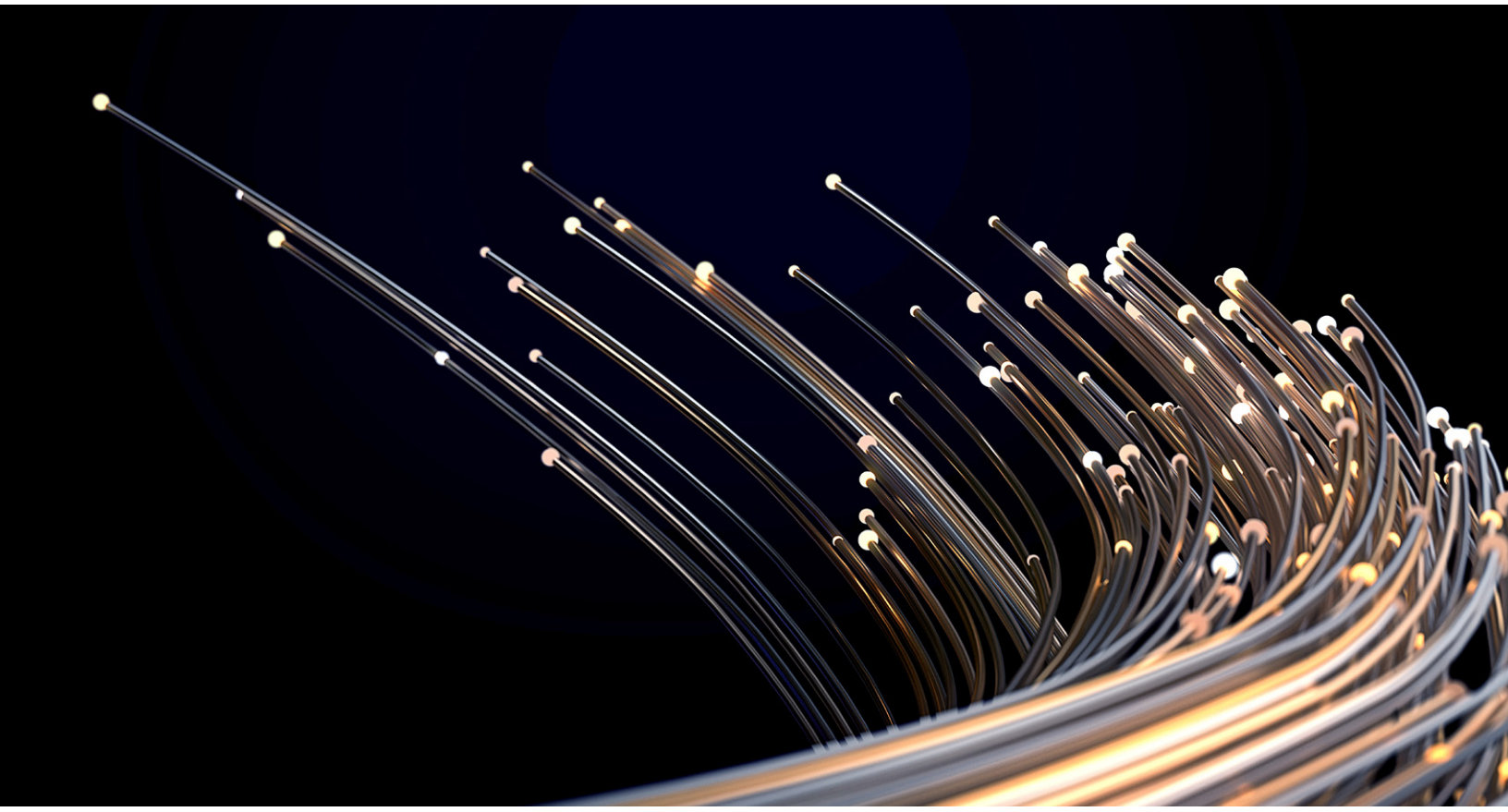
McKinsey & Company

Risk & Resilience Practice

New-business building: Six cybersecurity and digital beliefs that can create risk

In the race to build new businesses, decision makers often overlook risk management and cybersecurity. We have identified six misconceptions that executives often bring to the table.

