SECURITY INNOVATION

Ponemon INSTITUTE

2023 STUDY ON

Cybersecurity Training Benchmarks

The Value of Realistic Simulation

SPONSORED BY SECURITY INNOVATION
Independently conducted by Ponemon Institute LLC
Publication Date: April 2023
Ponemon Institute© Research Report

Introduction

To achieve a diverse and well-trained cybersecurity workforce, organizations recognize the value of a quality training program supported by the pursuit of cybersecurity certifications. A recent Ponemon Institute study found that on average nearly 50 percent of staff that perform cybersecurity functions hold at least two certifications.[1]

Sponsored by Security Innovation, this is the second study that aims to understand the current state of training programs and what makes such programs successful. The previous study was released in 2020. As part of its efforts to provide professionals with the tools necessary to achieve their educational and training goals, Security Innovation recently announced the release of its Cyber Skills Competency (SI-CSC) certification program that will offer 12 new certifications for developers.

This study involves 1,003 organizations in 17 countries that have a formal training program, an ad hoc program or no program at all. A key takeaway from the 2023 study is organizations' growing embrace of including realistic simulations in their training programs and rating this feature as highly effective (9 on a 10-point scale of 1 = low effectiveness to 10 = highly effective).

Since 2020, the percentage of organizations including realistic simulation in their training programs has increased from 36 percent to 60 percent. The ROI for cybersecurity programs that use realistic simulation increased from an average of 30 percent in 2020 to 40 percent in 2023.

Following are the features that define a successful IT security training program:

- Measures staff security proficiency, benchmarks and tracks improvements with detailed reports that identify skill gaps, measure improvement over time and demonstrates ROI.
- Addresses the security vulnerabilities of today and in the future. Vulnerabilities named in popular frameworks and compliance mandates like PCI-DSS, OWASP Top 10 and others are included. The program is continually updated with the latest threat intelligence.
- Creates cross-organizational excellence. Cybersecurity and DevOps teams can collaborate and prepare against common attacks and advanced threats.
- Ideal for all skill levels. The program has help guides, hints and challenges of varying complexity to ensure everyone can participate and gain insight into the impact of different classes and vulnerabilities.
- The program is engaging and is not a burden for learners.

[1] Achieving Diversity in the U.S. Cybersecurity Industry, conducted by Ponemon Institute and sponsored by Security Innovation and Cyversity, November 2022.

Following are the most salient findings:

- Eighty percent of the 1,003 organizations have either a formal (42 percent) or ad hoc (38 percent) cybersecurity training program. Most of these programs have been in place a minimum of four years to more than 10. Only 20 percent do not have a training program.
- The remote workforce has had an impact on training programs. In-person meetings or classroom venues have declined from 41 percent to 21 percent of organizations since 2020. Formal programs have decreased from 56 percent of organizations to 42 percent while ad hoc programs have increased from 29 percent to 38 percent and no programs have increased from 15 percent to 20 percent.
- On average, organizations with specialized cybersecurity training programs, either formal or ad hoc, spend an average of $3.5 million annually, an increase from $2.9 million in 2020. Larger-sized organizations with a headcount of more than 25,000 incur an annual cost of $6 million, an increase from $5 million in 2020. Organizations are spending the most on more frequent training and methods to measure effectiveness.
- Cybersecurity training programs strengthen an organization's security posture as measured by the Ponemon Institute's Security Effectiveness Score (SES). Organizations that have incorporated an average of 62 percent of the benchmarked practices have the highest SES score. Organizations in Germany, Canada and Australia have the highest SES scores.

Key findings

The findings in this report are derived from Ponemon Institute's Global Cost of Data Breach published in 2022. In this study, we benchmarked the specialized cybersecurity training programs of 1,003 organizations in 17 countries. According to the research, 417 organizations have a formal cybersecurity training program. We define a formal program as one that has a syllabus, measures of effectiveness, a budget and adequate resources.

Following are the 17 benchmarks we were able to collect from the companies participating. They are organized according to these topics: program content, measurement and governance and delivery.

Content

1. Training includes realistic simulation
2. Training content fits the learner's role
3. Training is attached to actual events
4. Self-study option is available
5. Content is in the natural language of the learner

Measurement

6. Methods are available to measure effectiveness
7. Learning gains and retention are measured
8. Immediate feedback is given to the learner

Governance and delivery

9. Results are reported to C-level executives
10. Training is mandatory
11. Training is part of the on-boarding process
12. Rollout of the program is top down
13. Training program is updated at least once a year
14. Training requirements cannot be waived
15. Training is conducted at least once per year
16. Training venue is an in-person meeting or classroom
17. Train-the-trainer and/or apprenticeship delivery options are available

KEY FINDING:

Most companies have either a formal or ad hoc training program.

