NINJIO

RANSOMWARE REPORT

22

EXECUTIVE SUMMARY

As the cost and frequency of cyberattacks continue to surge, cybersecurity training has become a major focus for companies across industries and sectors. While this is a healthy development, far too many cybersecurity education programs only exist to present the illusion of protection. Instead of rigorously assessing these programs to determine whether they're instilling healthy cybersecurity habits among employees and creating cyber-aware cultures, companies are implementing them so they can tout their commitment to digital security without doing the legwork necessary to keep their data and systems safe.

In this report, we'll take a look at how companies can move from cybersecurity **training** to **learning** – a transition that will lead to the creation of cyber-aware cultures and ensure long-term security for any organization.

Company leaders often face immense pressure from investors, consumers, and other stakeholders to share information about how they're working to improve their organizations' posture on a range of important issues. This is why companies publish reports and other materials on their ESG (environmental, social, and governance) efforts, workplace safety and employee well-being, and data privacy and security.

"Cybersecurity should never be a check-the-box exercise..."

Because companies have such powerful incentives to tell the world how well they're doing on X, Y, and Z, they often attempt to provide this information even when they don't have concrete programs in place or outcomes to report. When it comes to cybersecurity, a superficial approach is dangerous. If a company doesn't actually have a robust security awareness training (SAT) platform capable of changing employee behavior and keeping its information and systems safe, it will be vulnerable to a vast array of potentially devastating cyberattacks. Companies have to assess their cybersecurity capabilities honestly, proactively educate employees on how to avoid cyberthreats, and determine whether their training programs are having their intended effect.

The end goal of any effective cybersecurity training program is sustainable cultural change. Cybersecurity should never be a check-the-box exercise – it has to be second nature for all employees, whether they're opening an email, downloading a document, or doing anything else that involves access to company data or networks. Companies can facilitate cultural change by keeping employees actively engaged with the material they're learning, regularly testing their knowledge, and ensuring that cybersecurity is a priority across the organization.

CYBERSECURITY EDUCATION SHOULD ALWAYS BE PROACTIVE

Many of the most notorious cyberattacks over the past several years have been examples of ransomware operations – when hackers lock systems or hold data hostage until the victim agrees to pay. When Colonial Pipeline was attacked last year, the company paid the Russian cybercriminal syndicate DarkSide almost $5 million in Bitcoin to restore its operations. Companies responsible for critical infrastructure are especially susceptible to ransomware, as cybercriminals recognize that the vital services they provide can't remain offline for long.

Cyberattacks aren't just costly for companies in the infrastructure sector – they can have massive financial and reputational consequences for any organization. According to the most recent IBM Cost of a Data Breach Report, 2021 saw the highest average cost per data breach in the 17-year history of the publication: $4.24 million. The cost of a ransomware breach was even higher, at $4.62 million. IBM also found that it takes companies an average of 287 days to identify and contain a breach. It's clear that companies face long-term consequences for data breaches – lost business accounted for 38 percent of total costs.

These are all reminders that companies can't afford to wait until after a successful breach to address weaknesses in their cybersecurity platforms, but that's exactly what many are doing. According to Keeper's 2021 Ransomware Impact Report, almost one-third of employees lacked adequate cybersecurity training prior to a successful ransomware attack. In fact, 29 percent didn't even know what ransomware was before the attack took place.

> ***"...29 percent** didn't even know what* ***ransomware** was before **the attack..."***

Considering the fact that many ransomware attacks rely on social engineering, this lack of employee education is a particularly damaging liability. According to Keeper, phishing emails were integral to 42 percent of ransomware attacks, while malicious websites and compromised passwords were to blame for 23 percent and 21 percent of attacks, respectively. IBM reports that one-fifth of all data breaches could be traced to compromised credentials. Verizon's 2021 Data Breach Investigations Report found that 85 percent of breaches involved a human element. It's no surprise that companies take a much more active interest in cybersecurity training after they suffer a successful attack, but by then a huge amount of damage has already been caused.

When companies are hit with a ransomware attack, 87 percent say they enact more robust cybersecurity measures. For example, while 93 percent of companies were forced to tighten budgets after making a ransomware payment, more than two-thirds increased their spending on cybersecurity. The biggest post-attack shift was the emphasis on education: 90 percent of companies say they provided employees with more cybersecurity training. Although it's a good sign that companies are realizing that under-trained employees pose a grave cybersecurity risk, it's disturbing that an attack is necessary to spur action.

