EDUCATION

SPONSORED BY:

KnowBe4
Human error. Conquered.

2023 SECURITY AWARENESS TRAINING REPORT

MARKET PREDICTED TO GROW FROM $5.6B IN 2023 TO $10B+ IN 2027

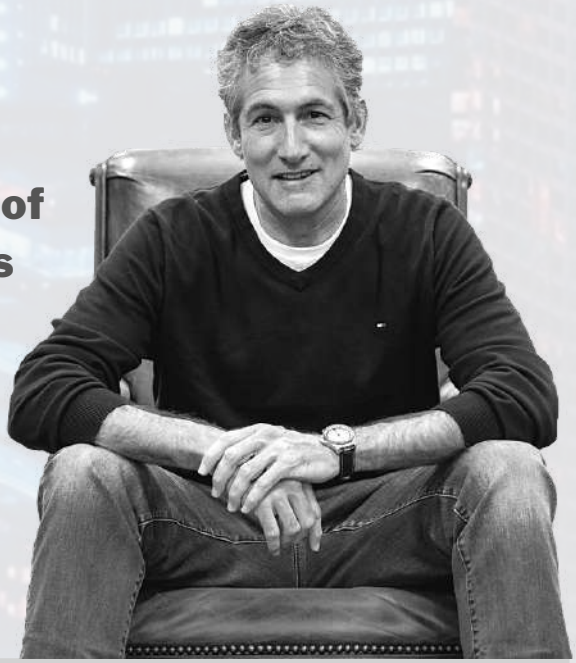
CYBERSECURITY VENTURES

SECURITY AWARENESS TRAINING

BOOMING MARKET

Cybersecurity Ventures predicts the security awareness training market will exceed $10 billion annually by 2027.

Steve Morgan, founder of Cybersecurity Ventures



As the damage caused by cybercrime continues to escalate, industry leaders are bolstering their efforts to combat the threat. Consequently, the demand for security awareness training will continue rising, and new entrants with venture funding will crowd into the space.

– Steve Morgan, founder of Cybersecurity Ventures and Editor-in-Chief at Cybercrime Magazine

SECURITY AWARENESS TRAINING

TABLE OF CONTENTS

SECURITY AWARENESS TRAINING

INTRODUCTION

In Jan. 2023, the U.S. Department of Justice announced the disruption of the Hive network, a ransomware group known to have sabotaged hospitals, school districts, financial firms, and critical infrastructure worldwide.

Charlie Osborne, Editor-at-Large
Cybercrime Magazine

While prolific and dangerous, Hive is only one entity in a broad criminal ecosystem predicted to inflict $8 trillion in damages in 2023 alone – making cybercrime the world's third-largest economy behind the U.S. and China.

Cybersecurity Ventures expects cybercrime costs to grow by 15 percent per year over the next two years, reaching $10.5 trillion USD annually by 2025.

INTRODUCTION

As the situation worsens, governments, industry leaders, academia, and private companies are taking action.

In 2021, The White House issued an executive order intended to improve the nation's cybersecurity posture by promoting zero-trust architectures and enforcing supply chain security standards, among other decrees.

Cybersecurity has also entered the boardroom. The most experienced workers are in high demand in a zero-unemployment marketplace. Organizations are adopting technologies including automation, machine learning (ML), and artificial intelligence (AI) solutions to cope with current and emerging threats.

However, security requires a holistic approach. Improving device and network security with tools and technologies is important, but is only one part of the solution: a crucial area of improvement that must not be forgotten is security awareness training.

INTRODUCTION

Training and improving security awareness are necessary when employees are the gatekeepers to corporate networks, assets, and data.

Cybersecurity Ventures predicts that the overall market for security awareness training products and services, including security awareness computer-based training (SACBT) solutions, will be worth $10 billion annually by 2027.

As cybercrime evolves, so must our methods for preparing our employees to recognize, detect, and contain threats.

Education and SACBT options are essential, but security awareness training must be treated as a journey to be truly effective. There is no "one size fits all" solution, so computer-based training must be combined with other microlearning opportunities to properly prepare staff for today's modern cyberattacks.

