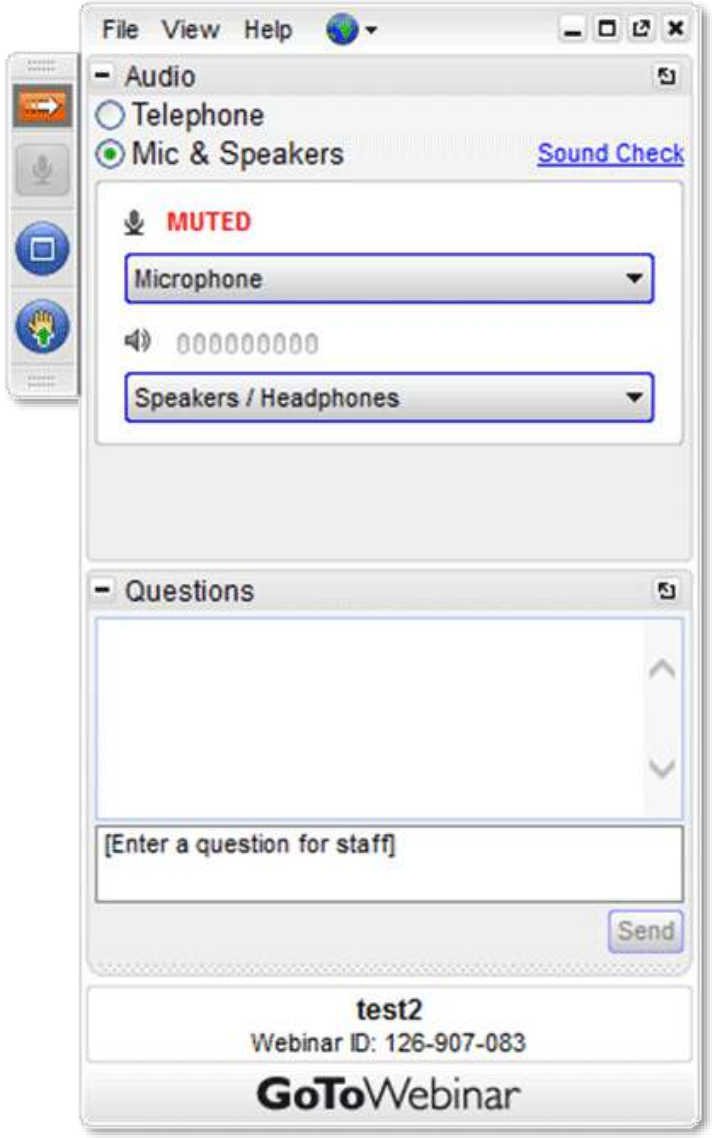
Cyber-Enabled Workforce: What it Means & How to Ensure Your Company is Prepared

Joshua Hester, **CyberVista**
Sonata Ožemblauskaitė, **Questionmark**

To ask questions, use the “Questions” feature



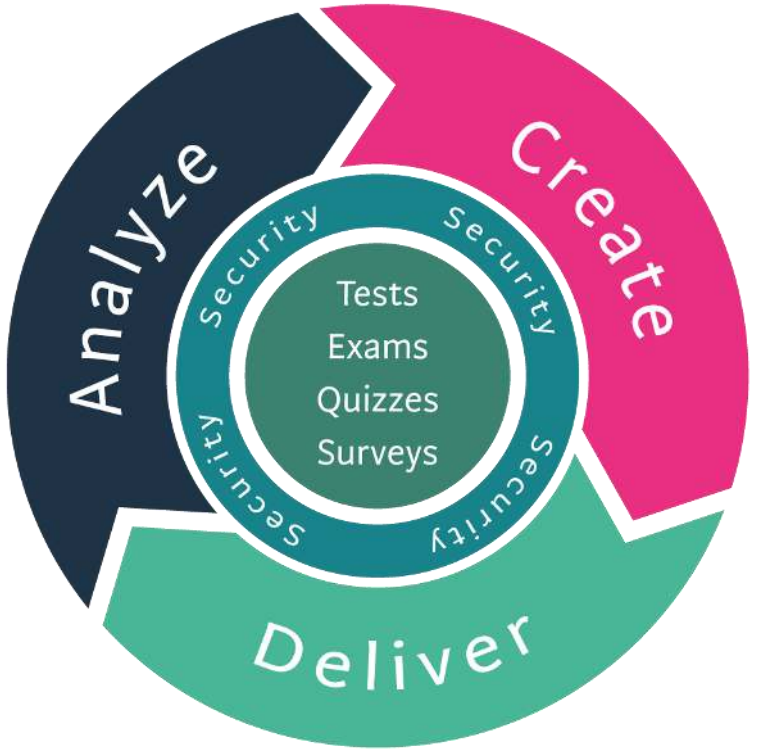
Watch for an email after the webinar:

- Download slides (PDF)
- View a recording

About Questionmark

Background

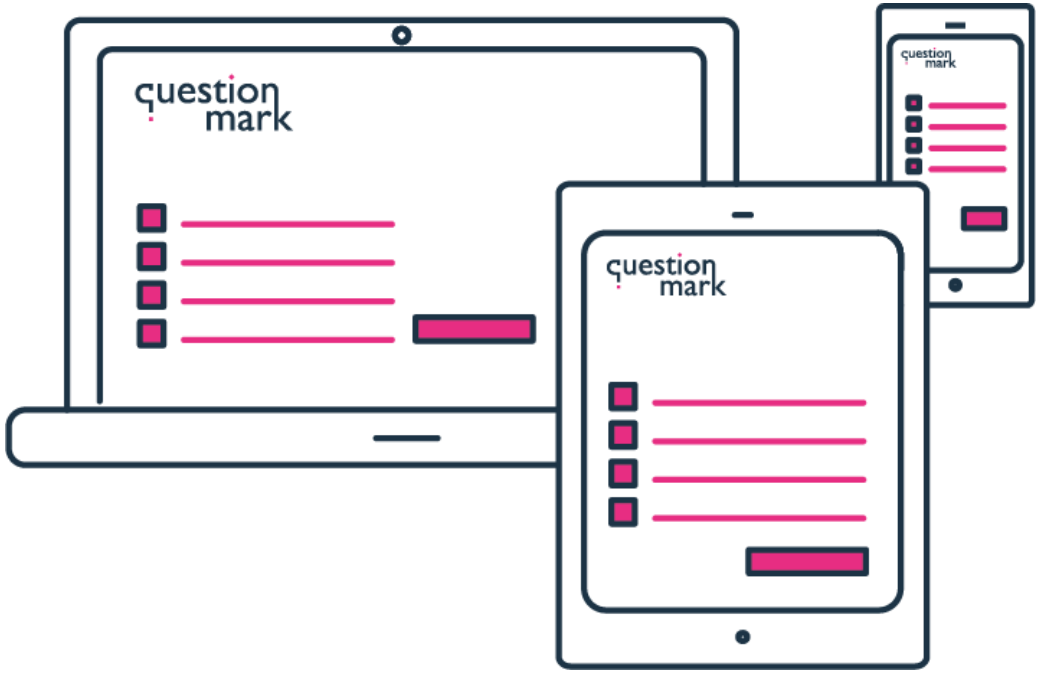
- Founded in 1988
- Assessment solutions to measure knowledge, skills, abilities and attitudes securely for certification, regulatory compliance, workforce learning, sales-force readiness and higher education
- ISO/IEC 27001 Certified (Learn more: www.questionmark.com/trust)



- *Questionmark OnDemand*
- *Questionmark OnDemand for Government*
- *Questionmark OnPremise*

Agenda

- What cyber-enabled means
- What job roles should be cyber-enabled
- How to build cyber culture within your organization
- How assessments can help your organization's security posture
- Q&A



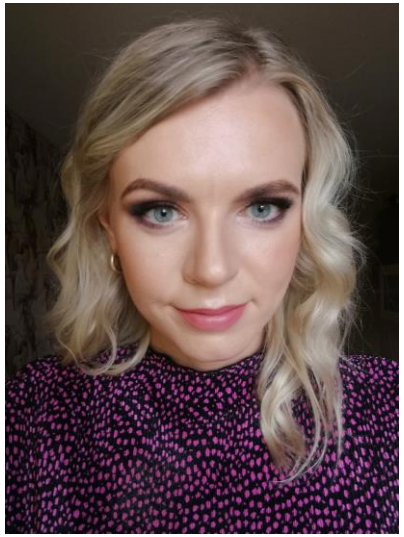
Today's Presenters

Joshua Hester, CyberVista

Executive Director, Professional Education

- PMP, PMI-ACP, CISSP, CEH
- Career Pathways Director, IT Certification Council (ITCC)
- MSEd in Instructional Technology
- BA in English and Computer Science
- 6+ years' experience in cybersecurity education