Table 1 presents the countries or regions represented in our 2022 annual cost of data breach study.[2] According to the table, the United States, Japan and the United Kingdom have the most formal programs, 41, 32 and 32 programs respectively. Brazil and the UK have the most ad hoc programs, 43 percent and 40 percent respectively. As shown, 202 organizations do not have a cybersecurity training program.

Table 1. The number and type of training programs in 17 countries or global regions

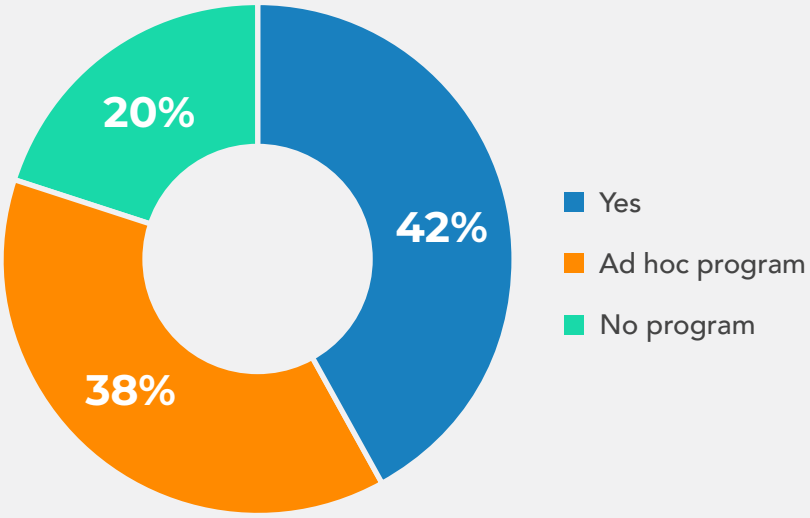
COUNTRIES	Organization provides a formal training program	Organization provides an ad hoc training program	Training program is not provided by the organization
United States	41	20	25
India	28	16	13
United Kingdom	32	40	17
Brazil	29	43	12
Germany	25	26	16
Japan	33	17	12
France	29	16	14
Middle East	23	19	11
South Korea	25	16	7
Australia	27	26	15
Canada	15	19	10
Italy	23	14	13
ASEAN	20	21	8
LATAM	17	16	5
South Africa	14	34	9
Scandinavia	20	16	6
Turkey	16	25	7
TOTAL	417	384	202
PERCENT	42%	38%	20%

[2] See the Global Cost of Data Breach (Sponsored by IBM), Ponemon Institute: July 2022

Figure 1 shows the overall percentage frequency for the types of training programs offered.

Forty-two percent offer specialized training for IT security personnel. In contrast, only 20 percent of respondents say their organization does not offer specialized training for members of the cybersecurity team. Another 38 percent say the specialized training is "ad hoc" – which means the program is loosely structured and/or not formalized within the organization.

Figure 1. Does your organization provide specialized training for cybersecurity staff?

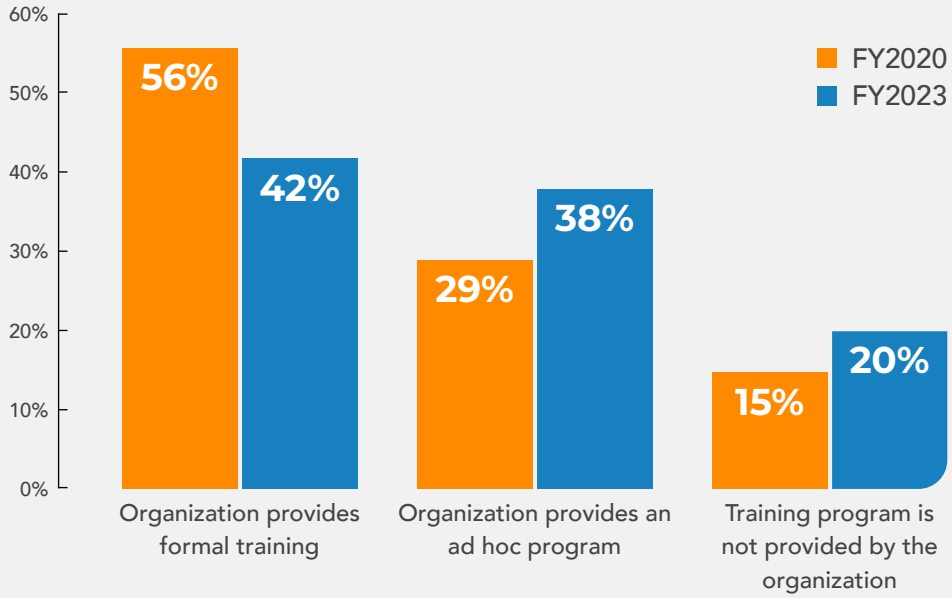


KEY FINDING:

Since 2020, ad hoc programs have increased while formal training programs decreased.