> ***"...phishing emails*** *were integral to* ***42 percent*** *of* ***ransomware attacks..."***

The direct costs of a ransomware attack are often immense, but the indirect costs can be even higher – such as a loss of brand trust and loyalty. At a time when 81 percent of consumers say the potential risks of companies collecting their data outweigh the benefits, it's essential for companies to demonstrate that they're managing customers' personal information responsibly. This begins with a proactive cybersecurity platform built around teaching employees how to identify and mitigate cyberthreats.

FINANCE REPORT
ACCOUNT
REPORT
DASHBOARD
INCOME
OUT GOING
DASHBOARD > INCOME
DAILY
WEEKLY
MONTHLY
TOTAL INCOME
37.91%

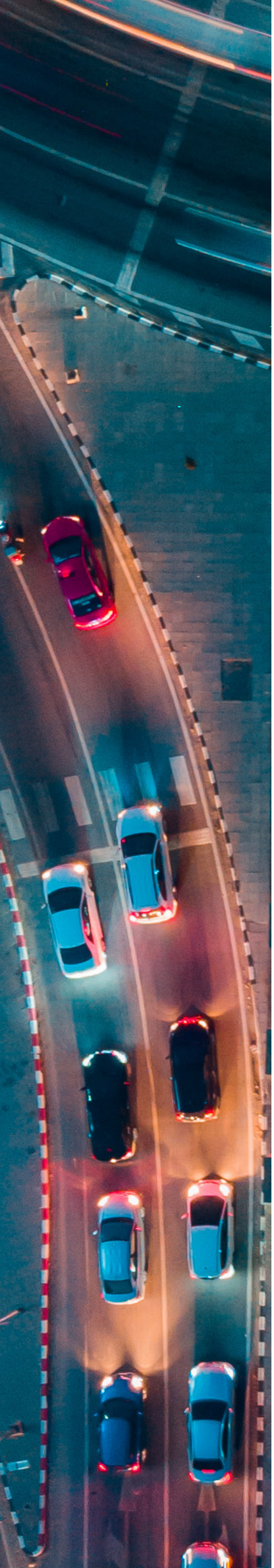
FROM CYBERSECURITY TRAINING TO LEARNING

There's a clear difference between training and learning. While the former is an **input** which provides information about a company's cybersecurity priorities, the latter is an **output** which demonstrates how effective the company's cybersecurity training platform actually is. It's critical for companies to focus on cybersecurity learning – evidence that employees are capable of putting their training into practice and keeping the company safe from real-world threats.

Unfortunately, there are many impediments to building an effective, outcome-based cybersecurity awareness program. For example, security awareness professionals say engaging employees is one of the top challenges they face. This is a significant problem, as engagement makes all the difference between check-the-box cybersecurity exercises and programs that lead to sustainable behavioral – and ultimately cultural – change.

> ***"It's critical for companies to focus on cybersecurity learning…"***

A core part of developing a culture of cybersecurity is getting stakeholder buy-in at every level of the organization. While IT, HR, and legal departments are often supporters of stronger cybersecurity education initiatives, these initiatives can encounter resistance from company leaders responsible for managing costs and productivity. It's important for cybersecurity advocates to reach out to skeptical colleagues and explain why a secure organization is good for everyone. They should also address any concerns about cost, efficiency, and other factors that concern managers and department leaders who may be less familiar with the long-term benefits of cybersecurity training. It may seem more efficient to let employees use whatever productivity tools they want in the short term, for instance, but this can increase the risk of a cyberattack which will have significant repercussions.



Cost-conscious department leaders may be tempted to create perfunctory training programs so they can check the cybersecurity box and move on, but this will do nothing to keep the company safe. It's necessary for companies to develop rigorous metrics to track the success of their cybersecurity awareness programs. As companies dedicate more of their budgets to cybersecurity, they should invest in analytical tools that will help them track concrete outcomes and ensure that their resources are being put to good use. The proportion of organizations focused on performance metrics has increased in recent years, and this trend will only pick up momentum as company leaders continue to discover that a cyber-aware culture is indispensable to keeping their data, networks, and systems protected.

> ***"…43 percent** of companies have increased the **employee** report rate on **phishing tests."***

There are many ways to test employees' cybersecurity aptitude – a crucial component of developing a proactive and effective training platform. For example, companies can use evaluative tools such as phishing tests to determine whether employees are capable of putting what they've learned to use by identifying one of the most common types of cyberattacks (a recent PwC report found that 43 percent of companies have increased the employee report rate on phishing tests). When managers deploy microlearning content such as cybersecurity training videos, they can quiz employees to ensure that they remember the key points. They can also follow up weeks or months later with supplemental information and fresh quizzes to reinforce what employees have learned. Gamification is another tool with a proven record of engaging employees and helping them retain information.