Sonata Ožemblauskaitė, Questionmark



Group Security and Compliance Manager

- CIPP/E; CIPT
- Member of International Association for Privacy Professionals (IAPP)
- LLM in International Law
- BA in Internal Law and Internal Politics
- 5+ years' experience in working in legal and security matters

About CyberVista

Background

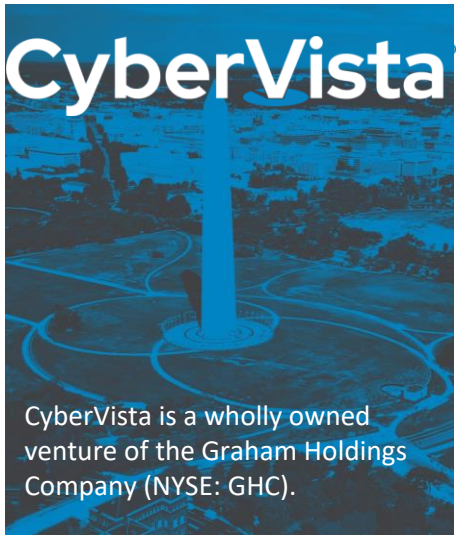
- Founded in 2016, with parent Graham Holdings Company and sister company Kaplan, Inc
- Company dedicated to cybersecurity training, education and workforce development
- Mission – Eliminate the skills gap by creating job-ready professionals

TRUSTED BY

Microsoft

Allstate.

