# A new age of cybersecurity culture

## How to harness AI to promote secure workplace behaviors

**KPMG. Make the Difference.**

KPMG International | kpmg.com

# Introduction

> A strong cybersecurity culture is when people do the right thing, understand why cybersecurity is beneficial for the business, encourage and challenge others, and admit when something has gone wrong.



**Akhilesh Tuteja**
Global Cyber Leader
KPMG International

In today's digital and highly interconnected business environment, organizations are rapidly adopting Artificial Intelligence (AI). While this is exposing organizations to new risks, it is also creating countless opportunities, such as new ways to improve operations and efficiencies, unlock value, and grow competitive advantage.

Some forward-thinking organizations are experimenting with AI in their cybersecurity function, to improve risk detection and response. However, an aspect that holds great potential, but is somewhat unexplored, is how AI can help organizations to boost their cybersecurity culture, especially when it comes to cyber Human Risk Management (HRM).

Cyber HRM is essential to cybersecurity culture, as the way people manage technology is the window through which threat actors can infiltrate organizations. A Verizon study found that 68 percent of cybersecurity breaches involved a non-malicious human element, such as a person falling victim to a social engineering attack or making an error.[1]

In all organizations, but particularly ones with diverse ways of working across geographies, building a comprehensive and sustained cybersecurity culture can be challenging. Cybersecurity culture complexities can include how to overcome change resistance, how to adopt emerging technologies securely without slowing down innovation, how to manage interconnected systems securely, how to make the most of metrics and measurement, and more. Therefore, KPMG, along with Cybersecurity at Massachusetts Institute of Technology (MIT) Sloan (CAMS), part of Sloan Management School Cybersecurity Research Division, set out to gain a better understanding of cybersecurity culture, its challenges, and how AI could make an impact.[2]

To explore this idea, in early 2024 KPMG and MIT undertook a quantitative survey of approximately 40 cybersecurity leaders, subject matter experts, and cross-industry executives from diverse industries and forums.[3]

This survey asked about the current level of cybersecurity culture in organizations, views on the potential of AI to influence cybersecurity behaviors, and current approaches to measuring cybersecurity culture.

The survey was supported with qualitative research via eight in-depth interviews with cyber executives, including Chief Executive Officers (CEOs)/Co-founders, Vice Presidents (VPs), Chief Information Security Officers (CISOs), Cyber AI/Automation Leads, and cyber HRM professionals across multiple regions.

In early 2024 we undertook a quantitative survey of approximately **40 cybersecurity leaders**, subject matter experts, and cross-industry executives from diverse industries and forums.

[1] 2024 Data Breach Investigations Report | Verizon

[2] This work is based on research done with MIT CAMS and KPMG. See, K. Pearlson, J. Coggeshall, A. Fecteau, B. Lawrence, L. Lykos, B. Sandoval and M. Prakash, "AI Impact on Cybersecurity Culture", September 2024, CAMS working paper 24-1110, MIT Sloan School of Management.

[3] Respondents were from one of the following forums: The International Information Integrity Institute, a global knowledge and experience-sharing forum for senior information security leaders; MIT CAMS (Cybersecurity at MIT), which is a research consortium focused on the managerial issues in cybersecurity; SANS Institute, which is a community of cybersecurity professionals.

This report draws on this research, as well as the experience of the MIT and KPMG teams, and explores how AI can impact cybersecurity culture. Firstly, it defines the characteristics of a strong cybersecurity culture and the key challenges that organizations face in creating one. It then explores the potential of AI to enhance cybersecurity culture, and offers some actionable use cases for organizations to apply — including content personalization for high impact, enhancing measurement capabilities to support cyber HRM, real-time risk recognition and remediation, tailoring security controls to different people, and more. This report offers seven considerations to transform your cybersecurity culture through embracing the power of AI.

> This study is one of the first to consider the impacts of AI on cybersecurity culture. While we see AI impacting just about every aspect of our business today, the impact it is having (and potentially will have) on the way our people do their jobs is something every manager must consider. To ignore the impacts of AI on the values, attitudes, and beliefs that drive the behaviors of our colleagues is to leave open one of the biggest vulnerabilities from cyber threats that our organizations face today.

**Dr. Keri E. Pearlson**
Executive Director, Cybersecurity at MIT Sloan
MIT Sloan School of Management

# About Cybersecurity at MIT Sloan

Cybersecurity at MIT Sloan (CAMS) is a research consortium filled with some of the most well-known companies in the world. CAMS conducts and publishes fundamental research on the managerial, strategic, organizational, and governance issues in cybersecurity leadership. Actionable insights on risk management, cyber governance of boards of directors, operational technology cybersecurity, cyber resilience and many more areas are part of the research agenda in addition to building and managing a cybersecurity culture.

# Secure behaviors

## The foundation for cybersecurity culture

**The rapid adoption of new technologies, in particular AI, is increasing the attack surface for organizations and introducing new risks across the enterprise. Managing cyber risk needs to be addressed through broader organizational measures, which combines technical controls with a human-centric approach, and is not solely managed by the cybersecurity function. This is where fostering a cybersecurity culture is key.**

> You need leaders who are willing to invest the time into cybersecurity culture. It is essential that leadership properly embed cybersecurity into every business process, as the CISO can't be everywhere at once.

**Jonathan Dambrot**
CEO
Cranium AI, Inc.

Cybersecurity culture, as defined by MIT's Dr. Keri E. Pearlson and her co-author, is "the values, attitudes, and beliefs that drive employee behaviors to protect and defend the organization from cyber-attacks."[4]

Pearlson and her co-author have developed the CAMS Cybersecurity Culture Model (see visualization on next page), which shows how values, attitudes and beliefs at leadership, group, and individual levels across the enterprise help drive secure behaviors. For example:

- **At the leadership level,** cybersecurity culture is evident by the priority placed on cybersecurity projects, how leaders actively aim to keep their organization secure, and keep up their knowledge of cybersecurity.
- **At the group level,** cybersecurity culture comes through understanding community norms, seeing teams work together to help keep the organization secure, and through helping each other with technical skills. It is an environment where employees feel comfortable reporting security incidents, and help each other to implement security practices into their business operation.
- **At the individual level,** cybersecurity culture comes through employees' self-belief that they can make an impact, and their awareness of policies and cyber threats.

