Cybersecurity starts at the top

Every time a major corporate cybersecurity breach occurs, the response looks pretty much the same: Cry “Havoc!” and call in the cyber first responders to close the breach. But by the time an executive or two stands before a few government committees, proffering some explanation and pledging to beef up security protocols, people—including the hackers—have largely moved on. And with each breach, the cycle accelerates: People either dismiss the threat—it probably won’t happen to them—or accept it as an unavoidable pitfall of modern life.

The truth is that the threat posed by cybersecurity breaches is both acute and avoidable. The key to mitigating it is to understand that cybersecurity isn’t simply a technology issue; it is also an urgent strategic issue that should be at the top of the agenda for every board and management team. After all, from Yahoo! to Equifax, data breaches have often been rooted in internal forces of human error, carelessness, or even maliciousness.

Already, the scale and speed of attacks is massive. It has now emerged that the 2013 Yahoo! data breach affected all three billion accounts. In May, the WannaCry ransomworm attack affected dozens of the UK’s National Health Service trusts, and spread globally at lightning speed.

The recently revealed Equifax data breach—which occurred during two months when the company had a patch to a known security vulnerability, but hadn’t applied it—gave the hackers access to 145.5 million consumers’ personal and sensitive data. According to testimony provided by now-former Equifax chief executive officer Richard F. Smith to the US Congress, the breach reflected the negligence of one individual in the information technology (IT) department.

The risks are only growing. The UK’s National Cyber Security Centre, founded last year, has already responded to nearly 600 significant incidents. The department’s director recently predicted that our first “category one cyber-incident” would occur in the next few years.

One problem is that many organizations simply don’t have cybersecurity on their radar. They believe they are too small to be a target, or that such breaches are limited to the tech and finance sectors. But, just recently, the US fast-food chain Sonic —not exactly a tech giant—revealed that a malware attack on some of its drive-in outlets may have allowed hackers to secure customers’ credit card information.

The fact is that many types of companies use, if not depend on, technology. And they collect many types of data, about everything from customers and employees to distribution systems and transactions. Consumers often don’t comprehend the extent of companies’ data collection, failing to understand even the basics of the “cookies” being used when they surf the web. According to a March 2017 report by the Pew Research Centre, many Americans, for example, “are unclear about some key cybersecurity topics, terms, and concepts”.

Of course, consumers must be informed and vigilant about their own data. But even those who are, find that if they want to engage fully in modern life, they have little choice but to hand over personal data to organizations in both the private and public sectors, from utility and finance companies to hospitals and tax authorities.

With automation, this trend will only accelerate, with people counting on technology to do everything from ordering groceries to turning on the lights and even locking the doors. The power this gives to the likes of Google and Amazon, not to mention an ever-growing array of start-ups, is obvious. What is not obvious is that consumers can rely on companies’ knowledge and duty of care to protect the information they collect.

No company can afford a laissez-faire attitude about cybersecurity. Yet even tech companies took some time to recognize the extent of their technical responsibilities, including the need for a C-level executive to manage their technology needs. Not long ago, such companies often maintained a “helpdesk” mindset: Just make sure people could use the product and have someone to call if something went wrong.

But, with data breaches proliferating, often with business-critical consequences, there is no excuse for such inertia. Such breaches can cripple companies both operationally and financially, owing to the direct theft of funds or intellectual property and the cost of plugging the security hole or paying punitive fines. They can also diminish a company’s reputation and credibility among investors, business partners, and communities, even in cases when the breach is minor and doesn’t compromise sensitive information.

While board members do not all have to be technology experts, they do need to keep up with the state of their company’s technology, including how well secured it is. A board’s risk committee can conduct in-depth reviews. But regular status updates to the full board, like those for other crucial issues affecting the business, are also needed.

In today’s world, no organization—public or private, commercial or non-profit—has an excuse not to be supremely vigilant and proactive about securing their data and systems. It is not enough to meet legal requirements, which don’t keep up with technological change. Instead, those requirements should be viewed as a starting point for a much more robust, closely monitored, and effectively adapted system that truly protects the data on which our societies and economies increasingly depend.

Data breaches are not a fact of modern life. They are an artefact of modern indifference.

Lucy P. Marcus is chief executive officer of Marcus Venture Consulting.

END