WHITE PAPER

From Zero to Hero: Why Zero Trust Adoption is Struggling

June 2023

By Charlie Hosner, Matt Dibble, Hasan Muchhala, Sophie Cole & Lachlan George

Many businesses are failing to reap the rewards of Zero Trust despite taking the approach they believe is correct. In this two-part series, we explore the challenges organizations are facing and share our recommended keys to success.

Zero trust is rapidly becoming a buzzword the security community are tired of hearing. When walking around any major security conference, one finds many vendors claiming that their solutions offer “Zero Trust in a box.” Unfortunately, “Zero Trust” has become the anchor word for a plethora of vendor products and services, which are usually pitched as being “silver-bullets” or “simple” to use. These narratives have led many to believe that adopting Zero Trust is straightforward, and that implementation just involves deploying new technology solutions.

Unfortunately, myopic technology-led approaches often do little to improve the cybersecurity resilience of an organization. Instead, IT and security architectures become a Jenga tower of half-implemented technologies, overlapping solutions, in-efficient and ineffective security controls, and fragmented operating models. As a result, organizations frequently experience increased costs and reduced cybersecurity, the exact opposite of what Zero Trust should provide.

Vendors and pundits are always fast to evangelize new technology paradigms, and the same is happening now. Famous past examples have included SSL VPNs, Web Application Firewalls, Next Generation Firewalls, Cloud, and XDR, with trends like resilience and Artificial Intelligence beginning to attract the same attention.
These technologies and concepts are presented as the holistic solution to all our cyber needs, as packaged game changers that will make the problems go away. Zero Trust, like many of the trends that came before it, is an excellent step forward for our industry, but it will only be effective and widely deployed if we come to terms with what it really takes to embed it in a modern organization.

Gartner predicts that whilst over 60% of organizations will embrace Zero Trust by 2025, more than half of organizations will fail to realize the benefits[1]. The purpose of this paper is to present our views on why Zero Trust is failing to deliver valuable business benefits, and to convey our suggestions on how to successfully approach the concept.

[1] John Watts and Jeremy D'Hoinne, "Predicts 2023: Zero Trust Moves Past Marketing Hype Into Reality," Gartner, December 6, 2022, https://www.gartner.com/en/documents/4021946.

What is Zero Trust?

At its core, Zero Trust is a security model that helps keep your data and systems secure in a flexible, adaptable way. Zero Trust forms logical, granular boundaries around protected resources, ensuring that only the intended users have access. This access is continuously re-evaluated to ensure that valuable resources are used in a safe, secure and predictable way by authorized entities. It does this through a blend of identity capabilities, a policy engine tool for directing (or stopping) traffic, which is based on aspects of identity and behavior, as well as a highly flexible, informed view of risk.

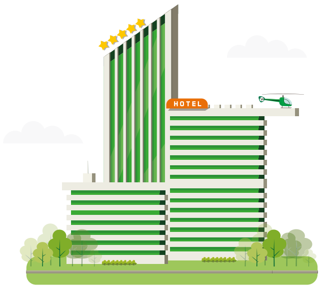
To help better understand what a Zero Trust security model does, we can use the simple analogy of a 'castle & moat' vs. a 'hotel' (see Exhibit 1).

Exhibit 1 - Castle and moat vs hotel model

PAST/PRESENT (CASTLE & MOAT)

"Castle and moat" perimeter and in-depth security layers – **but trusting when inside**

FUTURE (HOTEL)



"Hotel" security with granular checks – **trust nothing, verify everything**

Current security models have typically been built like the 'castle & moat,' with a single perimeter protecting an environment in which everything is trusted. Zero Trust security models are more like a hotel, where you are required to authorize yourself at every step: on initial entry, to access your floor, your specific room, and so on. This significantly improves security because access is limited and verified at each step. When this system is in place, even if a malicious actor has access to the hotel, any damage or theft they cause would be compartmentalized and contained.