This commentary is a collaborative effort by Justin Greis, Ari Libarikian, Patrick Rinski, Joy Smith, and Marc Sorel, representing views from McKinsey's Cybersecurity Practice and McKinsey Digital.



December 2023

If it's a great idea, just do it. In boardrooms around the world, entrepreneurial leaders understand that successful business building is about putting words into action. Nobody ever created a unicorn by having another meeting. Still, while business leaders are renowned for their ability to get things done, there is a flip side to the value creation gene. In the rush to market, it is easy to forget that the world's most successful companies have often withstood early threats to their viability. Indeed, our experience shows that business leaders who build resilience into their strategies are most likely to create winning propositions.

Business building is high on CEO agendas: in a recent McKinsey Global Survey, eight in ten CEOs cite new-business building as a top five priority, despite heightened economic volatility.[1] Business leaders are building 50 percent more new businesses per year than they did two to five years ago. And every dollar of revenue from new businesses generates almost twice the enterprise value of every dollar of core business revenues.

Still, new businesses also create unseen risks. For instance, in digital-business building, one commonly overlooked area is cybersecurity—the protection of information systems and networks from attacks by malicious actors. At the current rate of growth, it is estimated that cybercrime costs will reach about $10.5 trillion annually by 2025—a 300 percent increase from 2015 levels.[2] Still, decision makers often fall victim to "normalcy bias," or the tendency to underestimate the likelihood or impact of a potential hazard based on the belief that things will continue as they did in the past. In other words, "It won't happen to me."

Actually, it might. As testified by Julia Houston, chief strategy and marketing officer at Equifax, victim of a 2017 data breach: "Every executive needs to be a student of crisis."[3] Moreover, given the importance establishing trust when starting a new venture, there is no better time to be a student than early on.

If a new business integrates a discipline of risk management into its strategy and planning from the start, cybersecurity will almost inevitably be identified as a potentially catastrophic threat to its operations. When this does not happen, it is often testament to the blind excitement and energy required to set up the business and

Cybersecurity can be a product's greatest feature, creating trust and confidence in the minds of consumers that can extend a company's competitive lead in the market.

[1] The online survey was in the field from July 19 to September 1, 2022, and garnered responses from 1,007 participants representing the full range of regions, industries, company sizes, functional specialties, and tenures. To adjust for differences in response rates, the data are weighted by the contribution of each respondent's nation to global GDP.
[2] Steve Morgan, "2022 Cybersecurity Almanac: 100 facts, figures, predictions, and statistics," *Cybercrime Magazine*, January 19, 2022.
[3] "Managing a cyber risk event: 'Be a student of crisis,'" McKinsey, March 3, 2023.

McKinsey commentary — Vinnie Liu, CEO, Bishop Fox

"In cybersecurity, a common misconception prevails: many assume that attackers exclusively target large enterprises. The reality, however, is quite the opposite. Attackers have evolved to strategically focus on the weakest links within a business's ecosystem, spanning supply chains, vendors, subsidiaries, and newly incubated ventures. They exploit these smaller, less protected targets because the risk–reward balance heavily favors them. Furthermore, these smaller entities often hold trusted relationships with larger organizations, providing exploitable entry points.

Another prevalent misconception is that attackers are only interested in customer records or personal data. The underground economy has evolved considerably, making any type of data valuable. Credit card details and personally identifiable information represent just a fraction of the broader spectrum. The black market value chain's industrialization gives value to a diversity of data types, while also creating opportunities in non-data-related theft (that is, ransomware). This shift is evident as nearly all companies, regardless of industry, now safeguard not only their assets but also their critical operational capabilities—as demonstrated by recent incidents involving critical infrastructure like oil pipelines, ocean shipping, and meat processors.

For most organizations, the failure to prioritize security from the outset is akin to hanging drywall in a building before installing the plumbing. An emerging trend in enterprises is for buyers to require that suppliers and vendors exhibit a suitable level of cybersecurity diligence commensurate with their stage and size. While not every security measure is mandatory, a lack of sufficient safeguards is no longer acceptable."

attract new customers. But in the race to success, new companies (NewCos) are missing an opportunity to lay the groundwork for future rapid expansion.

