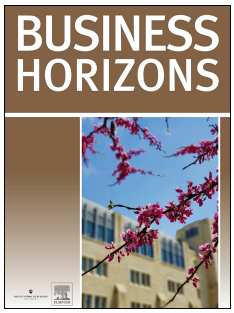

Ignorance is not bliss: A human-centered whole-of-enterprise approach to cybersecurity preparedness

Dave Chatterjee, Anne Leslie

PII: S0007-6813(24)00153-8

DOI: https://doi.org/10.1016/j.bushor.2024.10.009

Reference: BUSHOR 2019

To appear in: *Business Horizons*

Please cite this article as: Chatterjee D. & Leslie A., Ignorance is not bliss: A human-centered whole-of-enterprise approach to cybersecurity preparedness, *Business Horizons*, https://doi.org/10.1016/j.bushor.2024.10.009.

Ignorance is not bliss:
A human-centered whole-of-enterprise approach to cybersecurity preparedness

Dave Chatterjee*
Pratt School of Engineering
Duke University
Durham, NC 27708
USA
dchatte@gmail.com

Anne Leslie
Cloud Risks and Control Leader Europe
IBM
anne.leslie@ibm.com

*Corresponding author

Ignorance is not bliss:
A human-centered whole-of-enterprise approach to cybersecurity preparedness

Abstract

The overwhelming nature of the cybersecurity challenge, further exacerbated by continuously growing attack surfaces and artificial intelligence-enabled attacks, often drives organizations into a state of learned helplessness when employees and their leaders realize that no amount of preparedness can guarantee immunity from cyber-attacks. This sense of inevitability demotivates organizational leadership from prioritizing cybersecurity readiness. Embracing the 'ignorance is bliss' mindset, very often, the message from the top is to do the bare minimum to achieve cybersecurity regulatory compliance. However, the consequences of not being willing to face the challenge head-on and going above and beyond the compliance checklist can be severe. In this paper, we shed light on a whole-of-enterprise approach that focuses on engaging and optimally utilizing the competencies of individual organizational members. This human factors-focused approach is based on the fundamental premise that cybersecurity readiness is everybody's business, and organizations must find ways of galvanizing organization-wide support and commitment. Insights gained from in-depth interviews with business leaders and subject-matter experts reveal five characteristics of a human-centered whole-of-enterprise approach to cybersecurity preparedness: (1) Enlightened and engaged leadership; (2) Capitalizing on people's best intentions and creativity; (3) Looking inwards before looking outwards; (4) Getting ownership, responsibility, and accountability right; and (5) Measuring the right thing, incentivizing the right behavior.

KEYWORDS: Cybersecurity readiness; Human-centered approach; Commitment-preparedness-discipline framework; High-performance information security culture

1. Cybersecurity readiness is everybody's business

Do organizations need to get hacked to identify their vulnerabilities and adopt robust security measures? That seemed to be the mindset of a senior information security leader involved in public health and cyber operations, who remarked, "We don't truly understand our own risks until it's made plain to us by the hackers." The unwieldy, vulnerable, and vast healthcare network makes tracking and patching the ever-expanding attack surfaces difficult. Trying to bulletproof the organization from potential attacks is often viewed as wasting time, money, and effort. During a senior leadership meeting at a major healthcare organization, the Chief Executive Officer (CEO) encouraged the team to focus on providing quality healthcare. This senior leadership mindset of despair and helplessness is not uncommon across industries (Abraham et al., 2019). As one chief information security officer noted "for many companies, only after major breaches and losses does information security come to the agenda. It is often an afterthought"(Lourenco, 2022).

