Publication date:
November 15, 2022
Author:
Curt Franklin

The Myths of Training Cybersecurity Professionals

Brought to you by Informa Tech and Cybrary

Omdia commissioned research, sponsored by Cybrary

Contents

Omdia commissioned research, sponsored by Cybrary

Training myths can reduce preparedness

But the increase in incidents is causing organizations to snap to attention

> *Omdia's research shows that the benefits of professional training to the organization include improvements in cybersecurity effectiveness and efficiency, as well as in professional staff retention, if managed correctly.*

Despite the best efforts of data-driven managers, many aspects of business continue to be informed as much by myth and tradition as by data. Myths and legends about the effects and effectiveness of enterprise-provided professional cybersecurity training can call the value of that training into question.

Among the myths are some that discourage companies from offering professional training to their employees; myths like training making employees less satisfied in their positions or more likely to accept a new, higher-paying position with a competitor.

Now, research conducted by Omdia's cybersecurity practice examines why companies provide ongoing professional training and the actual impact it has on the costs and benefits of preparedness, security, and employee retention. Is this an area where the myths have a strong basis in fact, or does data support more training rather than less?

Omdia's research shows that the benefits of professional training to the organization include improvements in cybersecurity effectiveness and efficiency, as well as in professional staff retention, if managed correctly.

Omdia commissioned research, sponsored by Cybrary

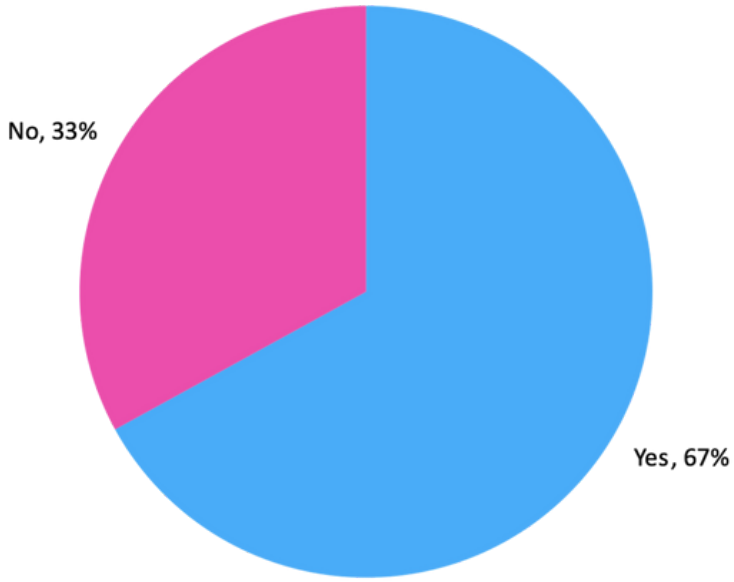
Why train cybersecurity professionals?

One principal reason that companies invest in training cybersecurity professionals is because management feels that better security results are required. Many companies have their attention called to the deficiencies in their existing cybersecurity postures by a cybersecurity incident. In the 2022 Dark Reading Decision Maker's Survey (in which Omdia participated) 47% of cybersecurity executives say that a shortage of skilled employees is an issue that most affects their organization. At the same time, the "snap to attention" that an incident brings may be required, since according to that same survey 90% of cybersecurity executives are either confident or very confident in their organization's security controls.

In the separate Cybersecurity Professional Training Study conducted for this report, two-thirds of the companies Omdia surveyed reported that they invested in professional cybersecurity training following a security incident (see **Figure 1**). Companies in the large SMB to small enterprise category (those with 5,000 to 15,000 employees) are the most likely to launch training programs following an incident, with 70% reporting the relationship between incident and training. Large enterprises (those with 15,000+ employees) are the least likely to wait for an incident to begin a training program. This result suggests that companies with larger, more mature cybersecurity teams are most likely to understand the importance of continuous professional training without the need for a reinforcing jolt from a security incident to spur them to action.

Omdia commissioned research, sponsored by Cybrary

Figure 1: Did you invest in professional cybersecurity training due to an incident?



