cloudshare

Under Attack!

How CISOs Should Respond to the Cybersecurity Crisis

> Cyber attackers have the upper hand – they only need to be successful once.
>
> Your people – all of them – have to be aware and capable to make the right decisions, every time they're exposed to different cyber risks.

Nick Wilding, AXELOS
Head of Cyber Resilience

Securing the Enterprise Is a People Problem

Protecting your digital assets has, and always will be, your most serious challenge. So you fight the good fight, all day every day, in every way. You invest in technology without hesitation. The same goes for your investments in process and policy.

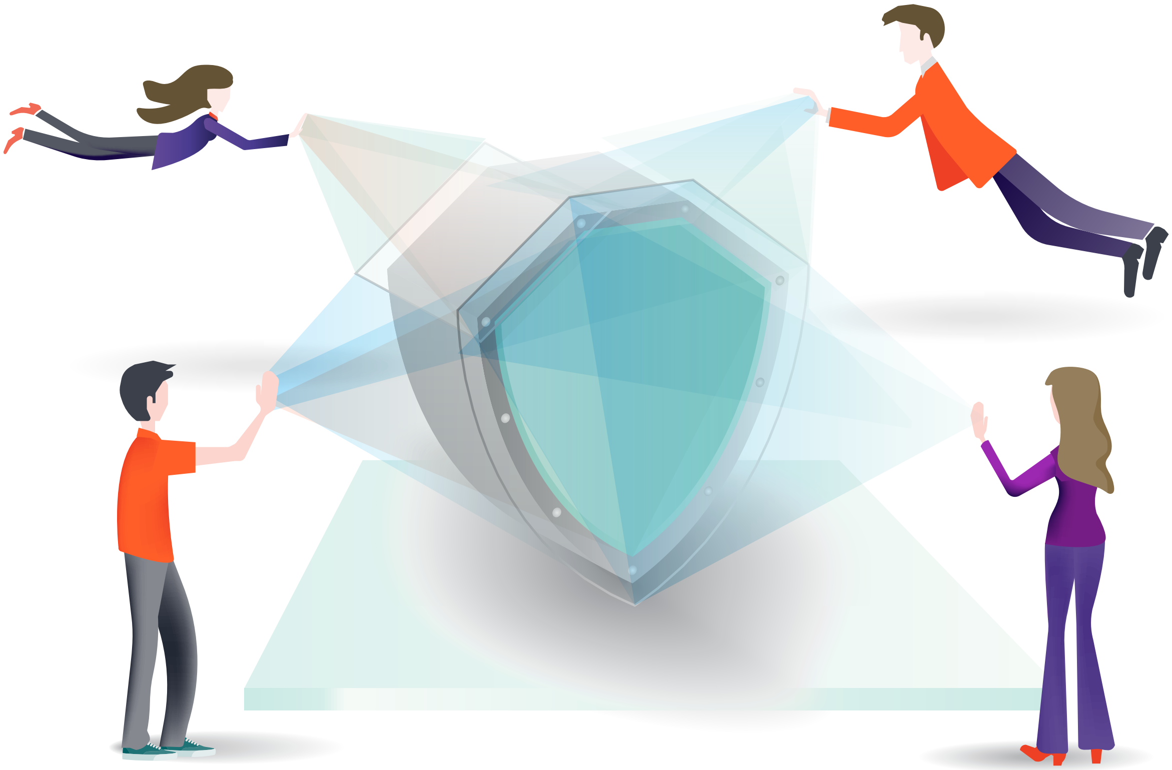
Now stop to think about this:

Do you invest in your people with equal commitment? Doing so is absolutely critical. People have the largest impact on security.

Gartner states, “Security needs require chief information security officers (CISOs) and employee communications leaders, such as human resource managers, to recognize the increasing impact of employee behavior on enterprise security and risk management efficacy.”

The bottom line is the future of your company depends on empowering your people to make it increasingly cyber resilient. **Now is the time to act.**

In this report, we’ll examine the state of cyber resilience and the skill-building strategies needed to strengthen lines of defense across the enterprise.



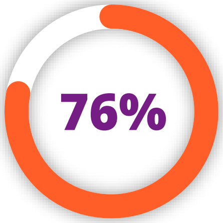
Is Cyber Security Getting Weaker?

