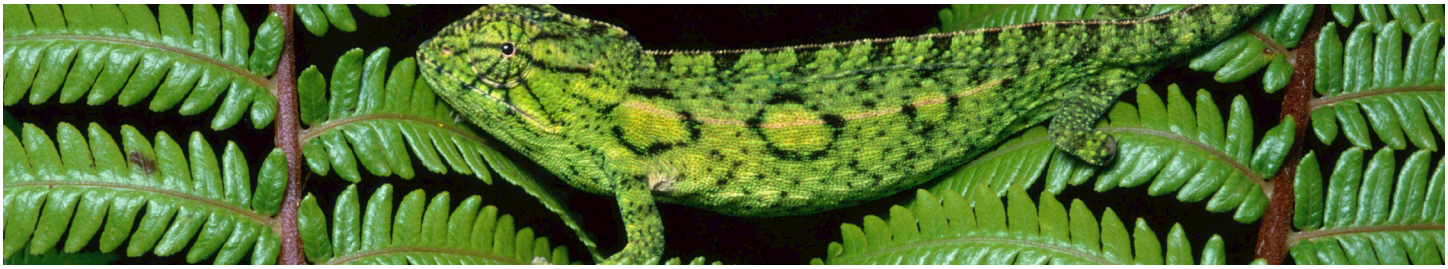


# Adaptability is the key to an effective cyber security culture

As business needs and outcomes change, your company's security mindset and tactics must evolve to stay in sync.

### Key takeaways

- **Changes in the threat landscape require changes in how a company thinks about security.** New ways of working expose businesses to novel threats. Strong organizations will recognize this and adapt their thinking and behavior accordingly.
- **Adaptability is key to a strong security culture.** Companies should focus on skills that allow employees to develop a mindset that treats security as an ever-evolving objective that requires constant review, rather than a "set and forget" approach.
- **A strong security culture covers the basics but doesn't stop there.** Established training methods like phishing simulations are still important, but they must be augmented with other forms of education and engagement that raise employees' awareness of new and evolving security threats and reflect the specific goals of a business.

Cyber security is a mindset and a technology challenge. Businesses in every industry depend as much on informed workers as they do on strong protocols and effective cyber security tools. The way a company thinks about itself, in terms of protecting its most essential assets (e.g., confidential data, operating systems or internal networks), is a function of what is commonly called a "security culture." But what exactly defines that culture?

This is not a new or rhetorical question. A 2020 study found that while 94% of organizations surveyed believed that establishing a security culture was an important business goal, there was little agreement on which metrics could measure that culture's effectiveness.[1]

Given the rapid pace of change in the security field and business operations, defining a security culture is now even more difficult. As workflows, technology tools and threat landscapes shift, companies may struggle to maintain a cohesive approach that applies to every employee, regardless of their role, seniority or level of responsibility.

Adaptability is one fundamental principle that can help any business build a culture that is attuned to challenges and capable of harnessing new methods and tools efficiently.

While any company will need to respond to new trends and opportunities, changes in recent years have been so significant — including the shift to hybrid or remote work policies, the proliferation of data and the evolution of security tools — that they may require a rethinking of what it means to be secure in mindset and practice.

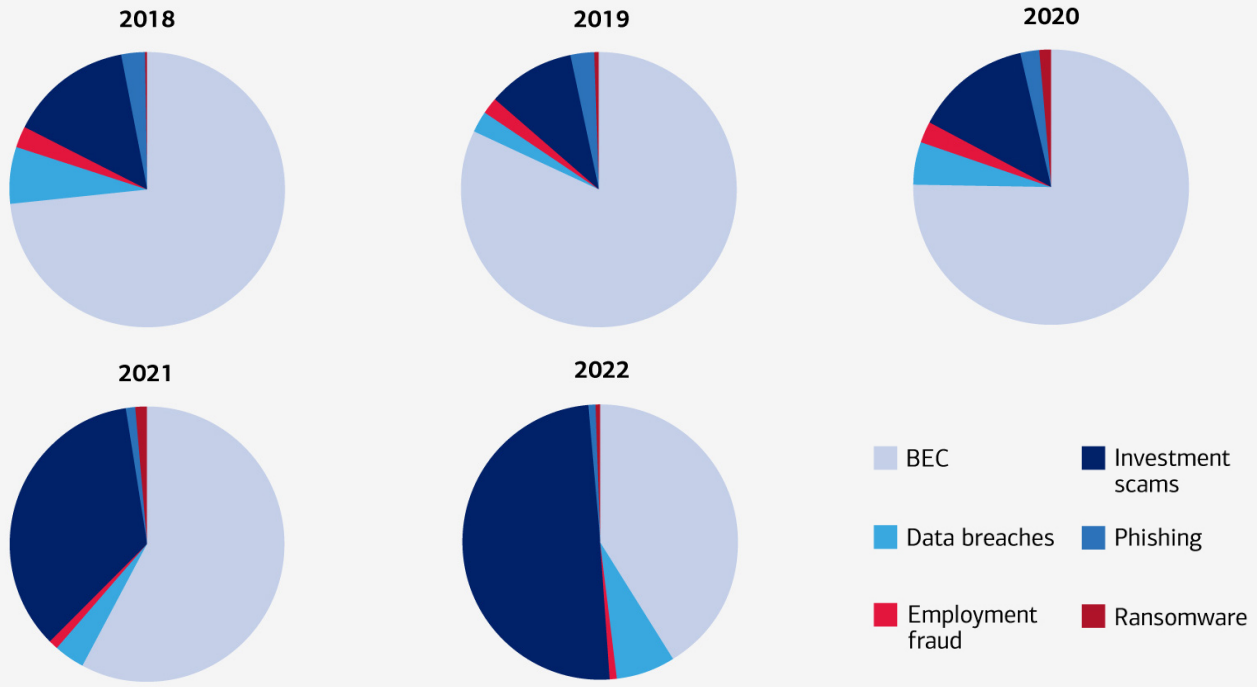
[1] KnowBe4 and Forrester Consulting, "The Rise of Security Culture," April 2020.

