WLAN SECURITY FOR REGULATED INDUSTRIES

The Background

A wireless network security company wanted to promote its technology to regulated industries.

The Challenge

Governmental agencies, the military, healthcare organizations and financial institutions have strict security requirements. At the time of this project, some industries were trying to avoid the wireless security problem by avoiding wireless technology altogether. But as wireless communications grew in popularity and functionality, the head-in-the-sand approach was no longer an option.

The Request

"We need a series of briefs that highlight how our services can benefit organizations where a breach is literally life-and-death. We need to prove that we can deliver on our promises."

The First Step

At the time, I had experience with the real-world challenges and regulatory compliance hurdles facing healthcare organizations and financial institutions. I needed to do my research on use cases within government and military, and better understand the challenges that each group faced.

Through a series of brief, targeted interviews with internal resources and select customers, I identified the pain points for each industry, and which product features delivered the most benefit for each.

This helped me to develop a grid of challenges and solutions for each vertical, and identify where similarities and differences could be found.

What Changed?

- The briefs were short, easily digestible summaries of how the company could address each industry's pain points.
- Product features were translated into customer benefits: How does X help you to achieve Y?
- All briefs focused on reducing complexity and exposure while improving user experience.
- In addition to proving technical competence, it was also critical to emphasize the availability of compliance reporting, an essential part of regulated industry operations.

The Company

Revenue: Privately held

Employees: Undisclosed

Industry: Wireless Network Security

Image courtesy seth schwiet via Unsplash.com.

The Structure

Each two-page brief followed the same basic pattern.

1. The pain: A summary that showed our understanding of their pain points.
2. The solution: Demonstrate wired-equivalent security in life-or-death situations, such as in military and healthcare applications. Show proactive management of network performance. Explain blocking of threats for protection. Demonstrate audit-ready logging of reliability and compliance.
3. The technical information: The details that supported the claims made within the solution section.

As with most of my writing, the brief was broken out with clear, skimmable subheads. The customer can be handed a document in the course of conversation, and still glean important information without drawing their attention from the sales rep. Clear technical information is available for after the meeting, when the customer has time to read in detail.

The Result

The series of four solution briefs were primarily distributed by sales reps at customer meetings or industry events.

The briefs were also available on the website as a downloadable lead generation tool, giving prospective customers a chance to download the brief in exchange for sharing their contact information. The government and healthcare briefs in particular generated strong lead gen traffic until the company was acquired.