Summarizing the benefits

Zero trust has built up a lot of hype, and some of it for very good reason. When done right, it can provide significant improvements to an organization's security profile, but it can help realize several other high value business benefits as well. There is a lot to play for when organizations get the delivery model right.

From significant cost reduction and cost avoidance, to risk reduction and enhanced business agility, an effective Zero Trust approach will have a multifaceted positive impact on your operations. Businesses cannot afford to miss out on these advantages in the current market, or the opportunity to improve things like user experience. A breakdown of the many benefits of effective Zero Trust can be found at the end of this paper (Exhibit 3).

Why is Zero Trust failing?

Despite the long list of benefits organizations can realize through Zero Trust concepts, successful adoptions are limited, and organizations are failing to capitalize on its benefits. Gartner estimates that only 1% of large enterprises currently have mature, measurable Zero Trust programs in place, and that this will increase to 10% by 2026 [1].

We believe that organizations are becoming disillusioned with Zero Trust, and that the constant hype, coupled with silver-bullet promises, have led to two main archetypes emerging:

1. **Archetype 1: Organizations that have started with tactical, isolated point deployments of Zero Trust technologies with no big picture plan.** For example, during the recent pandemic, Zero Trust Network Access (ZTNA) was a hugely popular starting point to help combat overloaded Virtual Private Networks (VPN). It came with the promise that it could increase security and reduce costs. Whilst it is true that ZTNA can increase security (when deployed properly), many organizations have unfortunately implemented this technology as a like-for-like VPN replacement, which has diluted its benefits. Because of corner-cases and resilience concerns, we see organizations holding on to the traditional VPN, resulting in negligible cost reductions, and if anything, increased costs due to running two similar capabilities with the associated license and support costs.

2. **Archetype 2: Organizations that have attempted to design and launch large scale, monolithic Zero Trust programs.** These programs often attempt to boil-the-ocean, laying out a grand target state architecture without consideration for what the business really needs. The programs are planned as multi-year journeys and are usually accompanied by huge budget estimates. In our experience, these programs either fail to launch altogether, or they get shut down within 12-18 months when they fail to deliver proximate value.

Archetype 1 is tactical by its very definition, and rarely results in the big picture benefits Zero Trust has to offer. We believe that an integrated vision and guidance is important, but the key to success lies in how the Zero Trust program is designed and executed. Failures, in our experience, tend to come from human-centric sources, limitations in legacy IT environments, or a lack of clarity regarding the program's direction. As such, we have compiled a list of the top reasons we see Zero Trust programs failing.

Absence of a clearly articulated "why?"

We frequently encounter Zero Trust programs with either weak or non-existent strategies and business cases. The rationale for why Zero Trust is being pursued and the benefits it will deliver are often either absent or described in vague terms. Key examples include risk or cost reduction, with little to no additional insight provided. In organizations demonstrating this level of understanding, we frequently found huge disconnects between stakeholder groups and the absence of a clearly articulated "why?" This led to many forming their own view of what Zero Trust is and what it would deliver.