But there is another way, an alternative mindset and approach, that delivers a very different set of enterprise security outcomes. Let's illustrate this through the real-world example of a young woman called Jenny. Jenny was a customer support agent working in a private bank operating in Europe. Diligent, conscientious, and hardworking, Jenny was the kind of team member all organizations like to have on their payroll. Very engaged, committed to serving her customers, and loyal to the bank that employed her, she always had in mind how she could do her best work. One day, she received a support phone call ostensibly from a known customer who wanted to transfer a large amount of money. Requests like this weren't unusual. But something felt 'off' with this one. Jenny couldn't quite put her finger on what was wrong – but neither could she shake the feeling that there was something wrong. Jenny could very well have ignored that inkling. She could simply have applied a rote process and gone about her day. But she didn't. She chose not to ignore her instinct; She stalled the customer, pleading a system outage and called her internal security team, alerting them to the transfer request and sharing her misgivings with them.

As it turned out, post-investigation, Jenny's instinct was spot-on: the request she had received was part of a very sophisticated cross-border campaign orchestrated on behalf of an adversarial nation-state that was successful in fraudulently extracting vast amounts of money from the global banking system. The difference between a massive loss to the bank and a neutralized social engineering attack was a crucial split-second decision that a front-line support agent made to contact her internal security team and invoke their help and expertise to address a situation that she had identified as suspicious but couldn't address on her own.

The bank now uses this example systematically as part of its security training and awareness activities. The security team analyzed in detail what had prompted Jenny to act the way she did and how they could re-create the conditions for that behavior to become the default for employees across the organization. They even went so far as to create an annual 'Jenny Award,' an employee recognition program that calls out and celebrates the actions and contributions of team members who go above and beyond in protecting the bank while doing their jobs. They took necessary steps to create a security culture of enablement, not fear.

Jenny's example shows how impactful individual employees can be in driving positive security outcomes, even when they are not security specialists and don't even sit in the security organization. The behaviors Jenny demonstrated illustrate what a whole-of-enterprise can look like on the ground, when employees are engaged in what they are doing, proud of the organization they work for, informed, and psychologically safe enough to flag a potential issue to the internal security team because they see them as partners who will help rather than potentially hostile interlocutors who will ignore or chastise.

While the fallibility of the 'human element' to cyber-attacks is well-known (Alsharida et. al, 2023), the above example symbolizes a reality that the human factor can be a significant strength and an integral part of a defense-in-depth security solution. Emphasizing the criticality of human factors, Dr. Eric Lang, Director, Personnel and Security Research Center (PERSEREC), United States Department of Defense, contends that "without individuals' sincere commitments, the most extensive insider threat policies will fail" (Lang, 2022). In a similar vein, another cybersecurity leader commented, "When anyone asks how big is your security team, I say about 1300 some people because that's what my company size is. All of them are part our security team, and they are the security champions, and they helped me manage and drive the security program to the next level"(Shah, 2024).

Cybersecurity research recognizes the importance of the human factor in establishing and sustaining a strong defense (Jones, 2024; Sewak, et al. 2023). On a related note, creating and sustaining a security conducive organizational culture is also found to be a very important success factor (Al-Somali et al., 2024; Chatterjee, 2021; Georgiadou et al., 2020; Uchendu et al., 2021). The paper distinguishes itself by drawing upon practitioner insights and experience to make actionable recommendations on how to create organizational conditions that will stimulate and sustain desired level of cybersecurity readiness. It builds upon the high-performance information security culture framework (Chatterjee, 2021) by operationalizing some of the success factors associated with the three cultural traits – commitment, preparedness, and discipline. These traits are associated with several success factors, ranging from informed and committed leadership to robust governance processes and involved and motivated personnel. Based on in-depth interviews with business leaders and subject matter experts, the seventeen success factors are distilled into five characteristics of a human-centered whole-of-enterprise approach to cybersecurity preparedness (see Figure 1): a) Enlightened and engaged leadership, b) Capitalizing on people's best intentions and behaviors, c) Looking inwards before looking outwards, d) Getting ownership, responsibility, and accountability right, and e) Measuring the right thing, incentivizing the right behavior.

