EXPERT INSIGHT

Cyber Minds

Insights on cybersecurity across the cloud, data, artificial intelligence, blockchain, and IoT to keep you cyber safe

Shira Rubinoff

Packt>

Cyber Minds

Insights on cybersecurity across the cloud, data, artificial intelligence, blockchain, and IoT to keep you cyber safe

Shira Rubinoff

Packt

BIRMINGHAM - MUMBAI

Cyber Minds

Acquisition Editor: Andrew Waldron
Acquisition Editor – Peer Reviews: Suresh Jain
Content Development Editor: Alex Patterson
Technical Editor: Aniket Shetty
Project Editor: Tom Jacob
Proofreader: Safis Editing
Indexer: Pratik Shirodkar
Presentation Designer: Sandip Tadge

First published: January 2020

Production reference: 1080120

Published by Packt Publishing Ltd.
Livery Place
35 Livery Street
Birmingham B3 2PB, UK.

ISBN 978-1-78980-700-4

www.packt.com

packt.com

Subscribe to our online digital library for full access to over 7,000 books and videos, as well as industry leading tools to help you plan your personal development and advance your career. For more information, please visit our website.

Why subscribe?

- Spend less time learning and more time coding with practical eBooks and Videos from over 4,000 industry professionals
- Learn better with Skill Plans built especially for you
- Get a free eBook or video every month
- Fully searchable for easy access to vital information
- Copy and paste, print, and bookmark content

Did you know that Packt offers eBook versions of every book published, with PDF and ePub files available? You can upgrade to the eBook version at www.Packt.com and as a print book customer, you are entitled to a discount on the eBook copy. Get in touch with us at customercare@packtpub.com for more details.

At www.Packt.com, you can also read a collection of free technical articles, sign up for a range of free newsletters, and receive exclusive discounts and offers on Packt books and eBooks.

Contributors

About the author

Shira Rubinoff is a recognized cybersecurity executive, cybersecurity and blockchain advisor, global keynote speaker, and influencer who has built two cybersecurity product companies and led multiple women-in-technology efforts. She currently serves as President of the NYC-based technology incubator Prime Tech Partners and the social-media-security firm SecureMySocial. She also serves on the boards of the Executive Women's Forum for Information Security, Leading Women in Technology, the blockchain company Mainframe and the **artificial intelligence** (**AI**) companies TrueConnect and Pypestream.

An expert in the human factors of information technology and security, Ms. Rubinoff was named one of New Jersey's Best 50 Women in Business, was named by CSO Magazine as a Woman of Influence, was honored by CSO and the EWF with their "One to Watch" award, and was honored as the 2017 "Outstanding Woman in Infosec" by the CyberHub Summit. She has also been calculated by analysts to be the top female cybersecurity influencer globally on social media. Ms. Rubinoff also created numerous video series, including a series of interviews with the top executives of the most prominent cybersecurity and technology companies. She has published many articles, and lectures, on topics related to the human factors of cybersecurity, blockchain, and related topics, and holds several patents/patents-pending in areas related to the application of psychology to improve information technology and cybersecurity.

About the reviewer

Peter Cohen has a wealth of experience in helping organizations defend against targeted cyber-attacks—particularly those facing a legitimate threat from a nation state. His research into the long-term impact of cyber-events has been presented globally.

Peter is the EMEA Managing Director at HolistiCyber, a specialist cyber defense consultancy.

Table of Contents

Preface

This book is inspired by my career journey, in which I've advised countless startups and have repeatedly witnessed remarkably similar cyber security challenges across a multitude of organizations. Given my educational background in psychology, I've always approached technology and cybersecurity from a vantage point that seeks to decipher the interplay of human factors with rapid technological advancement. That's why I've dedicated this book to outlining why humans are at the front and center of many problems, and in turn many solutions, in cybersecurity.

Human factors remain the key issue in cybersecurity around the world. Amidst an increasingly complex landscape, cybersecurity has always boiled down to the people, the process and the technology—three elements that must work together to maintain a cybersecure environment. Implementing technology to buttress your proactive and reactive posture will always be inadequate, unless the human element within an organization is addressed as well. In the end, the ultimate determinant of success in cybersecurity is implementing the right process, which is the bridge between people and technology.

This work is a comprehensive human-centric treatise that seeks to impart the professional lessons I've learned. These lessons are meant for business leaders to take back to their own organizations, as they confront their most profound cybersecurity challenges. This book is especially relevant to those in the C-suite who want to see a cohesive and realistic strategy, designed for humans, that can be deployed to create the conditions that foster proper cyber hygiene.