96 percent of survey respondents in a cooperative research project by ESG and ISSA strongly agree: cybersecurity professionals must keep up with their skills or their organizations will face a significant disadvantage against cyber-adversaries.

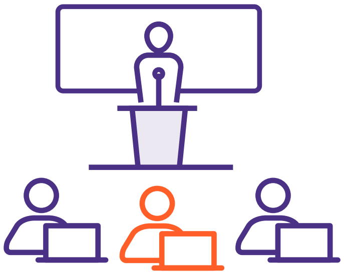
The dilemma is clear—and alarming. Protecting your enterprise from cybersecurity threats requires a proactive approach for arming your people with the right skills. Yet the majority of cybersecurity professionals do not receive the right level of training.

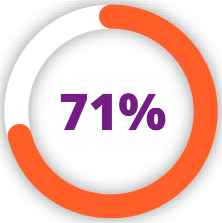
Enterprises do appear to hear the alarms. *The Life and Times of Cybersecurity Professionals* report cited above claims 69 percent of organizations planned to increase cybersecurity spending in 2017. But it also delivers some sobering news: **The cybersecurity skills crisis is getting worse and causing a rapidly widening business problem. Organizations continue to fall behind in providing adequate training. The problem is now a leading contributing factor to security incidents.**

However, cybersecurity professionals know what they need. When asked how they improve their knowledge, skills and abilities, they responded as follows:

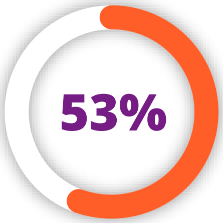


Attend cybersecurity training courses

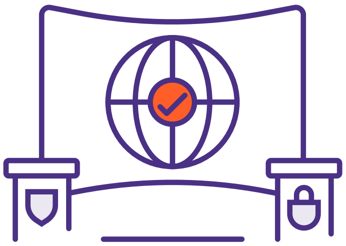




Participate in professional organizations



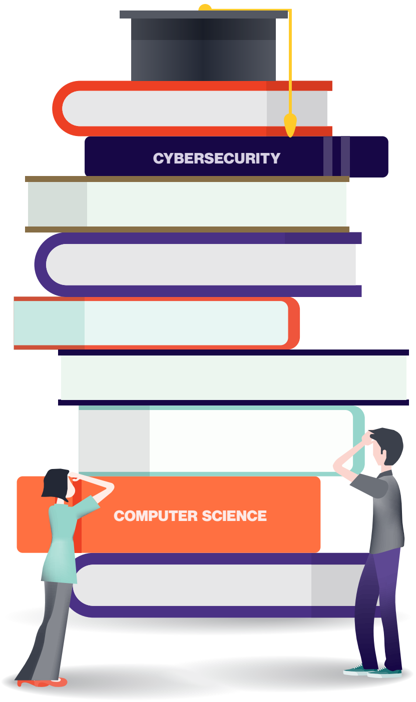
Attend industry trade shows



Can You Count on the Colleges?

Apparently not—it appears U.S. universities don't require much in the way of cybersecurity education. Data from a 2017 study by Cyberbit claims:

- None of the top 10 U.S. computer science programs require a cybersecurity course for graduation.
- Only one of the top 121 schools requires 3 or more cybersecurity courses for graduation.



Higher education is the most common route into a cybersecurity career; however, a report from McAfee suggests it is far from sufficient. When cybersecurity professionals were asked how well they thought their higher education supported them in their jobs, only 23 percent felt that their education fully prepared them for the real world of cybersecurity.

That said, there does appear to be an increasing number of cyber courses being introduced in universities. In fact, more than two hundred higher education institutions in the US are participating in the Centers of Academic Excellence in Cybersecurity program, jointly sponsored by the National Security Agency and the Department of Homeland Security, to help equip the country with more cyber defense professionals.

It's clear. You can't sit tight waiting for the graduates of the future. You have to train existing employees now.

Recruiting and Retaining Top Talent

Another pressing challenge the CISO must face is retaining their talent. According to the ESG/ISSA report, only 40% of cybersecurity professionals claim a high level of satisfaction with their jobs.

Research from CSIC and McAfee claims nearly 50% of security leaders cite lack of training or qualification sponsorship as a common reason why professionals move on.

Clearly, skills development is a critical component of job satisfaction.