[Insert Figure 1 About Here]

2. Five characteristics of a human-centered whole-of-enterprise approach to cybersecurity preparedness

2.1. Enlightened and engaged leadership

The critical role of executive leadership in setting the 'tone at the top' cannot be overstated. For too long, cybersecurity was relegated to the minor league status of being a technical topic for

technical people, resulting in very little executive airtime. The context, however, is changing, not least because of some high-profile examples of Chief Information Security Officers at firms like Capital One and Uber suffering the personal consequences of their companies enduring major breaches during their tenure. Be it through the enlightened realism of individual leaders or thanks to the salutary nudge of intensified regulation (KPMG, 2023) we are observing Boards and corporate executives increasingly embrace the mission-critical nature of cybersecurity and the accountability they hold for driving better security outcomes (Pearlson and Hetner, 2022).

To set the right tone and mindset, leaders themselves need to be convinced of the strategic significance of developing cybersecurity capabilities. Sharing his vision of the future of cyber governance, Kal Sambhangi, Senior Vice President, Cybersecurity Strategy and Architecture at Truist, said: "The leadership mindset needs to change whereby they are optimistic and opportunistic about cybersecurity and view developing cybersecurity capabilities as a source of competitive advantage."

Leaders in exemplary organizations view cyber threats as a strategic opportunity to retain and grow their customer base by demonstrating their commitment and superiority in protecting sensitive data and related digital assets. They won't hesitate to continuously learn about their organization's information security strengths and vulnerabilities. In other words, they will lead from the front to enhance cybersecurity awareness and skillsets. They will serve on cross-functional committees that oversee all aspects of cyber governance – from strategizing to intelligence gathering, threat monitoring, implementing security controls, and performance review.

The role of the senior management team is also to have the courage to ask the questions that matter and have a blend of courage and humility in the face of complex decision-making. They should clearly and skillfully facilitate a shared understanding of the organization's cyber risks and vulnerabilities and then empower the experts lower down the hierarchy with a clear mandate backed by adequate resources and capabilities to actively defend against the threats that matter. Admiral Hyman Rickover, who successfully ran the US Nuclear Navy for thirty years, established a high-reliability organizational culture that, among other things, encouraged a questioning attitude and empowered the submarine personnel with the necessary training and depth of knowledge to report matters of concern to the highest level of command (Winnefeld Jr. et al., 2015).

Progressive leadership also strives to create a culture of enablement, not fear. They ensure that team members have continuous access to customized and immersive training and recognize and reward employees who admit to mistakes, such as unintentionally clicking on a phishing link.

2.2. Capitalizing on people's best intentions and behaviors

As mentioned earlier, people are frequently referred to as an organization's biggest vulnerability. While there is an element of truth to that assertion, it is the framing that negates the hugely positive impact that harnessing human energy, engagement, and commitment can have on an enterprise cybersecurity program. The truth is that, with the right incentives, encouragement, and context, people naturally want to contribute because we all find motivation in being of service and united in something bigger than ourselves.

Cybersecurity professionals are often characterized by an innate drive to protect. To many practitioners, information security is more than a job; it's a cause they want to defend. The most progressive organizations are exploring how to leverage human-centered methods, such as design thinking, to identify how to design security programs that channel the best of what makes us human and complement these capabilities with processes and tooling that augments people's skills instead of hindering them. Design thinking, a user-centered agile innovation methodology, represents a rigorous, reflective, and deliberate approach to problem solving. It consists of four stages – Empathy, Idea Definition, Prototype, and Testing – to generate and test ideas of change in a congenial and user-friendly manner (BASE4 Security, 2023). Such an approach involves interacting with cybersecurity practitioners and enquiring of them, "How might we make your day go better at work? How could we go about allowing you to have more impact? What might we be able to do to take obstacles out of your way? While these are seemingly simple questions, rare are the organizations where such questions get asked and where the answers are genuinely acted upon. Many cybersecurity professionals start out in their careers with a powerful desire to serve and defend, but the weight of organizational bureaucracy, misaligned objectives, and executive disinterest ends up diluting even the most robust resolve. Leaders who are authentically seeking to enable their cybersecurity team to achieve a bigger collective impact for the business and more individual fulfillment should never underestimate the power of consistently showing that they care about their people.

