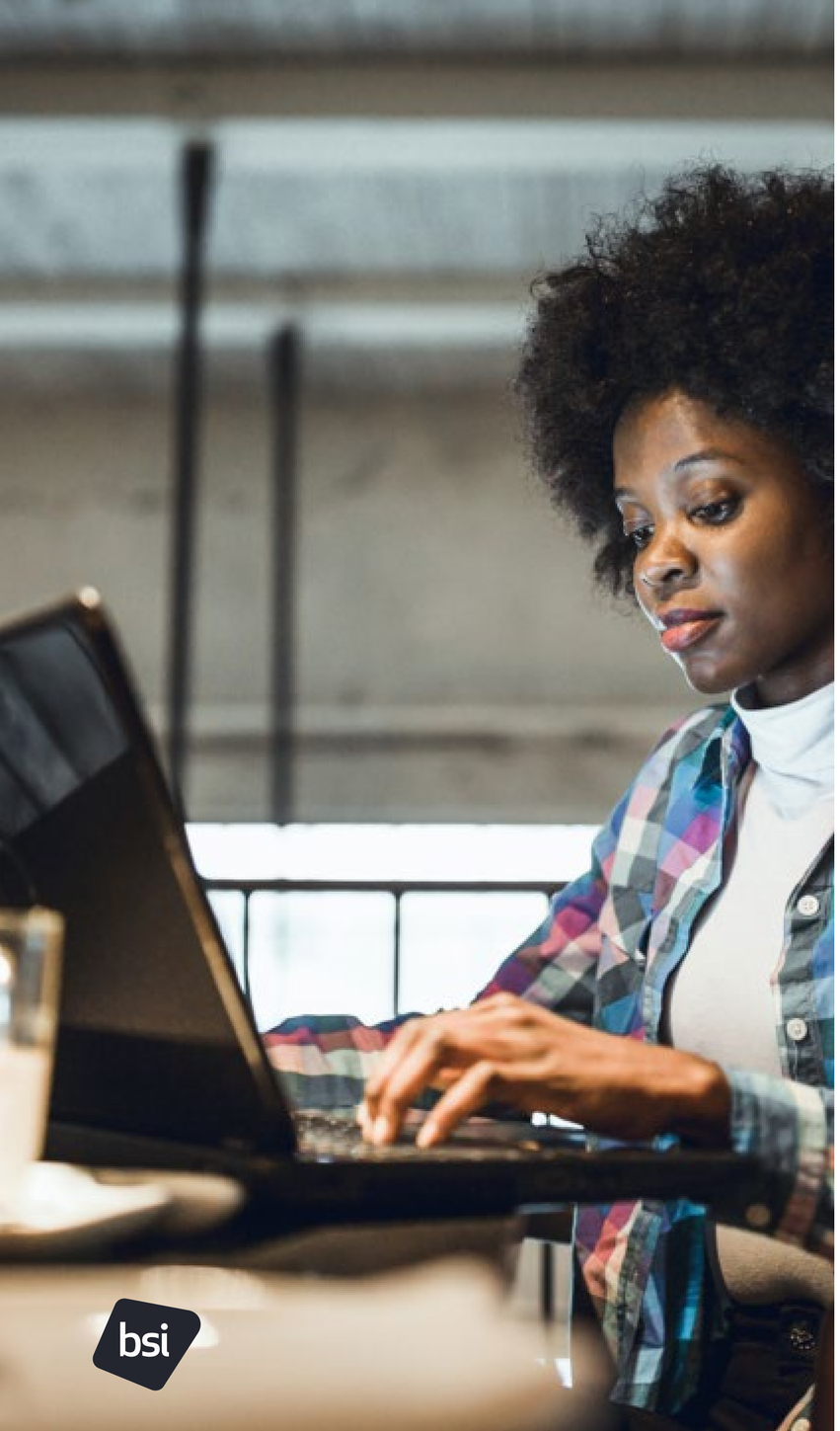
Bridge the Perception Gap in Digital Trust

Strengthening digital trust through training and qualifications



Pressure to meet digital trust expectations

Digital trust can influence a business's success.

It plays a fundamental role in customer loyalty and organizational growth. It's also a key component in driving forward responsible and sustainable innovation.

So how effectively are organizations meeting customer expectations and employee needs when it comes to digital trust? And what processes are they putting in place to sharpen their cybersecurity, privacy and data governance processes?

In this guide, we explore how organizations can inspire confidence and strengthen digital trust practices through the use of training.