The CAMS Cybersecurity Culture Model shows that those values, attitudes and beliefs are impacted by both external influences and managerial mechanisms.

- **External influences** can be things such as national cybersecurity culture, rules and regulations, and the behavior of partner organizations.
- **Managerial mechanisms** include the behavior of leadership around cybersecurity, performance evaluation, training and awareness campaigns, organizational learning, and tailored communications.

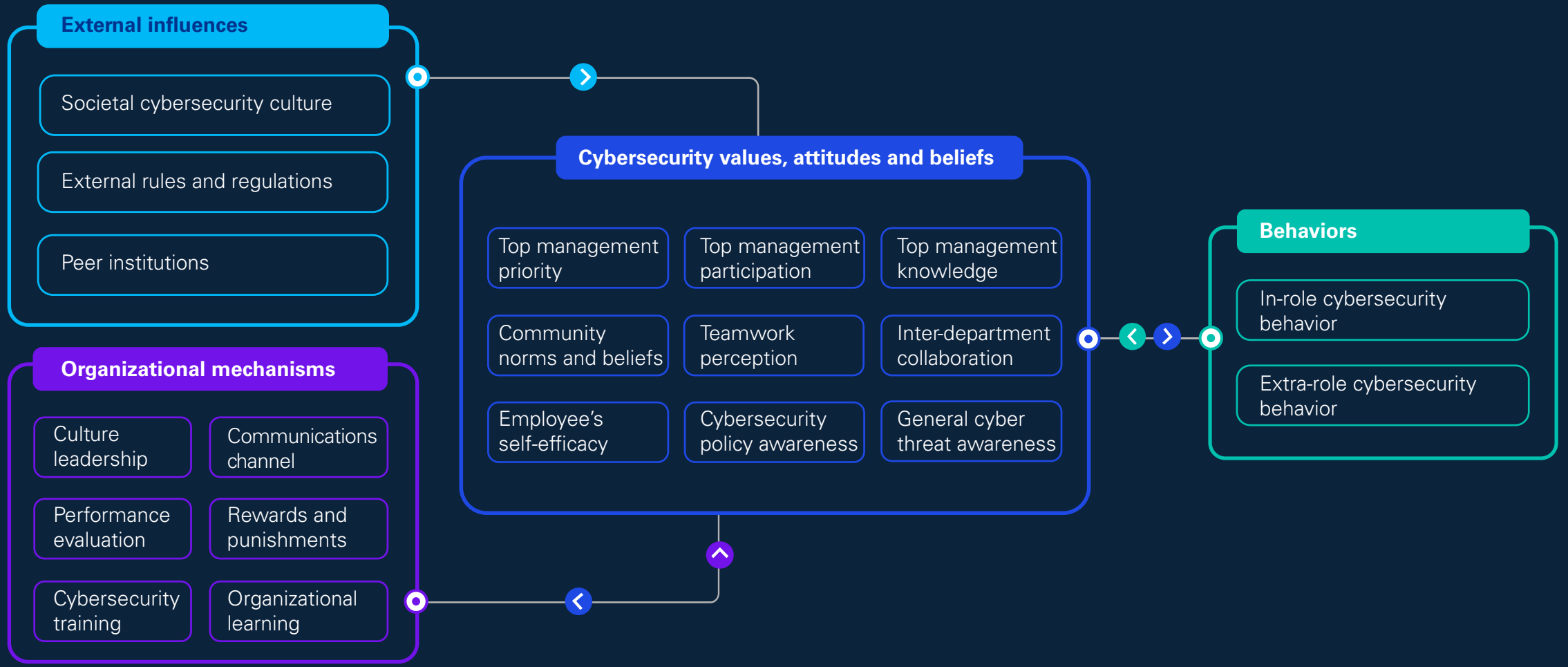
## Cybersecurity success starts with cross-functional leadership

Building on this academic approach, it is vital that cybersecurity culture is holistic across an organization, extending from an individual level to the full ecosystem of the business and its suppliers and partners. Leaders need to drive cybersecurity culture through the managerial mechanism of demonstrating secure behavior themselves — 'walking the walk and talking the talk'. Leadership roles in addition to the CISO that need to be at the heart of this include the Board, CEO, Chief Risk Officer (CRO), and Chief Technology Officer (CTO) among others. Leadership needs to understand where cybersecurity 'sits' within the organization, and how it is prioritized. If the words from leadership don't align with actions, cybersecurity culture cannot flourish.

Leaders need to **drive cybersecurity culture** through the managerial mechanism of demonstrating secure behavior themselves — 'walking the walk and talking the talk'.

[4] Huang, Keman; Pearlson, Keri, *For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture,* MIT Sloan School of Management, 2019.

# CAMS cybersecurity culture model




This framework is used with permission of MIT CAMS and Dr. Keri Pearlson.

# Current state of maturity

Every organization is on their own journey to fostering a strong cybersecurity culture across their enterprise. We found that most respondents self-rated their organization's cybersecurity culture as a

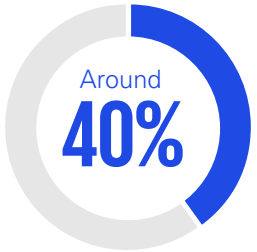
**3/5** or below, where one represents an 'ad hoc' approach to cybersecurity culture, and five is 'dynamic' and 'highly responsive' to the changing threat landscape.

> Cyber culture encompasses the actions people take 'when no one is looking'. It is about innate secure behaviors that endorse and encourage 'cyber equity.' It is how the collective mindset, behaviors and practices/procedures come together and the consistency, from the individual to the ecosystem.

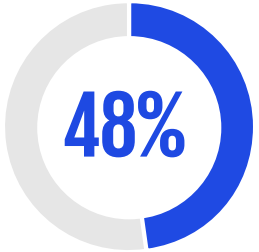
**Dominika Zerbe-Anders**
Cyber Human Risk Partner
KPMG Australia

At level three, organizations have a 'managed' cybersecurity culture, featuring a leader who has ownership of creating, managing, and maturing the culture. Their employees are engaged in part because of the examples set by leadership.

