Case Study

NotInc, Inc. provides consulting services. Their specialty is widgets. They have a handful of Fortune 500 companies as clients where they coach design through distribution of these widgets.

Kelly, COO, for NotInc recently received an email from their second largest client. It read:

"Kelly – We are tightening up our security controls and our risk management team would like you to fill out the attached questionnaire. It's all routine security stuff, I'm sure you're already doing everything already. If you could fill this out and return it to me in the next week or so, that would be great. I'll get this to the correct risk management team member internally here and they will upload your answers into our tracking system."

Kelly wasn't concerned yet, but then opened the attachment. Included in the Excel document were pages and pages of questions, guidelines, and multiple choice answers. To make matters worse, each answer then had to be graded on a maturity level.

Here is where Kelly called CCI Team. Compliance management is a specialty of ours. Let's break down this scenario so far.

- The Target breach of 2013 started a watershed process for cyber security. Target was compromised through a trusted vendor. Yes, they missed many alarm and opportunities to stop the breach. But, the original penetration happened through a vendor. The attackers then moved laterally through the network.
- Many organizations recognized they carried similar risk. They had shared network connections, data entrusted to 3rd parties, contractors on their VPN – many points of vulnerability.
- These organizations' risk management teams began vetting their contractors and providers. This vetting process is seen above. A questionnaire, often lengthy and highly technical, is sent. This document seeks to:
    - o Collect policies and procedures
    - o Gage alignment with cyber security industry best practices
    - o Learn about breach response and notification
    - o Document key individuals in the organization and their role.

CCI Teams' Engagement

CCI Team came alongside NotInc. We translated the requirements into plain English. We helped NotInc. understand where the gaps were between their current practices and what their customer was looking

for. We put a plan in place to fix these gaps. We assisted in crafting policies that fit their business practice and also satisfied the requirements of their customer.

Summary – we took the pressure/pain off NotInc. We engaged and walked them through the compliance process. How did NotInc benefit?

- Increased cyber security posture. NotInc is safer as a result.
- Compliance with their customer's risk management department means keeping that customer.
- NotInc has this process behind them, next compliance request they receive – they ready.