According to **Figure 2**, formal training programs decreased from 56 percent of organizations to 42 percent of organizations and ad hoc programs have increased from 29 percent to 38 percent. A possible explanation for the increase in ad hoc programs and no programs is the impact of Covid-19 and remote working.

Figure 2. Does your organization provide training for IT and security personnel?



KEY FINDING:

Most cybersecurity training programs have been in place for several years.

According to **Figure 3**, 45 percent of these specialized cybersecurity training programs (11 percent + 13 percent + 21 percent) have been conducted for five or more years. Another 27 percent have offered specialized training between 4 and 5 years. Sixteen percent of organizations have offered such training between 1 and 3 years. Only 12 percent have a cybersecurity training program that has been offered for less than one year.

Figure 3. How long has your organization offered specialized training for cybersecurity personnel?

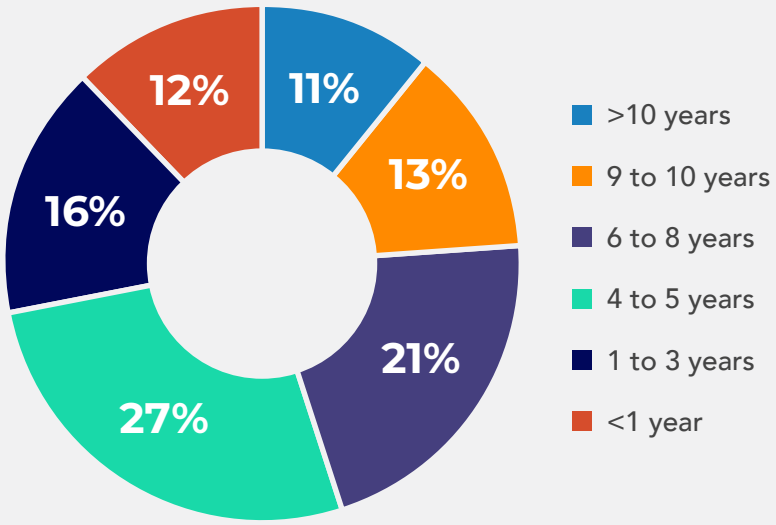
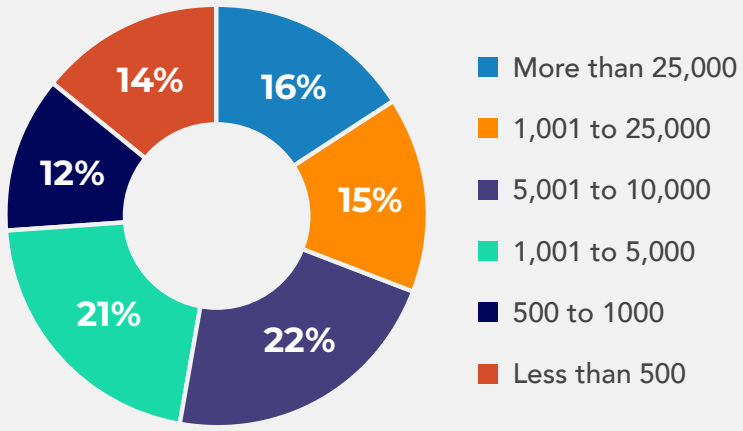


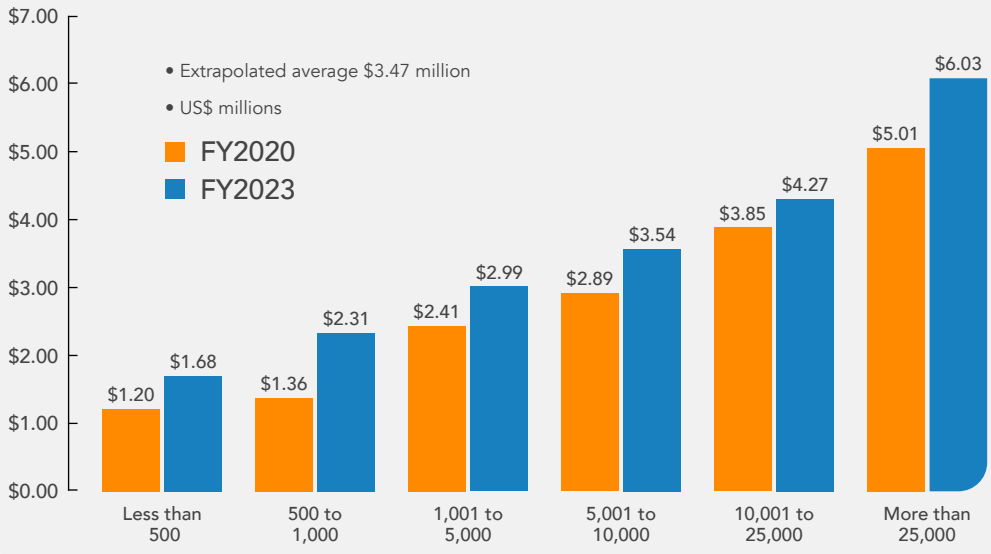
Figure 4 shows the percentage distribution of participating organizations based on headcount as a surrogate for organizational size. The smallest-sized organizations, with less than 500 employees, represent 14 percent of the sample. The largest-sized organizations, with more than 25,000 employees, represent 16 percent of the sample.