When investigated further into whether AI was currently being used to improve cybersecurity culture, organizations said they were even less mature.




said "**yes**", for things such as protection within **apps, phishing simulations and monitoring data channels, sources, and destinations**.




said "**no**", with some comments including that they were unaware if they were doing so, they were **unsure if it would improve culture**, or they were in a discovery phase.

Clearly, organizations are early in their cybersecurity culture journey and more so when it comes to using AI to support it. Organizations appear to be in the 'trialing' mode of the more obvious use cases of AI in this area, such as setting up phishing simulations.

**The five levels of cybersecurity culture maturity, as defined by MIT's Dr. Keri E. Pearlson and her co-author are:[5]**

**01.** **Level 1 — Ad hoc:** Cybersecurity is a criteria for IT systems and management. There are activities such as orientation and training programs to advise employees.

**02.** **Level 2 — Defined:** Management has identified secure behaviors they seek from employees and have put in place some additional activities beyond traditional training and awareness programs to shape the culture.

**03.** **Level 3 — Managed:** There is a cybersecurity culture leader with ownership of creating, managing and maturing the culture. Employees are engaged in part because of the examples set by leadership.

**04.** **Level 4 — Developed:** Cybersecurity is a top priority of management, and leaders actively demonstrate how 'cybersecurity is part of everyone's job'. Employees are actively involved in doing things that help to support and drive security.

**05.** **Level 5 — Dynamic:** The processes that drive cybersecurity culture adapt naturally to respond to the changing cybersecurity landscape. Employees are highly engaged in keeping the organization secure and resilient, often creating their own security programs and activities.

[5] Pearlson, Keri and Prakash, Mridula, "Cybersecurity Culture Maturity Model", March 2024, CAMS Working Paper 24-1109, MIT Sloan School of Management.

# Confronting cyber culture challenges

**Barriers and challenges to building enterprise-wide cyber culture come in many forms. The survey showed four overarching themes: the human behavior factor, emerging technologies, interconnected systems, and measuring cybersecurity culture.**

> The behavior I am most interested in measuring is the reporting rate of phishing attempts. Most mature organizations have technical controls in place to help them mitigate the risk of a link being clicked. But having a workforce that's well informed, knows how to look for suspicious messages, and knows how and where to report them demonstrates a security-aware culture.

**Matthew Posid**
Chief Information Security Officer
KPMG US

## The distribution of responses regarding challenges to cybersecurity culture


**Source:** Responses from the survey question on challenges to cybersecurity culture presented by, K. Pearlson, J. Coggeshall, A. Fecteau, B. Lawrence, L. Lykos, B. Sandoval and M. Prakash, "AI Impact on Cybersecurity Culture", September 2024, CAMS working paper 24-1110, MIT Sloan School of Management.

## 1 The human behavior factor

The top two cybersecurity culture challenges are aligned to human behaviors. The number one concern is "resistance to change", and the second, "managing human risk factors and creating a strong cybersecurity culture."

Often, an organization's approach to cybersecurity culture is siloed and made the sole responsibility of one department such as IT and/or the cybersecurity function. When organizations focus primarily on technology solutions rather than human behaviors, it can lead to employees feeling disempowered and struggling to make the right decisions around cybersecurity. Similarly, CISOs are often tasked with driving a cybersecurity culture, but often don't have the sphere of influence, authority, or support to change the culture. It only takes one breach, and everyone looks at the CISO for not preventing it.

Where and how people work can also impact cybersecurity culture. Many employees work from home, are on the road seeing clients, are on their feet with customers, or are in other non-desk-based or office-based scenarios. These people interact with cybersecurity risk in different ways, via different systems and devices. As a result, organizations require different sets of controls for influencing security behaviors and culture depending on these factors and their risk profiles. A one size-fits-all approach to building a secure culture simply won't work.

## 2 Emerging technologies

Emerging technology, and particularly AI, is a potential enabler to the broader business, and for helping cybersecurity culture challenges, but can present new risks and issues too. The survey respondents noted several key challenges related to emerging technologies that could impact cybersecurity culture, including:

- Automating and streamlining cybersecurity capabilities to defend against complex new risks
- Insufficient security policies, procedures and supporting technologies
- Defending against ransomware and advanced persistent threats
- Managing cybersecurity risks in increasingly interconnected Internet of Things (IoT) devices.

Regarding AI specifically, 60 percent of respondents thought it would offer both a positive and negative impact on cybersecurity culture. Positive potential included that it could nudge people toward more secure behaviors in their daily work, while negative included concerns about cyber criminals having access to the tools, or that AI doesn't always get the answers right, which could deter people from using it.

In general, there can be reluctance to use AI due to the unknown return on investment, concerns about misuse, and its readiness for use — such as the need to ensure data privacy and security, or sufficient training for individuals. There is a fear about the unintended consequences that arise from the use of a powerful tool that may be simple to operate (such as ChatGPT and its easy, conversational interface). Generative AI (Gen AI) can increase these concerns, as was revealed in the KPMG 2024 CEO Outlook, which found in a survey of over 1300 global business leaders, that:

- Top challenges for deploying Gen AI include: ethical (61 percent), lack of regulation (50 percent), technical capability and skills required to implement (48 percent), the spread of misinformation (42 percent), understanding and adoption amongst employees (35 percent), and security and compliance (33 percent)
- Seventy-four percent agreed that building a cybersecurity-focused culture is central to successful integration of AI across the enterprise.

## 3 Interconnected systems

Securing an increasingly interconnected ecosystem of supply chain and external services providers and partners from cyber risk was another identified challenge. Threats to a business can come from third, fourth, or even fifth party suppliers, so both technical risk management and cyber HRM need to be integrated across this ecosystem.

Establishing a robust cybersecurity culture already presents a key challenge for most organizations. Extending those cyber-safe values, attitudes, and beliefs to suppliers and partners only adds complexity as they naturally have their own cybersecurity culture, which may or may not align with the organization's. Organizations need to leverage controls such as sharing information in accordance with third-party contracts, building secure expectations into procurement processes, and more.

**74%**

agreed that **building a cybersecurity-focused culture** is central to successful integration of AI across the enterprise.

## 4 Measuring culture

Collecting metrics and measuring cybersecurity culture can help to drive boardroom discussions and bridge any communication gaps, supporting more effective leadership, investment, and behavior change which all ultimately help to reduce cyber human risk. However, less than half of the survey respondents measure cybersecurity culture. The in-person interviews also found that this was in its early stages, if it existed at all.

