BANK OF AMERICA INSTITUTE

BANK OF AMERICA

Transformation

Creating a security-focused organization

07 March 2024

Key takeaways

- Thanks to ongoing shifts in the threat landscape, companies must continue to advance their approaches to security. With more than 1,800 data breaches across the US in 2022, 63% more than a pre-pandemic year, corporate leaders are under increasing pressure to implement cybersecurity controls that evolve with their business practices.
- Today, 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.
- We identify and explore five tenets to consider when building an adaptive, security-first company culture: capabilities, collaboration, communication, education and empowerment.

Adaptability: Key to an effective cybersecurity culture

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.” Today, businesses in every industry depend as much on informed workers as they do on strong protocols and effective cybersecurity tools. But what exactly defines an adaptive and effective cybersecurity culture?

The answer isn’t clear cut. In fact, 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]

In Cybersecurity: Landscape, impact, and what comes next we discussed how widespread corporate adoption of a post-pandemic hybrid working model meant that cybersecurity controls were sometimes bypassed, contributing to an increase in cyber threats throughout 2022. In fact, over the course of that year, there were more than 1,800 data breaches in the US, 63% more than a pre-pandemic year[2] and the average cost per incident in the US was $4.2 million, the highest in 17 years.[3]

Yet despite, or perhaps because of, the everchanging threat landscape, one thing is clear: adaptability is a fundamental principle that can help any business build a cybersecurity culture that is attuned to challenges and capable of harnessing new methods and tools efficiently.

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. And as workflows, technology tools and threat landscapes shift, companies need to focus on maintaining a cohesive approach that applies to every employee, regardless of their role, seniority, or level of responsibility.

This always-on, dynamic approach could be described as an “adaptive security culture,” one that 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.

1 KnowBe4 and Forrester Consulting, “The Rise of Security Culture,” April 2020.

2 Identity Theft Resource Center

3 2021 data, Cost of a Data Breach Report 2022, IBM

Identify the opportunities

To further lay out the need for an adaptive security culture, companies must first identify the trends that can affect the way they work, prioritize data, and train their employees, and note how these trends may have direct implications on their workforce and business goals moving forward.

- **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 artificial intelligence / machine learning and virtual reality are available to anyone, and criminals will continue to leverage them to work around modern defenses. See Caution: Safety first! for more.

- **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, which 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. Therefore, many businesses depend on advanced methods for prioritizing, storing, and transferring data, as well as protecting it wherever it resides.

- **Turnover reduces institutional knowledge.** The US Federal Reserve reports that during the pandemic actual retirements exceeded predictions by 2.6 million.[4] Many retirees took valuable cultural knowledge with them, not only creating a gap, but also opening an opportunity to instill security practices and prioritization in the workers who replace them.

Evaluate current practices

The first step in building and implementing an adaptive security culture, is to understand where important practices currently stand and identify what a successful security culture means to a business. 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, while also understanding 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.

To evaluate where their business currently stands, company leaders who are seeking to enrich their security culture can evaluate their current approach by examining and answering several fundamental questions:

How does the company currently create an adaptable, updateable security education program?

It's not unusual for a business to stick with a limited repertoire of tests and training materials. For instance, according to one analysis, phishing attempts increased by 61% in 2022 over 2021,[5] which might justify the need for enhanced training and awareness-building.

Companies should ask themselves when the training materials and tests were last updated and if there are emerging threats in the industry that are not reflected in trainings. They should also ensure that other methods for discussing threats and proper procedures have been explored (e.g., informal discussions, more advanced trainings) and that the trainings encourage employees to think proactively about security, and to ask follow-up questions.

Does the company's security posture reflect an expanded perimeter and new data protection requirements?

During the pandemic, many companies shifted work arrangements out of necessity and emphasized the continuity of business functions more than security. Now, however, if a business finds ongoing value in remote or hybrid work, it should undertake a corresponding update of security protocols. 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.

[4] Federal Reserve Bank of St. Louis, "Retirements Increased During the COVID-19 Pandemic: Who Retired and Why?" March 30, 2022.

[5] Security Magazine, "Over 255M in phishing attacks in 2022 so far," October 26, 2022.

Companies 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.