TRAINING OPTIONS

Security awareness training programs and solutions take many forms.

Traditional in-person classes, lectures, and seminars remain popular. Training may also be delivered through booklets, posters, and physical media, such as material provided by an employer to be taken home and read.

Other solutions leverage today's modern technologies. For example, security training can be delivered via the cloud, on-demand platforms, online training platforms, and pre-recorded videos – which may be easier to digest than physical tomes.

The escalation in cybercrime has also become a catalyst in the formation of vendors specializing in SACBT. These companies can be hired to implement computer-based security awareness training programs, including phishing simulations and Business Email Compromise (BEC) scam awareness schemes.

TRAINING OPTIONS

Security and IT teams can teach employees how to recognize the following:

- Social engineering including phishing attempts
- Business Email Compromise (BEC)
- Financial fraud
- Malware including trojans, spyware, ransomware
- Mobile and endpoint security threats
- Data theft

Some organizations also attempt to improve security awareness from the moment they onboard new hires. New staff members may represent a high risk for an organization as they are unfamiliar with genuine branding, correspondence, and security protocols.

While you can provide blanket training for general cybercrime awareness, it is also vital for organizations to educate employees on security requirements related to their roles, whether this impacts communication, data handling, networks, endpoints, or other assets.

MARKET OVERVIEW

There is a growing need for cybersecurity training solutions in the ever-increasing face of cybercrime, and by implementing effective, progressive training now, organizations may be able to avoid severe security incidents.

According to Gartner, by 2025, a lack of available talent (skilled staff) or human failure will be responsible for over half of significant cyber incidents. In addition, by 2025, insider risk will prompt half of organizations to adopt formal training programs to mitigate the risk of insider breaches, whether malicious or accidental.

A recent Tessian study found that only 39 percent of U.S. and U.K. employees are “very likely” to report a security incident in the workplace. Furthermore, 42 percent of respondents said that they wouldn’t know if they were the cause of a security incident in the first place, and 25 percent said they simply don’t care about cybersecurity enough to mention it.

MARKET OVERVIEW

These sentiments should concern business leaders, as it demonstrates we have a lot of progress to make in educating and encouraging a more positive attitude toward security.