Of the survey respondents that said "yes", the examples of use were basic and didn't specifically measure behavioral change (e.g., training-completion rates, phishing click and reporting rates, survey feedback, program feedback, the number of infected machines, and timely terminations). Of those that said "no", respondents either thought they weren't ready to do so, or were currently evaluating how they would go about this.

When asked more specifically if they were using AI to measure cybersecurity culture, just 12 percent said yes, and 61 percent said no. The rest were unsure.

In general, organizations often appear to be unclear about what metrics/KPIs they should collect to measure their cybersecurity culture and to assess behavior change, and even more so, how AI could help drive those measurements. Some examples of meaningful metrics that organizations could use to measure behaviors that drive cybersecurity culture include:

- Unauthorized downloads
- Secure password management (e.g., password strength, use of multi-factor authorization (MFA), password re-use, etc.)
- Timely installation of software patches
- Data loss prevention rule violations
- Potential or real security incidents reported.

**However, less than half of the survey respondents measure cybersecurity culture.**


# How AI can help shape culture

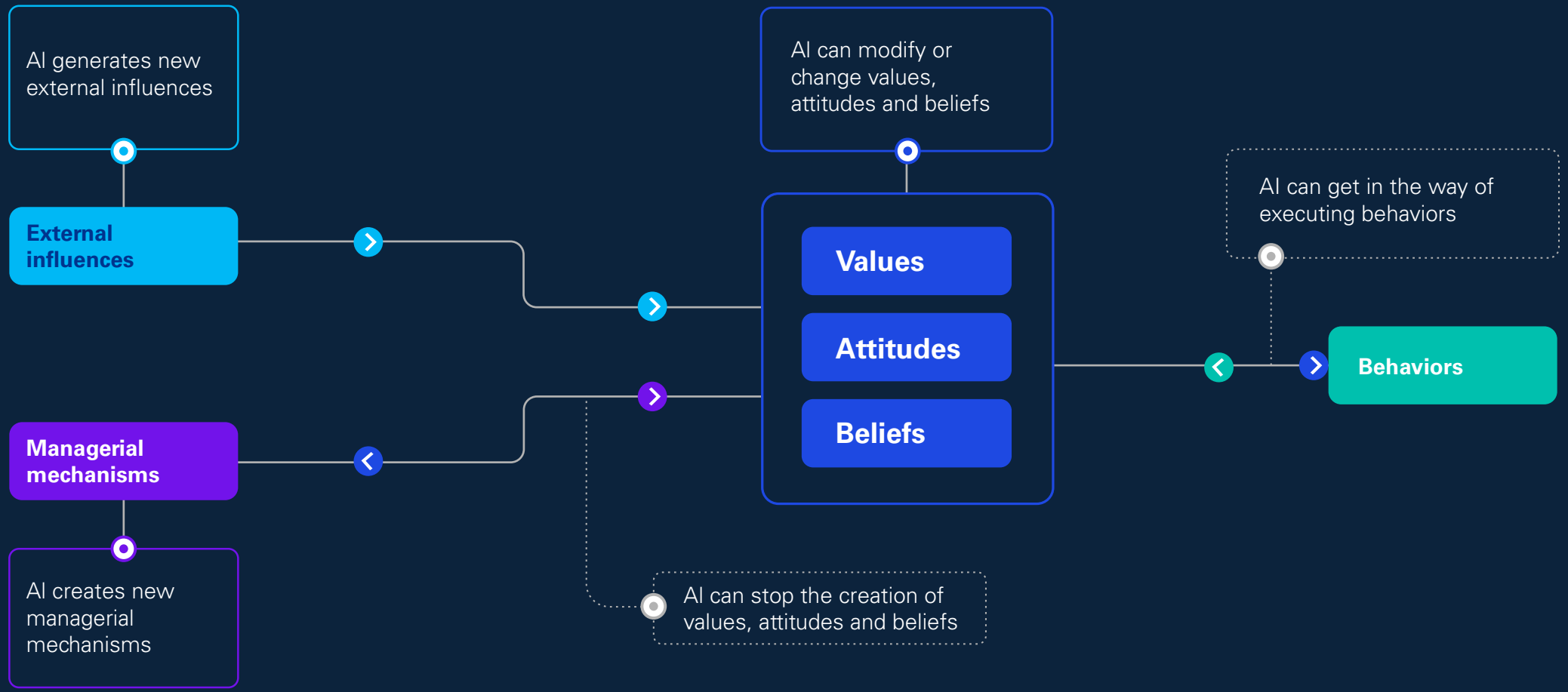
**Fostering a strong cybersecurity culture across enterprises and ecosystems is becoming more challenging. Cybersecurity is increasingly pervasive, threat actors are more sophisticated. Governments and regulators alike are increasing pressure on enterprises to up their game in risk management.**

When assessing the possible impact of AI on the CAMS Cybersecurity Culture Model, it was clear that there were pros and cons. But there were clear indications of how AI could be a powerful enabler for managerial mechanisms to positively influence cybersecurity values, attitudes and beliefs. The same applied to external influences — for example, some countries invest and support organizations in the adoption of AI, creating a different attitude than in countries that do not have these policies.

> AI's impact on cybersecurity culture is multifaceted, influencing how threats are identified and addressed, the efficiency of security measures, and the governance of AI itself…The key is leveraging AI to enhance effectiveness rather than merely increasing content.

**Oz Alashe**
CEO
CybSafe

# AI's impact to the conceptual framework of a cybersecurity culture

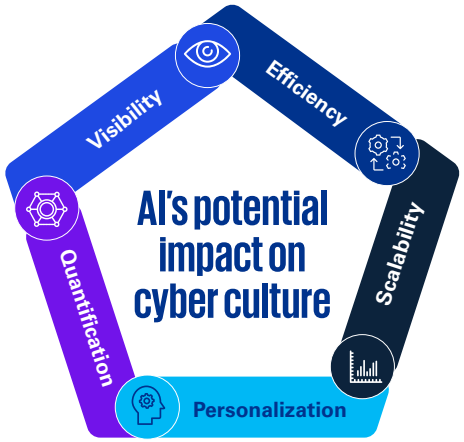


# AI's impact on cyber culture

In practical terms, the research team found that AI supports an organization building a strong cybersecurity culture through five key themes — visibility, efficiency and scalability, and providing personalization and quantification capabilities that CISOs have previously struggled to achieve. All five of these areas can act as key support mechanisms to the CISO and enable them to pursue a cyber HRM program that understands and prioritizes initiatives that help to reduce risks across the organization.