By unpackaging the human factors piece, you will be able to take a better overview of cyber hygiene and view it holistically and globally. My book provides a window into how to identify the pitfalls you may face as you work to strengthen your organization's cyber posture. Interviews with some of the top minds in the industry, coupled with my commentary, provide further insights, real-world examples, and lessons that are applicable and actionable to quell some of the most formidable cyber challenges I've seen throughout my professional journey.

I sincerely hope you enjoy the book, and look to it as a resource for you and your organization.

1

Integrating Humans and Technology – Four Steps to Cyber Hygiene

This book is about humans, the interaction between people and technology, and the process that surrounds that constant interaction. Throughout the book, you'll notice that technical and organizational dynamics are often discussed together. That's because it's hard to separate the two; humans are at the front and center of every cybersecurity decision and action you take.

While human factors are not the be all and end all in achieving a secure organization, they certainly play a crucial role in every organization's security measures. You have to talk about cybersecurity from a macro view that's inclusive of the human factors at every step of the way. Every organization needs, in my experience, to take four essential steps to build a culture of effective and meaningful cyber hygiene, and bind the human and technical foundations of cybersecurity together: continuous training, global awareness, regular updates, and Zero Trust. Cybersecurity doesn't exist in a vacuum, and effective guidance of your organization's cyber hygiene needs to take into account the cultural realities that make up your organization's environment.

To deliver the critical information needed to fully comprehend cybersecurity, I thought a lot about the people having a profound impact on our industry and the focus they could provide through their insight.

I engaged them, and through dialogue, interviews, and then subsequent takeaways that I present, I approached future concerns and corresponding solutions, and the overlap they have with the real-world challenges occurring as we speak.

After we fully examine the role of humans at every level of cybersecurity, we'll review how cybersecurity intersects with the following areas through wide-reaching conversations about blockchain technology, the cloud, proactive and reactive approaches to data breaches, the **Internet of Things** (**IoT**), augmented reality, and artificial intelligence.

Humans are the problem and the solution

Human factors and cybersecurity go hand-in-hand. First, to be cyber-secure, the elements of security technology must be addressed. While you're executing this monumental task, remember that human factors ought to be a fundamental consideration when creating your security protocols. How humans are approached when implementing security compliance will ultimately determine the level of security within a given organization.

The human is the weakest link in the cybersecurity chain; make them part of the solution, not the problem.

In my experience, this is the most powerful sentence to consider when thinking about the overall cybersecurity of an organization. I repeat, the human is always the weakest link in the security chain; and that's true on both sides of security. Security is built to protect humans, but it's built by humans and the bad actors attempting to break down security are human too. Humans are the common thread, always the centerpiece of both the security problem and the solution.

Given that there are humans involved in every step of the way, an organization can decide to take the view that humans are the problem and govern from that perspective. Alternatively, they can flip their vantage point and take the position that humans are the solution.

With that in mind, they can implement proper cyber hygiene in the organization, while simultaneously unifying their team, as humans take center-stage as the solution. Needless to say, the latter is a much more compelling and effective way to tackle your greatest security challenges.

Making humans the linchpin of your organization's security solutions empowers your employees. It also helps to lay the groundwork for a loyal and cohesive workforce, bound together and working in concert, ensuring your company is secure from the inside out.

Following this philosophy, you'll be much more likely to create an environment with proper cyber hygiene, which is crucial in today's ever-more-dangerous world. Cyber hygiene is pivotal in curtailing both malicious insider threats from disgruntled or opportunistic employees, and non-malicious insider threats from oblivious or negligent employees.

Organizational culture is the tie that binds people together, and that inevitably determines the efficacy of entire organizations. It's important to step back and review how the culture around cybersecurity has evolved substantially in recent times, and how it's become an entirely different process over the years.

Compliance culture versus security culture

Compliance culture was the norm for many years, adopted across countless organizations to promote cyber safety. That world is now long gone. Security culture is now the standard model that many organizations have embraced as a practical necessity for proper organizational cyber hygiene.

Compliance culture – top-down mandate

It's not rocket science: Compliance culture was exactly like it sounds. Be compliant!

If you take a peek at the definition in the Merriam-Webster Dictionary, you'll see that compliance is "the act or process of complying with a desire, demand proposal, or regimen."