paloalto NETWORKS

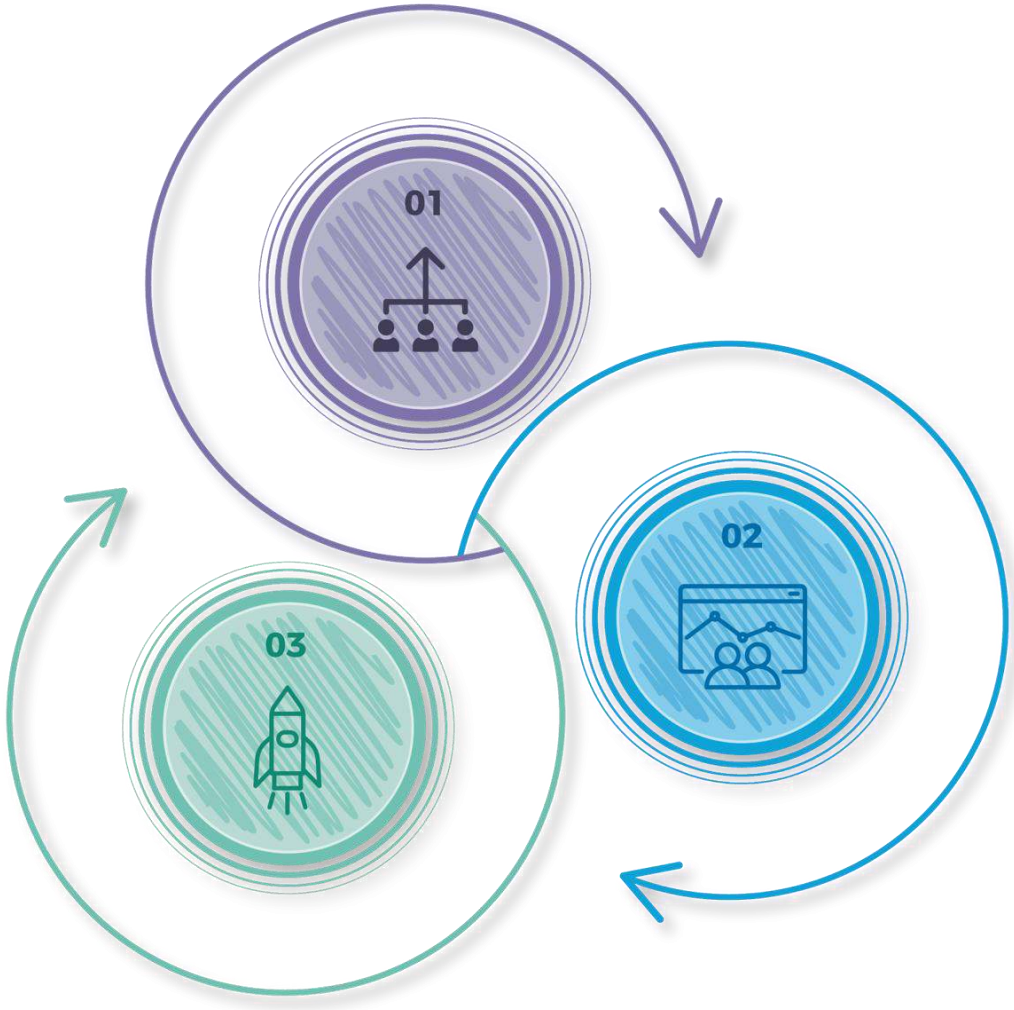


The CyberVista Method

01. ALIGN - Goal Setting

02. DEPLOY – Assessments & Training

03. GENERATE – Cyber Insights



Cybersecurity – why bother?

- Over 20 billion data records were leaked in 2020 across 1,120 data breaches and cyber attacks
- 47% of business feel more vulnerable since remote working
- 42% of business claim they do not know how to defend against cyber-attacks aimed at teleworkers
- 88% of data breaches are caused by human error

Global Risk Report 2021

Common challenges

- ***Increased risk of cyber-attack*** – The risk of cyber breaches has increased in recent years. Widespread remote working over the last year has led to organizations being even more vulnerable to breaches.

- ***Compliance breaches*** – A cyber-attack that leads to a data breach can cause organizations to incur hefty fines and reputational damage.

- ***External skills shortage*** – Employers are struggling to recruit people into specialist cybersecurity roles.

- ***Internal skills gap*** – Employers worry that there is a gap between the cybersecurity skills they need and those that exist among the current workforce.

- ***Learning and development*** – Employers are unsure which teams and job roles require further awareness of cybersecurity issues and what specific training they need.

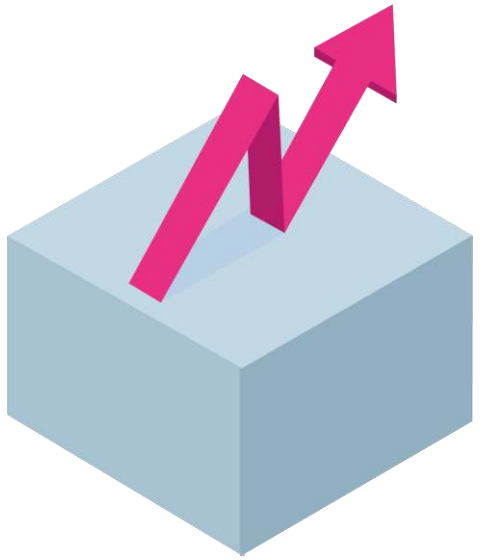
What does cyber-enabled mean?

Who are NOT cyber-enabled:

- General professionals
- Specialized cybersecurity roles

Who ARE cyber-enabled:

- Those who handle sensitive data
- Those who maintain or develop systems with sensitive data



Quick Poll

How many cyber-enabled professionals are in your company?