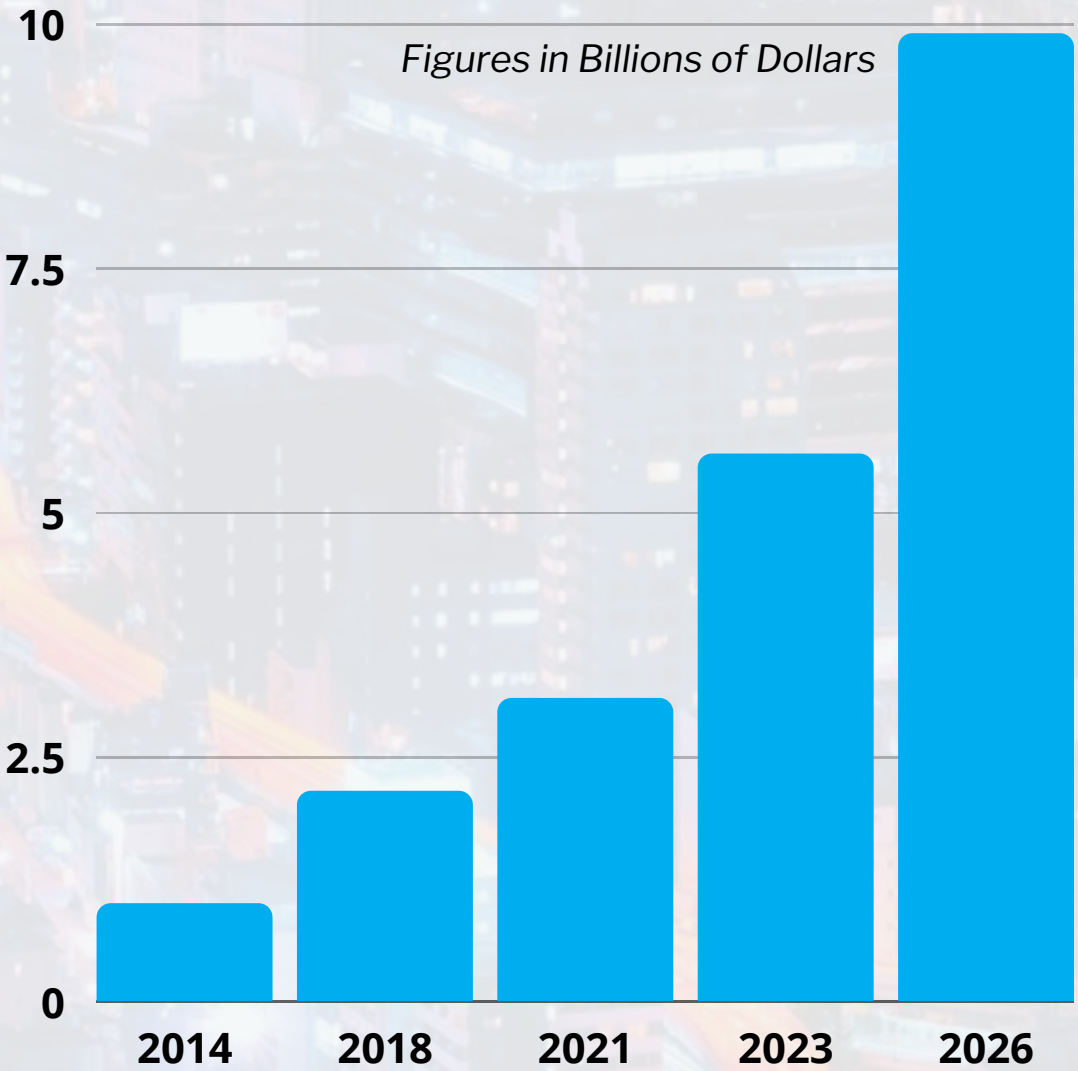
However, there is a silver lining – the research also found that when technology and training programs beyond tick-box training exercises are combined, they are considered the most positive influences in creating and maintaining an effective security culture.

The market has come a long way since 2014 when Gartner pegged the security awareness training market at around $1 billion in annual revenue worldwide, a fraction of where it is today.

SECURITY AWARENESS TRAINING

MARKET OVERVIEW

We predict the global security awareness training market will be around $5.6 billion annually in 2023.



EMERGENCE OF A.I.

Whenever a new technology is developed, there will, unfortunately, always be those who create ways to abuse it. Recent advances, such as artificial intelligence, are not exempt.

While we can utilize A.I. and machine learning technologies to augment existing security teams and reduce their workload, the same systems can also be abused for AI-enabled crimes, cyberattacks, to generate deepfakes, and fraud.

“By 2025, the consumerization of AI-enabled fraud will fundamentally change the enterprise attack surface, driving more outsourcing of enterprise trust and focus on security education and awareness,” according to Gartner. In response, Cybersecurity Ventures expects security leaders will double down on security training and awareness initiatives – as the human element may become one of the most important defenses we have.

THE HUMAN ELEMENT

Focusing only on hardware and software-based exploits and ignoring social engineering tactics can harm business security.

It is part of the human condition to make mistakes, and it is these experiences that we learn from. However, a simple human error can be costly to organizations.

For example, innocently clicking on a link in an email you believe was sent from your boss could spread a ransomware infection throughout a corporate network. Failing to check supplier bank account details sent in an email is a potential missed opportunity to flag a BEC scam. Allowing an unknown person into a restricted building without verification because they appear to be making a delivery, too, could mean an organization falls prey to social engineering and becomes a victim of theft or espionage.

According to Kaspersky research, business leaders'

THE HUMAN ELEMENT

most pressing concerns related to employee error are the prospects of staff inappropriately sharing data via their mobile devices, physically losing company devices, and inappropriately using IT resources.