2.3. Look inward before looking outward

While technology can be a powerful ally in augmenting human capacities for incident detection and response, it needs to be used purposefully and not as a substitute for cross-functional collaboration, proactive planning, and sound judgment exercised on the basis of a robust appraisal of known threats and vulnerabilities (Benz and Chatterjee, 2020).

Before looking outwards at the threat landscape, organizations of all sizes and profiles would be well served first to look inwards. In practical terms, what that means is establishing with as much clarity as possible a picture of what valuable information assets an organization has that an adversary might want:

- Do we know what our 'crown jewels' are?
- Have we inventoried them?
- Do we know where they are located?
- Do we know which attackers might be attracted to them?
- Do we know the tactics, techniques, and procedures (TTPs) of those attackers?
- Do we have an idea of the impact on our business if we were attached?
- Do we know precisely how to respond to an attack?

On the surface, those questions may seem deceptively simplistic. The reality in most organizations is that getting to an answer can be quite challenging. But that cannot be an excuse for not making a concerted and consistent effort to know the risks an enterprise faces as accurately as possible and prepare as diligently as practicable (Barbee, H. 2022).

The good news is that most organizations know more than they realize they do. A wholly constructive first step is to start by building 'connective tissue' between internal teams that may not naturally collaborate extensively. Skilled individuals and experienced practitioners hold a wealth of knowledge that can easily go untapped when collaboration occurs only in functional silos. However, with an investment of leadership buy-in, time, and solution-oriented curiosity, any organization can start ramping up its defensive capabilities by tapping into its people's intelligence.

Once internal intelligence sources have been fully leveraged and the organization has a clear picture of its top risks, that is when it starts to make sense to look outwards and begin consuming externally sourced threat intelligence from open source and/or commercial providers. To avoid flooding enterprise cybersecurity analysts with an overload of information that turns into nothing more than 'noise,' it is crucial to carefully curate the intelligence sources so that the choice is aligned with the organization's risk profile and delivers discernible value.

2.4. Getting ownership, responsibility, and accountability right

For a whole-of-enterprise approach to succeed, accountability for cybersecurity outcomes needs to be elevated from the IT department to the board, the CEO, and the senior executive level. In many organizations, this requires a shift that is more cultural than technical: when cybersecurity is considered a core enterprise risk, it is much more intuitive for it to be owned by the CEO and the Board. However, even when backed by the active stewardship of the CEO and Board, the Chief Information Security Officer (CISO) and their team cannot effectively secure organizational data and information systems without the active involvement and support of the operational unit and business-line unit heads. To gain cross-functional leadership support, they must strategize how best to protect their data and assets, and how to recover in case of disruption. Appropriate project approval procedures should be in place whereby business leaders thoroughly vet security projects and are willing to sponsor and own the approved initiatives. Such business ownership and partnership are also essential for smooth collaboration among the security, development, and operations teams. The opportunity to team and partner together enhances knowledge and awareness of each group's nature of work and challenges. When supported by rewards and incentives that are aligned and not conflicting, collaborative work structures build camaraderie and boost morale which contributes to better security outcomes.

This synergistic approach, where business, technology, and cyber defense leaders come together to lead and support security initiatives, needs to permeate the entire organization because a cyber threat to one part of the business is a threat to all of the business, and a vulnerable organization can too easily become a threat to all of its partners and ecosystem. As noted by a CISO, "Security demands the participation and commitment of everyone inside an organization…it is essential to prioritize security as a shared responsibility and foster an environment where security is not a burden but rather a norm."