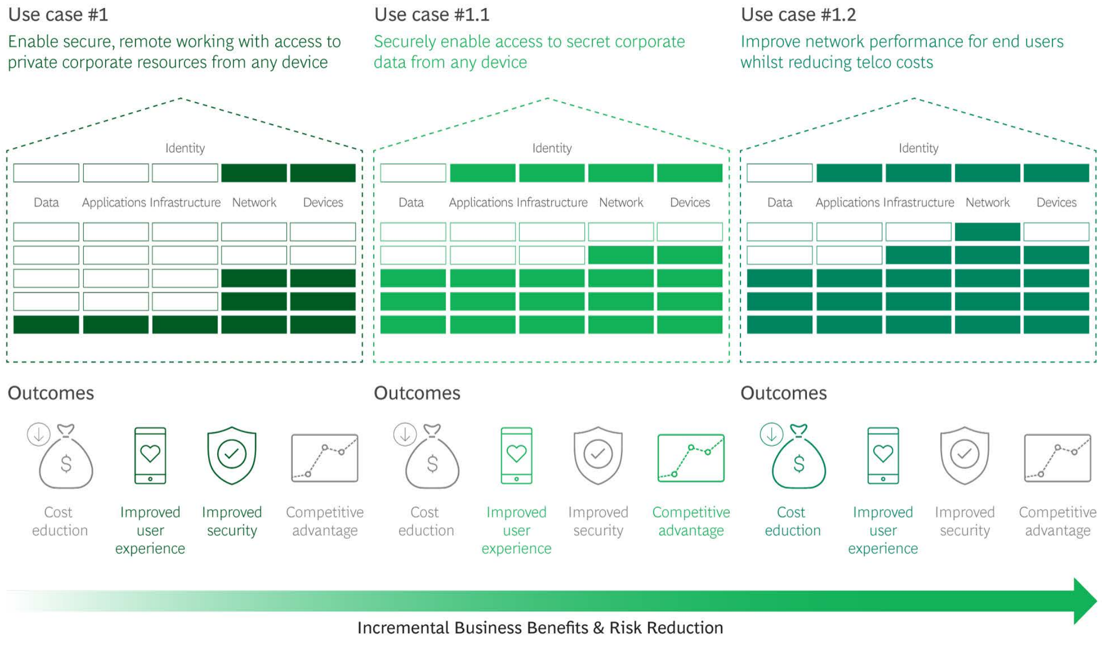
Without a strong articulation of "why," it is impossible to secure the required level of executive sponsorship, business buy-in and budget to launch and sustain a program of work.

We believe that successful Zero Trust programs must be backed by a comprehensive understanding of the “why” to link the program’s initiatives to the organization’s broader purpose, strategy, and objectives. This shared purpose forms the backbone of the strategy and business case, acting as a “North Star” to guide and direct all Zero Trust initiatives. It also serves as a constant reminder to all stakeholders of why Zero Trust is critical to the business, the specific use cases the organization is striving to satisfy, and the roles of specific initiatives and technologies. All team members need to understand this chain of ‘why,’ and be clear on how their individual contributions make the bigger picture a reality.

A failure to decompose Zero Trust into hierarchical, achievable use cases

In the section above, we introduced archetype two organizations, the ones that have attempted to design and launch large-scale, monolithic Zero Trust programs. One of the key challenges that these programs face, and the reason they often stall within 12 to 18 months, is that they fail to decompose Zero Trust into a set of linked, hierarchical use cases. These cases should be tailored to key business objectives and benefits, and be understood by the organization. This includes knowing the scope of each use case and where it can deliver value quickly.

Exhibit 2 - Three use cases


Use case #1
Enable secure, remote working with access to private corporate resources from any device
Use case #1.1
Securely enable access to secret corporate data from any device
Use case #1.2
Improve network performance for end users whilst reducing telco costs
Identity
Data
Applications
Infrastructure
Network
Devices
Outcomes
Cost eduction
Improved user experience
Improved security
Competitive advantage
Incremental Business Benefits & Risk Reduction

For each of the six Zero Trust technology domains, identity, data, applications, infrastructure, network, and devices, we plot the illustrative and relative capabilities required for each use case. In the exhibit above, we have highlighted the high-level outcomes that the use case will deliver. The first use case could translate to a foundational implementation of Zero Trust Network Access (ZTNA), where the primary factors relate to network, devices, and identity.

No understanding of granular architecture

Organizations need an intimate understanding of how their environments have been architected to implement Zero Trust effectively. Unfortunately, most organizations lack a long list of items that are crucial to do so. Top examples of these components include user journeys, data flow mappings, inter-process communication flows, hostnames, IP addresses, ports and protocols, user inventories, locations, and access rights.

A granular understanding of your organization's information and processes is vital, as Zero Trust involves identifying implicit trust relationships and deciding which will be subject to adaptive (zero) trust. One of the great strengths of Zero Trust is its ability to make authentication and access decisions at a very granular level. This capability is directly limited by how well we understand our asset environment and usage patterns. If our estate is a mess, our Zero Trust implementation will fall far short of our goals as a result.