Non-technical Employees Need Training Too

The majority of organizations admit to experiencing security incidents over the past two years. In fact, 46 percent have experienced more than one.

When asked to identify the biggest contributors to these events, the number one response was a lack of training for non-technical employees. These employees might download malicious files, click on dangerous links and fall for phishing emails.

An overwhelming majority of hacks result from employees clicking on emails containing some form of malware. 91 percent of cyber attacks and the resulting data breaches begin with a spear phishing email, according to a 2016 report from PhishMe.

The List of Actions Needed Is Long

According to the ESG/ISSA research report, *The Life and Times of Cybersecurity Professionals*: the top ten actions organizations can take to become more cyber resilient are as follows. Note how respondents call out training three times.

1. Add cybersecurity goals and metrics to IT and business managers.
2. Document and formalize all cybersecurity processes.
3. Hire more cybersecurity professionals.
4. Increase cybersecurity budgets.
5. Provide more cybersecurity training for non-technical employees.
6. Ensure cybersecurity and IT departments have the right tools and compensation.
7. Provide more cybersecurity training to the IT team.
8. Provide more cybersecurity training to cybersecurity team.
9. Include security oversight and testing in the application development process.
10. Replace legacy cybersecurity technologies with modern alternatives.

CISOs now need to ensure their staff—and employees across the enterprise—are better equipped to protect the company's IT assets.

Doing so requires commitment toward continuing education and training.

Let's look at how you go about it.

Four Tips to Strengthen Human Defense

A report by the Cyber Relience Think Tank and Mimecast identifies 4 ways to increase human defenses:

Conduct ongoing security training and awareness activities for all employees.

Don’t overcomplicate the process. Educate employees, track progress, and repeat.

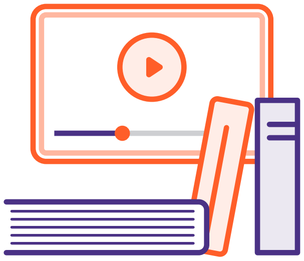
Talk to employees to find out what they experience and what types of training would be most beneficial.

Make security training a business requirement with measurable goals.

The CISO's Cybersecurity Training Options

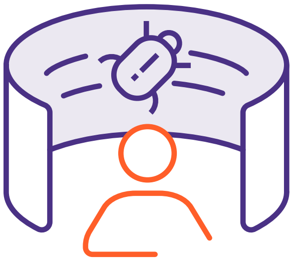
Static education programs are not effective enough. Changes in the workplace are driving the need for security education programs that are regularly updated, interactive, and measurable.

In *Three Critical Factors in Building a Comprehensive Security Awareness Program*, another report from Gartner, they suggest a comprehensive security awareness program has three pillars:



Engaging Education Tools

to help the audience understand their responsibilities in protecting the enterprise.



Attack Simulations

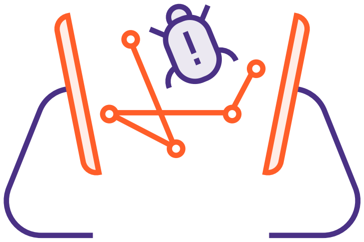
to identify key pockets of risk within the enterprise audience and to test their ability to detect attacks.

Pervasive Communication Tools

for ongoing reinforcement and rewards for taking action.

The security education market is a rapidly expanding market and evolving to provide measurable benefits to organizations. Popular options worthy of your consideration include:

Cyber ranges



A cyber range is a virtual environment used for cyber warfare training and development. While the concept comes from government and military applications, cyber range deployments are on the rise in the private sector.

An enterprise cyber range mimics real-world scenarios in the lab, providing network and IT technology personnel with a realistic and safe platform for training related to network attack and defense scenarios.

Cyber range training focuses on people, processes and technology. Participants work in offensive and defensive teams and learn how to evaluate situations and apply the correct policy/response for specific attack situations. Effective cyber range training creates a highly immersive team-building experience for results-driven (and fun) training.

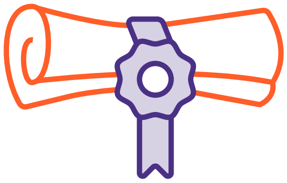
Most cyber ranges are run with onsite instructors and require participants to travel to the location.

