CASE STUDY

IT Company Assessing Risk to Protect Clients

A company managing clients' IT infrastructure can't afford a breach. That's why this IT solution provider took recommendations from their colleagues and hired Pratum to conduct a risk assessment.

Security Comes First

At Pratum we pride ourselves on providing the most secure resources for the businesses we work with. When we approached one of our Information Technology Management clients about doing a case study, they were concerned about sharing the identity of their organization. Being in a competitive market, with sensitive data to protect, opening up too much was a concern for the company's leadership. We offered to tell their story while allowing them to remain anonymous, and they generously agreed.

We want to be able to share how our services can help a wide range of industries, but we also value privacy and respect any company's wishes to keep our work together between us. Being a trusted security partner will always take top priority at Pratum. That's why for the sake of this article we'll refer to the business as "Tech".

TECH

Company: TECH
Industry: Information Technology Management
Established: 2003
Employees: 50
Pratum Services: Information Security Risk Assessment

> We wanted a large enough group to make a mature offering but wanted some Midwestern sensibility, as opposed to going to DC or Boston. They look at the Risk Assessment as a sales process. We just wanted someone to look at working with us as a business partner.
>
> **President, TECH**

The Need to Assess Security

For the team at Tech, deciding to do an Information Security Risk Assessment was a "no-brainer", as the President of the company puts it.

"As an IT solution provider who manages several companies' IT infrastructure there's not only a risk of us getting hacked, but also our clients getting hacked."

That's why they wanted to know for certain the security measures they had in place were strong enough to stand up against any hacking attempt or security breach. Tech's president was confident in the work of her team but wanted extra reassurance the processes initially put in place were still being followed and working properly.

She was also looking for new ways to enhance their already robust security program.

Choosing a Partner

While we can't say where in the United States Tech is located, we can say they are outside of the Midwest. So how did this IT Management company find Iowa-based Pratum? The simple answer - word of mouth.

When Tech's leadership decided it was time to assess their own cybersecurity, they turned to colleagues in the IT field for some guidance. What they found was a very satisfied client of Pratum's called Aureon. Not only did they receive rave reviews about Pratum, Tech also found the perfect fit for their mission.

That's exactly what they found when working with Pratum. From the very start of the company, Pratum has been built on the idea that clients should feel they are being empowered by a team of experts looking out for their best security interests. Pratum's CEO, Dave Nelson, emphasizes the importance of giving the clients what they really need, not upselling with the tactic of fear.

The Risk Assessment Process

The beginning of an Information Security Risk Assessment is a lot of information collection. This typically entails gathering data and uploading that information for Pratum's team to review. This helps the Pratum consultants get to know the business before the assessment process begins. Tech's president called the process "painless and easy".

After the initial review and meetings with Pratum on what Tech's leadership was looking to learn about their business, Pratum began the Risk Assessment. Tech's president felt it was important to tell her team ahead of time exactly how they should handle the work being done by Pratum.

"I had instructed our team that our goal from this wasn't to emerge from this with the best grade. Our goal is to be as secure as possible, not just perceived as such. We wanted to be open and honest."

Having this mindset allowed Pratum to examine the business properly and give a thorough review of the information security program within Tech. Trying to hide information during a Risk Assessment only harms the business being examined in the long run.

Lessons Learned Moving Forward

Tech's president says she was pleased with the report following Pratum's Information Security Risk Assessment. Not only was she comforted knowing the security procedures they had established were still being implemented, but it was also educational to learn a few ways they could boost their security portfolio even more.

"Cybersecurity is important to our clients and they can be no more secure than we are," said Tech's president, "So just like with operational maturity in any IT operation, we have to grow and mature our cybersecurity."

The report was also straightforward and very easy to understand, according to Tech's leader. The heatmap Pratum provided gives them a clear vision of what tasks need to take top priority moving forward. It also explains the severity of each task, along with how to go about making changes to fix them.

In the near future, Tech plans to review the Risk Assessment findings and decide which measures need to be implemented first. One of their biggest goals soon will be pursuing SOC 2 compliance; something they feel more confident in now with Pratum's information and guidance.

Recommending the Process and Pratum

Making the decision to invest in your business's cybersecurity needs should be something every organization is evaluating. Tech's president emphasizes just how crucial she believes this is for a company of any size.

Her analogy compares cybersecurity to home security. Locking your front door isn't just an option for most people, it's a necessity of security. The same can be said of cybersecurity. Taking the necessary steps to protect your business is important no matter the industry or size of your organization.

The first step of any cybersecurity initiative is recognizing strengths and weaknesses already in place.

Having an Information Security Risk Assessment conducted of your business may give you peace of mind, or it could be an eye-opening experience of work that still needs to be done. Either way, having that knowledge can empower your business to make the most educated decisions about cybersecurity moving forward. Something Tech's president is glad to have for the growth of her business and protection of clients.