We recommend organizations take two approaches that will de-risk the Zero Trust program:

1. **Ensure that the program prioritizes discovery to acquire the relevant data.** This ensures that the right information is selected to support the implementation of the key use cases. Data will likely be federated across various systems within the organization, such as configuration management databases, asset inventories, enterprise architecture tools, Endpoint Detect and Response (EDR) tools, and Active Directory. In other cases, specialist software may need to be procured and deployed. Either way, early investment in data discovery will go a long way toward achieving an effective outcome. It is essential to remember that no Zero Trust deployment can be more mature than the organization's underlying understanding of itself.

2. **Start with a contained deployment scope and expand once you have demonstrated value.** For example, pick an organizational unit, project, or a subset of business applications where the scope is relatively small and contained. Use this to determine and refine your data discovery approaches, technology configuration and operating model changes, then adopt a fail-fast approach and iterate rapidly. Doing this will allow you to declare some small victories and build momentum and buy-in for a larger investment case.

Ineffective integration between existing technology

Organizations typically have existing technology solutions that could, provided they were integrated, form a foundational Zero Trust architecture. Often organizational silos, a lack of architectural vision, weak governance, internal politics, and individual agendas lead to technology being selected and deployed in isolation without the necessary integrations required to unlock Zero Trust. This is bad news as organizations should be seeking to exploit the existing investments that they have made.

We recently worked with an organization that was seeking to segment its flat network. The organization believed that it required new micro-segmentation technology, but the organization already had multiple technologies that could achieve this objective. This pointed to the fact that technology was not the issue. What was missing was the integration between its existing network and its identity and access management capabilities. This lack of integration ultimately stemmed from organizational silos and internal politics.

We believe that organizations should work on the assumption that they already have many of the technical building blocks required for Zero Trust, and take stock of these capabilities before starting to procure more. Although it may sound obvious, the deployment of new technology seldom fixes people or process challenges. If a lack of integration is due to people or process challenges, then these need to be addressed, and the pretense that technology can be used as a band-aid must be dropped.

Poor executional structure & governance

Zero Trust programs are complex, and they significantly change an organization's technology and security architecture. These architectural changes will span identity, data, applications, infrastructure, and devices, requiring new operating models and some degree of change to existing business processes and ways of working. This level of change needs to be carefully structured, governed and managed to ensure that Zero Trust is efficiently and effectively delivered, ensuring that it is embedded within the organization.

Given this complexity, we suggest that a multi-disciplined Transformation Program Office (TPO) should be established consisting of cybersecurity architects, program managers, business analysts, architects, and change & communication specialists.

The TPO is active in defining and driving the Zero Trust program and initiatives forward, and its role includes:

- Establishing the Zero Trust program by defining the strategy and business case. Building the unbroken chain of why and embedding it in all further plans, designs, and communications
- Defining and prioritizing Zero Trust use cases
- Defining the target state Zero Trust architecture (people, process and technology spanning IT, cybersecurity, and business)
- Defining program and initiative level objectives and key results (OKRs)
- Establishing appropriate governance forums (e.g., Zero Trust Design Authority)
- Launching initiatives to deliver Zero Trust use cases in line with the architecture and roadmap, or linking to, and sponsoring, existing organizational initiatives
- Managing program and project dependencies
- Defining and executing a human centric change program
- Sourcing and making available current-state architectural information
- Resolving conflicts
- Managing benefit and value realization
- Reporting to executive sponsors

Technology-centricity over people

Companies often fail to understand that sustainable change relies on people's willingness to do things differently, regardless of how effective new technologies or processes may be. This is why predominantly technology-centric approaches rarely result in the delivery of sustained value.