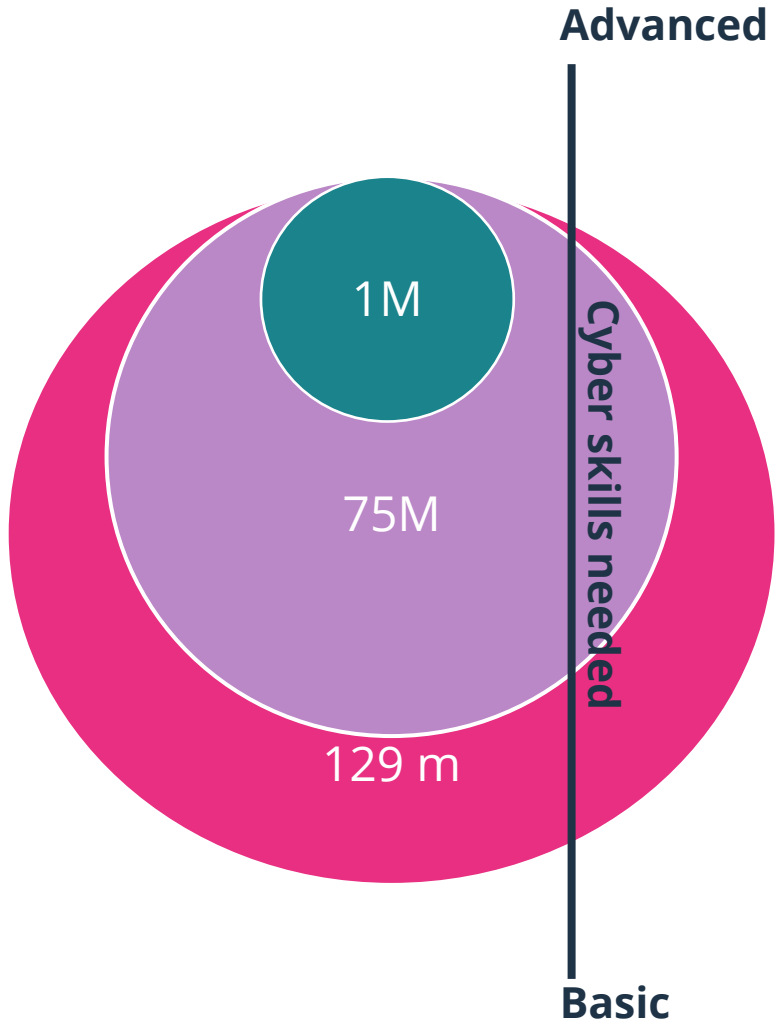
- Less than 10
- Over 50
- Not sure

How many professionals are cyber-enabled?

Cybersecurity
Dedicated personnel are a small portion of the workforce but require the most technical training.

Cyber-Enabled
A large subset of employees access sensitive data daily. Awareness training isn't sufficient.

General Workforce
An evolving regulatory environment across industries requires all employees to receive cybersecurity awareness training.



Cyber-enabled roles

General job titles

- Information Technology Personnel
- Database and Data Scientists
- Human Resources
- Marketing and Sales

Financial Services

- Risk and Compliance Professionals
- Financial Advisors
- Loan Officers
- Insurance Agents

Healthcare

- Clinical Engineers
- Medical Records Technicians
- Health Information Managers

Technology and Cybersecurity

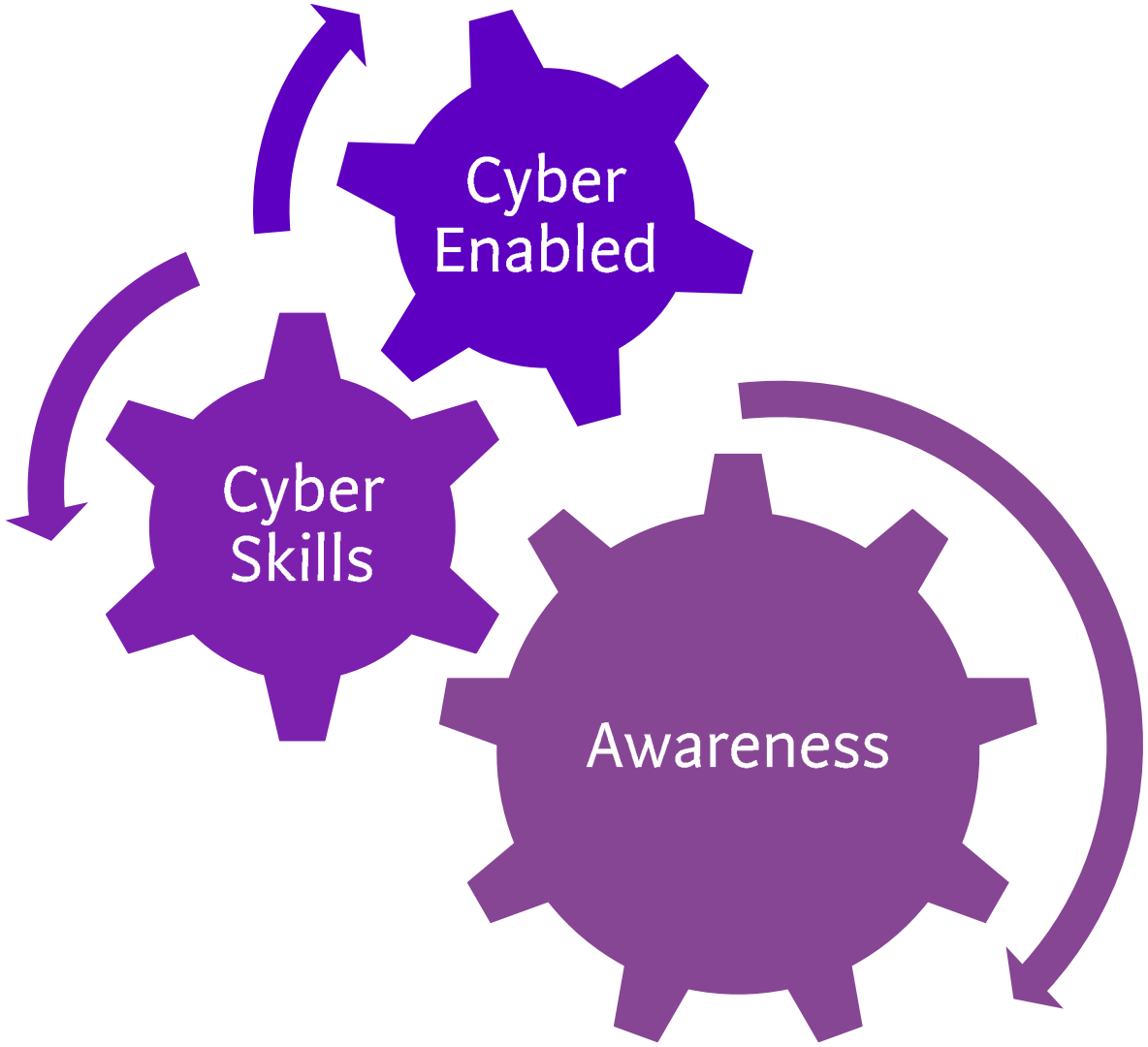
- Risk and Compliance Professionals
- Financial Advisors
- Loan Officers
- Insurance Agents