Companies should look at security as an ever-evolving challenge and business requirement. As security experts build new tools and methods for detecting and responding to threats, business goals and culture must keep up.

This always-on, dynamic approach could be described as an adaptive security culture. This culture should take shape in a company-wide mindset that augments technical tools and employee readiness to create a layered defense. Furthermore, the massive changes to the workplace present a unique opportunity for businesses to build a strong culture — or make it even more resilient and defined than it was before the impact of the COVID-19 pandemic.

## Losses due to key cyber crime types over the last five years

Because the threat landscape is constantly changing — as evidenced by the shift in dollars lost to various types of cyber crime from year to year — businesses must make adaptability an important factor when establishing a security culture. For example, losses from investment scams reported to the FBI increased by a dramatic 884% between 2020 and 2022 alone, due to a steep increase in crypto-investment fraud.




- **BEC (business email compromise):** A form of phishing that targets businesses or individuals who regularly perform transfer-of-fund requests.
- **Data breaches:** The use of a computer intrusion to acquire confidential or secured information.
- **Employment fraud:** Tricking individuals into believing they are being offered employment, but instead defrauding them of money.
- **Investment scams:** A deceptive practice that induces investors to make purchases based on false information.
- **Phishing:** The use of emails, text messages or phone calls to trick a victim into revealing confidential information and/or login credentials.
- **Ransomware:** Malicious software designed to block access to data or networks until a ransom is paid.

# Urgency and opportunity

Several trends that affect the way companies work, prioritize data and train their employees have direct implications for security culture.

- **Technology continues to improve — on both sides.** Defenses for cloud, networks, endpoints and smart devices have become much more sophisticated, meaning social engineering tactics aimed at humans (who may be tired, overworked or unsuspecting) remain effective and popular with bad actors. Moreover, technical advances in machine learning and virtual reality are available to anyone, and criminals will continue to leverage them to work around modern defenses.

- **Hybrid and remote work became and remain common.** Company networks in many industries were forced to expand during the pandemic, and many will never go back to exclusively in-office working arrangements. This creates a need to secure virtual networks and implement stricter authentication methods.

- **Data is the new front line.** Data harvested from smart devices and machines, partner companies, clients and many other types of third parties is critical to businesses — and it increasingly resides outside a business's traditional security perimeter. Businesses, therefore, depend on advanced methods for prioritizing, storing and transferring data, as well as protecting it wherever it resides.

- **Turnover reduces institutional knowledge.** The U.S. Federal Reserve reports that during the COVID pandemic actual retirements exceeded predictions by 2.6 million.[2] Many retirees took valuable cultural knowledge with them, creating a gap, but also opening an opportunity to instill security practices and prioritization in the workers who replace them.

# Questions for evaluating an adaptive security culture

In general, a security culture is likely approaching maturity when employees regularly think of their work and responsibilities in terms of how they may affect company defenses. There should also be general awareness that the security culture will evolve over time by necessity. The prevailing assumption throughout the organization should be that security awareness and adaptation are integral to business objectives and resiliency.

Company leaders who are seeking to enrich their security culture can evaluate their current approach by examining and answering some fundamental questions:

- **How does the company create an adaptable, updateable security education program?** It's not unusual for a business to stand pat with a limited repertoire of tests and training materials. For instance, according to one analysis, phishing attempts increased by 61% in 2022 over 2021,[3] which might justify the need for enhanced training and awareness-building. But when was the last time the training materials and tests were updated? Are there emerging threats in the industry that are not reflected in trainings? Have other methods for discussing threats and proper procedures been explored (e.g., informal discussions, more advanced trainings)? Do trainings encourage employees to think proactively about security, and to ask follow-up questions?

[2] Federal Reserve Bank of St. Louis, "Retirements Increased During the COVID-19 Pandemic: Who Retired and Why?" March 30, 2022.
[3] Security Magazine, "Over 255M in phishing attacks in 2022 so far," October 26, 2022.

- **Does the company's security posture reflect an expanded perimeter and new data protection requirements?** If a business finds ongoing value in remote or hybrid work, it should undertake a corresponding update of security protocols. Yet, during the pandemic, many companies shifted work arrangements out of necessity and emphasized the continuity of business functions more than security. Leaders should now consider whether there has been a sufficient review of where data travels and how it can best be secured as the definition of the security perimeter continues to change.

- **Are company security practices aligned with business objectives and corporate culture?** Independent of the individual protocols and processes, a company should review how it talks about the threats it faces, and how best to foster a holistic understanding of what employees should expect while doing their jobs. Companies all have different business models and goals that necessitate the acceptance of — and protection against — very specific risks. For instance, a medical practice's biggest security challenge might be securely storing patient data, while communicating with vendors securely might be the top priority for a manufacturing company. Is security discussed in terms of business objectives and outcomes? Is security culture discussed in terms that are consistent with how the company talks about its sales, operations or human resources culture?

It's important to note that even the most adaptive security culture is not infallible. Moreover, overloading employees with information will not make them alert, security-focused assets to the company. Business leaders will constantly need to look for ways to make trainings immersive, differentiated and interesting to ingrain the message that good business depends on secure practices. Even in a strong culture, it will take time to cultivate behavior and ultimately create an adaptable, security-first mindset. ■