Microsoft's "Digital Defense Report 2022" notes that nearly half of cybersecurity incidents impacting organizations involve "careless or uniformed staff" and are not the result of malicious behavior, but rather, mistakes.

Furthermore, the "vast majority" of cyberattacks are preventable with basic security hygiene.

However, if organizations adopt a multi-faceted approach to security awareness and ensure that employees are educated and supported, this can profoundly impact cyber defense.

Security needs to be intrinsic from the moment an employee is onboarded, and their education should

THE HUMAN ELEMENT

continue through progressive and constant security awareness training.

While this does mean that more resources and time need to be invested in the workforce, businesses are paid back in dividends through the reduction of risk when it comes to preventable security incidents – some of which could lead to costs reaching millions of dollars.

“Security awareness and training is the most important thing that a CISO is responsible for," says Kathy Hughes, CISO at Northwell Health, New York's largest healthcare system with 83,000 employees across nearly 200 sites.

“Given the sheer volume of events that take place within an organization and network,” Hughes adds, “you really do need your tools and technologies to help determine that, and to protect and respond when there are incidents. But the last line of defense, even in a cyberattack, is the person behind the keyboard.”

THE HUMAN ELEMENT

Security awareness and training does not only apply to employees outside of the C-Suite: it has also entered the boardroom.

According to PWC, corporate directors are more willing than ever to educate themselves on cybersecurity. Their willingness to invest time and energy into understanding the potential threats to their organization tends to lead to an increased frequency of meetings focused on cybersecurity and increased reporting on incidents.

REMOTE WORKERS

The COVID-19 pandemic forced organizations globally to pivot to remote and cloud-first systems. Since lockdown orders eased, many have debated as to whether hybrid and remote working practices will become permanent.

In any case, the rapid adoption of cloud technologies, bring-your-own-device (BYOD) policies, home offices, digitized supply chain operations, Internet of Things (IoT) endpoints and other remote technologies increased the pressure on existing security teams – who suddenly found the corporate networks they were responsible for expanding beyond the confines of on-prem systems and a limited number of mobile devices.

PWC's "2023 Global Digital Trust Insights" report found that today, fewer than 40 percent of organizations believe they have "fully mitigated" the risks created by the accelerated adoption of these technologies in 2020.

REMOTE WORKERS

While large enterprise firms were more likely to say these risks have been mitigated, fewer than three percent of those surveyed believe every risk has been managed, overall.

The primary concerns of today's executives are cybercriminal activities, mobile device compromise, email and cloud security failures, business account takeover, and ransomware.

Cybersecurity Ventures estimates that ransomware attacks a business at least every 11 seconds.

According to IBM's "Cost Of A Data Breach 2022" report, the average data breach cost is now at an all-time high, reaching $4.35 million USD in 2022, a 2.6 percent increase year-over-year.

Furthermore, remote work-related security incidents result in higher financial damages: approximately $600,000 more than the global average per incident.

SECURITY AWARENESS TRAINING

REMOTE WORKERS

In total, 83 percent of organizations said they had experienced more than one data breach.

However, by adopting a holistic approach to cybersecurity, organizations can reduce the cost of an incident – which, unfortunately, is often a case of when rather than if.

Alongside DevOps and maintaining an incident response plan, IBM found that cybersecurity training and awareness programs reduced the average data breach bill by almost $248,000.

Investing in cybersecurity training and awareness programs can reduce the likelihood and cost of a data breach, which is even more expensive when remote and hybrid working practices are in play.

CYBERSECURITY SUPPORT

Education and awareness are crucial but may not be fully beneficial unless augmented by support staff. While employees may be more prone to mistakes, it is made worse by a shortage of skilled cybersecurity professionals.

There are presently 3.5 million unfilled cybersecurity jobs globally. Cybersecurity Ventures expects the shortfall to remain consistent through at least 2025.

While demand remains high and cybersecurity is a near zero-unemployment market for the most experienced people, IT professionals are shouldering the burden in the interim – and every staff member has a role to play in protecting their organization.