Accordingly, you can probably already guess how an organization's compliance culture played out nearly everywhere. The rule set was established by the top of the organization, with the goal of complying with the relevant legislation at minimal cost, and implemented all the way down through every level of an organization. This was a one-size-fits-all model that harkened back to the command-and-control style of management that was prevalent in the 20th century.

Rules were made at the top and no-one else had any input whatsoever. This top-down rulemaking would percolate through all facets of the organization with little to no feedback from its employees. This was an iron fist model of "you do as the checklist says or else." Deviating from established processes, or going beyond the regulatory requirements, was frowned upon if not outright forbidden. Being a good "citizen" of a compliance culture meant not rocking the boat and staying in your lane.

Security culture – a secure environment

The security model approach is different in almost every way. The perception of security shifts and becomes geared toward a collective approach, with the goal of ensuring that the company remains secure. There's an understanding that legislation is just a starting point and the cost of an insecure system is far greater than the cost of good security. This philosophical foundation makes it widely understood that security is everyone's responsibility, and teamwork is an essential part of that process.

This seismic shift doesn't mean that compliance and jobs specifically focused on cybersecurity are replaced. Instead, their roles become better integrated with the rest of the organization. Seamless dialogue and collaboration are relentlessly encouraged to help bolster security measures. While protocol remains in place, it's tailored appropriately to the employees as humans who share collective responsibility for cybersecurity. Job descriptions don't absolve anyone of their individual responsibility to contribute to cybersecurity organization-wide.

Now that we've learned about how leveraging the human aspects of security is critical to ensuring success, and how security culture is the new norm, let's move on to the four steps I consider essential for instituting proper cyber hygiene.

Continuous training is the first building block in this process, as it gives new security measures a better chance of being embraced by your employees.

Four essential steps to achieve proper cyber hygiene

In today's world, your company's integrity hinges on protecting your data, and by extension your customer's data. That's why proper cyber hygiene is imperative. To execute this task, there are four steps to deal with both technological considerations and human factors that you should follow, to implement proper cyber hygiene and keep your organization secure:

1. Continuous training for all employees – from janitor to intern, to consultant to CEO, no matter what job they have in the organization, all employees need to be included.
2. Promoting a culture of global awareness throughout the organization.
3. Updated security and patching on a regular basis.
4. Implementing a stringent Zero Trust model.

Before we delve into the mechanics of the four steps in the implementation of cyber hygiene in your organization, I want you to fully understand the pivotal nature of human factors in any cybersecurity framework.

The human factors in proper cyber hygiene

The reason we're starting with the human factors, instead of the technological ones, is that if the human factors are not accounted for then all the security technology you might use is completely wasted.

It's convenient to ignore or bypass awkward or extended security, and if the people in your organization don't understand why the security protocols in place are necessary, then convenience will win out every time. In that case, even the most up-to-date security measures are wasted.

On the other hand, an engaged and informed workforce is a massive boost to any security endeavor, bringing the combined intelligence of your employees to bear on the problem of security and hunting down overlooked gaps in your defenses. Engaged people are the foundation of cybersecurity, so it's essential that we start by discussing how to engage them.

Step 1 – Continuous training for all employees

Training has to be open-ended, multifaceted, and varied in its methods to convey understanding and spark swift adaptation. Having multiple methods of continuous training empowers your employees to choose the option that suits them best.

Multiple methods are also critically important from both a morale perspective and a legal perspective. In terms of morale, the employee will feel more comfortable following their choice of training method and more satisfied by charting their own course. Legally, if the organization imposes a certain way of training for all employees, accusations of bias may arise where a person feels like they haven't been included.

In the end, the journey may be different for each and every person within an organization, but the end result will be the same. You're going to want to keep it relevant, interesting, and meaningful. I can't stress enough that appropriateness is everything when it comes to training, and a critical part of this step is knowing your audience.