2.5. Measuring the right things, incentivizing the right behavior

The old business adage says that what gets measured gets managed. And that's true of security in a great many organizations. However, there is a huge difference in outcomes between measuring the "right" things and measuring *some*thing.

In business, as in life, nothing exists in isolation, and we need to stop behaving as though the cybersecurity team can, all by itself, protect its organization. The key to success lies in meaningful cross-functional collaboration across enterprise silos so that information is shared, skills are blended, alternative viewpoints are considered, and security becomes a "whole of enterprise" endeavor instead of the remit of a small number of experts who inevitably risk becoming overburdened and subsequently disengaged.

The most frequent dysfunction that occurs is when IT and Security are measured on vastly different performance criteria which serve to discourage collaboration and, in some cases, fuel inter-team conflicts. Instead of enabling people, organizations unintentionally set them up for dissent and failure, because of antagonistic incentives and performance metrics.

Performance management systems are only useful when they drive desirable behaviors that deliver operational and strategic goals. When different teams in the organization have dependencies on each other for their individual success in delivering an outcome that matters to the business, it is crucial to make these value stream dependencies explicit and design processes and performance measurement systems that enable people to work well together in the creation of value. This is another area where Design Thinking can be hugely impactful.

3. Key recommendations

It is important to remember that cybersecurity is an enterprise-level responsibility that needs to be shouldered by a team of teams, with employees from outside of the IT and security functions playing a crucial role in maintaining the organization's overall security posture. By shifting the narrative from "humans are the weakest link" to focusing on human-centered cybersecurity preparedness, organizations can empower their team members to become the first line of defense against cyber threats. Leaning into the five core characteristics of a whole-of-enterprise approach to cybersecurity, the following are some actionable recommendations for a human-focused approach to cybersecurity preparedness.

3.1. Actively engaged leadership

Leaders should view cyber threats as a strategic opportunity to retain and grow their customer base by demonstrating their commitment and superiority in protecting sensitive data and related digital assets. They shouldn't hesitate to continuously learn about their organization's information security strengths and vulnerabilities. In other words, they must lead from the front to enhance cybersecurity awareness and skillsets. They should serve on cross-functional committees that oversee all aspects of cyber governance – from strategizing to intelligence gathering, threat monitoring, implementing security controls, and performance review.

3.2. Customized and continuous cybersecurity awareness and training

Educate employees about common cybersecurity risks and best practices and get creative so they feel engaged and interested. In addition to offering regular training sessions to help them recognize phishing emails, avoid social engineering tactics, and understand the importance of strong passwords, and providing resources like posters, newsletters, and online modules to reinforce the training, make sure that organizational leaders regularly and consistently communicate about why cybersecurity awareness matters by role-modeling the right behavior

from the top. Training programs should be customized to ensure organizational members better understand the dos and don'ts of cybersecurity associated with their specific roles. Incremental and continuous training is preferred to reinforce awareness among current and future organizational members.

3.3. Fostering a culture of prompt reporting

Encourage employees to report any suspicious activities or incidents promptly, along the lines of the prompt in the London Tube, "See it. Say it. Sorted." Establishing clear channels for reporting, such as a dedicated email address or an incident response hotline, is a good start. Making these channels easily accessible even in pressured situations and ensuring that employees feel comfortable reporting without fear of retribution are contextual factors that make the difference between having the right intention and generating the desired impact.

3.4. Creating a culture of enablement and not fear

People are frequently referred to as an organization's biggest vulnerability. While there is an element of truth to that assertion, the framing negates the hugely positive impact that harnessing human energy, engagement, and commitment can have on an enterprise cybersecurity program. The truth is that, with the right incentives, encouragement, and context, people naturally want to contribute because we all find motivation in being of service and united in something bigger than ourselves. Creating a culture of enablement and not fear where every organizational member is appropriately trained to protect strategic assets, feels comfortable owning up to mistakes, and are recognized and rewarded for their actions.