## Visibility

With AI infrastructure in place, CISOs and business leaders could gain a live view of their organization's activity (e.g., sensitive content being sent outside of the organization, access to critical systems / data, etc.), providing real-time visibility into behaviors that might cause security issues. AI creates the opportunity for identification and interpretation of patterns that were previously invisible to managers. Integrating AI into workflows, communications, and other processes allows for immediate investigation when potential cyber vulnerabilities arise.




## Efficiency

AI technologies can reduce the toil of repetitive tasks and time-consuming activities (e.g., the review of entitlement of access) through automation, while integrating security from the onset. This can enable the long-desired 'secure by design' and 'defense in depth' approach which balances the human element with processes and technology controls. Efficiencies are achieved when the quantity and quality of cyber protections are automatically invoked, as AI tools can both identify and take action to stop a threat from becoming a problem.

## Quantification

AI's ability to process and analyze humanly incomprehensible amounts of data in seconds promises to create metrics that derive meaningful insights that organizations have previously struggled with when it comes to establishing a cyber HRM capability. This could improve the quantification of risks, support leadership's ability to make data-driven investment decisions, and implement policies and controls that have the greatest impact to influence secure behaviors.

## Personalization

AI can help differentiate between low- and high-risk users, enabling organizations to prioritize and provide tailored security controls to individuals for maximum risk reduction. AI can analyze information about the behaviors, learner needs and styles, skill gaps, and capabilities of team members and customize at the individual micro level, while positively reinforcing secure behaviors. This can help enhance impact, by improving knowledge and awareness of how to behave securely in the workplace, with the right employees, at the right time.

## Scalability

AI enables faster scaling of security guardrails and policies. Efficiencies created through analyzing vast amounts of data quickly, and translating it into controls, can be scaled to help secure diverse persona groups, processes and technologies. Long term this has the potential to extend beyond the organization's internal operations to its entire supply chain, which is typically targeted by attackers as an entry to attack. Scaling controls to their broader ecosystem could enable organizations to play a larger role in improving cybersecurity culture across industries, and support those with fewer security resources.

# Giving culture a boost

With the support of AI, organizations can influence secure behaviors and cybersecurity culture. Whether it be support with training, data analysis, or even for gamification of simulated security breaches and responses, there are varied creative approaches to try. Suggestions from the survey respondents and interviewees include:

Creation of personalized training and/or micro-learning on topics including (but not limited to) data classification, how to identify and navigate deepfakes, understanding phishing, and more

Automated and tailored phishing programs for learning purposes

Data analysis of risky behaviors and proactive identification of future trends

Automated prevention of actions through interventions, nudges or ‘digital agents’

Quantifying human risk scores at the individual, group, and organizational levels regarding security performance

Cybersecurity education and support chatbots

Gamification of cyber risk events and responses

# AI in action:

## Practical scenarios

> There is potential to use AI for a cybersecurity culture diagnostic exercise, to look at people's perception of their behavior versus the behavior of their peers and senior leaders, and to use this information to promote culture in security discussions.

