Securing a City: Corpus Christi Assesses, Prioritizes, and Monitors Threats

Success Story

Challenge: Increase security awareness across the organization and detect and investigate attacks more easily.

Solution: InsightUBA, Nexpose, and Metasploit mitigate risk across all of Corpus Christie's assets with increased visibility and actionable information.

"Risk is real. That's the key message."

Bob Jones is the Information Security Manager for the City of Corpus Christi, Texas. When he first started in his current role, he was given a "blank slate" to build a comprehensive, robust security program for roughly 3,500 employees – so he started by promoting education and awareness internally.

"I'm working to secure a city, not a company, and the culture is primarily concerned with keeping things up and running. Which is understandable," he says. "But it also meant that initially I had to make people understand what we're trying to secure – so that they can understand what it means for an asset to be vulnerable, and why the changes I'm recommending are necessary. The key message is: Risk is real."

Bob knows firsthand that all too often people think of attackers as unseen foes located overseas who are interested in larger targets with juicier intellectual property, like multinational corporations or big-name financial institutions. But there are many different kinds of attackers nowadays with varying motivations, and organizations cannot assume that they'll be overlooked in favor of other prey.

In other words, at the start of the job Bob's work was cut out for him.

Being a Jack of All Trades

City infrastructures are unique, especially from a security perspective. Bob likens it to "about 30 separate SMBs operating under the umbrella of a larger parent company. You have your internal service departments (HR, IT) and then others – your water department, your police department. And you have to be flexible because they all have very different requirements and compliance regulations, depending on the environment."

At a high level, Bob's job is to identify risk and provide recommendations on how to mitigate it. His role is multifaceted; he performs many of the duties of an analyst, an engineer, and a penetration tester. "I wear a few hats," he laughs. "You kind of need to be a jack of all trades in this position."

Changing an embedded culture is never easy. As he embarked on the mission of educating his colleagues and peers at Corpus Christi, Bob came across various misconceptions about security risk. "One of the arguments I bumped into was, 'Why do we need this? We haven't had a DOS attack in years.' What I had to explain was that there are other factors to consider. For example, I was finding malware on computers from well-intentioned users who just happened to visit a malicious site."

Bob's second priority was establishing credibility with people like the CIO and IT Director. "Security and IT must be tightly aligned. Often, IT teams won't be agreeable to someone poking around on what they see as their systems. But you need to be able to work together to achieve the overall goal of supporting the organization. I started by saying, 'Hey, this is exposed. Here are screenshots of data; here is a cracked password.' And then we needed to get

> "It's so much more compelling to be able to say to someone, 'Not only is there a vulnerability in your system, but I was actually able to use that vulnerability to gain access to your system."
>
> ~ Bob Jones, Information Security Manager
> City of Corpus Christi, Texas

to work on prioritization and remediation." This strategy hinged on having the proper tools in place, so Bob would have a way to clearly and concisely relay information to colleagues. But first, he had to find the right vendor.

Addressing Challenges Head On

Bob's primary challenge was lack of visibility, a fairly common pain point among security professionals. Without having the right visibility into assets on the Corpus Christi network, Bob couldn't accurately qualify or quantify the level of risk. "You don't want to cite every possible security concern, because then you're placing a greater burden on the business. To add value, you need to prioritize remediation so that management knows what needs to be done first, based on your specific environment."

Bob began taking an in-depth look at Corpus Christi's data. "I looked at firewall logs, IPs – the more information, the better," he recalls. "Once I had established a baseline, I realized we needed to scan for vulnerabilities on a larger scale, and that I also need a way to understand things like how much risk users pose."

At this point, Bob began to evaluate certain security solutions; among them was Rapid7 Nexpose Enterprise. "It really felt like a fully baked product," he says. Certain features were especially appealing: "The reporting features were – and still are – great. And I really appreciated the fact that when, for example, a vulnerable password was found, Nexpose would take the liberty of enumerating all of the software installed on that machine. That was a huge time saver."

Since implementing Nexpose, the relationship between Corpus Christi and Rapid7 has deepened. Bob recalls how responsive the Rapid7 support team has always been, and how easy it is to get a hold of a support person who is knowledgeable about the product and can quickly answer customer questions. Purchasing Rapid7 Metasploit seemed like a natural progression.