Figure 4. Headcount (size) of participating organizations



Cybersecurity training budgets steadily increased. **Figure 5** shows the budget or discretionary spending level for cybersecurity staff training by the organization headcount. As can be seen, smaller-sized organizations with a headcount of less than 500 incur an average annual cost of $1.7 million, an increase from $1.2 million. Larger-sized organizations with a headcount of more than 25,000 incur an annual cost of $6 million, a $1 million increase since 2020. The extrapolated average value for this sample is $3.5 million per annum, an increase from $2.9 million in 2020.

Figure 5. Budget for specialized cybersecurity training based on headcount

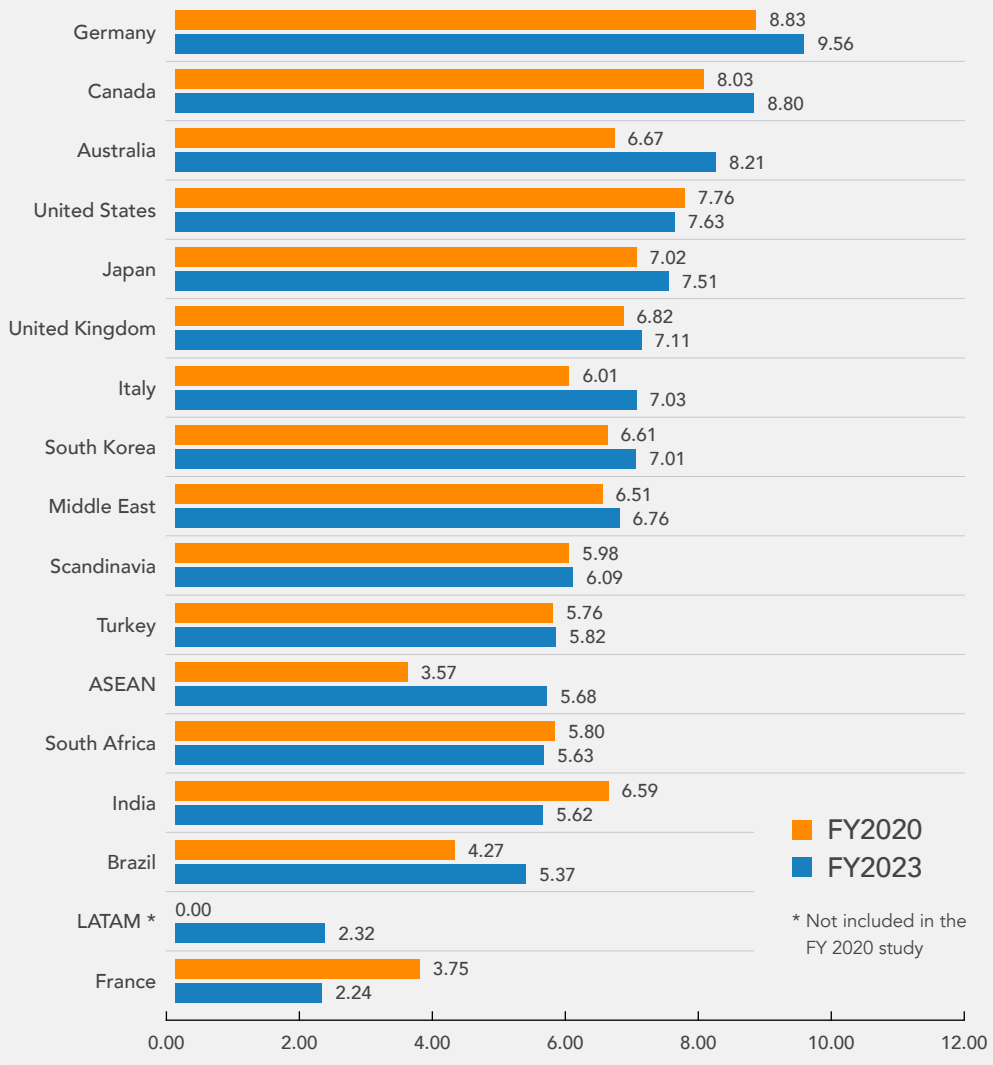


KEY FINDING:

Cybersecurity training programs are shown to strengthen organizations' security posture as measured by the Security Effectiveness Score (SES).