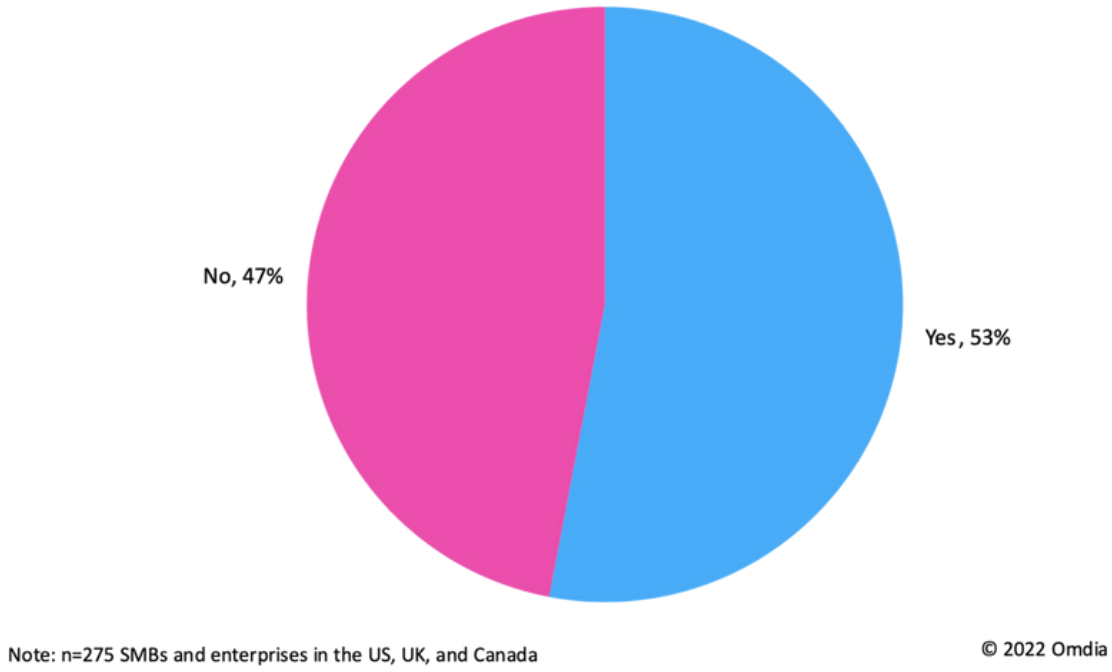
Note: n=275 SMBs and enterprises in the US, UK, and Canada

Source: Omdia

Money that flows to the bottom line can be another powerful incentive for enterprise action, and money saved on cybersecurity insurance premiums is becoming a significant impetus for the beginning of a professional cybersecurity training program. The cyber insurance companies themselves are maturing in their approach to working with clients to improve their risk posture by reducing their overall cyber risk. The audits performed as part of these risk-reduction efforts have an impact on company willingness to begin professional cybersecurity training programs, with more than half of those responding to Omdia's survey indicating that they had started a training program after an audit (see **Figure 2**).

Omdia commissioned research, sponsored by Cybrary

Figure 2: Did you invest in professional cybersecurity training due to a cybersecurity risk audit?



Source: Omdia

As was the case with security incidents, large SMB to small enterprise companies are the most likely to report that they have based their investment in a training program on the results of an insurance carrier's cybersecurity risk audit. Roughly two-thirds of these companies said that an audit had spurred training investment. Less than half of smaller SMBs and large enterprises reported a similar relationship.

Why not train cybersecurity professionals?

"Why should I train my professional employees when they'll just go to work for my competitors for a little extra money?" It's the classic myth about employer-provided professional training, and it's a myth that some security managers still believe and use as an excuse to avoid providing training to their professional employees. While many companies report that they are investing in professional cybersecurity training, these myths persist. It's worth examining some of these myths to see if any have a solid basis in reality.

