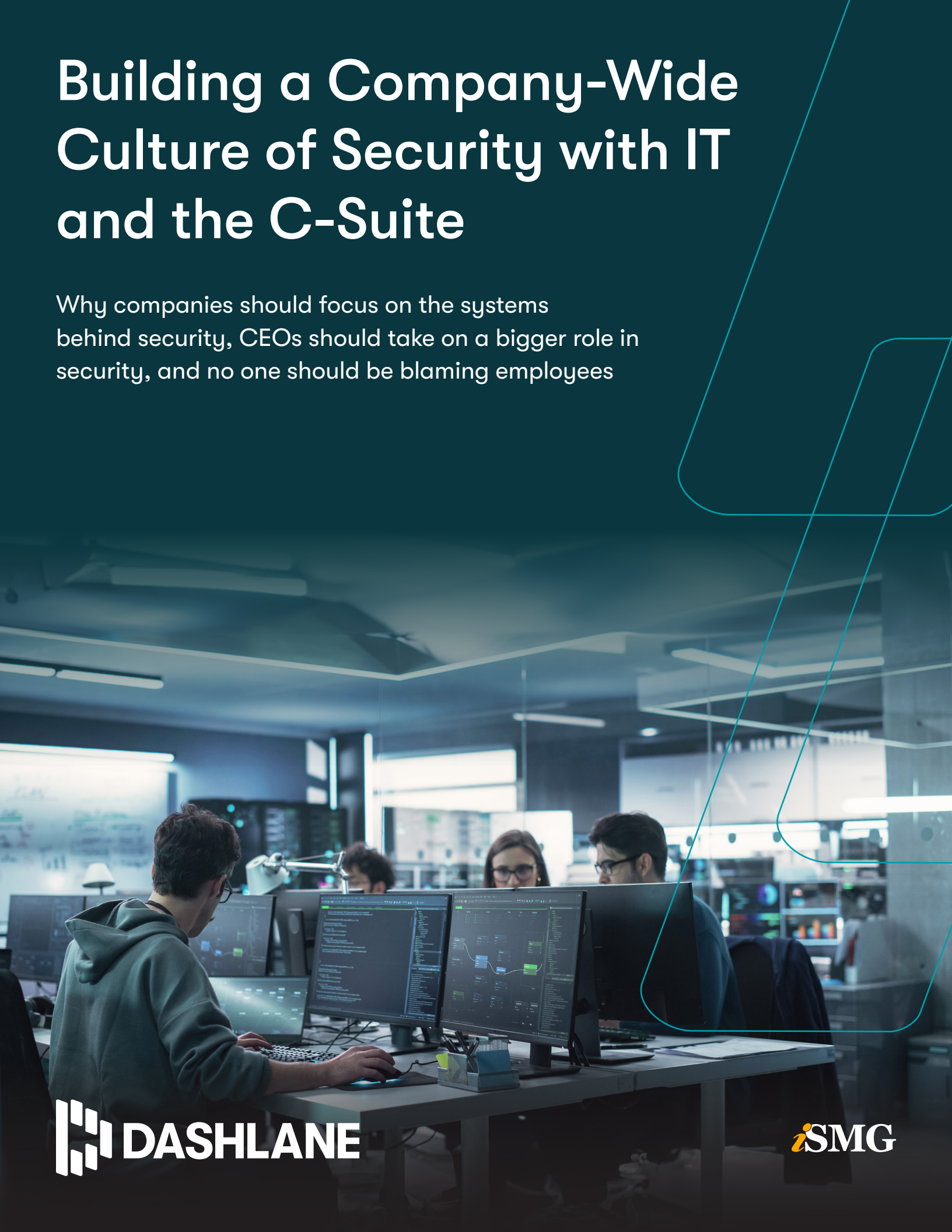
Building a Company-Wide Culture of Security with IT and the C-Suite

Why companies should focus on the systems behind security, CEOs should take on a bigger role in security, and no one should be blaming employees



DASHLANE

ISMG

Security Culture: The Forgotten Layer of Cyber Defense

As cyber threats continue to become more sophisticated, many organizations focus on the technical aspects of defense. Budgets are allocated for next-generation security controls and to properly staff security operations with expert analysts and threat hunters. Too often, however, organizational leaders and IT professionals forget that building a strong security culture is their best defense.