We measure the security posture of organizations using a well-defined performance measurement tool called the SES that has been validated in more than 50 independent studies conducted since its creation. The SES captures all the elements that lead to a strong security posture. The SES is scored on a scale from 1 (worst possible security posture) to 10 (best possible security posture). **Figure 6** presents the SES scores for the organizations in the countries represented in the study. Germany, Canada and Australia have the highest SES scores and, as a result, tend to have a better cybersecurity posture. The average SES score is 6.4 on a scale of 1 low SES to 10 = high SES.

Figure 6. Security effectiveness score (SES) by country sample



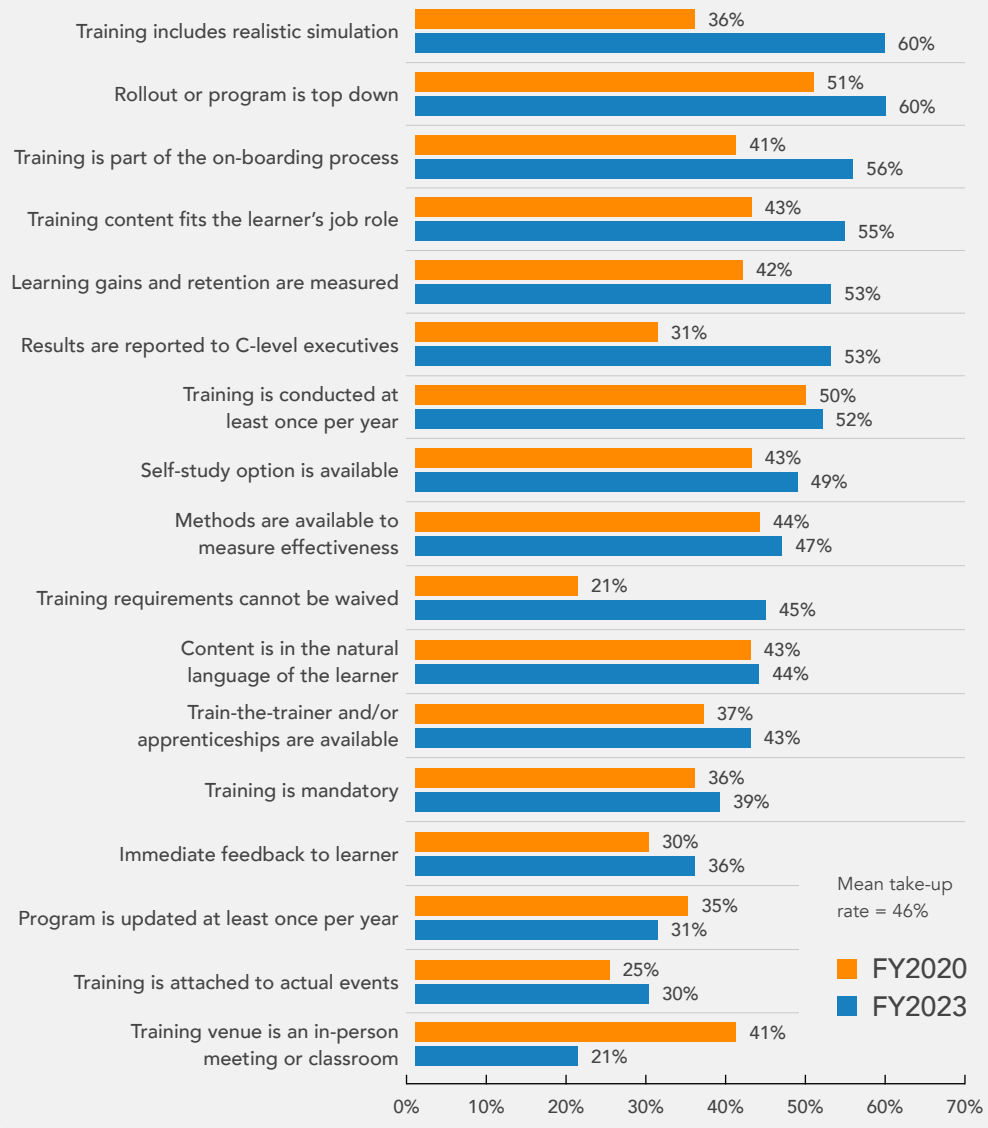
KEY FINDING:

The incorporation of realistic simulations in training programs has increased significantly.

