Leading in the New Reality

BCG

To BCG’s network around the world,

I recently had a fascinating conversation with a group of BCG’s cybersecurity experts, and I wanted to share with you some of the perspectives I came away with.

Cybersecurity is in the 21st century what workplace safety was in the 20th. At one time, accidents in mines and factories were common, but mindset shifts in how we address physical workplace risks have made how we keep people safe at the core of most companies’ agendas. “Safety first” has gone from rhetoric to reality in most companies.

Of course, we tend to talk about safety only when we notice the lack of it.

The invisibility of a strong cybersecurity program is what makes it so psychologically challenging to prioritize and continue to invest in. But as we keep hearing in the news, things do go wrong. Cyber attackers can target companies of any size, essential services, and hospitals—even entire countries. Potential risks range from annoying inconveniences to large data breaches to huge financial costs to loss of life.

Here are three basic principles that business leaders should be focusing on right now to ensure a smooth, safe, and secure tomorrow:

1. **Embed cybersecurity in design.** Workplace safety, again, is a good analogy. We don’t build a factory and then go back in and reconfigure it to protect workers from fire and other hazards. Safety is now part of factory design from the blueprint stage. By including cybersecurity at the beginning of each wave of digital transformation—rather than attempting to tack it on at the end—you’ll save time and costs and be better prepared to cope with cyber challenges down the road.

   We worked with one company that developed a software system, and then tested it for cybersecurity. This added 20% in rework costs and a 20% delay in production. With the design of their next system, the developers were trained in secure coding techniques and shown how to use cybersecurity testing in each sprint of agile development. They completed the system 15% faster, generating revenue sooner, and at a 15% lower cost—profits that more than paid for the training and testing.

2. **Champion cybersecurity from the top.** Because this is still a relatively new top priority, CEOs need to take the lead in communicating its importance, just as they would signal their strong support of any other fundamental change or the importance of safety. The CEO's role here is crucial, both in counteracting "optimism bias"—a sense that since things haven't gone wrong so far, you're in the clear—and in stressing that there is no cybersecurity silver bullet or shortcut. It's a process that evolves and will always take work and dedication. Make cybersecurity a part of company culture, keeping people aware and accountable. This is a priority that goes well beyond the technology team; human vulnerabilities across the organization carry some of the greatest risks.

3. **Be ready with a robust and tested response plan.** Cyber attacks happen at the speed of light and can have an impact on the entire company—causing high stress and leaving little time to think. Prepare your senior executives and critical managers through tabletop exercises with cyber attack simulations until they know their roles and can act quickly. Test your plans against a range of cyber attack scenarios, improve the plans, and then test them again.

   Although big cyber hits have made headlines lately, there are so many that we don't hear about at all—or the news is short-lived and the costs are low—because the targets had incident response and business continuity plans in place and the employees were practiced in implementing those plans efficiently and effectively.

Cyber attacks will only get more challenging. Some are becoming simpler to attempt, because of the anonymity of bitcoin payments and accessibility of cheap ransomware kits. Others are perpetrated by increasingly sophisticated actors with tremendous resources.

I remember visiting an industrial CEO a few years ago for a private meeting and asking him about his business. He started by saying, "We have gone nearly 500 days without a serious workplace injury." In today's world, we need to be as disciplined about cybersecurity as we've become about workplace safety, seeking to protect our people and our businesses in all contexts.

See below for related insights on this topic. Looking forward to connecting again next week.

Rich

Rich Lesser
Chief Executive Officer

Better Cybersecurity Starts with Honesty and Accountability

In this practical talk, cybersecurity expert Nadya Bartol brings this crucial topic out into the open, lifting the shame around tech mistakes and offering creative ways to celebrate and reward good cybersecurity habits at work and beyond.

CLICK TO READ MORE

Cyberattacks Are Inevitable. Is Your Company Prepared?

The first time you test your plan shouldn't be during a crisis.

How Health Care Providers Can Thwart Cyber Attacks

Cyber attacks pose a major threat to health care providers and can do severe damage if left unchecked. Fortunately, there are a few key actions providers can take to ensure security for the long term.