This report is intended to help executives, senior IT leadership, and board members understand the importance of their roles in protecting their organizations and how they can build better resilience and business success with a security culture centered on the people who make up their organizations.

What is security culture?

Security culture is the set of values, attitudes, and everyday habits that reflect cybersecurity best practices and an understanding that everyone plays a role in maintaining security. It defines the expected norms of behavior—what people do of their own accord when no one is watching or measuring.

> **Culture is like an iceberg. The bulk of it, the submerged part, comprises the shared beliefs and assumptions that are often shaped over generations and can sometimes punch a hole through titanic corporate initiatives.**
>
> **Ajit Kambil**, Global CFO Program Research Director, Deloitte
>
> Source

Building a culture of security delivers a wide range of benefits for organizations:

- Company-wide awareness and understanding, which leads to better day-to-day security behaviors and hygiene
- Protection of your organization's reputation and customers' trust
- Higher adoption rates of digital security tools, reducing risk and providing greater ROI
- Overall reduction in the risk of a damaging breach

Of course, this type of culture doesn't simply develop by accident. A culture of security is the result of carefully designed systems supported by strong advocacy from the CEO and the rest of the leadership team. When properly developed, a security culture helps employees to understand and embrace their important role in protecting the organization from threats.

Why is having a strong security culture so important now?

While a strong security culture has always been an advantage for organizations, it's quickly becoming a critical element of cyber defense today. AI and other innovations have allowed modern technical defenses to detect malware and malicious behaviors more quickly and effectively than ever before. These innovations have driven cybercriminals to explore new avenues for attack, which show a clear shift from exploiting technology to exploiting human behavior.

According to Verizon's 2023 Data Breach Investigation Report, 74% of breaches in 2023 involved a human element. The top two methods attackers used to steal credentials and access an organization were phishing and pretexting. In addition, attacks using social engineering and Business Email Compromise (BEC) have nearly doubled.

Attackers have learned that while technical vulnerabilities may be lucrative for a time, they are eventually patched, forcing expensive changes in tactics. Unfortunately, when it comes to exposures that arise from human behavior, there are no known patches. The best tool in our arsenal is to inoculate our teams with a culture of security.

What does a culture of security look like?

Achieving a healthy cybersecurity culture isn't simply a matter of rolling out a few posters with catchy slogans and occasional anti-phishing campaigns. When security becomes part of the company culture, the organization will see it reflected in both overall **awareness** and day-to-day **actions** across the workforce.

Awareness Employees feel responsible for the organization's security and understand their role in it.	• Employees are aware that security is part of everyone's job description. • Employees understand what issues should be reported, how to go about it, and where to go if they have questions. • Security topics and tips come up regularly, not just at annual training or during onboarding.
Action Employees reliably take appropriate actions to protect the organization from security threats.	• Security tools are broadly deployed, properly configured, and maintained across all departments. • Employees report phishing emails and similar malicious activity quickly through proper channels. • Employees feel comfortable reporting potential security issues without fear of blame. • Managers and execs lead by example, regularly exhibiting good security hygiene.

> **Beyond our IT team, data security has always been a part of our culture; it's even part of everyone's job description.**
>
> **Shirley Lio**, Chief of Staff to the COO, Finder

Where Do I Start?

So you've identified that your organization doesn't have a strong culture of security, and you're ready to do something about it. Where to start? Productivity guru Tim Ferriss once described culture as what happens when people are left to their own devices—and as an organization, you want their behavior to be aligned with your aims, values, and processes.