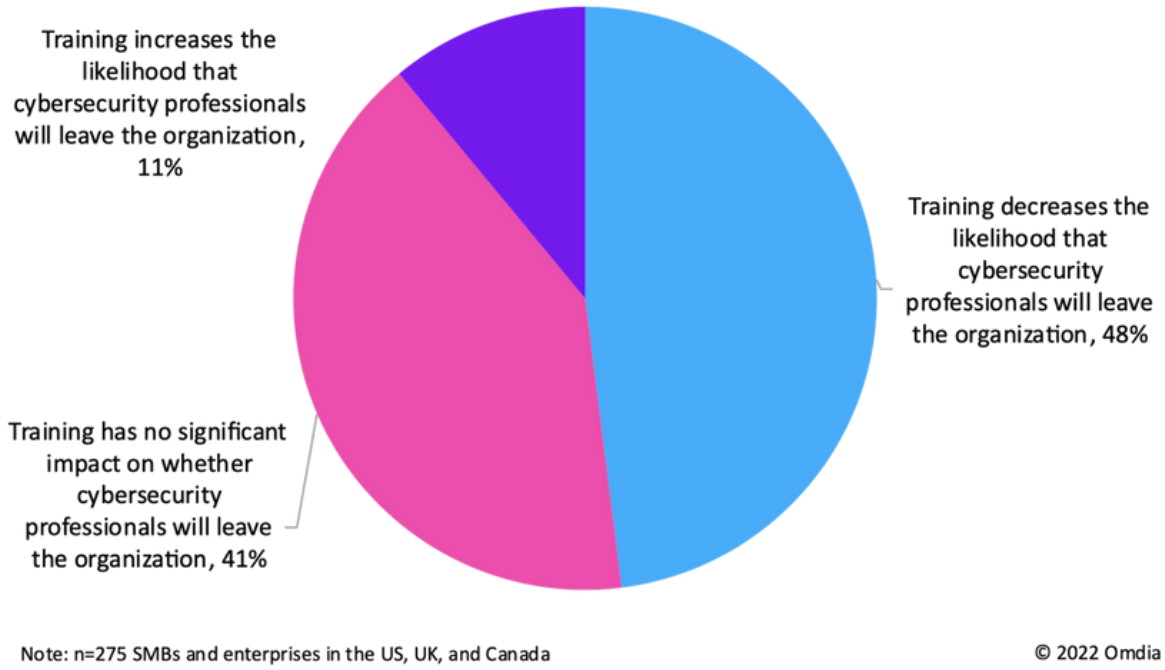
The myth of the migrating cybersecurity professional

Some managers believe that providing professional training increases the likelihood that employees will job-hop with their newly enhanced skills. Our survey data counters that belief. This survey found that roughly half of companies reported that the availability of professional cybersecurity training

Omdia commissioned research, sponsored by Cybrary

reduces the likelihood that an employee will leave, with another four in ten saying that it had no noticeable impact on employee retention. Indeed, only 11% report that professional training increases the chance that a particular employee will leave.

Figure 3: Which statement most closely mirrors your experience of the impact of professional cybersecurity training on professional employee retention?



Source: Omdia

The myth of unproductive investments

While a decision-maker resisting professional cybersecurity training might not believe the myth of the migrating cybersecurity professional, some managers feel that money spent on professional training programs for employees will never see returns that justify the investment. Wanting to see proof of the return possible with an investment is reasonable, and companies in Omdia's survey report a number of measurable results that reward their expenditure on professional cybersecurity training.

Omdia commissioned research, sponsored by Cybrary

> *The benefits of professional training are seen in the impact the employee has on the organization, in the overall risk posture of the organization, and on the costs associated with finding and retaining highly skilled employees.*

Academic research addressed the issue in a variety of specific industries and has been consistent in finding that there is value in professional cybersecurity training: "... professionals with well training and education will be needed to cover whatever gap is created by the advance of the so-called 'digitalization phenomenon' and the associated cyber risks. This in turn is indicating a need for continuous training activities to add more resources in the workforce pool, who should be equipped with the 'right' skills and fully updated with the newest IT trends," according to a paper presented at the 15th annual International Technology, Education and Development Conference/International Academy of Technology, Education and Development entitled *Assessing the Effectiveness of Cybersecurity Training and Raising Awareness Within the Maritime Domain.* (Canepa, M., Ballini, F., Dimitrios, D. and Vakili, S., 2021; https://doi.org/10.21125/inted.2021.0726).

The benefits of professional training are seen in the impact the employee has on the organization, in the overall risk posture of the organization, and on the costs associated with finding and retaining highly skilled employees. More details on these benefits will be provided later in this report, but the key takeaway at this point is that global business executives have recognized the tangible benefits that come from continuing professional cybersecurity education and the significant added risks that come from a workforce composed of undertrained individuals.

The enterprise is seeing results from training

> *Nearly three-quarters (73%) of those responding said that their cybersecurity performance was more efficient because of professional cybersecurity training.*

An overwhelming percentage of organizations say that professional cybersecurity training is important in helping stop breaches. On a scale of 1 to 5, with 5 designating "most important," 79% of those responding to Omdia's survey ranked professional cybersecurity training as a 4 or 5 in its

impact on the organization's ability to prevent or stop breaches. That very basic metric is the most important in assessing training's impact on the cybersecurity operation of an organization, but executives went into more detail on the specific impact seen.