Organizations need the correct combination of human-centric approaches alongside technology to correctly balance and integrate the two. In practical terms, changing the fundamental way your environment is architected changes the way you do IT, digital development, security and even business itself. Without the correct focus on behaviors and mindsets, leadership enablement, agility, and adaptability, as well as sufficient cultural change management, Zero Trust transformations will never be a success.

Zeroing in on a successful approach

Now that we have defined the two Zero Trust archetypes, highlighted the key reasons many are failing to successfully implement it, we have a firm foundation upon which to build. As emphasized earlier in this paper, having a clear understanding of your 'why' when introducing Zero Trust is an invaluable starting point. Once this has been established, it is critical to build an effective business case, strategy, capabilities, and culture. To learn more about the individual essential phases in the process of achieving an effective Zero Trust stance, read our follow-up paper on the topic. After all, this is an inevitable evolution of security architecture, and time is of the essence.

Exhibit 3 – A non-exhaustive list of business benefits that a Zero Trust transformation could deliver

ZERO TRUST BENEFITS

BENEFIT CATEGORY	BENEFIT	HIGH LEVEL EXAMPLE OF HOW THE BENEFIT COULD BE REALIZED	EXAMPLE MEASURES
Cost Reduction	IT and cybersecurity technology rationalization drives cost reduction	Rationalization of IT and cybersecurity technologies as part of the Zero Trust transformation. Non-strategic technologies and those with overlapping capabilities are decommissioned resulting in software license and support savings.	1. Reduction in software license and support costs ($)
	Reduction in outsourced IT and cybersecurity operations costs	Zero Trust allows for controls to be re-imagined. Integrated, modern and automated controls allow for a greater degree of in-sourcing, resulting in reduced need for outsources (e.g., reduced need for outsourced firewall ruleset management). Reducing operating costs.	1. Reduced number of operational tickets to outsourcers (n) 2. Reduction in outsourcing costs ($)
	Reduction in audit and compliance costs	Introduction of Zero Trust provides an opportunity to reconsider how controls have been implemented. Control rationalization can result in reduced cost of audit and compliance.	1. Reduced time taken to prepare and execute internal and external audits and compliance (#hrs) 2. External audit fee reduction as reduced need for manual, substantive control testing ($)

Cost Reduction *(continued)*	Reduced cost to onboard employee, third parties and contingent workforce	Zero Trust introduces capabilities that allow organizations to securely embrace bring-your-own-device (BYOD) and bring-your-own-identity (BYOI). These concepts allow costs savings to be realized in the form of reduced hardware (e.g., laptops) and reduced Identity and Access Management (IAM) process times (e.g., negates the need to create HR record and identity for contingent workers).	1. Reduced time to on-board employees and contingent workers and assisted employee and contingent worker cost efficiency savings ($) 2. Reduced cost of IT equipment ($) 3. Process efficiency savings, e.g., IAM, HR, End User Compute (EUC) ($)
	Reduced telco costs	Zero Trust introduces capabilities allowing internet connectivity to form a safe and secure communications backbone for the organization resulting in reduce "point to point" VPNs and telco costs.	1. Reduced telco costs ($) 3. Reduced number of site-to-site VPNs (n)
Cost Avoidance	Reduced cost of responding to cyber incidents	Zero Trust capabilities can provide increased logging and monitoring verbosity to the security operations center (SOC) and provide them with ability to contain cyber incidents at the user and device level (as opposed to network).	1. Reduced time to identify, contain, eradicate, and recover from a cyber incident 2. Reduced cost of business disruption ($)
	Negates the need for tactical audit remediation programs	Zero Trust provides the opportunity to exceed regulatory minimums through the introduction of adaptable cybersecurity controls avoiding year-on-year remediation programs in response to audit findings.	1. Costs saved by avoiding audit remediation programs (average of cost from last X years $)
Risk Reduction	Reduced likelihood and impact of ransomware causing enterprise-wide disruption	Zero Trust capabilities provide advanced security controls e.g., sandboxing, internet filtering, multi-factor authentication, least privileged access etc. These controls reduce the likelihood that an attacker would be able to gain access to systems, and even if they do logical micro-perimeters will contain the impact so that disruption is localized.	1. Demonstrate risk reduction via application of enterprise accepted risk models. 2. Kill-chain mapping to show value of controls relative to attack

