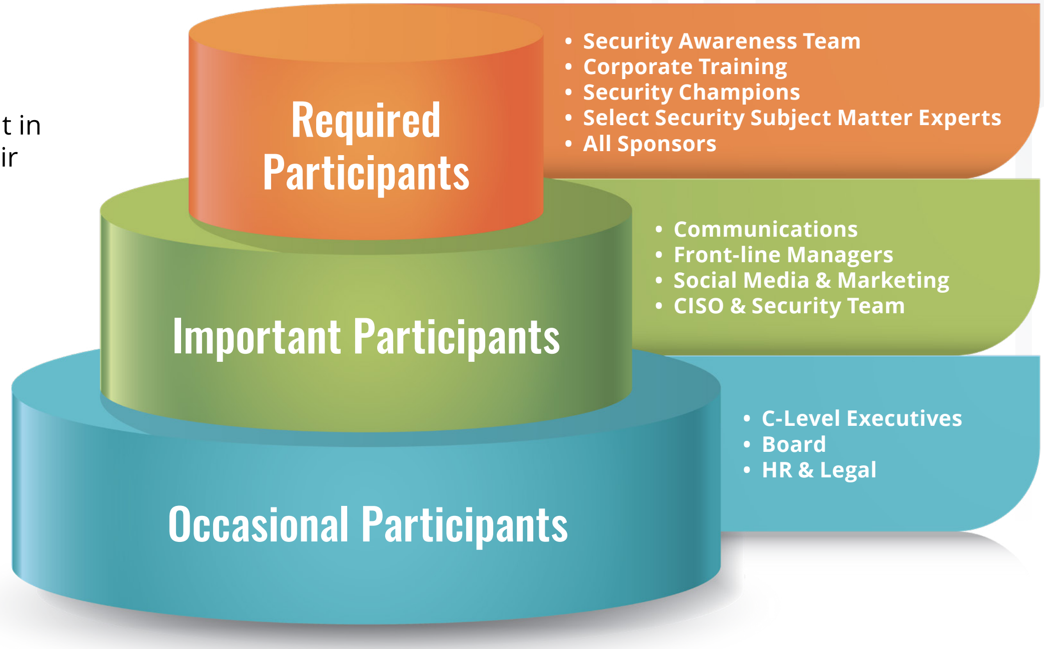
Note: The initial Phish-prone Percentage is calculated on the basis of all users evaluated. These users had not received any training with the KnowBe4 console prior to the evaluation. Subsequent time periods reflect Phish-prone Percentages for the subset of users who received training with the KnowBe4 console.

EXECUTIVE TAKEAWAYS

Security and risk management leaders need to understand that in order to favorably change overall security behaviors within their organizations, their programs must have:

- A clearly defined and communicated mandate
- A strong alignment with organizational security policies
- An active connection to overall security culture
- The full support of executives

Without consistent and enthusiastic executive support, raising security awareness within an organization is certain to fail.



Required Participants
- Security Awareness Team
- Corporate Training
- Security Champions
- Select Security Subject Matter Experts
- All Sponsors

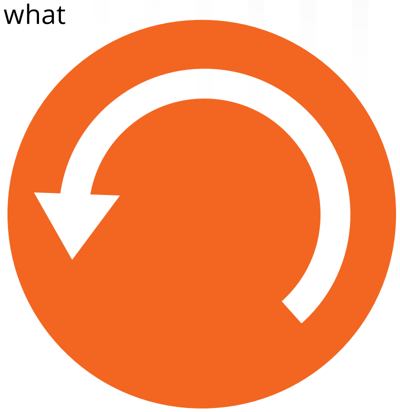
Important Participants
- Communications
- Front-line Managers
- Social Media & Marketing
- CISO & Security Team

Occasional Participants
- C-Level Executives
- Board
- HR & Legal

Security and Risk Management executives can ensure the success of their programs by:

- **Fostering a Security Culture:** The human element is the most critical part of an organization's security infrastructure. All employees should understand what their role and responsibility is to protect the organization and themselves from a cyber attack. Security culture, as defined by KnowBe4, is the ideas, customs and social behaviors of an organization that influence their security. Executives need to ensure they are fostering an environment that is security ready by investing in both the focus of their security awareness and training program and the readiness level of their humans.
- **Role Modeling:** If you expect your organization to do the right thing, you must lead them accordingly. Executives should be active participants in all aspects of driving security awareness throughout their organizations, which includes participating in the same security awareness training requirements that the rest of their employees are expected to complete.
- **Engaging a Pro:** Security awareness content is unlike any other. Expertise goes into not only the design of the content, but also ensuring that the content leads to a positive learning experience and ultimately favorable secure behavior change. In an industry where content is king, the recommendation is to align with a vendor that can provide you with multiple flavors, versions and varieties that appeal to all different learning styles. Forcing your audience into a singular learning style limits the experience, material consumption and overall retention. It may be tempting to leverage your internal training organization to lead this program development, or to partner with a vendor that provides a one-size-fits-all approach. Both options will lead to a long-term inability to shape your audience's security-related thoughts and actions.

- **Thinking Like a Marketer:** In parallel with content and simulated phishing campaigns, add frequent and relevant messaging in the form of ancillary supporting materials (posters, digital signage, newsletters, etc.) and find opportunities during cross-business meetings and presentations to reinforce the big takeaways. Holding "lunch and learns" for employees and table-top exercises during leadership meetings provides an engaging way to disseminate information and engage directly with your audience.
- **Mobilizing a Security "Culture Carrier" Program:** Most security and risk programs lack the necessary resources to properly engage a global organization. Security "culture carrier" programs go by many different names, such as "Security Champions," "Security Ambassadors," "Security Liaisons," "Security Influencers," and more. Regardless of what you call it, a culture carrier program provides an organizationally dispersed team of advocates who can reinforce security messaging and learning at local levels. The responsibility factor is also in play here. Many employees believe that driving security awareness is someone else's responsibility. By enrolling local influencers either through manager nomination or volunteering, you create a network of security go-to-people who can relate with local communities and start to help shape the overall security culture.
- **Adding Simulated Phishing Tests:** As we've shared through this research, by adding frequent simulated phishing campaigns to your overall security awareness program, you will increase your employee's resilience to being compromised, and also raise their ability to spot a suspicious email.
- **Increasing Frequency:** At all times, you are either building strength or allowing atrophy. Our research shows that most organizations not seeing favorable behavior change were limiting the frequency of their program (both content and simulated phishing) to annual, twice annual or quarterly. By testing so infrequently, you are essentially conducting moment in time baseline tests that you cannot meaningfully compare. The recommendation is to provide your audience monthly content and simulated phishing campaigns (twice monthly for high risk targets). There needs to be a regular cadence for the appropriate conditioning to take place and for behavior change to take hold. Security and risk management executives may fear that this frequency is too much, but in actuality, it is helping build the right level of security muscle memory to combat the aggressive and ever-changing attack strategies of today and tomorrow.
- **Hiring the Right People:** Security awareness programs are often led by security practitioners who were either chosen to take on the task no one wanted or had extra time to deal with this "training" stuff. However, managing a program like this requires a certain level of experience and expertise. Target creative candidates who are aware and well versed in how to drive organizational development and behavior change through learning.
- **Defining Objectives:** Determine upfront what the success criteria of your program are and how you will measure against them. Otherwise it is impossible to measure your program's effectiveness and determine inherent value.



- **Measuring Effectively:** The use of metrics that reinforce desired behaviors is important to help protect systems, employees and data. Don't fall into the trap of selecting too many measurement criteria; that only leads to measuring irrelevant areas and/or underdelivering on promised organizational outcomes. Employing measurable data and training that can be frequently quantified and qualified is paramount. Also, ensure that program metrics are connected not only to overall organizational security objectives, but corporate objectives.
- **Motivating Employees:** Be intentional and consistent in how you use positive and negative reinforcement to encourage your audience to complete required training, adhere to security policies and demonstrate ongoing, favorable, secure behavior. Using motivators increases accountability and the employees' overall role in driving a more secure culture.