**Dominika Zerbe-Anders**
Cyber Human Risk Partner
KPMG Australia

Approximately

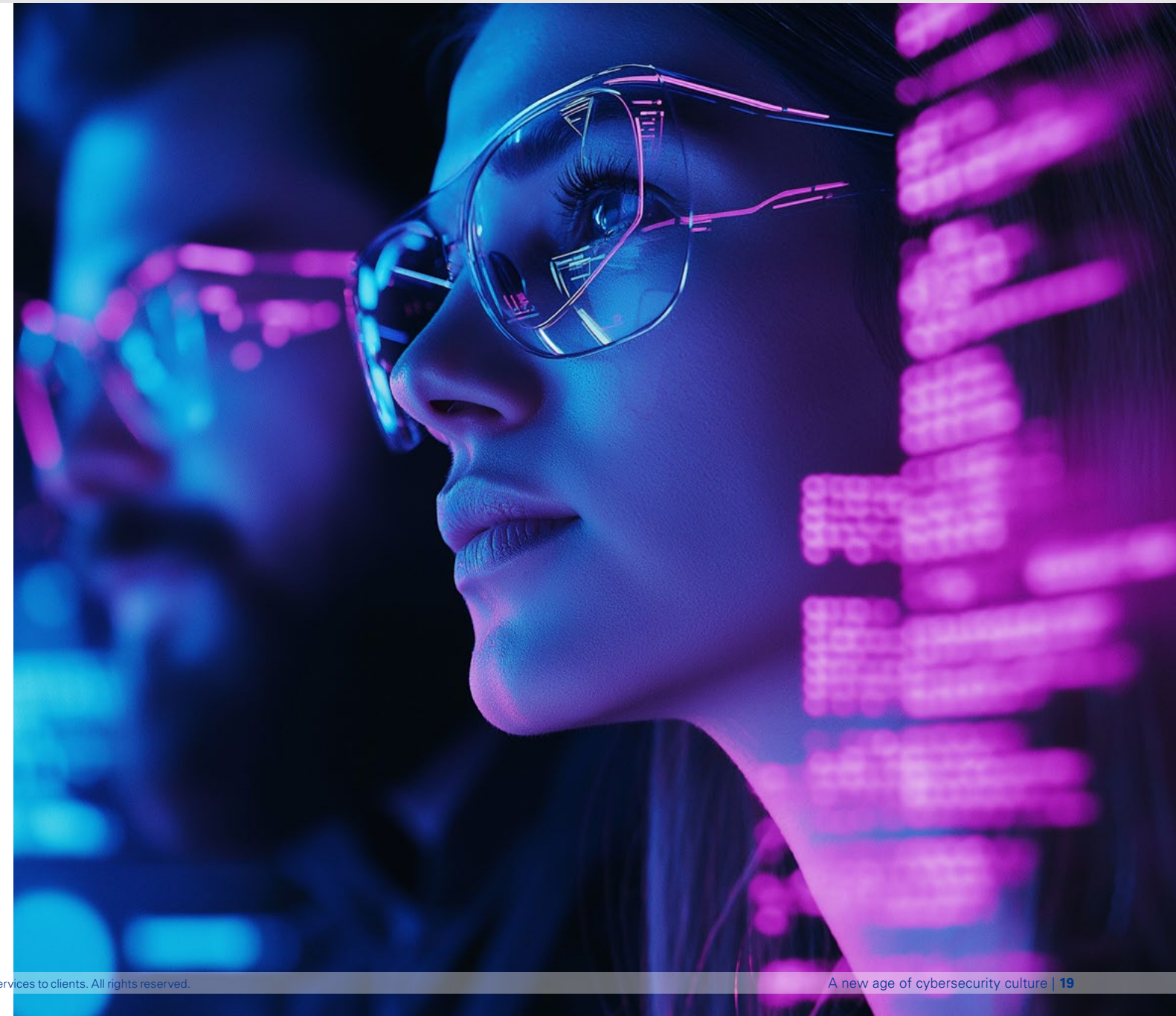
# 26 percent

thought **resource constraints were the biggest challenge**, and

# 8 percent

**said a lack of data**. While there are challenges to overcome, the six actions below (demonstrated through case studies) are among the possible ways that AI could make a significant difference to cybersecurity culture.

It is important to note that as you start to use AI to drive cybersecurity culture, the most progress will likely be made if you align transformation with your AI governance function. KPMG's Trusted AI Framework emphasizes that effective AI governance should aim to ensure that AI systems are transparent, explainable, and accountable, which aligns with essential directives and considerations such as privacy and security, risk mitigation (including prevention of bias, errors, and legal breaches etc.), as well as alignment of policies and end-user training.



# 01. Content personalization for impact

**Scenario overview:** Ayaan is the Director of Cyber HRM and is partnering with the Identity and Access Management (IAM) team to support the organization's adoption of MFA. Ayaan needs to create two communications tailored to two different employees, Arla, a Finance Manager, and Lina, the CIO, about the implementation of MFA, its importance, and instructions on what to do.

**AI use case:** AI aggregates and analyzes historical data points about the target audiences (e.g., job demographics, department, location, roles and responsibilities, engagement with communication platforms, technical proficiency and subject matter knowledge, past communication preferences — style, tone, format, etc.) and the company's marketing and communication processes (e.g., approved writing styles, brand and marketing guidelines, corporate communication templates, distribution vehicles, etc.).

Leveraging the data, the AI solution creates two persona profiles to inform tailored messaging and learning materials, and automatically distributes them using the audiences' preferred communication vehicles.

## Outputs:

- **Persona profiles:** A summarized view of Arla and Lina's roles, learning needs, and preferred learning style, communication delivery and motivators that will have the highest impact on their behavioral change.
- **Tailored communication and learning content**
  - **Lina, instant message** — An instant message that is a short and concise description of how the MFA initiative aligns with the organization's business goals and the need for Lina's leadership support and buy-in. Includes high-level steps Lina or her administration team can follow to install MFA.
  - **Arla, email communication** — A detailed email communication that describes what MFA is, relevancy to Arla's role, and MFA's capability to protect financial data. Includes a link to the knowledge management system with frequently asked questions (FAQs) and user guide instructions.

## Potential benefits:

AI quickly aggregates relevant information and generates personalized content, maximizing Ayaan's efficiency. It saves Ayaan time and effort in manually creating multiple communications and training offerings. AI also enables Ayaan to expand his reach to diverse groups across the enterprise by scaling distribution. This all means Ayaan can focus on other important tasks while also optimizing operations. The tailored messaging enhances engagement and understanding, motivating Arla and Lina to act.

> Cyber is a people problem, not a bits and bytes problem.

**Matthew Posid**
Chief Information Security Officer
KPMG US

# 02. Measuring human risk

**Scenario overview:** CISO Yuki is putting together her annual budget. She needs guidance from her cyber HRM Director on where she should invest resources to enhance the awareness and training strategy. Additionally, Yuki wants to include the KPIs that she will report to the board to measure the program's success.

**AI use case:** The Cyber HRM Director leverages AI to aggregate data across internal tools (e.g., Security Information & Event Management (SIEM), HR tools, past security assessment reports, phishing simulation results, past awareness and training campaigns, persona profiles, security policies, standards and controls, etc.) and external sources (e.g., threat intelligence, regulations and standards, etc.) to generate an executive risk analysis report, a proposed training and awareness strategy that will address the risks, and metrics that Yuki may consider to measure success.

## Outputs:

- **Risk analysis report** — A risk analysis report containing a summary of risky behaviors and potential insider threats/targets within the organization, industry specific risk scenarios, and an analysis of any gaps in the organization's current implementation of technical security controls.
- **Training and awareness strategy**— A program strategy and roadmap which includes strategic initiatives that are tailored to address the results of the risk analysis.
- **Cyber HRM scorecard** — A cybersecurity culture scorecard containing defined metrics that directly correlate cyber HRM efforts with business outcomes, establishes a foundational baseline, and enables the team to test effectiveness and report results to leadership.

## Potential benefits:

Leveraging AI to aggregate data creates increased visibility into cyber risks and behavioral changes that enables Yuki to make more data-driven decisions in how and where she should allocate resources that will have the most influence on risk reduction. AI's ability to create a tailored strategy and scorecard aligned to the risk analysis results streamlines the HRM Cyber Director's time, enabling them to focus on current state operations while supporting leadership's proactive approach to plan for the next year.

> You need strong leadership support for a strong cybersecurity culture, and metrics enable that.
>
> **Jonathan Dambrot**
> CEO
> Cranium AI Inc.

# 03. Real time risk recognition

**Scenario overview:** Cara is a software developer and is testing her code, and she needs realistic data for her test. She extracts sample live data from the production environment for user acceptance testing (UAT).

**AI use case:** The AI tool (e.g., digital agent installed on endpoint devices to monitor, prevent and remediate high risk behaviors) identifies this behavior as risky, and initiates a series of actions (e.g., nudges, interventions, alerts/notifications) through pre-configured workflows that prevents an incident from occurring, and encourages compliance with the company's security policies.