Start with an assessment of your company's security culture. There always is one, even if it's weak and hard to pin down.

Build the systems you need for a strong foundation

Starting by asking, "How can I build a culture of security?" It's like building a house without a foundation; it will likely fall apart long before it's finished and not stand the test of time. A strong culture of security is the end result of having effective security systems (tools, plans, and processes) that are understood company-wide and fully supported by executives and the board.

Start your assessment by looking at your organization's security systems and asking a few questions:

- What expectations and processes do you have for employees when it comes to cybersecurity? Are these documented and regularly updated? Are they shared broadly with employees?
- What tools are available to help employees work more securely, and do they all know how to use them? Do all execs and managers use them?
- Do you have communication channels and processes in place to share routine security updates and emergency notifications?
- Do you incentivize positive security behaviors and practices? Do you have any existing practices that might disincentivize an employee from coming forward with information about a security threat?

Having the right systems in place plants the seeds for a healthy security culture. As Dashlane CTO Frederic Rivain says, "Your systems and processes need to foster the right behavior and incentives across the organization. This is how you will generate a strong security culture, not force-feeding employees security warnings."

> **Our goal is to build a culture of security. When we have security built into our processes, our employees can focus solely on patient care.**
>
> **Gabe Kimbrough,** Chief Information Security Officer, Mercy Medical Cedar Rapids

Execs take on the role of cybersecurity champions

Culture is a thread that weaves its way through every part of the organization, and effective change requires deliberate and consistent focus from the top down. While every leader across the organizational hierarchy will have a role to play, change in security culture starts with the CEO and CISO.

The CEO is the leader of security culture

Since the CEO is on the frontlines of the organization, they are often a target of cyberattacks. This makes them uniquely positioned to make a call for change and communicate and model it for the organization. Critical steps for CEOs include:

- Becoming educated about modern cyber threats and the level of risk they bring and staying well informed as the threat landscape evolves
- Setting the strategic vision for the role of security within the corporate culture and how it supports the rest of the organization's culture and profitable business
- Sharing this vision consistently and widely at company-wide meetings and board meetings and in impromptu communications
- Communicating the strategic importance of and full buy-in to the security systems determined by the CISO
- Ensuring the culture of security is built and maintained effectively to keep pace with evolving threats.

> Security is the sum of everything. It starts from the CEO as the key accountable leader who needs to drive the vision, to the IT and security team that sets up systems and processes, to all employees that all have their part to play.

Frederic Rivain, CTO, Dashlane

CISO is the supporter and reinforcer

If the CEO is the conductor of cybersecurity culture, setting the vision, tempo, and direction, then the CISO is the lead violinist, deeply skilled and leading by example, playing the critical parts that drive the melody forward. Key aspects of the CISO's role include:

- Developing, implementing, and updating security policies and systems that match the CEO's objectives and risk management strategy. These guide behavior and decision-making processes related to information security across the organization.
- Overseeing education and awareness programs that inform and empower employees to act securely. By promoting a better understanding of security threats and safe practices, the CISO helps to embed security consciousness into the corporate culture.
- Working across departments to integrate security into all aspects of the organization's operations. By collaborating with other executives and stakeholders, the CISO ensures that security considerations are factored into decision-making processes, project planning, and strategic initiatives.
- Continuously assessing the effectiveness of security initiatives, identifying areas of improvement, and keeping the CEO informed.

> **It's important to us that we build security consciousness into our organizational culture.**
>
> **Eric Hyyppa**, President, National Educational Telecommunications Association (NETA)

Make Employees a Strong Link in the Cybersecurity Chain

With the right systems in place and solid support from executives, you're in a good position to bring cultural change to the rest of the organization. It's a common cliché that humans are the weakest link in cybersecurity, sometimes for good reasons. However, building a healthy culture of cybersecurity flips this notion on its head, leveraging engaged employees as valuable partners in protecting the organization's assets.