Implement a security-focused culture: Five pillars of adaptability

Whether a company is trying to bring a higher level of cybersecurity awareness into its culture or establishing a culture of adaptive security there are several key areas of opportunity. While these areas often overlap, defining them can help any employee think about their role in a new way, or help them become a security advocate among their colleagues.

Every company should talk about cybersecurity in a way that reflects its evolving business needs, goals, and culture. For this reason, a framework based on the following five tenets can provide a good starting point no matter how mature a company's cyber awareness may be. Additionally, we identify questions to help organizations and their employees establish a security-oriented company culture that's adaptable to both evolving threats and changing business priorities and goals.

1. Capabilities

For a company culture to be truly adaptable and responsive, it will require tools that are chosen not only for its ability to help employees do their jobs in a secure manner, but also for its adaptability to how and where employees are currently working.

For instance, if a company allows hybrid or fully remote work schedules, employees need tools and processes that aid secure sign-on, up-to-date device management and effective tracking and protection of data. If the culture is collaborative and security-conscious, it will be easier for workers to communicate how well these capabilities are serving them, and for leaders and experts to gauge how familiar the workers are with available protections.

Importantly, the capabilities should always be developed in line with business objectives. There is little to be gained by investing in tools or processes that do not protect the data that the company depends on or that don't align with normal activities. Questions that a company should ask, include:

- Do your tools provide employees with the most up-to-date security to protect the devices and data the company depends on — regardless of where they are working?
- Do these tools align with your business objectives?
- Do you have processes in place for employees to communicate how well your tools and capabilities are serving them?
- Do you have processes in place for leaders to measure how familiar workers are with available security capabilities?

2. Collaboration

Businesses rely on repeatable processes, but sound processes often originate in informal brainstorming sessions. Employees who work together should be given the opportunity to discuss what they need to securely perform their jobs and support each other's roles.

In part, this can mean more transparency and openness about mistakes with security implications, and certainly should include sharing up-to-date information about industry cyber news. If security processes are already in place, colleagues could arrange regular lunches or create internal messaging threads where the benefits and limitations of the processes can be discussed candidly.

Collaboration can also help remove barriers that keep security experts in the company siloed from other employees. Rather than one-way communication focused on experts telling employees what not to do, companies of all sizes can encourage dialogue where non-experts can ask questions and discuss the limitations of current processes. Important questions are:

- Do you have regularly scheduled cross-departmental brainstorming sessions for employees to discuss what is needed to create a secure work environment?
- Do you have a process in place for sharing up-to-date information about industry cyber news?
- Do you have a method for employees to ask questions about or provide feedback on current security processes?

- Do you have an easy way for employees to report possible security breaches or mistakes they've made that might have security implications?

3. Communication

As with any business objective, security must be discussed in language that is consistent to the organization, its priorities, and the industry in which it operates. It also must be a regular topic of communication for company leaders, who should take every opportunity in their messaging to pair security with overall company health and success.

Leadership can emphasize the cultural importance of security by making progress in training courses and test exercises a regular part of performance reviews. But employees should also be reassured that they will be valued for speaking up, even if it means confessing to mistakes or giving constructive feedback about security oversights or flawed processes. Company leaders should ask themselves the following:

- When you communicate with employees about security, do you use language that is consistent with your organization's priorities and those of your industry at large?
- Is security a regular topic of communication among all company leaders?
- Do leaders pair security with overall company health and success when communicating with employees?
- Do your employees feel valued for speaking up about security — whether to report their own mistakes or provide constructive feedback on security oversights or flawed processes?

4. Education

There are few areas that afford companies a better opportunity to emphasize cultural shifts and security priorities than education and training exercises. Changes in workforce composition — e.g., with tenured employee retirements and additions of new hires — contribute to greater demands on education and training to get back to equilibrium.

But training must be highly specific to the company's workforce and business function to be effective. It should be tailored to employees' savviness about technology and security and reflective of how the majority makes decisions — and it must be updated regularly to reflect emerging threats.