## Outputs:

- **Instant message —** Cara receives a real-time 'nudge' sent through the company's instant message platform which notifies her of the risks of using production data in a non-production environment, a link to the secure development policy and procedures, and instructions on where she can locate sample data that has been pre-approved for testing purposes.
- **Access revocation —** A technical security control is automatically employed which temporarily disables Cara's access privileges, preventing her from copying production data into a non-production environment which could cause a security incident.
- **Managerial action —** Cara's supervisor receives an automated email which includes a summary of the event, actions taken, and requests the manager to acknowledge they have counseled Cara before approving the re-enablement of Cara's privileges.

## Potential benefits:

The use of AI in this scenario detects risky behaviors 'as they are happening'. The AI solution automatically takes action to provide Cara with real-time guidance and prevention measures by implementing a technical security control. This holistic approach combines modernized behavioral techniques with technical preventative controls, enhancing the organization's ability to mitigate security risks.

> Most organizations still employ traditional techniques, such as training and awareness campaigns, but these are only a part of the solution and more often than not perceived as a 'check-the-box' exercise. Training/awareness/phishing are good for helping people to know what is right or wrong, but they are often at a point in time and people forget. Just because they know about it doesn't mean they will actually act upon it.
>
> **Adrian Kwitkowsky**
> VP — Manager, Enterprise Cybersecurity Training and Awareness
> First Citizens Bank

# 04. Tailoring security controls

**Scenario overview:** Karl is a CISO who is keenly aware of security fatigue amongst employees. He is concerned that they will look for workarounds when they feel that a security measure is unnecessary or slowing them down. Karl wants to implement a risk-based approach to balance security controls with business operational speed and the user experience.

**AI use case:** An AI-driven security system monitors user activity and analyzes risks against security control requirements. Over time, it identifies patterns where low-risk actions consistently pose minimal security threats. For example, an employee may access a non-critical system multiple times a day and is required to authenticate every time. The AI solution deems this activity as 'low risk' as it occurs during normal business hours and is accessed on a company-managed device that is connected to the corporate network. Then, the AI solution can dynamically adjust individualized security controls, such as reducing the need to reauthenticate, based on its analysis of the employee's risk profile.

## Outputs:

- **Risk profile —** Risk analysis results, including the user activity, evaluation criteria, (e.g., data/system classification, access privileges, time/location, compensating controls, frequency of activity, comparison of activity to similar users, past incidents, etc.), risk evaluation results, and adjusted security controls.
- **Modified authentication requirements —** The technical security control requiring reauthentication is automatically adjusted for that specific employee.

## Potential benefits:

Adjusting security controls using an AI-driven, risk-based, personalized approach can improve the security culture by 'reducing friction'. Importantly, it enables Karl to focus on implementing controls that will have the highest impact to reduce risk. Adjusting security controls for low-risk scenarios enhances the user experience by minimizing frustration and resistance, which incentivizes employees to comply with prioritized security measures. It also promotes a sense of balance between security and productivity.

> AI can help identify the optimal level of security controls for different individuals or groups based on their risk profile.
>
> **Masha Sedova**
> VP, Human Risk Strategist
> Mimecast

# 05. Tailoring security controls

**Scenario overview:** Adil is an Application Product Manager and frequently must approve access requests and perform entitlement reviews. He gets so many requests that he's become desensitized and often approves them without doing a detailed review.

**AI use case:** The AI platform that monitors user activity from internal tools such as User & Entity Behavior Analytics (UEBA) and SIEM, etc., detects a trend of increased access requests to an application by employees in the same department and sends the IAM team an alert with the analysis results. The IAM team reviews the results and determines that the requests are legitimate and implements role-based access by creating an Active Directory (AD) group to automate access to the application for future employees in specific roles or departments. Additionally, the team configures an automated workflow to perform entitlement reviews and manage privileges.

## Outputs:

- **Process optimization report —** A summary of access requests over the past 12 months, including analysis of departments and roles, assets, privileges, approvals, average time Adil has spent manually processing requests, and recommended groups where access can be automated.
- **Entitlement review workflow —** The AI tool will review access on a periodic basis and trigger a workflow to automatically decrease escalated privileges and remove users from the AD group after a period of inactivity or use of those privileges.

## Potential benefits:

The use of AI in this scenario helps the organization identify opportunities to streamline security processes that may be cumbersome and impact operations to reduce the risk of employees applying a workaround or shortcut. This fosters a more collaborative culture between security and the business in reducing operational overhead.

**The use of AI in this scenario helps the organization identify opportunities to streamline security processes that may be cumbersome and impact operations. This help reduce the risk of employees applying a workaround or shortcut.**

# 06. AI virtual assistant/ chatbot

**Scenario overview:** Beatriz is a third-party contractor clerk in Accounts Payable working late processing invoices before the fiscal year end. She opens an invoice that appears to be from a regular customer with a request to update their routing information before sending the payment. Beatriz wants to make sure the payment is processed on time; however, she is suspicious that this may be a social engineering attack and doesn't know what to do next as she is not familiar with the company's policies.

**AI use case:** Beatriz uses the company's AI-powered security chatbot (e.g., virtual assistant) which provides employees guidance on the company's security policies and procedures. Beatriz uploads the email to the chatbot and asks how she can determine if this is a legitimate request. The chatbot analyzes the email, evaluates cyber threat intel and trending cyberattacks, and provides Beatriz with a list of potential red flags in the email, a link to the procedures she can follow to assess its legitimacy, and report it if necessary.


## Outputs:

- **Chatbot security analysis —** Results of the chatbot's analysis of the specific document uploaded.
- **On-demand guidance—** Recommended actions with scenario specific links to company policies, procedures, etc.
- **Feedback loop—** Report summarizing the use of the chatbot to identify trends and potential risk areas and to inform leadership on areas of focus to optimize the cyber HRM strategy (training/ awareness, implementation of technical controls, etc.).

## Potential benefits:

An AI-powered chatbot can remove barriers to asking security related questions, quickly providing relevant results without employees sifting through myriad links and policies. It can also provide visibility into the areas where employees may need more help or guidance.