3.5. Establishing and rehearsing a clear incident response plan

As the focus on operational resilience intensifies, particularly in regulated sectors of the economy, the enterprise-wide assumption needs to be that "things break, disruption will occur". While the specifics of all potential incidents cannot be known upfront, it is reasonable to assume that their occurrence is not so much a question of 'if' but 'when.' Organizations that take the time to do the thinking and scenario-planning needed to develop a comprehensive incident response plan - detailing with unequivocal clarity the steps to be taken in case of a cybersecurity incident and the who-does-what - are eminently better positioned to respond and recover. Including clear roles and responsibilities for different team members, defining communication channels during an incident, and regularly testing and updating the plan to ensure its effectiveness are the crucial steps that too many organizations cut corners on. Getting the plan right is not an easy task. But trying to conduct incident response and recovery with a poorly defined plan or no plan is even harder.

4. Conclusion

Remember, cybersecurity preparedness is an ongoing process. The key to going from a strategy that exists only on paper to a whole-of-enterprise motion is to bring people together and put in place the conditions for them to build trusted relationships with each other across organizational layers and silos so that there is a clear sense of solidarity and 'shared fate.' Most importantly, tap into their intrinsic motivation to protect and serve a noble cause by encouraging them to envision how they want to contribute to defending the organization. And lastly, with the active

involvement of executive leadership and board members, empower them daily to precisely do that.

[Insert Appendix Here]

References

Abraham, C., Chatterjee, D., & Sims, R. R. (2019). Muddling through cybersecurity: Insights from the US healthcare industry. *Business horizons*, *62*(4), 539-548.

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in society*, *73*, 102258.

Al-Somali, S. A., Saqr, R. R., Asiri, A. M., & Al-Somali, N. A. (2024). Organizational Cybersecurity Systems and Sustainable Business Performance of Small and Medium Enterprises (SMEs) in Saudi Arabia: The Mediating and Moderating Role of Cybersecurity Resilience and Organizational Culture. *Sustainability*, *16*(5), 1880.

Barbee, H. (2022). Comprehensive Asset Discovery, Episode 37, The Cybersecurity Readiness Podcast Series, October 26, 2022.

BASE4Security (2023). Design Thinking applied to Cybersecurity, April 20, 2023, https://www.base4sec.com/research/en/Design-Thinking-Ciberseguridad/

Benz, M., & Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business horizons*, *63*(4), 531-540.

Chatterjee, D. (2021). *Cybersecurity readiness: A holistic and high-performance approach*. SAGE Publications.

Georgiadou, A., Mouzakitis, S., Bounas, K., & Askounis, D. (2022). A cyber-security culture framework for assessing organization readiness. *Journal of Computer Information Systems*, *62*(3), 452-462.

Jones, L. A. (2024). Unveiling Human Factors: Aligning Facets of Cybersecurity Leadership, Insider Threats, and Arsonist Attributes to Reduce Cyber Risk. *SocioEconomic Challenges*, *8*(2), 44-63.

KPMG (2023). SEC's final cybersecurity rules: A board lens, https://kpmg.com/us/en/board-leadership/articles/2023/sec-final-cybersecurity-rules-a-board-lens.html, accessed on May 31, 2024.

Lang, E. L. (2022). Seven (Science-Based) commandments for understanding and countering insider threats. *Counter-Insider Threat Research and Practice*, *1*(1).

Lourenco, D. A. (2022). Bridging the Gaps Between Intention and Practicality in Cybersecurity, Episode 32, The Cybersecurity Readiness Podcast Series, August 17, 2022.

Pearlson, K. and Hetner, C. (2022) "Is Your Board Prepared for New Cybersecurity Regulations**?** *Harvard Business Review*, Nov. 11, 2022.

Sewak, M., Sahay, S. K., & Rathore, H. (2023). Deep reinforcement learning in the advanced cybersecurity threat detection and protection. *Information Systems Frontiers*, *25*(2), 589-611.