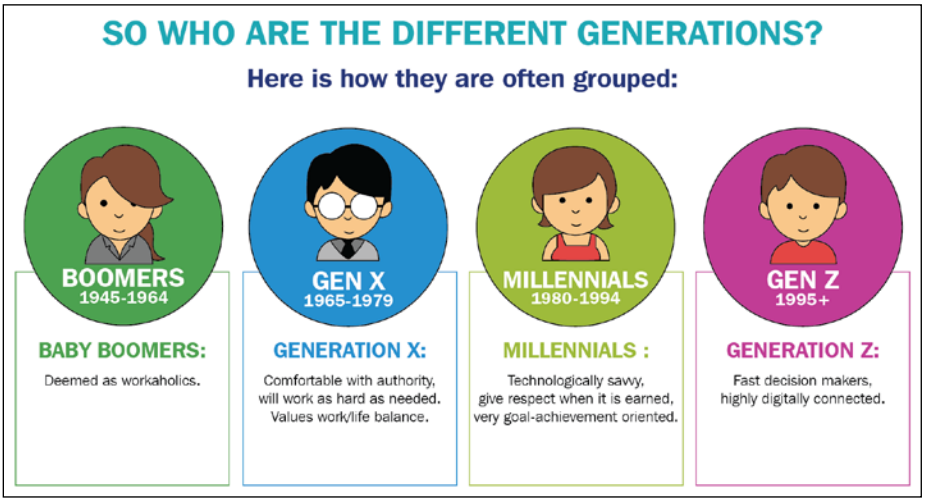
We need to lean on our understanding of human psychology, and how different cohorts, typically segmented by age, view the world. Age-specific messaging has cascading effects for a person within an organization, and can help them understand why these practices need to become an immediate part of their habits to solidify your organization's cyber hygiene.

Know your audience for training – communicating with different generational cohorts

We live in a transitional age, where the cross-generational employee population is more common than ever. That's why when we look at continuous training, we have to consider the demography and lens through which different generations view the world.

This is a good training practice for any new information, but I've found that it's especially important in cybersecurity.

We find ourselves at an inflection point in the workplace, as this is the first time in history where we have at least four generations working side by side – Baby Boomers, Gen X, Millennials, and Gen Z, all with different views on life, work-life balance, problem solving, communication, learning, and social sharing. Each generation has grown up in a very different world when it comes to the usage of technology and how it interplayed with their lives. Their stances on privacy, sharing or oversharing information, how best to work, and how to maintain a good work-life balance all differ from each other.



Communication is key for effective leadership within an organization, so by extension it's important to know your audience when you're training. Part of that is keeping aware of how each generational cohort processes information and instruction differently. As you train different folks within your organization and steer them toward your cyber goals, you'll discover that their different styles inevitably influence their workflow.

Some of these differences are readily apparent if you regularly interact with different generational cohorts. Boomers value face-to-face interaction, old-fashioned phone calls, and long-form conversations that convey, in full detail, the important message and all the other pertinent information that they need to know.

Any other form of communication might be considered impersonal, if not rude, to this generation that values human interaction more than their successors.

Jumping over to the other end of the age groups, Millennials and Gen Z often scoff at phone calls or in-person meetings, especially if the information could have been transferred by some form of messaging. In fact, most younger people are jarred by phone calls, don't use landline phones, and have the ringer on their cell phones on silent most of the time.

These stereotypes don't always hold up, but they're a good starting point. Gen X are especially mixed, and depending on their personality and work style, can embody a mix of several generations' communication style. These are starting points, and if you find they don't hold true for an individual, then your approach needs to change to take that into account.

New ways of training versus old ways of training

The era of annual training events is over. In the past, companies would hold a one-day event either once a year (or in the best case once a quarter) where employees would be taught, lectured, and made aware of security measures. The training would also speed through attacks that the employees should be aware of, a litany of compliance regulations, and relevant protocol that would be put in place.

These events were big splashes where engaging speakers were brought in, hands-on activities were conducted, cutting edge videos were shown, catered lunches and snacks were served, and even maybe a bit of entertainment was provided to take the edge off. These full day fetes were viewed as "home runs" because they captured the employee's undivided attention, with the expectation that they would remember, in full detail, what went on that day and fully comply with every single detail that was shared in this one-stop training.

You've probably gathered why we've moved far beyond this approach. We are human, and we don't remember things well unless we remind ourselves of them often. Unless a person has continuous training around security, they will likely remember snippets or barely anything at all.

When a business has continuous training in place, it remains "top of mind" for the employees. As the training is reinforced it will become second nature, part of the background culture of the organization.

Cybersecurity is ever-changing, so it's only reasonable to conclude that frequent training is needed; but that training should be continuous, rather than staccato, and woven into ordinary workflows instead of seeming like an occasional drip of new responsibilities.

Information dumps versus incremental training

Training for cyber hygiene is complex and extensive. It's a lot to digest all at once. That's precisely why continuous training must reject the old way of doing things, where informational dumps would unload what your employees needed to know to do their job properly.