In fact, when considered up front and built into products by design, cybersecurity can be a product's greatest feature, creating trust and confidence in the minds of consumers that can extend a company's competitive lead in the market. In a recent survey of over 3,000 consumers,[4] 53 percent made purchases and/or used digital services from a company only after making sure it had a reputation for being trustworthy with their data, and 40 percent stopped using digital services if they learned the company was not protecting customer data. In other words, trust and security matter when it comes to buying decisions in the minds of consumers.

Some business builders are not convinced that risk management and cybersecurity should be early priorities. However, those attitudes increasingly fly in the face of common practice: 95 percent of board committees, for example, discuss cyber and tech risks four times or more a year.[5] A common challenge for smaller companies is that leaders understand the importance of risk and cyber oversight but are uncertain about how to build and manage the required capabilities. In this article, we share six beliefs that reflect these perspectives, examine their implications in practice, and show how some forward-looking companies have tackled the challenge.

Six common beliefs that create unnecessary risks

Business leaders and entrepreneurs often bring a positive attitude that can drive the new venture forward, inspire others, and attract customer attention. However, these powerful creative instincts often lead to shortcuts in strategic thinking and six common misconceptions:

1. *Mistaken belief:* Because we are testing a new concept, we don't need "extras" like

[4] McKinsey Global Survey on Digital Trust, May 2022.
[5] BPI and McKinsey Cybersecurity and Board Governance Survey, August 2020.

McKinsey commentary — Alberto Yépez, cofounder and managing director, Forgepoint Capital

"As our lives become increasingly digital, we work, learn, collaborate, and transact via new applications often running on our mobile phones and other personal computing devices.

The developers of these applications are often most concerned with the [digital] customer experience, ease of deployment, and usability—they do not hesitate to spend the majority of their budgets on design studios and usability testing. When it comes to cybersecurity and privacy testing, it is often an afterthought and leaves the application security and privacy testing budgets to a minimum. The testing is often left to be performed by junior resources under pressure to meet aggressive deployment deadlines.

These dynamics often create a business risk for the program's or new venture's overall success that could be mitigated by good cybersecurity hygiene. Cybersecurity is a business enabler, foundational to innovation and growth.

As the saying goes, an ounce of prevention could be worth a pound of cure."

cybersecurity or risk management. We definitely don't need to be concerned about data privacy as we don't have any customers yet.

The reality: If an executive team has decided to form a NewCo around a business concept, then the concept is probably mature enough to warrant investment in resources including talent, tech, and processes. These are valuable assets that are susceptible to cyberattacks.

2. *Mistaken belief:* If we establish processes and/or cybersecurity measures, our launch will be delayed, and we will lose our edge. And other start-ups don't do cybersecurity, so why should we?

   The reality: Adding risk management and cybersecurity will consume time but not an unmanageable amount of time. Indeed, the effort required at the beginning will prevent rework in the end. Conversely, NewCos that rush to launch without structured risk thinking may face more significant problems—such as regulatory fines, data breaches, or lawsuits—down the road.

3. *Mistaken belief:* Spending on risk management and cybersecurity is not a guarantee of protection, so it is not worth assigning resources to these areas.

   The reality: There is often a mismatch in cyber spending and cyber maturity among large corporations, but at launch there is a foundational level of risk management and cybersecurity that every company needs. The basics are not difficult to implement, but they do require experience and expertise. And the longer they go unaddressed within the product development life cycle, the harder and more expensive it becomes to incorporate them into the product.

4. *Mistaken belief:* Our product guys have it under control. They understand our proposition and how bad actors might threaten it. Our chief technology officer says he knows about cyber controls, so I am comfortable.

   The reality: Product team leaders and team members have varying levels of knowledge, for example, in relation to the latest data encryption standards or security operations center monitoring solutions. Cybersecurity is a vast discipline that requires specialized knowledge; even the most experienced professionals seek

McKinsey commentary — William Lin, CEO and cofounder, AKA Identity

"After investing in security start-ups for a decade, I've discussed the risk of 'the cobbler's children have no shoes' at multiple levels, including the board level, CEO level, and customer level.