Rather than adopting the mantra that many employees are ill-equipped to handle cybersecurity threats or incidents, providing support and training can have other benefits: an employee that feels supported may be more inclined to admit a mistake or suspicious activity rather than stay quiet.

CYBERSECURITY SUPPORT

Training employees from onboarding and throughout their careers may also contribute to better retention of security teams. Improving overall security awareness can reduce the burden of already-overstretched cybersecurity teams and their leaders, some of which keenly feel the pressure in the current climate.

A recent report by Cynet says that 94 percent of CISOs report stress at work, and 65 percent said stress compromises their ability to protect their organization. In addition, just under three-quarters of respondents said team members quit last year due to the stressful nature of the job.

According to Gartner, nearly half of all cybersecurity leaders will change roles by 2025, of which a quarter will leave the industry entirely.

CISO COMMUNITY

Cybersecurity Ventures interviewed CISOs at more than a dozen large enterprises globally. We asked for their thoughts on cybercrime, cybersecurity, and specifically security awareness training.

“I don’t think we fully appreciate how big the problem is,” Bobby Ford, SVP and Global CISO at HPE, told Cybercrime Magazine. “Education and awareness have increased, and our employee base is much more aware,” Ford explains. “But the next evolution that we should be talking about is going from education to equipping our employees so they can help us in the fight.”

“We can never be complacent when it comes to cybersecurity training and awareness,” says Mary Rose Martinez, VP and CISO at Marathon Petroleum Corporation. “The statistics say that the majority of breaches involve the human element, and have to do with phishing.”

“Security awareness and training is the most

CISO COMMUNITY

important thing a CISO can is responsible for," says Kathy Hughes, CISO at Northwell Health, New York's largest healthcare system with 83,000 employees across nearly 200 sites. "For all the investment in security technologies that any company makes," she added, "it just takes one person clicking on one link that bypasses all those technologies in order for an organization to really become crippled."

"It's not just about spending on tools," Susan Koski, CISO at PNC explained. "We've tended to go for best-of-breed solutions, but if you buy a tool and you can't operationalize it, then it becomes shelfware." Look for integrated solutions, she advises, such as an email defense platform that also includes integrated security awareness training capabilities so that detected errors can be turned into teaching moments.

The frequency of training is one of several factors CISOs need to consider when planning cyber awareness strategies, Alissa 'Dr Jay' Abdullah, deputy

CISO COMMUNITY

CISO and SVP of emerging corporate security solutions at Mastercard, told Cybercrime Magazine. “At one point in time, we thought the normal annual training was going to be enough,” she explained, “but now the way people consume data and consume information has changed. We’re in a TikTok era, and everybody wants everything to be short and quick — so we have to move with that evolution.”

“If you’ve got $1 to spend, where are you going to invest it where you can make the biggest difference on the risk?” asks Paul Connelly, former CSO of Nashville, Tenn.-based HCA Healthcare — a Fortune 100 company delivering services across 182 hospitals and 2,300 sites in 20 states and the UK. Staffing remains a key issue for a company so large and so far-flung — yet Connelly believes recent industry efforts to bring people into cybersecurity are bearing fruit.

With cybersecurity staff increasingly testing the waters and often moving between companies as a

CISO COMMUNITY

result, Ian Anthony Baxter, CISO (UK) with the Bank of Ireland says, “recruiting is hard — and retaining is even harder. We’ve trained people up internally, brought them to a great level, and then off they go because the market is very active right now,” he explained. “We’re starting to realize that we’ll never fill all those vacancies. We will never get to the end of painting that bridge.”

“The reason we’re seeing such an inflated market [in terms of cybersecurity expenditure] is because some people are catching up” after years of relying on outdated tools," Laura Deaner, CISO at Northwestern Mutual, said, “and if you’ve looked at the tool sets that are out there, it feels like there’s a tool for everything. Yet it is important for CISOs to avoid focusing on tools too extensively." Real success, she said, comes from building “a solid strategy that includes people,process and technology.”

