Investing in IT Infrastructure and Cybersecurity Means Investing in People

SPONSORED BY

RSM

THE EXPERTS

Lou Brothers
IT Due Diligence Leader
RSM US LLP

Kevin Carpenter
Cybersecurity Due Diligence Leader
RSM US LLP

Business leaders who are not knee-deep in IT may view the function as so many blinking servers, lines of code and expensive line-items with odd names. But, increasingly, IT and cybersecurity are being viewed as valuable tools for protecting and adding value to a portfolio company — an investment, not a spend, and a function that needs to be state-of-the-art when it comes time to exit.

It is easy to forget an important ingredient for success in this area: people.

Whether this means finding a business-minded CIO, training staff to avoid cyberattacks or carefully approaching change management when a new system is installed, the investment in people is necessary if IT and cybersecurity are to be value-adding features of your business.

This viewpoint must come from the CEO as well as from the leadership of the IT department.

"KEEP THE LIGHTS ON"

According to Lou Brothers, IT Due Diligence leader of RSM, the Chief Information Officer should embrace the fact that "they're one of the few people who has a view across the entire business end-to-end."

Yet it is difficult to find leaders who have both the technical expertise and a business mindset. Brothers says that most CIOs come from a programming or infrastructure business background, and may not be as process-oriented as they should be to move the revenue needle. "More often than not, we're finding people who know 60 or 70 percent of the business," he says. "They don't feel the freedom to be unleashed. They say, 'My job is to keep costs down.'"

There has been much excitement lately around tapping into data science as an additional source of revenue; in other words, monetizing the data that a company captures in the course of its regular business. According to Brothers, data monetization is indeed a big opportunity, although harder to realize than many business leaders assume. Instead, Brothers says a bigger value that the IT team can bring to a company is optionality.

"IT's responsibility is to keep those options a little bit flexible so as the business needs suddenly change, they're right there," says Brothers. "They can say, 'You know what? We were thinking about that already, and we're prepared.'"

Brothers gives the example of the effect that COVID-19 has had on businesses of all stripes, notably retail businesses. Suddenly, many of these businesses have needed to double down on direct-to-consumer in order to survive. It is very apparent which companies had the systems in place that enabled them to quickly pivot, and which did not, says Brothers.

↓ CONTINUES ON NEXT PAGE

THE PHANTOM MENACE

A proper cybersecurity investment also largely comes down to an investment in people. That said, business leaders sometimes find it hard to appreciate a substantial investment in cybersecurity because, to them, it represents spending money on something that hasn't happened yet and may not happen, says Kevin Carpenter, Cybersecurity due diligence leader at RSM.

"There isn't a good way to gain visibility into what will happen if I don't do something," says Carpenter. "It's kind of a negative test. But there could be fines for privacy regulation breaches, PR disasters, lawyers getting involved. We've been having conversations with clients saying, 'If you're not willing to do these things, you put yourself at high risk, and that could result in a meaningful impact to your bottom line.'"

According to Carpenter, one of the most damaging forms of cyber crime currently is wire fraud, and this is often accomplished via social engineering, meaning a criminal tricking an employee into fulfilling an unauthorized payment or transaction. ACH scams are where the line blurs between cyber-hacking and old-fashioned swindling. Some of the best ways to defend against social engineering scams is through staff training and the enforcement of strict protocols around the finance function. And that's not a job for software only.

CHANGE MANAGEMENT

Brothers points out that it would be counterproductive to make a major investment in IT/Cybersecurity upgrades without also understanding how the business wants to function. By working with the people who will need to perform new security-related tasks adoption increases.

Brothers stresses that it is not enough to explain what the IT change is going to be — you need to get employees excited about why the change is taking place. He gives the example of a roll-out of a two-factor authentication system, requiring employees to check a code on their phones and use it to access the company system. Communicated the wrong way, it would give employees the idea that you are making their lives harder. Instead, describe how the new system benefits them.

"The benefit is that hackers won't be able to get into our systems," says Brothers. "Which means our system will stay up more, which means your job is more secure. And they'll say 'Okay, I'll take job security, typing in a six-digit code, thank you very much.'"

At the end of the day, and at the end of the life-cycle of a private equity hold period, an investment in IT and the people required to make it successful is table stakes for the next potential owner of the business, says Carpenter: "It's a bit like a home inspection. You want to make sure that you're prepared, because you know that buyers are going to come in and take a look." ■

GP VOICE

'Ever-Increasing Issue'

"Cybersecurity has obviously been an ever-increasing issue, not only in terms of businesses that can serve as a target, but also in the type of diligence that we do. What has been fascinating is that five to seven years ago, we thought very differently about compliance and technical diligence, about bringing in third parties to do cybersecurity audits on our own portfolio companies, or prospective companies. Then, on the other side, the opportunity in security is very interesting as well. You have just a whole host of businesses in that security space that are sponsor-owned, or that are public, that have grown and become very successful and very needed."

Rich Lawson
Chairman & CEO
HGGC