GETTING STARTED

KnowBe4 is helping tens of thousands of IT pros like you to improve their cybersecurity in fields like finance, energy, healthcare, government, insurance and many more.

With KnowBe4, you have the best-in-class phishing simulation and training platform to improve your organization's last line of defense: **Your Human Firewall**.

We enable your employees to make smarter security decisions, every day. We help you deliver a data-driven IT security defense plan that starts with the most likely "successful" threats within your organization—your employees. The KnowBe4 methodology really works. Ready to get started?

4 Steps for Phishing Your Users

It's clear that organizations can radically reduce vulnerability and change end-user behavior through testing and training. Take these steps to get your organization on the right track to developing your human firewall.

1 **Conduct Baseline Testing:** Conducting a baseline test is the first step in demonstrating the need for security awareness training to your senior leadership. This baseline test will assess the Phish-prone percentage of your users. It's also the necessary data to measure future success.

2 **Train Your Users:** Use on-demand, interactive, and engaging computer-based training instead of old-style PowerPoint slides. Awareness modules and videos should educate users on how a phishing or social engineering attempt could happen to them.

3 **Phish Your Users:** At least once a month, test your staff to reinforce the training and continue the learning process. You are trying to train a mindset and create new habits. It takes a while to set that in motion. Simulated social engineering tests at least once a month are effective at changing behavior.

4 **Measure Results:** Track how your workforce responds to both training and phishing. Your goal is to get as close to zero percent Phish-prone as possible.

Plan Like a Marketer, Test Like an Attacker

While every leader can reduce risk by targeting employee PPP, there are several best practices that can bring about lasting change.

01 **Use real-world attack methods**

Your simulated phishing exercises must mimic real attacks and methodologies. Otherwise, your "training" will simply give your organization a false sense of security.

02 **Don't do this alone**

Involve other teams and executives, including Human Resources, IT and Compliance teams, and even Marketing. Create a positive, organization-wide culture of security.

03 **Don't try to train on everything**

Decide what behaviors you want to shape and then prioritize the top two or three. Focus on modifying those behaviors for 12-18 months.

04 **Make it relevant**

People care about things that are meaningful to them. Make sure your simulated attacks impact an employee's day-to-day activities.

05 **Treat your program like a marketing campaign**

To strengthen security, you must focus on changing behavior, rather than just telling staff what you'd like them to know. Give them the critical information they need, but stay focused on conditioning their security reflexes so your workforce becomes an effective last line of defense.

CREATE YOUR HUMAN FIREWALL

Free Phishing Security Test

Ready to start phishing your users? Find out what percentage of your employees are Phish-prone with your free phishing security test. Plus, see how you stack up against your peers with the Phishing Industry Benchmarks! You can accomplish the same dramatic end results of the study with KnowBe4's Phishing Security Test.

ADDITIONAL RESOURCES

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 actors do

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

ABOUT KNOWBE4

KnowBe4 is the world's largest integrated security awareness training and simulated phishing platform. Realizing that the human element of security was being seriously neglected, KnowBe4 was created to help organizations manage the problem of social engineering through a comprehensive new-school security awareness training approach.

This method integrates baseline testing using real-world mock attacks, engaging interactive training, continuous assessment through simulated phishing, and vishing attacks and enterprise-strength reporting, to build a more resilient organization with security top of mind.

Tens of thousands of organizations worldwide use KnowBe4's platform across all industries, including highly regulated fields such as finance, healthcare, energy, government and insurance to mobilize their end users as a last line of defense and enable them to make smarter security decisions.

For more information, please visit www.KnowBe4.com

KnowBe4
Human error. Conquered.

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