Using exclusive research and insights from digital trust industry leaders, we'll reveal:

- **Why digital trust perception gaps exist**
- **The firsthand experiences of IT leaders who manage digital trust**
- **How organizations can build resilience through training**

What is digital trust?

Digital trust is a domain of organizational resilience that empowers organizations to safeguard their information, people, systems, and technology to ensure safety, security, compliance, privacy, ethical requirements, and brand reputation to enable business effectiveness and efficiency.

Digital trust: a balancing act

The evolution of digital technology has created numerous opportunities for organizations over recent years. It has enabled data-driven decision making, driven the development of hyper-personalized products/services, and unlocked the potential of Artificial Intelligence (AI). All of this has benefited customers, who place a strong level of trust in organizations when it comes to protecting their data.

Yet, there is a disconnect between customer perception of digital trust and the reality of coverage within organizations.

Research from McKinsey shows that 70% of customers believe that companies they deal with protect their data, which strengthens digital trust. Meanwhile, 57% of executives have reported that their organization suffered at least one material data breach in the last 3 years[1].

Cyberattacks on corporate networks rose 30% year-on-year globally in Q2 2024.

While most organizations have implemented robust information and data management processes to prevent cyber threats, these breaches can damage trust with customers, stakeholders, and regulators.

Research by the Information Systems Audit and Control Association (ISACA) surveyed more than 5,800 digital trust professionals who said that organizations with a low level of digital trust also suffer[3]:

- more privacy breaches and cybersecurity incidents;
- loss of customers;
- less reliable data for decision-making;
- a negative impact on revenue; and
- a slower ability to innovate.

While this undoubtedly adds pressure to organizations, it also unlocks a new opportunity. Those who are able to proactively combat cyberattacks and strengthen resilience can protect their brand reputation and protect revenue. This, in turn, can help build trust with customers and stakeholders while strengthening competitiveness.

So, how much value do organizations place on digital trust? And what measures are they putting in place to strengthen it?

70%

of consumer respondents believe that the companies they do business with protect their data

57%

of executives report that their organizations suffered at least one material data breach in the past 3 years

VS

“Organizations with a low level of digital trust primarily experience reputational decline[2].”

[1] McKinsey, Why digital trust truly matters, September 12, 2022
[2] ISACA, The Trust Gap, May 29, 2024
[3] ISACA, State of Digital Trust Report 2024, May 29, 2024

Understanding the state of play for organizations

During our interviews with IT leaders, we found that many professionals acknowledge the importance of digital trust and the value it can bring to their organization. Some also revealed a need to sharpen their digital trust skills to strengthen future-readiness and better navigate the evolving digital landscape that organizations are currently navigating.

Digital trust is business-critical…

Many respondents indicated that their personal opinions on the importance of digital trust align with their organizations' stances and budget allocations.

"The digital trust of my customers is important because we handle some of the most sensitive data there is."

"The importance of digital trust is well understood by most of the organization."

"In financial services, this is a must. Our organization focuses on digital trust and invests significant time and resources to ensure expectations are met."

…Yet organizations are struggling to stay ahead

Many respondents noted that they would need to strengthen their digital trust capabilities and make continuous improvements to stay ahead of cybersecurity challenges.

"The challenge is the emerging threats … in areas like generative AI. There are new considerations about how data is managed, digital rights, and the trust of data that we consume as customers and corporations."

"Even if current measures might be considered enough, there is the need to constantly evolve, update, and review."

"We are really behind industry peers and need to move quickly to diffuse the growing cybersecurity threats."

"While our current digital trust measures are robust, they may not fully cover emerging near-term risks. Ongoing evaluation and adaptation are crucial."

Perception gap: digital trust training

While our research shows that there are high levels of awareness surrounding digital trust, organizations can do more to strengthen digital trust skills and implement robust processes.

This insight is supported by research from ISACA that revealed another perception gap: while 94% of IT professionals believe digital trust is relevant to their organization, only 27% of organizations are providing any kind of digital trust training to staff[4].

Several respondents we interviewed felt that while their organizations provide basic digital trust training, there is a need for more advanced and frequent training sessions to address emerging cybersecurity threats effectively.