Figure 7 presents the 17 benchmarked elements of a cybersecurity training program and the percentage of organizations that incorporate these elements. Training that includes realistic simulation increased from 36 percent to 60 percent of organizations. A top-down rollout of the program increased from 51 percent to 60 percent of organizations.

Other improvements have been made such as the increase in training as part of the on-boarding process, training content fits the learner's job role, learning gains and retention are measured, results are reported to C-level executives and training requirements cannot be waived. In-person training has declined significantly. Probably due to more remote workers.

Figure 7. The percentage take-up rate of 17 training benchmarks

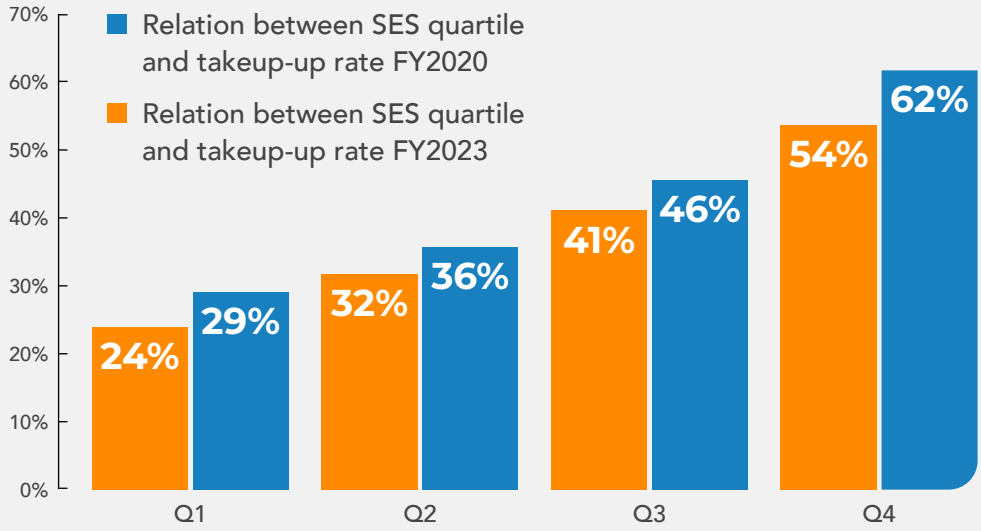


KEY FINDING:

The more cybersecurity training practices adopted, the higher the SES score.

As shown in **Figure 8**, organizations that have adopted an average of 62 percent of the training practices are in the highest SES quartile, an increase from 54 percent in 2020.