Online courses

A growing number of on-demand courses are offered online. For instance, the SANS Institute provides intensive, immersion training designed to help workers master useful cybersecurity techniques. A variety of courses address both security fundamentals, awareness and the in-depth technical aspects of the most crucial areas of IT security.

Another example is KnowBe4, which offers security awareness training and a simulated phishing platform. The company offers a comprehensive approach, including various forms of penetration tests to improve employee resistance to different kinds of social engineering attacks.

Certification programs



Cybersecurity certifications are administered by independent accrediting organizations like CompTIA, InfoSec Institute, EC Council, GIAC, ISACA and (ISC)2.

Entry-level certifications teach basic foundation principles, best practices, important tools, and the latest technologies. Intermediate and expert-level certifications are offered to those with extensive job experience.

Vendor trainings

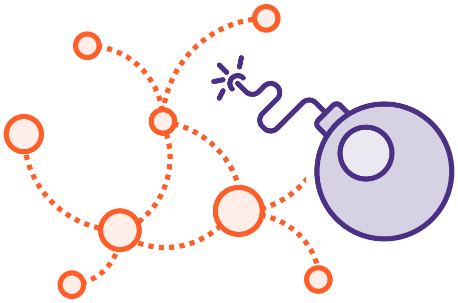
It's important to make sure your employees participate in regular trainings from your cybersecurity vendors to make sure they are aware of the latest features and follow best practices. Vendor trainings are often offered in multiple formats, from recorded trainings to hands-on labs.

Cybersecurity events

Cybersecurity events are a mecca of information, innovation, and inspiration. Tech enthusiasts, security experts, and industry leaders share their knowledge and thoughts on how to improve cybersecurity. A thorough cybersecurity conferences directory is published at https://infosec-conferences.com/

Virtual training labs

Enterprises can employ their own *virtual training labs* to provide their employees with laser-focused cyber-attack training on exact replicas of their environment. Scripts can be injected into individual isolated student environments and employees can practice responding to realistic scenarios.



By enabling remote virtual instructor-led training on demand, virtual labs provide a cost-effective solution. They can be used to onboard new employees, eliminating the need to send trainers and employees to a distant classroom. Attendees can continue to perform their normal job duties between sessions to maintain productivity.

10 Tips for Creating a Corporate Cybersecurity Culture

The TechRepublic article, *How to make your employees care about cybersecurity,* advises:

Eddie Schwartz, Chairman
ISACA Cyber Security Advisory Council

> *If we look at security breaches over the last five to seven years, it's pretty clear that people, whether it's through accidental or intentional introduction of malware, represent the single most important point of failure in terms of security vulnerabilities.*

Perform "live fire" training exercises

"Live fire" is today's best training modality. Users undergo a simulated attack specific to their job.

Get buy-in from the top

The CISO must bring everyone in the C-suite aboard and secure budget for people, hardware, software, and of course, training.

Start cyber awareness during the onboarding process

Begin building a cyber resiliency mindset for new hires the day they join the company.

Conduct evaluations

Perform evaluations on employees and systems to find out how vulnerable your organization is to attack.

Communicate

Create a plan for communicating cybersecurity information to all employees and learning best practices.

Create a formal plan

Develop a formal, documented plan for cybersecurity training. Review and update it regularly.

Appoint cybersecurity culture advocates

Tech leaders should appoint a cybersecurity advocate in every department that acts as an extension of the CISO and keeps employees motivated.

Offer continuous training

Cybersecurity training should continue year-round, at all levels of the organization, specific to each employee's job.

Stress the importance of security at work and at home

Help employees understand the importance of cyber hygiene at work and at home.

Reward employees

Reward users that find malicious emails, share their stories and help raise cybersecurity awareness.

> The importance of fostering an environment of security and risk awareness, shared ownership of cyber risk, and cyber risk resilience is only going to grow. CISOs who are able to step beyond a tactical, technical level are more likely to gain credibility and support among leaders across the enterprise, including the board, CxOs, and business unit leaders.

The New CISO, Leading the strategic security organization, by Taryn Aguas, Khalid Kark, and Monique François, Deloitte Review

The Time is Now for Cybersecurity Training

Joanna G. Huisman, Analyst
Gartner

People impact security outcomes much more than any technology, policy or process."