Nearly three-quarters (73%) of those responding said that their cybersecurity performance was more efficient because of professional cybersecurity training. Efficiency tends to speak to those parts of the cybersecurity operation that are "behind the scenes" – activities such as asset inventory, threat intelligence, and compliance. While these may not have the high-glamor visibility of immediate incident response, they are no less critical for successful cybersecurity.

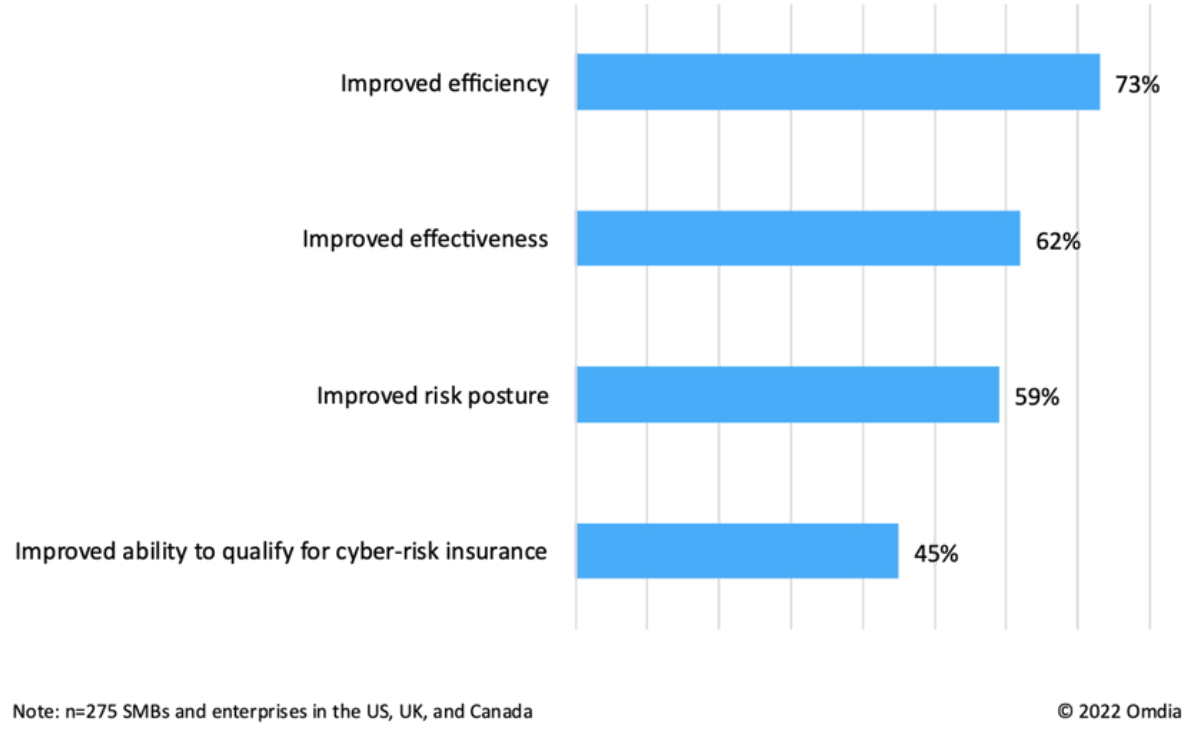
While improved efficiency was the top response regarding the impact of professional cybersecurity training on enterprise cybersecurity, 62% of respondents said that the training had improved their organization's cybersecurity effectiveness. (Executives were able to select more than one response to the question.)

Efficiency in security is more difficult to quantify than effectiveness, but a decrease in the number of intrusion attempts that become breaches can be seen as a useful metric in effectiveness, as can the number of annual security events compared to industry and vertical market averages.

Another pair of results speaks directly to the bottom-line arguments referenced earlier in this paper. More than half (59%) of those responding said that professional cybersecurity training had improved their organization's risk posture, while nearly half (45%) put a finer point on the statement by saying that professional cybersecurity training had improved their organization's ability to qualify for cybersecurity risk insurance. Both of these are, by their nature, quantifiable results that indicate a real, measurable impact of professional cybersecurity training on the organization (see **Figure 4**).

Omdia commissioned research, sponsored by Cybrary

Figure 4: Has professional cybersecurity training improved your organization's cybersecurity performance in the following ways?