Shah, C. (2024). Creating a Security-Minded Culture Creating a Security-Minded Culture, Episode 66, The Cybersecurity Readiness Podcast Series, May 22, 2024.

Shepherd, T. (2024). Dave Chatterjee Drops the Cybersecurity Jargon, Encouraging Proactiveness Rather than Reactiveness, *USA Today*, April 8, 2024.
Uchendu, B., Nurse, J. R., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. *Computers & Security*, *109*, 102387.

Winnefeld Jr, P. A. S., Kirchhoff, C., & Upton, D. M. (2015). Cybersecurity's human factor: Lessons from the pentagon. *Harvard Business Review*, *93*(9), 87-95.

Research methodology

Data was gathered from primary and secondary sources. A multi-method approach of literature review, focus groups, and expert interviews was used to collect data. In-depth interviews with business leaders and subject matter experts were important sources of insight. The interviewees represented a wide range of industries: from higher educational institutions to government agencies, information technology services, healthcare, financial technology (fintech), supply chain management, insurance services, security and information management solutions, food and beverages, and communications and information technology. Table 1 presents a sample set of interviews that helped identify the five characteristics of a human-centered whole-of-enterprise approach to cybersecurity preparedness: (1) Enlightened and engaged leadership; (2) Capitalizing on people's best intentions and creativity; (3) Looking inwards before looking outwards; (4) Getting ownership, responsibility, and accountability right, and (5) Measuring the right thing, incentivizing the right behavior. Qualitative data from the interviews were analyzed using a thematic analysis approach. The NVivo analysis tool was used to code the data and extract the themes.

Table 1. Sample interview data set

Interviewee role	Industry	Human-centered whole-of-enterprise approach characteristics
CEO	Insurance	• Enlightened and engaged leadership • Capitalizing on people's best intentions and creativity • Looking inwards before looking outwards • Getting ownership, responsibility, and accountability right • Measuring the right thing, incentivizing the right behavior
Deputy CISO	Education	• Capitalizing on people's best intentions and creativity • Looking inwards before looking outwards • Getting ownership, responsibility, and accountability right
Executive VP & CTO	Information technology services	• Enlightened and engaged leadership • Capitalizing on people's best intentions and creativity • Looking inwards before looking outwards • Getting ownership, responsibility, and accountability right
CISO	Healthcare	• Enlightened and engaged leadership • Capitalizing on people's best intentions and creativity • Looking inwards before looking outwards • Getting ownership, responsibility, and accountability right
Director, Personnel & Security Research Center, Department of Defense	Government agency	• Enlightened and engaged leadership • Capitalizing on people's best intentions and creativity • Looking inwards before looking outwards • Getting ownership, responsibility, and accountability right • Measuring the right thing, incentivizing the right behavior
President, IoT Security Institute	Supply chain management	• Enlightened and engaged leadership • Capitalizing on people's best intentions and creativity
Founder & CEO	Security & Information management	• Looking inwards before looking outwards • Getting ownership, responsibility, and accountability right • Measuring the right thing, incentivizing the right behavior
Senior VP, Cybersecurity Strategy & Architecture	Fintech	• Enlightened and engaged leadership • Capitalizing on people's best intentions and creativity • Looking inwards before looking outwards • Getting ownership, responsibility, and accountability right • Measuring the right thing, incentivizing the right behavior
Cybersecurity Awareness & Training Expert	Food & Beverage	• Enlightened and engaged leadership • Capitalizing on people's best intentions and creativity • Looking inwards before looking outwards • Getting ownership, responsibility, and accountability right • Measuring the right thing, incentivizing the right behavior
Executive Director	Communication t Information Technology	• Enlightened and engaged leadership • Capitalizing on people's best intentions and creativity

		• Looking inwards before looking outwards • Getting ownership, responsibility, and accountability right • Measuring the right thing, incentivizing the right behavior

Figure 1. Characteristics of a human-centered whole-of-enterprise approach