Businesses can also consider tabletop exercises or simulated events that help employees visualize how a genuine cyber event might occur and think through the steps of their specific response. Leadership can reinforce trainings with regular updates about security practices and industry-specific threats, or through surveys that gauge the extent of employees' knowledge of cyber security without the pressure that comes from a formalized test. Education-focused questions, include:

- Are your security education and training programs tailored to your specific workforce and business functions?
- Do you regularly update education and training to reflect emerging threats?
- Do you include tabletop exercises or simulated events to help employees visualize how a cyber event may occur and how they should respond?
- Do you periodically test employees on practices for avoiding cyber risk?

5. Empowerment

When employees believe security is a secondary consideration, or someone else's responsibility, they are not well-positioned to be responsible participants. Since any employee has the potential to unknowingly precipitate a cyber incident, each needs to understand the importance of their role and how they contribute to a secure work and business environment.

Because distraction and fatigue are often cited as causes of cyber incidents, employees should feel that slowing down is justified and valuable when they receive suspicious emails or requests. For example, employees who must authorize payments should feel they have discretion to act — or delay action — until they can confirm the legitimacy of a request. If this employee works in a security-focused culture, they will be conditioned to think beyond simply completing the task.

In fact, according to one study, 82% of data breaches involve people and the choices they make.[6] Another found that while 36% of people surveyed had made a mistake that compromised their company's cybersecurity, 21% of employees say they didn't tell their IT team about a mistake they had made.[7]

[6] Verizon, "2022 Data Breach Investigation Report," May 2022.

[7] Tessian, "The Psychology of Human Error 2022," March 2022.

All employees should be encouraged to ask security-focused questions, or to reach out to a security expert with their concerns. Most of all, they should feel empowered to report an incident, even if it involves a mistake they've made, such as responding to a phishing email. Company leadership should answer the following questions:

- Do you encourage employees to contribute to cyber security defense by empowering them to act (or delay action) when they suspect a potential risk, such as a questionable email?
- Do you have clear and easy processes for employees to report incidents (or mistakes) without fear of reprisals?
- Do your employees understand the importance of their role in contributing to a secure work and business environment?

Create an effective security framework

Cybersecurity is a technical challenge for any business, but a more comprehensive view of cybersecurity involves considering the human factor. Making adaptive security an essential part of company culture can have a positive impact on a business's overall success and encourage employees to keep security top of mind.

While a cultural shift requires leadership support, a top-down approach isn't enough. Employees at every level, job description and degree of technical expertise need to think about cybersecurity as a business objective — one that requires their cooperation and focus. For a business to harness the power or an adaptive security culture, all employees need to think of their essential responsibilities, processes, and tasks in terms of security — and understand that security needs to adapt as both cyber threats and business objectives evolve.

Contributors

Vanessa Cook

Content Strategist, Bank of America Institute

Sources

Bank of America Cyber Security Journal

Kristopher Fador

Chief Information Security Officer, Bank of America

Roland Chan

Cyber Crime Defense Executive, Bank of America

Disclosures

These materials have been prepared by Bank of America Institute and are provided to you for general information purposes only. To the extent these materials reference Bank of America data, such materials are not intended to be reflective or indicative of, and should not be relied upon as, the results of operations, financial conditions or performance of Bank of America. Bank of America Institute is a think tank dedicated to uncovering powerful insights that move business and society forward. Drawing on data and resources from across the bank and the world, the Institute delivers important, original perspectives on the economy, sustainability and global transformation. Unless otherwise specifically stated, any views or opinions expressed herein are solely those of Bank of America Institute and any individual authors listed, and are not the product of the BofA Global Research department or any other department of Bank of America Corporation or its affiliates and/or subsidiaries (collectively Bank of America). The views in these materials may differ from the views and opinions expressed by the BofA Global Research department or other departments or divisions of Bank of America. Information has been obtained from sources believed to be reliable, but Bank of America does not warrant its completeness or accuracy. Views and estimates constitute our judgment as of the date of these materials and are subject to change without notice. The views expressed herein should not be construed as individual investment advice for any particular person and are not intended as recommendations of particular securities, financial instruments, strategies or banking services for a particular person. This material does not constitute an offer or an invitation by or on behalf of Bank of America to any person to buy or sell any security or financial instrument or engage in any banking service. Nothing in these materials constitutes investment, legal, accounting or tax advice.