Risk Reduction *(continued)*	Reduced likelihood and impact of a data breach	Zero Trust capabilities provide the ability to encrypt files by default and limit access using discretionary access control lists. Even if files are exfiltrated they remain encrypted and cannot be opened. In addition contingent workers will be unable to access files once their contract ends, no matter what device the file resides on (e.g., BYOD).	1. Demonstrate risk reduction via application of enterprise accepted risk models (e.g., value at risk etc) 2. Kill-chain mapping to show value of controls relative to attack
Increased Business Agility	Increases the organization's ability to safely and efficiently execute mergers, acquisitions, and divestments	Zero Trust capabilities are used to ensure that the "blast radius" of merged and acquired companies is managed to limit damage. Zero Trust's foundational IAM capabilities make it simple to integrate acquired systems as well as to manage the divestment process.	1. Reduced cost of technology carve-in /out ($) 2. No negative impact to enterprise cyber risk posture as a result of mergers, acquisitions, or divestments (risk models)
	Ability to securely adopt SaaS cloud services	Zero Trust's foundational IAM capabilities (e.g., identity federation, access requests and re-certification) make it quick and easy to securely adopt new SaaS cloud applications using common patterns in response to business demands.	1. Reduced time to on-board new SaaS applications vs other types
User Experience	Improvement to end-user experience	Secure BYOD and BYOI removes friction for employees, partners and contingent workers, and provides the ability to work securely from any device. Modern security capabilities (e.g., biometrics, encryption by default) are largely transparent making them less intrusive for users on a day-to-day basis.	1. Improvement to IT satisfaction surveys

About the Authors

Charlie Hosner is a Managing Director in BCG's London office. He is an expert in cybersecurity strategy and transformation serving clients around the globe and across all market segments with a specific focus on heavy industry, infrastructure and energy. You may contact him at hosner.charlie@bcg.com.

Matt Dibble is an Associate Director in BCG's London office and is an expert on the topics of Identity and Access Management (IAM) and Zero Trust. He has helped numerous organizations define and implement IAM and Zero Trust strategies. You may contact him at dibble.matt@bcg.com.

Hasan Muchhala is a Project Leader in BCG's London office. He is passionate about cyber strategy & transformation, enterprise recovery, and zero trust to solve cutting-edge problems and push the boundaries of what's possible in the field. You may contact him at muchhala.hasan@bcg.com.

Sophie Cole is a Consultant in BCG's London office. She works with clients across industries to understand their strategy and business case for starting the Zero Trust journey. You may contact her at cole.sophie@bcg.com.

Lachlan George is an Associate Director in BCG's London office. He assists clients with complex cyber risk management, business-aligned cyber strategy development, post-incident operation and capability recovery and rebuild, and large-scale cyber transformation delivery. You may contact him at george.lachlan@bcg.com.

