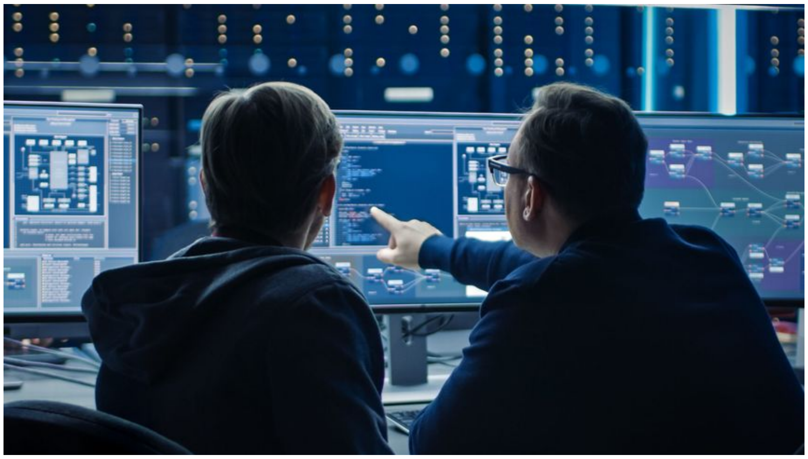
THE EXPERTS | LEADERSHIP

Why Small Cybersecurity Decisions Can Expose Companies to Cyberattacks

Too often, corporate leaders fail to consider the potential consequences of minor decisions. They pay a high price.



Unless organizations fix the internal decision-making that allowed a cyberattack to occur, they could be vulnerable to further breaches, researchers say.

PHOTO: GETTY IMAGES/ISTOCKPHOTO

By Stuart Madnick

Follow

March 19, 2022 11:00 am ET

Stuart Madnick is the John Norris Maguire Professor of Information Technologies, Emeritus, at the MIT Sloan School of Management and the founding director of the Cybersecurity at MIT Sloan (CAMS) research consortium.

In the aftermath of a major cyberattack, we usually hear a lot about "what" happened, some about "how" it happened (say, hackers exploited a system vulnerability) but almost nothing about "why" it happened (that is, what gave rise to the vulnerability in the first place).

That reveals a huge and costly blind spot: Unless organizations study the "why," the circumstances that made the cyberattack possible won't be addressed.

Consider this simple example. Your house is robbed and all your possessions stolen. That is the “what.” The “how” is that you accidentally left the front door open. In many cases, that is the end of the story. Leaving the door open was an unfortunate accident, one that anyone might make.

THE EXPERTS

The Experts are a group of industry and academic thought leaders who weigh in on topics covered in the The Journal Report.

WSJ

But digging deeper, we find you left the door open because you had overslept and were rushing to work. You overslept because your alarm clock didn’t go off. You knew the clock was faulty because you had overslept before, and your office mates had urged you to replace it. But instead of buying a new clock, you decided to spend the money on going to the movies. I call this “semiconscious decision making,” because a decision was made—to not buy a new clock—but the possible consequences of that decision—the loss of all your possessions—wasn’t considered. In essence, a decision was made that created the circumstances, in this case, for the theft.

Every major cyberattack researchers at MIT examined involved such semiconscious decision making, but it is rarely studied and often not corrected.

Like the example above, many breaches are reported as if they are single, simple accidents—say, criminals exploited a website vulnerability or an unpatched piece of software, or gained access to critical files because of a cloud setting that was misconfigured. If the identified problem is quickly fixed, one might assume there is nothing more to worry about. Yet the decision-making process that gave rise to that vulnerability (and usually many others) remains in place.

In reality, most successful cyberattacks are only possible if there are multiple flaws in a company’s defenses. In fact, one of the most popular descriptions of a typical cyberattack, developed by the nonprofit Mitre Corp., identifies up to 14 steps that attackers need to take to steal information. These are areas where a breach could be stopped or mitigated.

Yet we found that leaders often miss the connection between what might seem to be a minor decision related to cybersecurity and the potential consequences of that decision. They decide to cut corners on certain cybersecurity measures—say, they neglect to patch a piece of software or they let security certificates expire—without consciously and realistically weighing the benefits of doing so against the increased risk of a breach that could cost the organization hundreds of millions of dollars or more. In one case, we identified at least 18 instances of such semiconscious decision making, from middle management up to the board, that either contributed to the data breach we were examining, or that would have made other such data breaches possible.

Another common theme in many major cyberattacks is that directors essentially allowed management to take unlimited security risks in pursuit of an aggressive growth and increased profits strategy. It isn't surprising, considering boards usually consist of more directors with leadership expertise than cybersecurity expertise. While these directors may be familiar with assessing risks, such as deciding where to a build a new plant, evaluating risks associated with cybersecurity decisions aren't usually part of their past practices.

The solution to semiconscious decision making is straightforward: Every decision regarding cybersecurity must weigh the benefits of not doing something (cost savings or the faster growth) against the increased risk to the organization. In some cases, management may decide the risk is worth it. But today, too many companies don't perform this calculation at all.

To be sure, it may not be possible to recognize all risks in advance. This factor is often used to try to excuse the semiconscious decision making around cybersecurity. But, like office mates complaining about the faulty alarm clock and the late arrival at work, in almost every case that we studied there were "red flags" (often many red flags) that management chose to ignore—with disastrous consequences.

Write to Dr. Madnick at reports@wsj.com