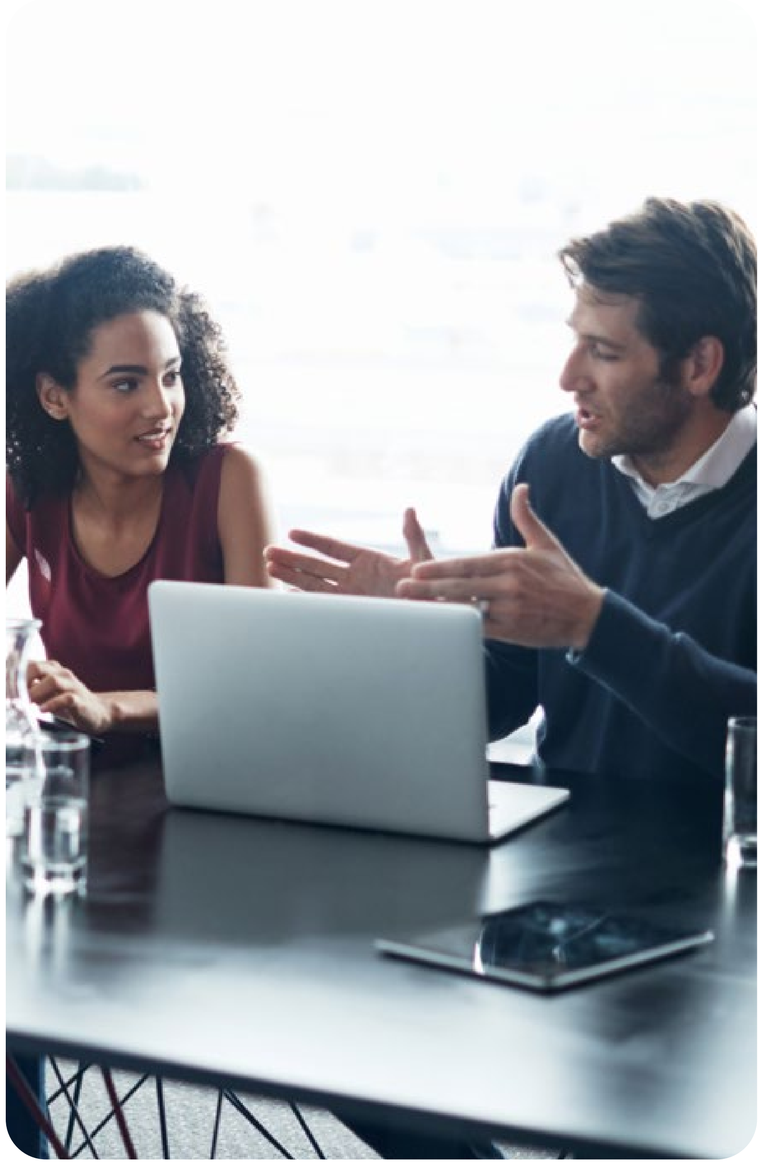
Digital trust training isn't always readily available

"Nothing is provided. I am not even sure if it would exist anywhere in the organization."

"[I] do not receive much training and want more. Digital trust is critical, and [I] have to search on my own for this type of training."

"We are working on implementing some plans in this area, but nothing concrete has happened yet."

"While 94% of IT professionals believe digital trust is relevant to their organization, only 27% of organizations are providing any kind of digital trust training to staff[4]."



[4]The Digital Trust Paradox, May 9, 2023:

Harnessing the power of digital trust training

It’s understandable why many organizations may struggle to find the time and resources to undertake digital trust training.

It is, however, one of the most effective tools your organization can leverage to strengthen resilience and combat cyberattacks. By equipping your people with the right training and skills, they can handle cybersecurity, privacy and digital governance more effectively and unlock a new trajectory of success.

Having a highly knowledgeable and skilled workforce in digital trust will also enable an innovative environment to prosper. This can unlock new market opportunities and help attract new customers while strengthening loyalty.

Recent research by the ISACA[5] reveals the wide-ranging benefits digital trust creates for organizations. They include greater resilience, accountability, customer confidence, and growth, as well as:

positive reputation (71%);