In my experience, information dumps lead to information overload in just the same way as antiquated annual training. Companies used to, and sometimes still do, overload their employees with everything they need to know about security, compliance, and protocol all at once – along with every possible scenario that might arise, all in one mighty lump of information. It often went with an even bigger handbook, and a phrase like "Here you go, employee, study this so you know it all, and every possible scenario that may come from it. Do not forget anything because everything is important." Clearly, this method sets nearly everyone up for failure.

I've found, and I'm sure you have too, that no employee is able to digest information of that magnitude and fully integrate the new material into their routine overnight. We can't fight nature, and that's why incremental training makes more sense; both from a time perspective and when taking into account the limits of the human ability to consume information.

Schedule training accordingly, and break it down into categories. Make each category meaningful in its own right, with relevant scenarios to explain the importance of the information you're sharing. In the end, that gives your employees a much greater chance of retaining essential information.

Universally applicable versus situationally relevant

Be vigilant in avoiding the fallacy that anything is universally applicable, and that training sessions can be universal as a result. Just because one person wholeheartedly believes that they've identified the best way to train employees, in a very cost- and time-effective way that trains many groups all at once, doesn't mean they're correct.

Picture a universal training session: a huge room with a thousand people in it, all from different disciplines, markets, and sectors. Up at the podium stands a speaker poised to give a very important talk about privacy, security, compliance, and real-world scenarios. The speaker begins to speak, delivering a broad-ranging conversation to cover a hodgepodge of dissimilar sectors, such as healthcare, finance, insurance, government, and every other industry.

Next, she spits out an alphabet soup of regulations with which the audience may or may not be familiar: HIPAA, SEC, EPA, and so on. Undoubtedly, there are scores of people that are already completely lost, or at best encountering content that they're woefully unfamiliar with, because it's far beyond their background. That universal training session has instead become an information nightmare that's going to be anything but effective.

In stark contrast to universal training is situationally relevant training. If you have a room full of people from the same background or industry, dealing with similar issues, regulations, and compliance concerns, you can deliver laser-focused training for that specific demographic. For example, the financial industry will have very specific compliance concerns that differ from healthcare: pension regulations, financial privacy laws, and a very different public perception of the industry to name a few.

You can keep attention and focus on these people's specific sector, discussing relevant information pertaining just to them. Privacy, compliance, and regulations can all be seamlessly covered to inspire meaning and lay the stakes for acquiring habits.

A very broad setting is a recipe for one to tune out from the get-go. It's important to get and keep the attention of someone you're training; their ability to find themselves in the stories you tell and find real relevance in the discussions that follow will build their capacity to achieve proper cyber hygiene.

Stage real-life scenarios

Security shouldn't just be a concept that is discussed, but a reality that is lived. That's why, for training purposes, simulating real-life scenarios can be greatly influential. Walk your team through what they should do when problems arise by using these simulations. Afterward, have the team dissect and discuss what went wrong as a group, and how "we" could have improved the outcome or the end result.

Stress the "we," as in "we are a group that supports each other through these critical moments." It may sound trite, but remember that working as a team is infinitely stronger than working alone.

Think about human physiology. If you make a fist without using your thumb, it has no strength. Just like the strength is in the hand as a whole, we are only as strong as our weakest link, and that weakest link can be any employee from any level within the organization.

Everyone has to be supported, and it's imperative that every team member operates as an integral and indispensable part of a collective unit. This lays the foundation for a globally aware culture, which is Step 2 in your quest toward achieving meaningful cyber hygiene.

Step 2 – Global awareness and culture for cyber hygiene

In an age of unprecedented interconnectivity and globalization, your organization has to reflect today's realities. We're in a competitive labor market, and getting and keeping quality talent is a constant challenge. It's sad but true: millions of jobs are left open because of the dearth of relevant skills among today's workforce, and this is especially the case in the field of cybersecurity.

Today's big corporate players prioritize company culture and promote purpose as a matter of necessity. These things were previously thought of as squishy and hard to define, but now they're recognized as more pivotal than ever to modern employees. Belonging and overall workplace satisfaction are essential components in any company's effectiveness and competitiveness.

We can look to any part of our lives, and wherever we feel appreciated, valued and heard we naturally feel more aligned, loyal and productive in that environment. By natural extension, we'll practice better cyber hygiene, too.

A globally aware culture that promotes cyber hygiene does so by promoting a positive environment, where constant dialogue and unfettered collaboration are key indicators of organizational health. As mentioned earlier, employees are seen as part of the solution instead of the problem, and are made aware of changes that are needed via relevant flows of communication.