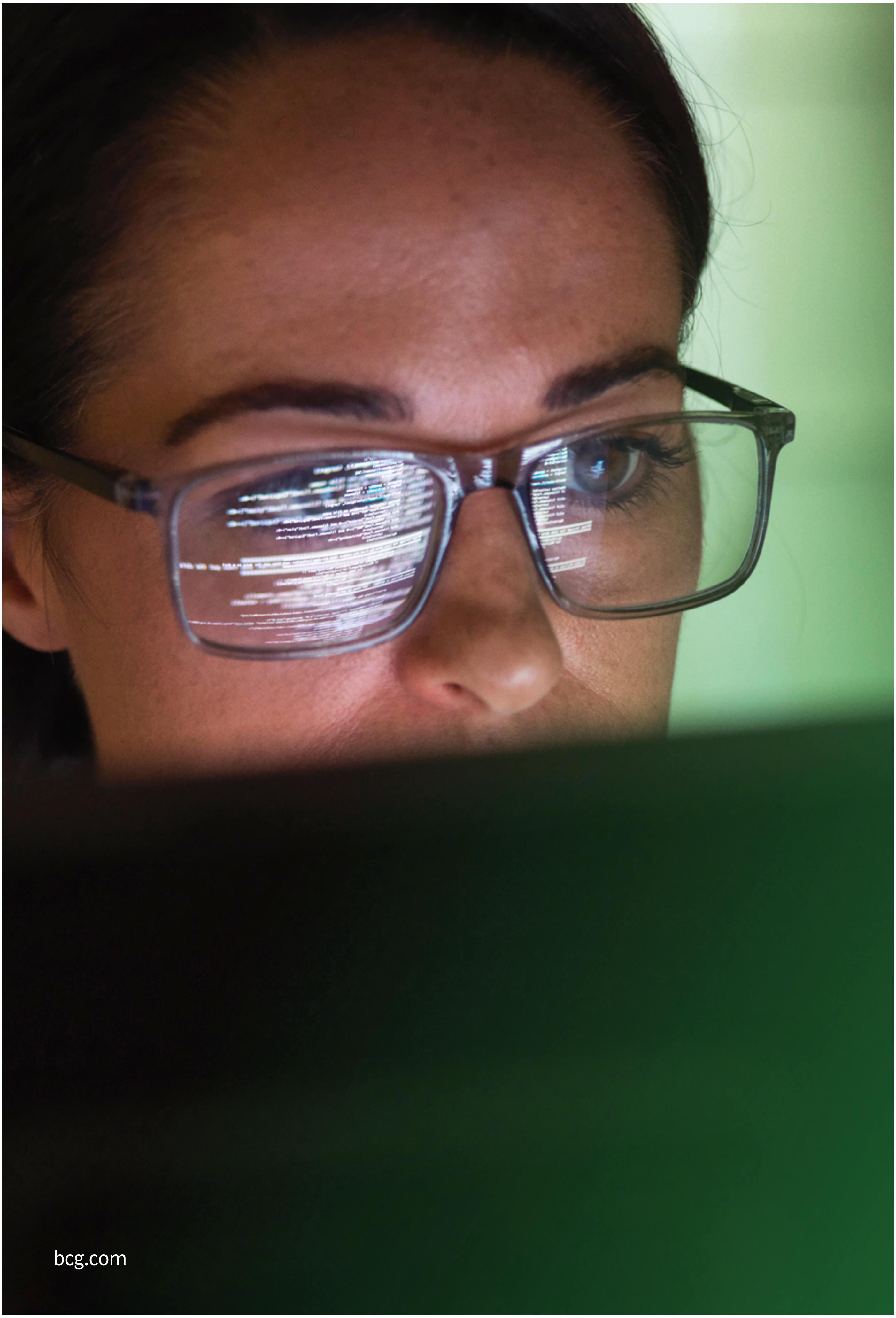
For Further Contact

If you would like to discuss this report, please contact the authors.

Boston Consulting Group partners with leaders in business and society to tackle their most important challenges and capture their greatest opportunities. BCG was the pioneer in business strategy when it was founded in 1963. Today, we work closely with clients to embrace a transformational approach aimed at benefiting all stakeholders—empowering organizations to grow, build sustainable competitive advantage, and drive positive societal impact.

Our diverse, global teams bring deep industry and functional expertise and a range of perspectives that question the status quo and spark change. BCG delivers solutions through leading-edge management consulting, technology and design, and corporate and digital ventures. We work in a uniquely collaborative model across the firm and throughout all levels of the client organization, fueled by the goal of helping our clients thrive and enabling them to make the world a better place.

For information or permission to reprint, please contact BCG at permissions@bcg.com. To find the latest BCG content and register to receive e-alerts on this topic or others, please visit bcg.com. Follow Boston Consulting Group on Facebook and Twitter.



bcg.com