OffSec Brief

A Short Guide to Essential Cybersecurity Learning Metrics

Cybersecurity learning is a critical part of any cybersecurity program. Cybersecurity professionals must continuously upgrade their knowledge to cope with the rapid evolution of cyber threats. Organizations need new skills to confidently deploy emerging technologies that power competitive advantage. Often, upskilling existing employees is the only way to fill vital security positions.

But how can you know if you are getting the most value out of cybersecurity learning? The answer: metrics. The right measurements will enable you to make optimal use of your training resources and gain the support of management. Here is a short guide to four types of essential cybersecurity learning metrics.

1. Metrics to Optimize Training Activities

Registrations

Number of registrations in cybersecurity learning activities; Percentage of eligible employees registering.

Completions

Number of modules, learning paths, or courses completed; Completions as a percentage of registrations; Percentage of eligible employees completing a learning activity.

Achievements

Assessments or tests passed and certifications received; Milestones achieved as a percentage of activities started; Percentage of eligible employees achieving a milestone.

Learner satisfaction and engagement

Hours spent learning (by individuals/teams/departments); Satisfaction with learning activities.

These metrics enable organizations to assess demand for training on specific topics, determine how well training activities are meeting learner expectations, and track improvements in individual learning activities and the cybersecurity training program as a whole. They also provide data and baselines for many of the other metrics listed below.

2. Metrics to Measure Impact of Learning on Cyber Readiness and Business Performance

Post-training change in existing organizational KPIs and OKRs

Comparison of KPIs and OKRs for teams with and without training

Do you find it challenging to connect security-related activities with business objectives? You don't have to invent new metrics. Show how training influences KPIs (key performance indicators) and OKRs (objectives and key results) already assigned to teams and departments. You can (a) compare the performance of an organization before and after training, or (b) compare the performance of organizations that have received training with comparable groups that have not.

You can show that cybersecurity learning has increased revenue or reduced costs through greater cyber readiness, for example by reducing website downtime from DDoS attacks, or by containing attacks faster to minimize data breach costs. You can also demonstrate how training has helped the organization achieve business objectives by rolling out a secure new application faster or reducing the time to enter a new market with systems that support additional security and privacy regulations. Or, connect training to human resources goals like improving the retention of skilled security professionals or increasing the retention and promotion of employees from diverse backgrounds.

3. Metrics to Track Individual Development and Performance

Job productivity

Post-training improvements in cybersecurity metrics such as alerts triaged, vulnerabilities remediated, and trouble tickets resolved.

Management and peer evaluations

Improved performance assessments by managers, team members, and internal customers.

Acquisition of key skills

Proficiency in high-priority skills (based on achieving milestones or managers' assessments).

Promotions and positive mobility

Promotions and lateral movement into high-priority cybersecurity roles attributable to training and acquisition of key skills.

These metrics help cybersecurity managers document improved individual productivity and track the achievement of departmental staffing goals such as filling key cybersecurity roles with internal candidates.

4. Metrics to Assess Job Satisfaction and Employee Retention

Job satisfaction ratings

Impact of training on learners' job satisfaction.

Job enablement ratings

Learners' assessment of the impact of training on their job performance.

Employee Net Promoter Score (eNPS)

Likelihood learners would recommend the organization as a place to work.

Post-training retention

Comparison of retention rates of employees who have completed training courses with those who haven't.

These metrics can help cybersecurity and HR managers assess the impact of training on learners' job satisfaction (and by extension the likelihood that they remain with the organization), the impact of learning activities on their productivity, and how retention patterns differ between groups that have received training and those that haven't.

The Bottom Line

Organizations can gain a lot by investing a little imagination and effort in expanding the range of learning metrics they track. Data on enrollments, completions, achievement, and engagement help fine tune training offerings. Data can connect training with job productivity, the acquisition of key skills, and the organization's ability to fill high-priority cybersecurity positions through upskilling existing employees. You can track the impact of education on job satisfaction, and ultimately on the retention of skilled, hard-to-replace cybersecurity veterans. And with a little creativity, you can link learning activities to cyber readiness and through that to business objectives by showing how training affects existing KPIs and OKRs.

To learn more, see the blog post:
Essential Metrics to Boost Support for Your Cybersecurity Learning Program