It's very easy to point fingers at someone and call them the problem, rather than dig for the root cause of risky or unsafe behavior. Empower your employees to be part of the solution. Continuous training and awareness will keep the protocols fresh, and their minds sharp, but it's also essential in my experience to gather feedback and let information flow both ways.

In our cut-throat world, it's of utmost importance that your employees feel supported by the management team. They need to be aware that if they report a potential problem or misaligned behavior, it will be welcomed, not frowned upon for possibly "blowing a false whistle." The worst-case mindset for your employees is that if they stay quiet, and just do as they're told, they can't be held responsible for a problem. More often than not, this is the current case in most organizations when it comes to speaking up or reporting a problem.

I've found that transparency is the best sanitizer. Transparency is a key ingredient in a globally aware organization to preserve a stellar work environment for their employees. If you encourage feedback, and allow your employees to question what has been implemented, you may discover you haven't been asking the right questions. This new way of looking at things may uncover a faulty part of your security, which when fixed will strengthen your defenses throughout the organization. Your employees may have "eyes and ears" in areas that you may not be focused on – encouraging their feedback will likely help you find areas that need strengthening in your organization. Utilizing this most valuable resource, your employee, benefits you from a morale and security standpoint.

Building an inclusive workforce – diversity is at the heart of global awareness

When we think about diversity, we often hone in on obvious demographic indicators such as gender, age, culture, demographic, and socio-economic status. These are definitely important and should not be trivialized, but as a globally aware organization, you should frame diversity differently. For companies, demographic diversity boils down to diversity of thought, approach, and viewpoints. Diversity means having employees who view the world quite differently from one another because of the lenses of their background, upbringing, education, and a multitude of other factors that have shaped and molded them.

Think about a phenomenon we see far too often: A company entirely made up of people of a similar gender, age group, culture, race, demographic, or socio-economic status. This situation almost never improves organically, because recruiting through existing employees' social networks at monolithic organizations tends to reinforce this demographic disaster.

Without diversity, any organization will consistently yield remarkably narrow and irrelevant conclusions and attack problems in a very limited way, especially in their approach to security and privacy. How could it not? A monoculture is scientifically vulnerable to disease because of its lack of genetic diversity. Similarly, creating an echo chamber within organizations through limited demographic diversity leads to suboptimal outcomes, including woefully inadequate security.

The pitfalls of a demographic monoculture

Let's walk through two scenarios to better illustrate the difference between diverse and globally aware organizations, and those that are painfully stuck in the past.

For the first scenario, picture a group of 10 employees, all 40- and 50-year-old Caucasian men, all of whom have attended top Ivy League schools and come with strong business and finance experience. They all have their MBA, were raised in upper-middle- or upper-class households, played sports in college, are married with two to three kids, and have similar religious beliefs.

Before any serious business dialogue even begins, they have a chance to socialize for a little while, and quickly discover the immense number of similarities they have in common. Differences will be cast aside, and these jaw-dropping similarities are going to create a warm feeling of comfort and belonging in the room. Dissention and discomfort will be non-existent in this remarkably cookie-cutter crowd.

Imagine that this group is then presented with a topic to problem-solve. One person is appointed to lead the discussion, and to encourage collaboration, communication, and feedback. He gets up and starts the ball rolling, with the new colleagues to whom he has already bonded.

The die has been cast for this monoculture of men, and each one of them will behave as if they "belong to a club." In effect, they will create an echo chamber in which if one person makes his position clear, there will be little to no dissention from his other colleagues. As the building blocks of an idea are laid out, complete collaboration will take hold, with few alternatives.

Welcome to the world of a monoculture of people and ideas. As ideas are thrown out into the discussion, the nods and words of encouragement and agreement are seen and heard. If one disagrees, the nature of that group will lend itself to words like, "We're all on the same page." Rarely will someone rock the boat and propose a competing idea in such a bonded group of like-minded men.

Now, consider scenario two: Envision a room with 10 people that's teeming with diversity. This group is gender-balanced, from a breadth of cultures, a variety of socio-economic backgrounds, and a wide range of beliefs. This cohort is also racially and ethnically diverse, bringing together a plethora of educational backgrounds, personal hobbies, and career journeys.

It's the first scenario turned on its head, as the people in the room rapidly discover the immense number of differences they have with each other. Inevitably, those differences will be highlighted and even embraced, creating an inquisitive buzz and interest in the room.

If this diverse set of folks is presented with the same problem as the previous group, their radically different walks of life will encourage collaboration, communication, and especially feedback.