Good systems, education, and support drive good behavior

Cybercriminals often exploit common human behaviors, such as seeking shortcuts and workarounds, to gain an initial foothold in an organization. For example, Dashlane research shows that nearly half (44%) of passwords are reused globally, often because it's simpler to remember and employees don't have a secure place to store their dozens or even hundreds of passwords. This makes it much easier for cybercriminals to access sensitive information across multiple accounts with very little effort.

In an organization with a good cybersecurity culture and the systems to support it, employees know that security is everyone's job. More importantly, they're empowered with the tools, skills, and support they need to follow through consistently.

With these systems in place, it's no longer up to every individual to learn about password security best practices and find a way to implement them on a daily basis; it becomes an integral part of the organization's security culture.

Erase "blame culture"

When security incidents happen (and they do, in even the best-protected organizations), time isn't on the defender's side. Every minute before an attack is identified increases the likelihood of a damaging breach. Lower-level employees are often in a position to provide the earliest warning, but they may not sound the alarm for fear of being blamed.

Too often, organizations blame employees for not having perfect security hygiene, causing employees to associate cybersecurity with feelings of fear and overwhelm. They may be afraid to report to IT that they clicked a link in an email that, on second thought, may not have been trustworthy. Or, they may not know how to report the incident and feel too anxious or embarrassed to ask. Regardless of the reason, these fears slow down response and increase risk for the organization.

Cultural Components

A strong cybersecurity culture includes the following:

Technology

A simple, secure tool that stores passwords and provides an easy way to generate strong ones.

Knowledge

Education about how to use that tool and how it fits into their everyday workflow.

Executive Support

Knowledge that all execs and managers use it and encourage its use.

Benefits of a blameless security culture

Establishing a blameless security culture is also a prerequisite to conducting an effective postmortem. In the aftermath of a successful cyberattack or data breach, it's vital to establish the facts and learn from what happened so that weaknesses can be strengthened and flaws rectified. However, in a blame culture, people will seek to defend their actions, are less forthcoming about details, hide root causes, and may seek to cast blame elsewhere.

Eliminating blame and punishment from the security culture is a critical step in ensuring that every employee plays their part in protecting the organization. If you want colleagues to help identify attacks at the very earliest stages, you have to avoid shooting the messenger and also accept false positives with equanimity.

As Dashlane CTO Frederic Rivain notes, "It's easy to blame employees when incidents happen. But shouldn't we blame a poor system that should have prevented employees from being a risk in the first place? That's the role of leadership with the support of the security team: Minimize the opportunity for an employee to become a risk factor."

> **Core to creating an effective cybersecurity culture is recognizing that people make an organization secure, not technology.**
>
> Tom Everard,
> Cyber Culture Expert

Conclusion

Implementing a culture of security ensures all employees are aware of the cyber risks facing their organization and the potential impact of a breach. It also gives them the necessary tools and knowledge to take the appropriate actions. With the right systems in place, paired with clear and consistent support from leadership, your organization's workforce transforms into an essential component in cyber defense, simultaneously reducing risk and strengthening cybersecurity.

Learn More

Learn more by visiting Dashlane's Culture of Security Hub or checking our an expert-led digital event.

About Dashlane

Dashlane is a web and mobile app that simplifies password management for people and businesses. We empower organizations to protect company and employee data, while helping everyone easily log in to the accounts they need—anytime, anywhere.

For more information on how Dashlane can help you improve password security, please reach out to us today.

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 38 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CAREERS INFO SECURITY® CU Just for Credit Unions INFO SECURITY

Data Breach Today HEALTHCARE INFO SECURITY® GOV INFO SECURITY® infoRisk Today

CyberEd.io FraudToday.io PaymentSecurity.io DeviceSecurity.io

CyberEdBoard OT.today AIToday.io CIO.inc

QG MEDIA ATHENA CYBER THEORY GREYHEAD AN ISMG COMPANY Xtra mile LIFECYCLE MARKETING

iSMG

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io