Expert Discussion

Beware *the* Knock-On Effects of IT Cost-Cutting

SPONSORED BY RSM

To many CEOs, a company's IT function can appear to be "expensive," and therefore get a cost-cutting target placed on it. While there are smart ways to reduce the cost of IT and cybersecurity while maintaining quality, corporate leaders should be aware that cost-reduction without proper planning can have second-order, deleterious effects on the operations and security of the business.

"Historically, security has been seen as a kind of overhead," says Kevin Carpenter, cybersecurity due diligence leader at RSM. "When times get a little tough or budgets get a little tight, there tends to be this misconception that IT and cyber are areas where you should be able to easily cut budgets."

Making changes to IT and cybersecurity the wrong way typically begin with the misconception that the budget for this area constitutes spending instead of investing. Carpenter makes the point that IT is not a static technology, but one that is constantly evolving. Making cuts down to the "bare minimum" may not only weaken the digital effectiveness and security of the business today, but may require an outsized budget in the future once it becomes clear that the company needs to catch up to best-in-class systems.

"The hackers and the attackers out there are not taking breaks during your budget cuts and constraints," says Carpenter.

One line-item within IT and cybersecurity that often gets reduced or cut entirely in a budget reduction is penetration testing — the hiring of "ethical hackers" to test systems, look for holes and make recommendations for how to improve security. Too many organizations view regular "pen testing" as a nice-to-have seal of approval, instead of a critical exercise for avoiding disaster. Companies that cut pen testing "really do fall behind," says Carpenter.

Carpenter adds that IT and cybersecurity budgets shouldn't necessarily be off-limits, but there should be a thoughtful approach to cost-cutting that takes into account what industry the business is in and what data it is trying to protect. And, to be sure, simply looking to cut the biggest line-items is not a thoughtful approach.

"If you do scale back, we advise clients to take a different view," says Carpenter. "We ask, can you use a different tool that doesn't have all of the fancy bells and whistles but still gets to the heart of what you're trying to protect? Do you understand where your largest threats are coming from? Does it make sense to put more emphasis on social engineering exercises, or should there be more security and monitoring around ensuring endpoints aren't getting infiltrated with ransomware?"

THE EXPERTS

Lou Brothers
IT Due Diligence Leader
RSM US LLP

Kevin Carpenter
Cybersecurity Due Diligence Leader
RSM US LLP

↓ CONTINUES ON NEXT PAGE

© 2020 Privcap LLC

OFFSHORING AND THE CLOUD

Likewise, Lou Brothers, IT Due Diligence leader at RSM, notes that cost-cutting per se can be a valuable exercise, but only with the proper "homework" done up front. He brings up the examples of cost cutting via offshoring, and by changing cloud computing contracts.

"Someone might say, 'Okay, my offshoring ratio is wrong. Let's offshore additional people,'" says Brothers. "But is your organization even shaped properly? Do you have the right headcount? Are they doing the right things? Have you done all your homework first to really optimize and then make decisions about right-sizing? Or have you just gone right to the right sizing?"

Another cost-cutting idea for many companies has been to move data from physical infrastructure to a cloud-based service. On the back of an envelope, this data migration might promise cost savings of 70 percent or more. But that is after the migration has taken place. Much more analysis needs to be done around the costs and potential limitations of making that move to the cloud.

Brothers lists a litany of barriers: the not-small matter of people who are employed overseeing the physical infrastructure, agreements with customers who specify that their information not be stored in the cloud, the contract you may have with a local data center. "Those are the knock-on effects that you've got to do more homework around," says Brothers. "We can all create a spreadsheet and say, 'Here's cloud versus infrastructure. If I'm spending $1 million a year, I could spend $300,000.' Yes. But, how much is it going to cost you to get there?"

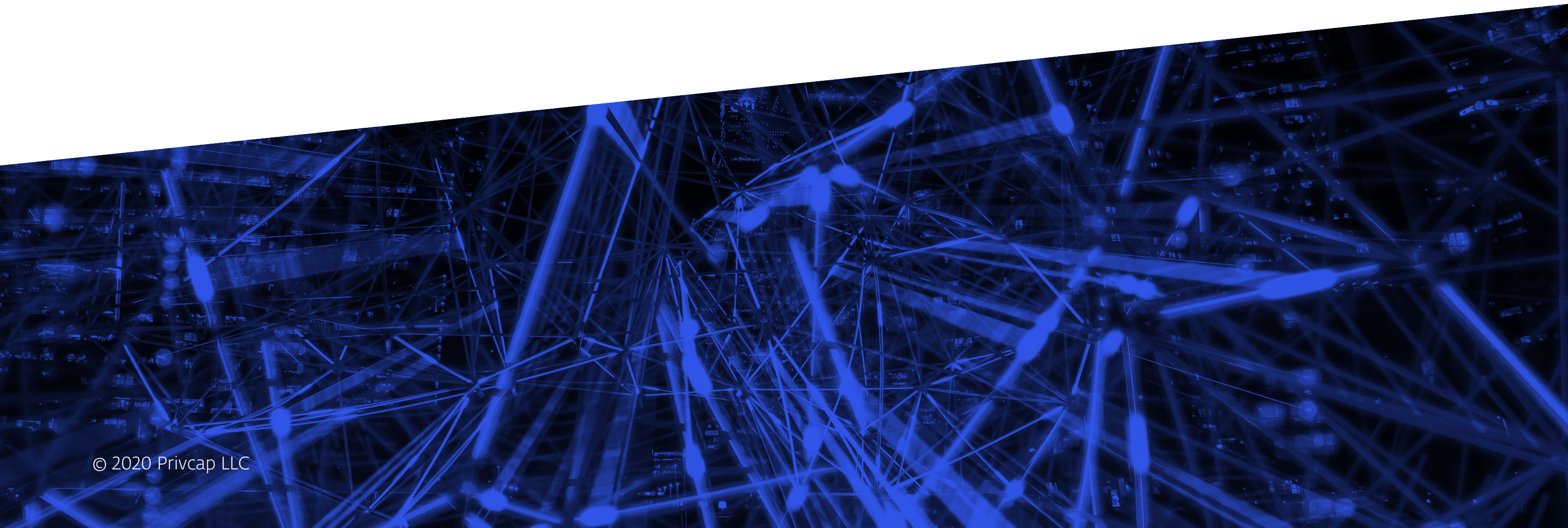
With the amount of business activity taking place online growing exponentially, corporate leaders will need to view IT and cybersecurity less as utilities in support of the brand and more as the brand itself, with the requisite investment to match. ■

GP VOICE

'Critically Important'

"As a technology investor, as a matter of course through standard diligence, we perform a technology assessment for every new portfolio company. Within that, we consider cyber security to be critically important. Whether it's a DDoS attack, phishing or anything else, we want to know what the company's vulnerability is. Also important is whether they have procedures in place to deal with an attack if one occurs."

Brian Rich
Managing Partner
Catalyst Investors



© 2020 Privcap LLC