It's the type of thought that sits in the back of your mind. It rides around with you all day as you go about your routine. When you're getting ready for bed, it bubbles to the surface again. In an age when everything is connected, is everything a target? Is your company vulnerable to security breaches?

Risk Mitigation: Hindsight Is 20-20

by Sam Noyd and Yosef Beck

It is vital to carve out time to address system security issues in advance, before you have the pressure of a full-blown data breach.

You're trying to keep your company off the front page of the newspaper at a time when more and more companies are suffering incursions into their systems and their data. How can you keep your company's systems—and the data or devices employees and customers have entrusted to you—safe and secure in an age when everything is connected and easily accessible?

Let's take a step back. How did we end up here? Several years back, many companies turned to mainframes and dumb terminals to help power and drive their businesses. Times changed, and companies shifted to a more distributed model. The increasing power and decreasing size of PCs helped to fuel this transition.

But times are changing again. With the rise of cloud computing, it has become attractive for companies to shift processing power, data, or both to offsite locations on either private- or public-cloud environments.

Shifting from a consolidated model to a more distributed one expands the system and introduces additional complexity. With additional complexity comes additional risk—more chances for things to break down. In many cases, this is perfectly acceptable, but it's important to realize this trade-off along the way and try to identify failure points in advance. By understanding the trade-off, we can look for opportunities to simplify along the way and limit the complexity we introduce.

Many companies are exploring whether a third party should power their move to the cloud. Let's walk through that scenario by way of an analogy: Consider a bank. While moving your savings from under your mattress to a bank account reduces your risk, it does not eliminate that

risk. As other people move their savings from under their mattresses to the bank, the bank is responsible for more assets. As assets increase, the bank becomes more and more attractive as a target for those wishing to do harm. Again, in many cases this trade-off is perfectly acceptable.

Now, let's see how this analogy would apply to cloud computing. If we view your data or your business-critical information as money, we can see the connection to our bank example. It's important to make sure you are putting your trust (and your assets) with someone who is reputable and prepared to manage the increased risk associated with having so many assets under their care.

Meanwhile, don't overlook the transportation of assets. If we revisit our banking example, the assets started with your mattress and ended at the bank, but we can't neglect the transportation. In this case, it might have involved armored trucks. There is a reason they are armored.

The same applies to your data and business-critical systems. You may protect your servers with all the security in the world and top-notch access control to the physical locations. But if you are sending unencrypted personally identifiable information over the open internet, you are leaving yourself vulnerable.

Security and risk mitigation may never be at the top of most companies' strategic hopes and dreams. But it is vitally important to carve out time to address the issue in advance, before you have the pressure of a full-blown data breach or investigation. A little time invested up front can save countless hours (and headaches) down the road.

How should you start? It comes back to simplicity. Keep what you need and only what you need. If you don't need to store customers' credit card information or employees' Social Security numbers, then don't. If you do, you are responsible for it.

Once you've identified what information you must keep, sit down with your team and walk through the process from start to finish. Where in the cloud are you storing the data—within U.S. borders or internationally? Who has physical and digital access to the data? How do you transport the data along each step in the process?

Once you start looking for ways to reduce risk, you may find it difficult to stop. Keep in mind that risk mitigation will always be a bit of a balancing act. If you listened to the security community, everything would be locked up tighter than Fort Knox. But you must balance security with the need to do business and interact with your employees and customers.

It wouldn't make sense to have to fill out a full credit report, pass a retinal scanner, and enter multiple secret passwords just to fill your tank at the local gas station. There's a balancing act between security and convenience, but keep in mind: Information is becoming more valuable—and the more valuable it gets, the more protection it will need.

From there, look for ways to simplify the process and lean on trusted parties. These parties might be internal, if you have that core competency on staff, or you might need to look externally for some guidance. Just know that no matter what path you take, make sure you feel comfortable with and trust the parties you involve. That will make it much easier to sleep at night, and will go a long way toward keeping your company off the front page of the paper. ***

Sam Noyd
sam.noyd@jabian.com

Yosef Beck
yosef.beck@jabian.com

Keep what you need and only what you need.