Building cyber culture

- Going beyond Awareness – the WHY behind security

Which will:

- Establish a proactive cybersecurity mindset
- Invest in talent and career pathways
- Increase company communication
- Elevate overall security posture



Topics to cover in cyber-enabled training

Learning objectives

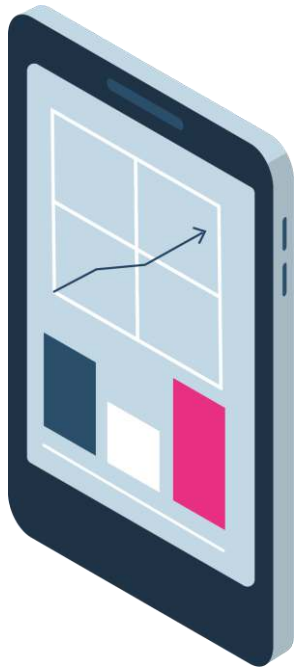
- Why security is important
- Create behavior changes
- Build foundational cybersecurity knowledge
- Develop necessary soft skills *

What to consider when deploying training:

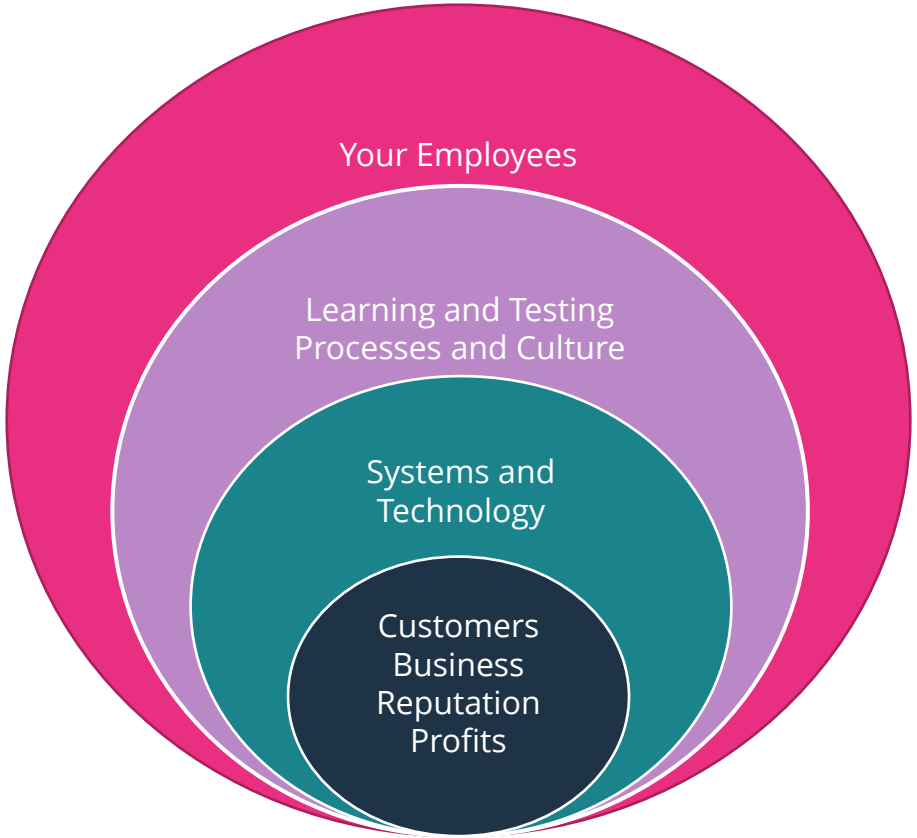
- Length of coursework
- Content delivery methods
- Ability to measure improvement