As a longtime user of Metasploit Community – the free, entry-level edition – Bob was already familiar with Metasploit and had used it for penetration testing. "I wasn't sure that I need the Pro version," he admits. But Metasploit Pro, with its automation and closed-loop vulnerability validation features, soon proved its worth. "It's so much more compelling to be able to say to someone, 'Not only is there a vulnerability in your system, but I was actually able to use that vulnerability to gain access to your system.' It motivates action that way, and the fact that we're demonstrating real risk adds value."

Tackling User Risk

Once Corpus Christi was up and running with Metasploit and Nexpose, Bob began to investigate Rapid7 InsightUBA, which detects and investigates attacks targeted at users.

Bob remembers getting involved during the very early stages of the beta: "Those are awesome opportunities; how often do you get the chance to provide feedback on the design of a product before it goes to market? It's really rare that organizations have such a symbiotic relationship with their vendors. Ultimately, we ended up getting a product that we were already familiar with; our input had even been incorporated into its creation."

InsightUBA proved its value by detecting attacks targeted at users, and simplifying the discovery of risky user behavior within the firewall as well as across cloud services and mobile environments. "It was already providing actionable information about threats – things that wouldn't have been detected with any of our other solutions...For example, just yesterday it alerted me to a multiple-location VPN login, which luckily turned out not to be anything nefarious. What happened was that someone at Corpus Christi was helping a vendor in India to update their password. But at least I knew about it and was able to investigate."

The chief purpose of InsightUBA is to detect an attacker's entry and lateral movement with the network without the need to build rules and manually parse data logs, but its benefits extend even farther. "I did forensics work for one of my previous employers," Bob explains. "And the ability to 'tie a user to a chair,' so to speak, is incredibly useful. Knowing who logged in and who I need to contact with questions is critical in the early stages of incident response, and InsightUBA gives me all that. I pop into it on a daily basis, to check out

> "This data that I'm helping to secure – it's not just employee data. It also belongs to my family and friends."
>
> ~Bob Jones, Information Security Manager, City of Corpus Christi

what's happening from a user perspective. It's become my go-to tool for bringing together pieces of information from different places and providing me with a way to quickly print out the data and say to a colleague, 'Hey, I'm responding to this alert and need to know if I should be concerned – got a minute?'"

A steady increase in deception-based attacks has shown a spotlight on user risk. Like many of his industry counterparts, Bob mitigates user risk by promoting internal awareness to ensure they're less likely to fall victim to a social engineering ploy, for example. Another important aspect of mitigating user risk hinges upon having the right tools and technologies in place to protect endpoints. Bob uses Rapid7 to measure how well critical security controls are deployed and configured. He tracks progress to improve endpoint security using an advanced threat model based on the SANS Top 20.

Lessons Learned

Over the course of his career Bob has learned to fine-tune security programs in order to produce optimum results. Meanwhile, the security industry has undergone its own evolution. "As a security professional, having strong familiarity with your systems is key," he advises. "It helps you understand how to fix things. People used to have a mentality of 'Don't patch if it isn't broken.' I've learned to patch in a controlled, thorough manner."

There's no denying that Bob's approach to patch management has yielded real results for the City of Corpus Christi. Thinking back on past years, he estimates that integrating Nexpose into their operational procedures has dropped the average of missing patches by about 75 percent – and climbing. "I'm always striving for the best possible outcome," he says. "I want to see a real reduction in the number of malware reports, virus infections, etc."

Nexpose helps ensure alignment with patch management best practices, which in turn gives Bob peace of mind. But that's not the only piece of the security puzzle; the human element is often an organization's Achilles' heel. "[Users] really can be the weakest link," he admits. "Security pros should be prepared to spend a lot of time sitting down explaining things, educating people and promoting general awareness."

He's also learned how to help other departments see the value of security. Compliance regulations are frequently a motivating factor for strengthening security controls; fear of non-compliance or failing an audit drives many organizations to simplify risk management. It's a strategy which Bob has employed to his advantage: "Compliance gaps are a good starting point – it can really give your suggestions some teeth if you tie security failures to actual financial loss. Being able to inform compliance with clear, prioritized action plans is essential, and a big part of how I use Nexpose and Metasploit."

Bob also understands the importance of collaborative work relationships. His advice to industry peers? "Don't take anything personally. You need to be patient; people will come around, but cultural shifts take time. Security departments need to learn to work closely and effectively with IT operations."

If Bob seems like a particularly dedicated security professional, it may be because there's a personal element to his work. "I don't work for a company, in the traditional sense," he says. "This data that I'm helping to secure – it's not just employee data. It also belongs to my family and friends."