“We think about all the crimes that have been perpetrated for centuries in the physical world, and

CISO COMMUNITY

that's what we are experiencing right now in the cyber world," says Devon Bryan, Global CISO (former Global CISO) at Carnival Corporation. "I'm encouraged by some of the technology innovation that is increasingly being brought to bear as a force multiplier to help cyber defenders keep our companies, our communities, our cities, and our citizens safe."

One of the biggest mistakes many companies — and vendors —make is to continue discussing cybersecurity in terms of fear, uncertainty and doubt (FUD) by focusing on the dramatic potential consequences of failing to focus enough on cybersecurity. Threatening that a company may be the next one to be compromised "is not the dialogue of the business," says Adam Keown, Global CISO at Eastman Chemical. "That's the talk of a pharma company or a government agency — but it's not the talk of a manufacturing plant, or of Amazon.com."

The high profile and potentially extreme damages of

CISO COMMUNITY

ransomware have been particularly helpful in getting users to appreciate the magnitude of the threat they face: “I’m not a FUD guy and I don’t like to [use that to] sell what I do,” says Jason Rader, CISO at Insight Enterprises, a Fortune 500 IT Consultancy, “but I think ransomware has made a lot of people pay attention.” Education and ongoing engagement are crucial to ensure that users keep paying attention, Rader says, no matter what technology or security policies are being implemented.

“Humans are humans and they will always find the quickest and easiest path to do something,” Jason Lay, CISO at Crypto.com, explains. “As a result, it can create risks for the user and also for the company. But if you want to learn something, you’ve got to really learn it — but if people don’t put in the time and effort to learn the concepts, it becomes really challenging for the organization to embed security into its culture.”

Education is a key tool in Teresa Zielinksi's arsenal of

CISO COMMUNITY

cybersecurity defenses — and sometimes, the SVP, Global CISO and Product Security at GE Gas Power says, "the way cyber leaders engage with employees can make all the difference." A new cybersecurity training campaign, for example, is called “People: Our Strongest Link” — an inversion of the conventional cybersecurity-industry mantra that humans are the weakest link in enterprise security. “I don’t think of it like that,” Zielinski said, “because I feel like that’s when you’re reprimanding folks. It’s all about the culture of training and awareness, getting better, and having somebody raise their hand and ask a question and not feel like they’re going to get reprimanded.”

SECURITY AWARENESS TRAINING

SPONSORED BY KNOWBE4

"It's a game of Whac-A-Mole,", says Erich Kron, referring to the cat-and-mouse play between the cybercriminals and the cyberfighters. We get better at defending, they get better at attacking."

Erich Kron, Security Awareness Advocate & Technical Evangelist KnowBe4

"We've just reached a point of maturity on both sides that's pretty significant and there's a lot of money involved." Kron notes that users have also upped their game and they know more about cyber threats than employees did a decade ago. Part of the reason is that cyberattacks and ransomware are front page news. The tipping point for CISOs and security leaders is culture. Security culture is the ideas, customs, and social behaviors of an organization that influence their security.

SECURITY AWARENESS TRAINING

SPONSORED BY KNOWBE4

KnowBe4 is the world's first and largest New-school security awareness training and simulated phishing platform that helps you manage the ongoing problem of social engineering.

The KnowBe4 platform is user-friendly and intuitive. It was built to scale for busy IT pros that have 16 other fires to put out. Our goal was to design the most powerful, yet easy-to-use platform available.

Customers of all sizes can get the KnowBe4 platform deployed into production twice as fast as our competitors. Our Customer Success team gets you going in no time, without the need for consulting hours.

We are proud of the fact that almost 50 percent of our team are women, where the average in cyber security is just 25 percent.

To learn more, visit https://knowbe4.com

KnowBe4

SECURITY AWARENESS TRAINING

2023 SECURITY AWARENESS TRAINING REPORT is written by Charlie Osborne, Editor-at-Large for Cybercrime Magazine. Steve Morgan, founder of Cybersecurity Ventures, and the editors at Cybercrime Magazine contributed.

Cybersecurity Ventures
83 Main Street, 2nd Flr., Northport, N.Y. 11768
info@cybersecurityventures.com