

Cybersecurity and the Internet of Things: Executive Summary

FEBRUARY 12, 2018

By: Ken Daubenspeck

How secure is the Internet of Things (IoT)? Not secure enough to prevent many of the world's most recognizable internet services—including Amazon, Netflix, and Paypal—from being successfully disrupted by a malicious network composed of hundreds of thousands of hijacked devices. The rise of the internet things presents new challenges to business, and these challenges will increase as the number of connected devices in the workplace continues to expand.

Despite its risks, the benefits created by internet of things technology are too great to pass up on. Securing these devices requires high-level talent that understands the industry's unique challenges; however, this is easier said than done.

The demand for general cybersecurity skill sets already far outstrips the available labor supply; expertise in securing IoT, an infant technology that only emerged onto the mass market in 2014, is even more rarefied.

We have the experience necessary to overcome the cybersecurity labour gap. As networks increase in complexity and connect more directly to vital processes, talent must possess both the level of knowledge necessary to secure systems and the executive skill set required to translate that knowledge into actionable policy. With fifteen years of experience recruiting cybersecurity specialists, we know how to find individuals who have both the skills to secure your connected devices and the experience to apply those skills at a senior-level.

Of the 85% of firms who have or plan to install IoT devices, only 10% are confident they can adequately secure them. We can provide the talent that provides this confidence. Our experience includes successful global recruitment of top cybersecurity talent for both domestic and foreign positions. We have successfully helped firms in a variety of industries to protect themselves, including banking, power grids, manufacturing, healthcare, upstream exploration and production of petroleum and natural gas, and midstream transportation and delivery.

This breadth of experience is integral to our ability to recruit the right person for the job. Different industries face different types of threats, ranging from profit-motivated criminal gangs to nation-state actors. Our background allows us to recruit talent that possess both the industry-specific knowledge necessary to safeguard your networks *and* the ability to appreciate the specific business imperatives they need consider when securing your system.

Our firm has recognized the growth of cyber-threats since the early 1990s. We understand the potential of a data breach to do long-lasting damage. That understanding guides us to focus on finding high-integrity talent that will invest in the success of your business and dedicate themselves to advancing that success for years to come. As cybersecurity becomes part of every facet of the workplace, we look beyond basic technical skills to ensure that the talent we recruit will provide the right fit for your organization's specific culture and values.

Your network is a vital long-term investment, we can ensure the people who protect it are too.