The reality is that, when stepping back from the security lens, there are numerous risks that can threaten a start-up's ability to conduct business. The main short-term focus revolves around capital, runway, and execution.

In the hierarchy of needs, capital, whether through revenue or investors, is indeed the most fundamental requirement for a company. However, it's not the sole requirement for success.

The issue that many industries have faced before the maturation of various expertise areas like sales, marketing, engineering, product, legal, and finance, is not knowing what they don't know. Each of these skill sets can one day become fundamental pillars of an organization and serve as business enablers. Cybersecurity is the most recent expertise undergoing transformation to become an enabler.

This presents start-ups with a significant opportunity to be mindful and to incorporate the value of cybersecurity early in their journey. They can establish a foundation for these skills to grow organically within the organization, to compound through investment, and ultimately become business enablers."

opinions and consultations from others when innovating new products and services.

5. *Mistaken belief:* We are small and insignificant, but our parent is a behemoth. I am sure it is on top of our risk management and cybersecurity.

   The reality: Frequently, parent company security teams do not have the capacity to secure the NewCo. This may be because of tech stack mismatches (for example, the parent has not yet moved to the cloud). The parent company's security resources are usually already stretched, which means it cannot pay a lot of attention to the NewCo when decisions need to be made.

6. *Mistaken belief:* We already have a tool, which we paid a lot for, so I am pretty sure that we are at least covered for the main risks.

   The reality: A tool alone is never sufficient. A combination of process, people, and technology is required. Also, you can buy the best tool on the market, but will its utility reflect your needs? After investing, many NewCos don't have the capabilities to leverage more than 80 percent of the solution.

Strategies for effective NewCo cybersecurity and risk management

Cyber resilience is critical to consider and build into your new business. However, the way and the speed at which you do so may differ from cyber in the core business. With that in mind, a strategic approach and structured rollout can go a long way toward avoiding potential pitfalls. The key for decision makers will be to incorporate risk-based thinking into the wider business plan, and then to execute diligently to ensure all the bases are covered. The following are key principles that can help illuminate the way forward:

A good rule of thumb is that if a concept merits investment, it is worth an executive's time to consider and mitigate risks. In addition, in a fast-growing business, it is vital to engage early. That means putting in place a framework to help identify major risks and mitigation measures. Some of these will apply to almost every business, while others will be situation dependent. But all should be assessed with a view to future growth and the user experience.

Forward-looking NewCos see cybersecurity as a core element of business architecture. Where

they don't have the internal skills to put it in place, they recruit external experts to provide input, accelerate delivery, and coordinate controls. Decision makers find the most efficient way to address both product/software and enterprise security is to ensure that cyber experts work closely with the business.

The role of the parent will vary, depending on leadership engagement, crossover potential, and the priorities of the new company. Ideally, a nuanced collaborative approach is required, which means working with the parent company to meet (and typically exceed) established risk and security standards but leveraging the parent company resources only where it makes sense.

When it comes to implementation, a key principle is to ensure that risk management and cybersecurity are embedded from product ideation to final delivery. For tech-based companies, it makes sense to adopt the principles of DevSecOps (development, security, and operations), integrating security testing at every stage of the software development process. Tools should be tailored to specific operational focus areas, ensuring key areas of investment are property protected.

A business that has reached the stage of launching a minimum viable product has assets, investments, and trust-building goals that are worth protecting. In that context, enterprise risk management and cybersecurity are no longer optional. Even in a resource-constrained environment, investment in risk management is likely to drive operational resilience and provide the assurance that will foster trust in the brand as the business grows.

Justin Greis is a partner in McKinsey's Chicago office, **Ari Libarikian** is a senior partner in the New York office, **Patrick Rinski** is a partner in the São Paulo office, **Joy Smith** is an alumna of the Philadelphia office, and **Marc Sorel** is a partner in the Boston office.

Designed by McKinsey Global Publishing