How to create a security-focused culture in your company

A cyber-aware organization requires open dialogue, incisive action and empowered employees. Here are five tenets to consider when building an adaptive, security-first company culture.

Key takeaways

Security culture must evolve with the business
Whether you are a company leader, a seasoned mid-level worker or a new employee, you have a role in maintaining company security and a responsibility to keep learning. Keeping these points in mind can help you be part of the solution:

- **Lean on existing company culture.** The language used in sales, operations, human resources and every other aspect of business communications usually reflects and is consistent with the company culture. Security is no different: It should always be discussed in terms that are consistent with how the business at large promotes and evaluates itself.
- **Align security with business goals.** Every employee should think of security in terms of the company's overall success. Leaders should take every opportunity to connect good security habits with successful outcomes.
- **Remember that security must always evolve.** As the means of doing business change, the ways employees are trained and tested must adapt to reflect those changes. Regularly revisit the exercises used to evaluate employee readiness and use all communication channels to keep new and changing security threats on the company's radar.

Cyber security is a technical challenge for any business, but a more comprehensive view of cyber security involves considering the human factor.

According to one authoritative study, 82% of data breaches involve people and the choices they make.[1] Another found that while 36% of people surveyed had made a mistake that compromised their company's cyber security, 21% of employees say they didn't tell their IT team about a mistake they had made.[2]

Making security an essential part of company culture can have a positive impact on these statistics and on a business's overall success. Encouraging every employee to think about security means that in certain circumstances technology is de-emphasized and the human component is acknowledged through open discussion.

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 cyber security as a business objective — one that requires their cooperation and focus. 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.

[1] Verizon, "2022 Data Breach Investigation Report," May 2022.
[2] Tessian, "The Psychology of Human Error 2022," March 2022.

Whether a company is trying to bring a higher level of cyber security awareness into its culture or establishing a foundational objective of adaptive security — that is, security that evolves dynamically as threat vectors and business needs change — there are several key areas of opportunity. These areas often overlap with each other; however, defining them can help any employee think about their role in a new way, or help them become a security advocate among their colleagues.

Five pillars of an adaptive security culture

Every company should talk about cyber security 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:

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

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.

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.

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.

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.

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. ■

Creating an effective security framework

There are many models for developing a security-focused culture in businesses; most are useful guides rather than strict plans. The zero trust model, for instance, provides a framework for operations and is based on the principle that trust and access should be granted only on an as-needed basis. The National Institute of Standards and Technology describes zero trust in terms of "guiding principles," such as:

- **Prevent** unauthorized access to data and services.
- **Minimize** "implicit trust zones."
- **Secure** all communication, regardless of network location.
- **Consider** all data and computing services to be valued resources.
- **Enforce** dynamic authorization protocols, including multifactor authorization.
- **Update** security via ongoing collection of data and insights related to enforcement.[3]

[3] NIST, "Zero Trust Architecture," August 2020.

Five pillars of an adaptive security culture checklist

Apply these questions to your organization and security program to establish a security-oriented company culture that's adaptable to both evolving threats and changing business priorities and goals.

Capabilities

- ❑ 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?

Collaboration

- ❑ 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?

Communication

- ❑ 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 your company leaders?
- ❑ Do your 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?

Education

- ❑ 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?

Empowerment

- ❑ 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?

For use in external marketing and communications materials when the content of the material discusses both products and services offered through the bank and broker/dealer affiliates.

"Bank of America" and "BofA Securities" are the marketing names used by the Global Banking and Global Markets divisions of Bank of America Corporation. Lending, other commercial banking activities, and trading in certain financial instruments are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Trading in securities and financial instruments, and strategic advisory, and other investment banking activities, are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, by locally registered entities. BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA.
Investment products offered by Investment Banking Affiliates:

Are Not FDIC Insured	Are Not Bank Guaranteed	May Lose Value