No matter what strategies your company uses to educate employees, the focus should always be on tracking and reinforcing what they've learned. It's easy to develop a cybersecurity "training" program that does little more than distract employees a few times a year with random emails and meetings, but efforts like these will leave your company just as vulnerable to attack as it was before. A real cybersecurity training platform will give employees the skills they need to spot and prevent many different types of cyberattacks and adapt to new threats.

CULTURAL CHANGE IS THE ULTIMATE GOAL

The first step toward developing an effective cybersecurity platform is the establishment of an engaging training program. The second step is ensuring that the program is actually educating employees. And the third step is building that education into the culture of the company and making cybersecurity awareness second nature for all employees.

> *“...**research suggests** that another way to **engage learners** is through **narrative-based content...”***

It's impossible to educate employees without keeping them engaged, but it's clear that this is something companies struggle to do. According to the 2021 Gallup State of the Global Workforce report, just one-fifth of employees around the world say they're engaged at work. This leads to turnover, collapsing morale, and low levels of productivity, and Gallup estimates that it costs the global economy $8.1 trillion per year. Engagement is also a critical element of education. In a case study conducted at Kingston University in London, researchers increased student engagement with "message boards, recorded lectures, use of social media, [and] online forums," and this led to "improved retention and achievement figures compared to modules that were delivered without digital intervention." A considerable body of research suggests that another way to engage learners is through narrative-based content, such as the story-driven microlearning videos offered by NINJIO. The end goal of these strategies isn't just information retention – it's the creation of cultural norms that make the deployment of that information automatic for employees across the company.

> ***"Engagement** is also a critical element of **education."***

Despite the central importance of building a cyber-aware culture, many companies haven't been able to do so. According to survey data published by Quinnipiac University, 60 percent of organizations don't believe they have successfully secured employee buy-in for their cybersecurity initiatives, while 42 percent don't have a plan for developing a cyber-secure culture. More than half believe the CISO should "own" the process of developing a cyber-aware culture, despite the fact that cybersecurity should always be a company-wide priority. A 2019 study conducted by researchers from MIT Sloan summarizes the failure to prioritize the cultural components of cybersecurity: "Managers continue to invest in upgraded technologies and, in many cases, resist investments in organizational mechanisms that would increase resilience."

> ***"...60 percent** of organizations don't believe they have **successfully secured employee buy-in..."***

According to a recent PwC survey, the organizations with the most advanced cybersecurity platforms are twice as likely to report progress on "instilling a culture of cybersecurity." The MIT study outlines several ways for companies to build a cybersecure culture:

1. Making cybersecurity a part of performance evaluations and reward systems.
2. Holding employees accountable for failing to observe cybersecurity protocols (according to Accenture, just 16 percent of CISOs say their companies are doing this).
3. Developing healthy communication around cybersecurity.
4. Providing consistent and up-to-date cybersecurity training.

Beyond observing these guidelines, companies have to ensure that their cybersecurity cultures are capable of keeping up with emerging threats. A recent report by Kaspersky Labs found that 93 percent of cybersecurity professionals recognize that their field "needs to evolve with the current and future landscape." But in many cases, this isn't happening. According to a 2020 study conducted by the Ponemon Institute, the proportion of companies that believed they had an effective cybersecurity platform fell from 71 percent before the COVID-19 pandemic to just 44 percent. One likely cause is the fact that companies aren't adapting to the shifting threat landscape – just 43 percent say they have "programs that inform and educate remote workers about the risks created by remote working."

Human behavior remains the biggest liability – and asset – companies have in the development and maintenance of their cybersecurity platforms. Multiple studies have found that employees remain the weak link in companies' efforts to defend themselves from cyberattacks, but this means cybersecurity education can have a powerful impact for any organization. As more and more companies recognize the value of cybersecurity training, it has never been more important to take a close look at what employees are actually learning and how they're deploying this knowledge to keep the company safe.

"...companies** aren't **adapting** to the shifting **threat landscape..."

Cybersecurity training is a means to an end: the creation of a cyber-aware culture where all employees recognize that they have a responsibility to protect themselves and the company. This is why it's vital to incentivize proactive cybersecurity habits and measure performance (as well as engagement) with tools such as phishing tests, employee reporting mechanisms, and company-wide security assessments. When companies take cybersecurity education seriously, they won't be satisfied with the mere existence of training programs. They'll build their cybersecurity platform around the facilitation of long-term behavioral change among employees, a process which will eventually lead to a robust and permanent cyber-aware culture.

NINJIO

805.864.1999 | info@ninjio.com | www.ninjio.com