Knowledge acquisition and improvement

- Set a goal
- Train your employees
- Assess your employee knowledge
- Implement additional training if needed
- Assess whether the additional training improved the gap of knowledge



Why should you test your employees?



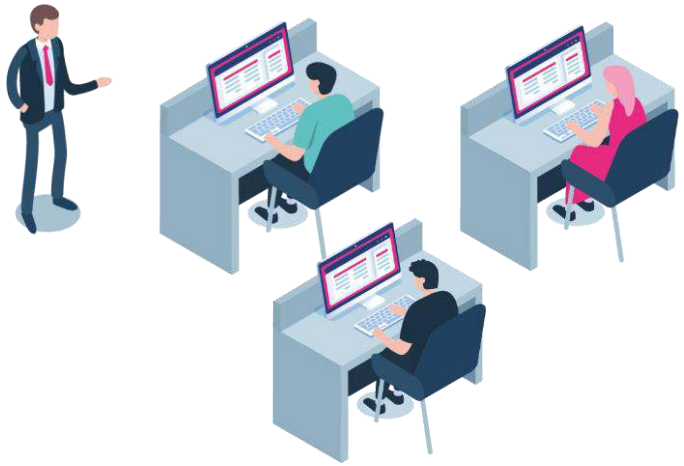
People run the processes and technology to comply with regulations and meet business objectives.

Assessments help you manage competencies of your people

- More than 50% of new work from home employees are using their own personal computers for business use
- 45% haven't received any new training
- More than 50% of respondents don't know of any new company policies related to customer data handling, password management and more

IBM Study

How to Document Training:
Assessments Document Understanding Not Just Attendance



- Taking attendance proves someone turned up but doesn't show they paid attention and understood.

- Getting an employee signature shows more but may sign without taking seriously or without understanding.

- Giving someone a test checks understanding of rules and knowledge of know what rules are and how to follow them.

Cybersecurity for Home-based workers

About the test:

- Measures general understanding of good cybersecurity practices when working at home
- Covers browser, network and device security, disposal and social engineering risks
- 25 questions in 45 min

Results:

- Getting a clear picture
- Identifying appropriate training
- Ensuring business continuity

Sample item

You are surfing the web and encounter a free download of software which is normally quite expensive. What is the biggest risk of downloading the software?

a. The software will require expensive configuration to work on your system
b. The software may allow access to your system by an attacker
c. The software might not work properly on your system
d. The software may interfere with the working of other software on your device

Case study – NT-ware

NT-ware is a print and document management software business, headquartered in Germany with offices worldwide. They purchased the **Cybersecurity for Home-based Workers** test this spring to assist employees to switch to remote working.

Outcomes:

- They have used it with all their 155 employees
- 93% of their employees have passed the test

According to them, the assessment **achieved two goals:**

- It **raised employees' awareness about the threats**
- It **informed** the employer **about cybersecurity training needs** and topics to cover

The employees found the test challenging, but insightful. The questions 'made them think'.

The **Cybersecurity for Home-based Workers** will become a standard part of their onboarding program.