Source: Omdia

Enterprises are also measuring the results of professional cybersecurity training within their organization. Nearly two-thirds (65%) of those taking the survey said that their organizations measure the costs and benefits of professional cybersecurity training. The measurements used showed the priorities that companies place on understanding the value of training. Two-thirds listed efficiency as a metric employed by their organization, while 57% said that incident reduction or prevention was a metric. Just over half (51%) are in organizations that use effectiveness as a metric for measuring cost and benefits, while slightly less than half (48%) said that ROI is a measurement used. The most important factor in this response is that large numbers of organizations are using quantifiable enterprise metrics to judge the ROI for professional cybersecurity training and finding the investment worthwhile.

Omdia commissioned research, sponsored by Cybrary

Training is improving staff turnover rates

> *If your company does not otherwise offer good opportunities for career advancement, the mere fact that it provides professional cybersecurity training is unlikely to be enough to determine whether or not cybersecurity professionals stay.*

Many companies have difficulty retaining qualified cybersecurity professionals. The companies responding to the Omdia survey were not exceptional in this regard, with more than half (58%) of executives saying that their companies see more than 15% annual cybersecurity staff turnover. The question for many managers that have heard stories of newly educated cybersecurity professionals jumping to higher-paying jobs is whether training programs will have a positive or negative impact on turnover rates. Almost half (48%) of those responding to the survey said that professional cybersecurity training decreases the likelihood that cybersecurity professionals will leave the organization. Another 41% said that training has no significant impact on professionals' odds of leaving. Only 11% reported that they felt professional cybersecurity training increases the likelihood that cybersecurity professionals will leave the company.

The difference in experience and expectation between different companies may come down to issues beyond the training itself. In a 2011 article in the *Journal of Applied Psychology*, the authors wrote: "... development support was associated with reduced voluntary turnover when perceived career opportunity was high, but it was associated with increased turnover when perceived career opportunity was low." (Taken from "Antecedents and outcomes of organizational support for development: The critical role of career opportunities." Kraimer, M. L., Seibert, S. E., Wayne, S. J., Liden, R. C., and Bravo, J., 2011; *Journal of Applied Psychology*, 96(3), 485–500. https://doi.org/10.1037/a0021452)

Put simply, if your company does not otherwise offer good opportunities for career advancement, the mere fact that it provides professional cybersecurity training is unlikely to be enough to determine whether or not cybersecurity professionals stay. If, however, it is seen as a company that provides good career opportunities, then ongoing professional cybersecurity training is likely to induce trained professionals to extend their tenure with the organization.

How are companies training their employees?

Training on endpoint and cloud topics are at the top of the list

The amount of money spent on training for a particular topic closely tracks the extent to which the topic is considered a major subject of concern for the organization – companies are, in general, putting their money where their worries are. In 2022, the number one worry for companies is