In the Gartner report, *Three Critical Factors in Building a Comprehensive Security Awareness Program*, analyst Joanna G. Huisman states, "By 2020, organizations that use a multipronged approach to security awareness will experience a 40% increase in overall employee security competency compared to their position in 2017."

CISOs must respond to today's urgent cybersecurity demands with end-user focused education and training programs.

It's time to ask tough questions and make proactive decisions. The authors of an e-book from Resilia suggest addressing the following questions:

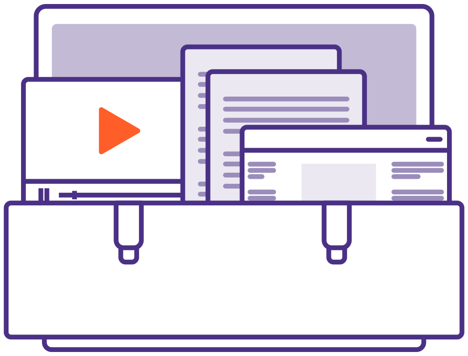
- Is everyone who needs awareness learning receiving it?
- How do you know people are engaging with your cybersecurity learning?
- Is your awareness learning giving people knowledge they can use?
- Does your cybersecurity awareness learning have the support and financial investment from senior executives?
- How do you know your cyber awareness learning and training is effective?

There is no one-size-fits-all solution. There is a broad range of models that enable enterprises to deliver context-specific cybersecurity training content to both IT and non-technical workers. Use and combine them or create your own.

But you must start acting now. If not, you may find that inertia can become your worst nightmare.

We certainly don't want that to happen to you. It is our hope that the data, ideas, and resources in this e-book inspire you to examine your options and take immediate action.

Resources



- Huisman, Joanna G. "Magic Quadrant for Security Awareness Computer-Based Training." Gartner, Inc. 2017.
- Oltsik, Jon. "The Life and Times of Cybersecurity Professionals." ESG and ISSA, collaborative research. November 2017.
  http://www.esg-global.com/esg-issa-research-report-2017
- "Hacking the Skills Shortage: A Study of the International Shortage in Cybersecurity Skills." McAfee. July 2016.
  https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hacking-skills-shortage.pdf
- "Enterprise Phishing Susceptibility and Resiliency Report." PhishMe. 2016.
  http://www.nexustech.com.ph/sites/default/files/PhishMe_Enterprise_Phishing_Susceptibility_and_Resiliency_Report_2016.pdf
- "Strengthen Your Defenses Against Cybercrime." Cyber Resilience ThinkThank and MimeCast. 2017.
  https://www.cdwg.com/content/dam/CDW/brands/mimecast/cyber-resilence-planning-for-email.pdf
- Rayome, Alison DeNisco. "How to Make Your Employees Care About Cybersecurity." TechRepublic. June 2017.
  https://www.techrepublic.com/article/how-to-make-your-employees-care-about-cybersecurity-10-tips/
- Aguas, Taryn, Kark, Khalid and Francois, Monique. "The New CISO: Leading the Strategic Security Organization." Deloitte Touche Tohmatsu Limited. 2016
  https://www2.deloitte.com/insights/us/en/deloitte-review/issue-19/ciso-next-generation-strategic-security-organization.html
- "30 Cybersecurity Statistics and Charts to Help You Justify Your Future Training." Cyberbit. 2017.
- Huisman, Joanna G. "Three Critical Factors in Building a Comprehensive Security Awareness Program." Gartner, Inc. 2017.
  https://www.gartner.com/doc/3802564/critical-factors-building-comprehensive-security
- "Are Your People Playing an Effective Role in Your Cyber Resilience?" Alexos/Resilia.
  https://www.axelos.com/Corporate/media/Files/cyber-awareness.pdf

About CloudShare

CloudShare is a leading provider of cloud-based training labs, enabling cost-effective hands-on training in safe, real-life environments, when and where needed. Trusted by leading organizations worldwide, our specialized training lab solution is particularly well-suited to support the needs of instructors and students in the cybersecurity industry.

To learn more about how CloudShare's advanced IT lab solutions can help bring your cybersecurity training into the real world, visit us at: *www.cloudshare.com*

Trusted by worldwide industry leaders:

SOPHOS ATLASSIAN paloalto NETWORKS

DELL hp FORGEROCK

To get started, contact us today!

www.cloudshare.com *sales@cloudshare.com*