Figure 8. Relationship between SES quartile and take-up rate

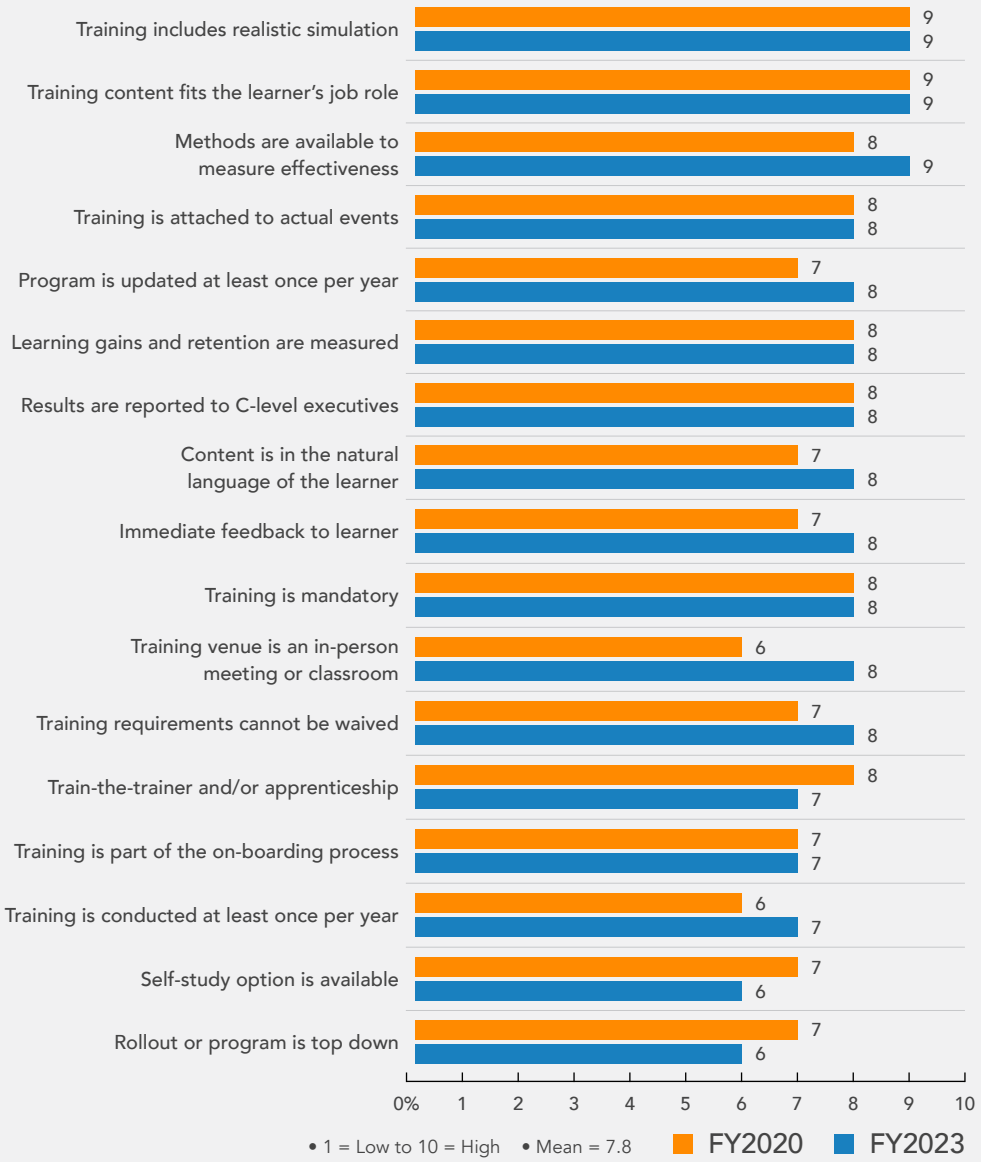


KEY FINDING:

Realistic simulation and training content that is relevant for the learner is most effective, and as discussed, is increasingly adopted by organizations.

Figure 9 presents the effectiveness of the 17 training benchmarks on a scale from 1 = low effectiveness to 10 = high effectiveness. The top three training benchmarks are realistic simulations, content fits the learner's job role and methods are available to measure effectiveness. While fewer organizations are having in-person meetings, respondents believe that they are very effective (8 on the 10-point scale). The average effectiveness of the training benchmarks is very high (8 on the 10-point scale).

Figure 9. The effectiveness of 17 training benchmarks



KEY FINDING:

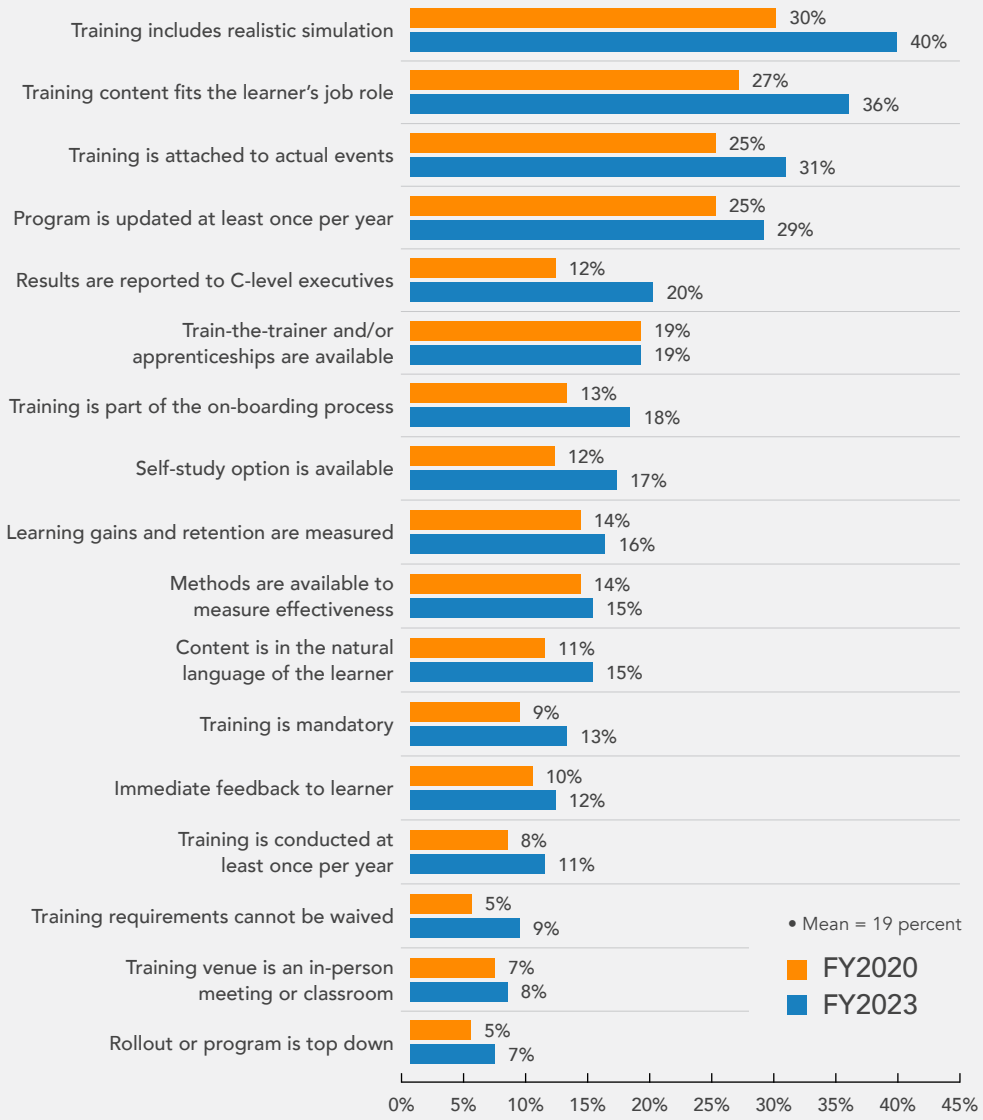
Organizations are spending the most money on more frequent training and the use of metrics.