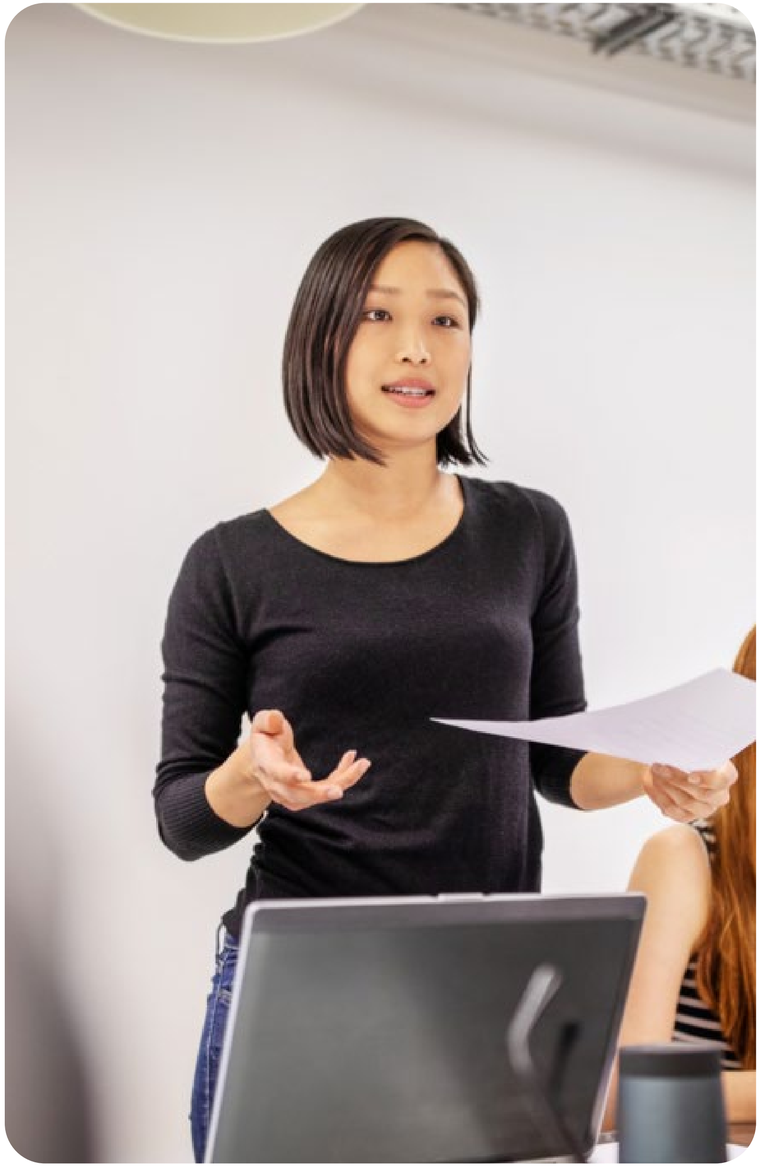
more reliable data for decision-making (60%);

fewer privacy breaches (60%);

fewer cybersecurity incidents (59%);

stronger customer loyalty (56%); and

greater agility due to confidence in your technology and systems (44%)[6].



[5] ISACA, State of Digital Trust Report 2024, May 29, 2024:
[6] Cyber Magazine, Research: digital trust strategies are not a priority, May 25, 2023

Bridge the gap with BSI Digital Trust Training

Take the first step to bridging the perception gap today. As your partner in progress, we can help you continually improve digital trust and reap the rewards of increased resilience, customer confidence, and growth.

All of our digital trust training courses and qualifications are led by experts in the field. They are designed to help you learn in a way that works for you, whether that's live online, in person, or self-paced with on-demand eLearning.

Explore our range of courses:

Cybersecurity and privacy

Cybersecurity
Gain the knowledge and skills you need to build resilience around your information security management.

Our cybersecurity courses include the fundamentals of blockchain, Certified Ethical Hacker (CEH) training, and Certified Information Systems Security Professional (CISSP) training.

Data and privacy
Apply best practice in achieving and maintaining compliance with EU data protection standards across differing regulatory environments with our GDPR and Information Compliance training courses.

Demonstrate data privacy and plan and implement measures in preparation for proposed new regulation. Explore our range of ISO 27701 Privacy Information Management and BS 10012:2017 Personal Information Management System (PIMS) data privacy training courses.

Digital governance and risk control

Artificial Intelligence
Prepare for upcoming AI regulations to create a safer and more beneficial environment for AI-enabled products, services and management systems. Understand the ethical, legal, and compliance aspects of AI.

Our AI training courses cover core areas such as AI Concepts and Terminology, Artificial Intelligence Management Systems (AIMS), and neural network robustness.

Digital Supply Chain
You operate with a diverse, complex and interlinked digital supply chain in a fast-moving business ecosystem. You also rely on factors such as quality, reliability, security, and speed to ensure business as usual.

Our training courses help you understand the modern digital supply chain and embed best practices that will prepare you for future success.

Let’s build a more resilient digital future together

For more information about which digital trust courses are right for your businesses, or to speak to one our experts, visit: www.bsigroup.com/th-th/forms/general-enquiry/

Call: +66 2 026 5297
Visit: **bsigroup.com/**th-th