Omdia commissioned research, sponsored by Cybrary

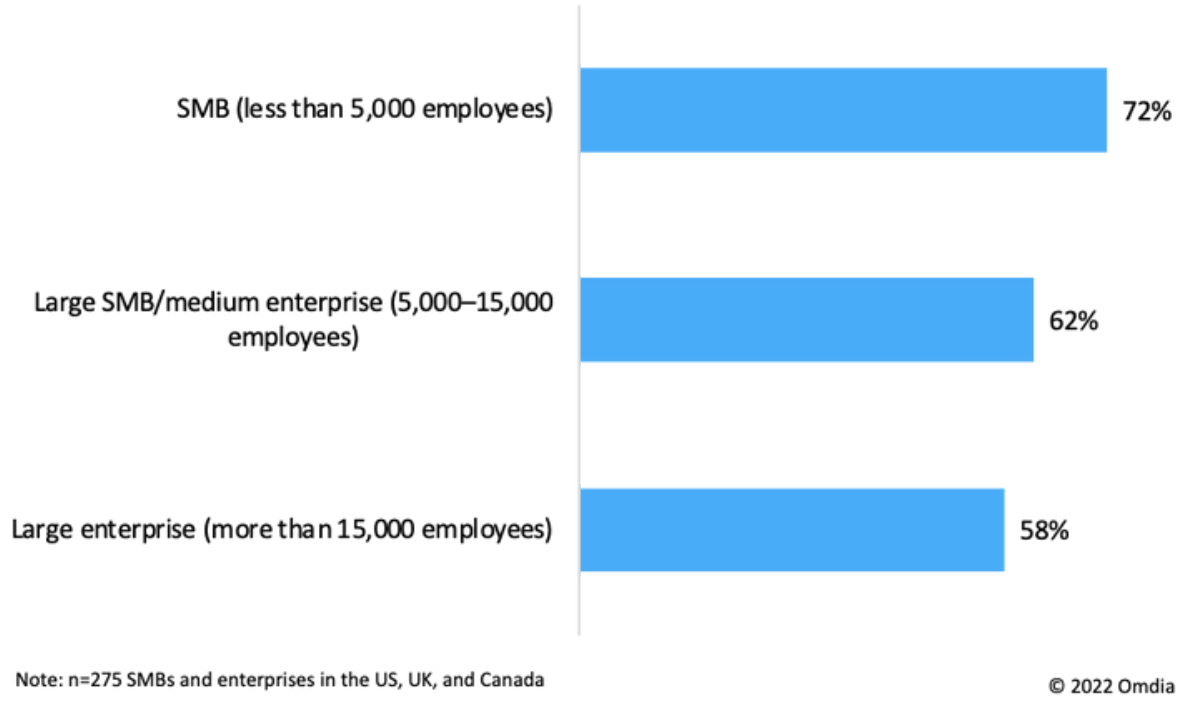
endpoint security, followed closely by data center security and cloud security. Those rankings are echoed by the percentage of professional cybersecurity training budget allocated to the topics, with endpoint security in the lead, followed by data center security. Secure access service edge (SASE), remote security, and cloud security are very closely bunched together as the next three spending targets, though all are among the seven security topics receiving very nearly the same emphasis within the training budget.

Interestingly, in 2022, cloud security is ranked high on the list of topics for training, matching its placement on the 2022 Dark Reading Decision Makers' Survey as a topic of primary concern in the enterprise – and a topic where the greatest lack of skill is seen in the professional staff. After more than a decade of existence, cloud computing remains a topic in which professional skills are seen as lacking in the enterprise – a lack that is keenly felt by many executives.

Integrating training and daily work reinforces employee benefits

In order to minimize overall investment and maximize return, companies are keeping employees on the job while training rather than adding travel and large blocks of time off to the overall cost of training (see **Figure 5**). This coincides with a growing training trend of integrating training into the daily practice of the professional rather than treating it as a separate exercise that might or might not have an immediate bearing on the employees' daily work.

Figure 5: What percentage of cybersecurity professional training budget is online vs. in-person?



Source: Omdia

Immediate integration of lesson and work can be useful to demonstrate to the employee that training will have an impact on job satisfaction and advancement opportunities – a factor in retaining employees following training. As has been seen in previous research, this integration of training and career opportunity is an important factor in making training a positive influence on employee retention after training – in fact, the lack of these career opportunities is the only consistent factor that can lead to professional staff seeking new employment post-training.

Reality supports training

When persistent myths about the possible downsides of continuing professional cybersecurity training are weighed against the experience of the enterprise and results of research, the balance swings firmly in favor of developing a program of professional cybersecurity training. The benefits of improved cybersecurity efficiency and effectiveness more than justify the investment an organization might make. The risks of cybersecurity professionals taking their new skills to a competitor can be eliminated by providing opportunities for career growth within the company.

While there might be justification for adding training modules to address particular topics after a security incident, there is no compelling reason to wait for an external event – either a security incident or a cyber-insurance audit – to begin a program of professional cybersecurity training. A delay in beginning a program of ongoing training can only serve to benefit threat actors and deny the organization the improvements in risk posture that come from cybersecurity professionals with enhanced knowledge.

Appendix

Methodology

This report was based on interviews with a random sample of firms in the US, the UK, and Canada. A total of 275 executives, directors, and security professionals who either procure or influence professional cybersecurity training were interviewed using a computer-aided telephone interview (CATI) methodology. In addition, further primary and secondary research from Omdia's ongoing coverage of cybersecurity training was brought to bear in the analysis.

Author

Curt Franklin
Senior Analyst, Enterprise Security
curt.franklin@omdia.com

Get in touch

www.omdia.com
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision-makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa Tech, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Copyright notice and disclaimer

The Omdia research, data and information referenced herein (the “Omdia Materials”) are the copyrighted property of Informa Tech and its subsidiaries or affiliates (together “Informa Tech”) or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa Tech, and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice and Informa Tech does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an “as-is” and “as-available” basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa Tech and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa Tech will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.