According to **Figure 10**, The average budget for security training benchmarks is approximately $4 million. Training benchmarks well above the average are more frequent training ($5.05 million), methods to measure effectiveness ($4.78 million) and content is in the natural language of the learner ($4.46 million).

Figure 10. Annual budget or discretionary spending on security training benchmarks

Figure 11 summarizes the estimated return on investment (ROI) realized by organizations for each one of the 17 cybersecurity training elements. At a mean value of 19 percent, organizations deployment of simulation methods, customization of content and the allocation of training content to actual events, experience a substantially higher ROI than other training program elements.

Figure 11. ROI for cybersecurity training program elements



The return on investment calculated for each cybersecurity training element is defined as: (1) gains from the investment divided by (2) cost of investment (minus any residual value). We estimate a three-year life for all technology categories presented. Hence, investments are simply amortized over three years.

The gains are the net present value of cost savings expected over the investment life. From this amount, we subtract conservative estimates for operations and maintenance cost each year. The net present value used the prime plus 2 percent discount rate per year. We also assume no (zero) residual value. The estimated average ROI for all 17 training program elements is 19 percent.

Benchmark limitations

Our study utilizes a confidential and proprietary benchmark method that has been successfully deployed in earlier research. However, there are inherent limitations with this benchmark research that need to be carefully considered before drawing conclusions from findings.

1. Non-statistical results: Our study draws upon a representative, non-statistical sample of global entities experiencing a breach involving the loss or theft of customer or consumer records during the past 12 months. Statistical inferences, margins of error and confidence intervals cannot be applied to these data given that our sampling methods are not scientific.

2. Non-response: The current findings are based on a small representative sample of benchmarks. In this global study, 1,003 companies completed the benchmark process. Non-response bias was not tested so it is always possible companies that did not participate are substantially different in terms of underlying data breach cost.

3. Sampling-frame bias: Because our sampling frame is judgmental, the quality of results is influenced by the degree to which the frame is representative of the population of companies being studied. It is our belief that the current sampling frame is biased toward companies with more mature privacy or information security programs.

4. Company-specific information: The benchmark information is sensitive and confidential. Thus, the current instrument does not capture company-identifying information. It also allows individuals to use categorical response variables to disclose demographic information about the company and industry category.

5. Unmeasured factors: To keep the interview script concise and focused, we decided to omit other important variables from our analyses such as leading trends and organizational characteristics. The extent to which omitted variables might explain benchmark results cannot be determined.

6. Extrapolated cost results: The quality of benchmark research is based on the integrity of confidential responses provided by respondents in participating companies. While certain checks and balances can be incorporated into the benchmark process, there is always the possibility that respondents did not provide accurate or truthful responses. In addition, the use of cost extrapolation methods rather than actual cost data may inadvertently introduce bias and inaccuracies.

Ponemon INSTITUTE

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.

ABOUT SECURITY INNOVATION

Security Innovation is a pioneer in software security and trusted advisor to its clients. Since 2002, organizations have relied on our assessment and training solutions to make the use of software systems safer in the most challenging environments – whether in Web applications, IoT devices, or the cloud. The company's flagship product, CMD+CTRL Cyber Range, is the industry's only simulated Web site environment designed to build the skills teams need to protect the enterprise where it is most vulnerable – at the application layer. Security Innovation is privately held and headquartered in Wilmington, MA USA. For more information, visit www.securityinnovation.com or connect with us on LinkedIn or Twitter.

SECURITY INNOVATION