Critical Cyber Diagnostic - Overview

- **Purpose of the test:** to measure proficiency in cybersecurity knowledge and skills based on the NICE Cybersecurity Framework
- **Targeted audience:**
  - Those who regularly access sensitive systems and data, including IT and HR;
  - Professionals and managers who have specialized security roles, such as security analysts and incident responders;
  - Any role within an organization that supports the overall security posture.
- **Items written** by subject experts and evaluated by several professional reviewers
- **Covered areas:** network fundamentals, threats and attacks, network security, security engineering, risk management and governance, security operations, offensive and defensive schema
- **Questions:** 21 out of 28 questions in 30 minutes; assesses application-level knowledge and analysis skills
- **What does it mean to score high/low:** a high score indicates mastery of the relevant knowledge and skills. A low score indicates that additional support may be required

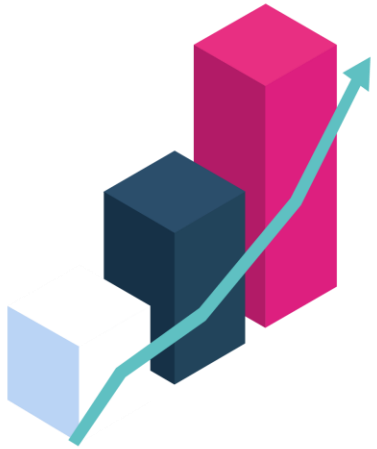
How could these tests help your organization?

- ***Improved cybersecurity*** – Highlight areas of weakness. Leaders can introduce training and improve performance.
- ***Reduce risk*** – Help employers address areas of weakness. This reduces the risk of costly data breaches.
- ***Demonstrate compliance*** – Enable employers to demonstrate that workers understand requirements to regulators and stakeholders.
- ***Better recruitment*** – Used in the pre-hire process. Hirers can ensure they are bringing people with the right skills into cybersecurity roles.

question mark

Questions?

White papers, infographics, reports, eBooks and more!



www.questionmark.com/resources

Upcoming webinars

Questionmark 2021 Q3 Feature Release Briefing

- August 12, 2021 - 11:00 am to 12:00 pm (EDT)

An in-depth look into your third quarter product feature release, this briefing is jam packed with key new features that will ensure you are delivering valid and reliable assessments.

Click to Register

Introduction to Questionmark's Assessment Platform

- August 24, 2021 - 12:00 pm to 1:00 pm (EDT)

Learn the basics of authoring, delivering and reporting on surveys, quizzes, tests and exams. This introductory webinar explains and demonstrates key Questionmark features and functions.

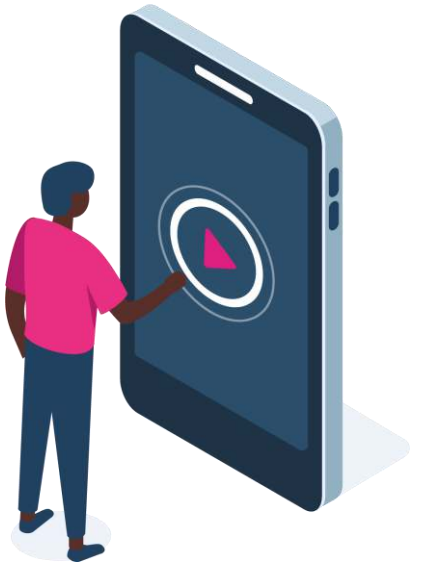
Click to Register

Test-Item Database Design – Your Key to Fairness

- August 26, 2021 - 11:00 am to 12:00 pm (EDT)

Learn the importance of the initial design of a test-item database. This session will cover how the initial design or layout of topics affects several outcomes down the line including locating test-items within the database, item selection for assessments, using reports to identify knowledge gaps, and decisions on how to score the examination.

Click to Register

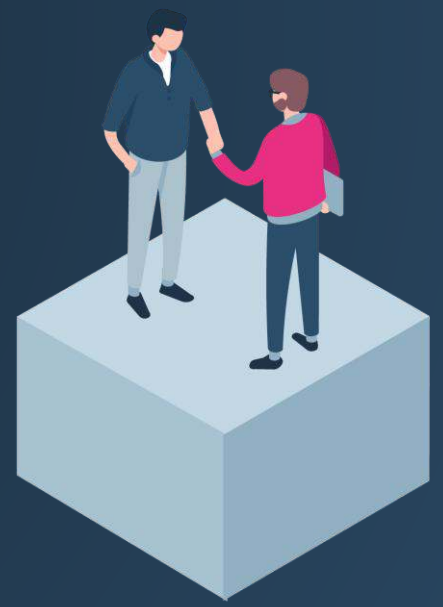


How to Evaluate

Request a one-on-one demo

The Questionmark team will contact you to arrange a demonstration tailored to your needs and questions

www.questionmark.com/request-demo



Thank you for attending!

GET IN TOUCH WITH US

Reach out to Sonata – sonata.ozemblauskaite@questionmark.com

Reach out to Joshua – Joshua.hester@cybervista.net