# Seven considerations

## to help transform your cyber culture

**It is important to note that as you start to use AI to drive cybersecurity culture, the most progress will likely be made if you align transformation with your AI governance function. KPMG's Trusted AI Framework emphasizes that effective AI governance should ensure that AI systems are transparent, explainable, and accountable, which aligns with essential directives and considerations such as privacy and security, risk mitigation (including prevention of bias, errors, and legal breaches etc.), as well as alignment of policies and end-user training.**

AI can be a game changer in developing a robust cybersecurity culture. To make the most of it though, you need to be clear on your goals, consider evolving risks, monitor and measure progress, and never lose sight of the human dynamic.

**Orson Lucas**
Principal, Advisory, Cyber Security Services
KPMG US

# To help build a stronger cybersecurity culture with the support of AI, here are seven considerations to keep in mind as you embark on the journey:

**01. Outline your aspirations:**

Take time to understand the current state of your cybersecurity culture and mark this as the baseline. Establish what data can support the measurement of this current state. Then, set goals and aspirations for where you want to be in the future, and how this will support the organization's overall objectives. Identify the gaps between the current and desired state. These gaps may or may not be addressed using AI, but it can give you a starting point.

**02. Secure support and investment:**

Any major initiative that impacts an entire organization, like growing cybersecurity culture, requires unwavering support from the top (the Board, C-Suite, etc.) to be successful. All leaders must set the tone as the CISO cannot do this alone. Build a business case that demonstrates how actions and investments should enable the organization to reach its desired state, and how that supports enterprise-wide objectives. Seek support from parts of the organization that already have capabilities to develop and embed AI across functions. It is likely that experimentation and implementation is already taking place elsewhere that you can tap into from a skills or integration perspective.

**03. Explore and experiment:**

Investigate the gaps in your current capabilities and explore options for using AI through the definition of use cases. Pilot these in the form of proof of concepts, and experiment with what works and what has most impact in reducing cyber human risk. Scan your ecosystem of partners to see whether these use cases should be built in-house or bought externally. Pilot technologies everyone can benefit from using, and that are not just reserved for people with high technical proficiency. This can help build excitement, enthusiasm and participation.

**04. Prioritize and implement:**

Once you know which AI use cases have the most impact in driving a stronger cybersecurity culture and reducing risk, focus on implementing and scaling these across your organization. Start small with a particular business function before expanding fully, particularly those that are the highest risk.

**05. Collect and measure what matters:**

Ensure you have the right data in the right formats to be able to measure your current cybersecurity culture and identify any data gaps. An upfront focus on data and its quality can enable you to get the best out of your AI use cases, and can avoid impacts to the accuracy of your AI models.

**06. Be mindful of new risks:**

Consider what the AI tools and technologies can and can't do and the risks that may come with them. Consider how to embed trust in AI through controls that manage the security and privacy risks, as well as risks such as information bias, hallucination, and ethical and regulatory compliance.

**07. Prioritize the employee change journey:**

AI can introduce ample and continuous change for employees and teams, which requires strong leadership. Prioritize employee wellbeing throughout change with the right communication, training, and recognition. Help people to see how working with AI solutions may improve their daily life.

**KPMG has a full report on how to harness AI in the workforce. You can read more here in the Future of work.**

# Key authors

**Akhilesh Tuteja**
Global Cyber Leader
KPMG International

In addition to serving as the Global Cyber Security practice leader, Akhilesh heads the IT Advisory and Risk Consulting practices for KPMG in India. He is passionate about how developments in information technology can help businesses drive smart processes and effective outcomes. Akhilesh has advised many clients on cybersecurity, IT strategy and technology selection and helped them realize the business benefits of technology. He is also knowledgeable in the area of behavioral psychology and is enthusiastic about addressing the IT risk issues holistically, primarily through the application of user behavior analytics.

**Orson Lucas**
Principal, Advisory, Cyber Security Services
KPMG US

Orson is focused on helping complex, global organizations to enhance the maturity of their security programs to protect their most sensitive information assets, and current leader for KPMG's Human Risk Management service offering. He has over 18 years of information technology and security experience spanning numerous disciplines, with a focus on regulatory and technical compliance and technology as an enabler of business efficiency. Orson has spoken at over two dozen conferences on various technical topics and has authored several papers in this space.

**Dr. Keri Pearlson**
Executive Director Cybersecurity at MIT Sloan (CAMS)

Keri is driven by projects asking the some of most difficult questions facing leaders who want to keep their organizations secure and resilient. In addition to her work on cybersecurity culture, Keri has published extensively in academic journals, as well as Harvard Business Review, Sloan Management Review and the Wall Street Journal, about reporting cyber risk to the board of directors, building cyber resilience thinking, and creating cyber critical communications. Currently she is working on strategies for building trust after a cyber incident, cyber culture maturity, and cyber risk versus uncertainty.

# Contributors


**Ashley Fecteau**
Manager,
Cyber Security Services
KPMG US

**Breah Sandoval**
Director, Advisory,
Cyber Security Services
KPMG US

**Jason Coggeshall**
Manager,
Cyber Security Services
KPMG US

**Billy Lawrence**
Senior Manager,
Cyber Security Services
KPMG International

**Leonidas Lykos**
Global Cyber Innovation
Assistant Manager
KPMG International

**Mridula Prakash**
Graduate Research Assistant
Cybersecurity at MIT Sloan
(CAMS)

**Marc Martínez**
Partner,
Consulting Corporates
KPMG in Spain

**Javier Aznar**
Partner,
Consulting Corporates
KPMG in Spain

**Sergi Gil**
Partner,
FS Consulting
KPMG in Spain

**Sergio Gómez**
Partner,
FS Consulting
KPMG in Spain

**Juan Manuel Zarzuelo**
Partner,
Consulting Corporates
KPMG in Spain



KPMG International would like to recognize and thank MIT Sloan Management School for the qualitative research conducted in 2024 to approximately 40 cybersecurity leaders, subject matter experts, and cross-industry executives from diverse industries and forums. Special thanks to Dr. Keri Pearlson, Executive Director, Cybersecurity at MIT Sloan, for her expertise, insight, and contribution to this paper.


**kpmg.com**




Designed by Evalueserve.
Publication name: A new age of cybersecurity culture | Publication number:139683-G | Publication date: December 2024