Booz | Allen | Hamilton

Commercial Solutions

THE PROBLEM WITH IoT

When everything is connected, everything is at risk.

Managing the Hype

The Internet of Things (IoT) is on the lips of everyone in business, from the C-suite to the social media spheres. With the rise of a connected society, organizations and individuals can now connect to one another and to various data sources like never before, creating a wide variety of opportunities for businesses to capture value through new products, services, and—ultimately—customer experiences.

The market is aflutter with new devices and software that offer faster, smarter connectivity. You can change your home temperature from your phone. You can track an athlete's pulse from her shirt. You can gauge your factory's efficiency from the airport. The competitive landscape, as so often occurs in the technology space, rewards those who make it to market first with the newest, coolest, most useful tools for a connected life.

While the possibilities certainly abound, smart leaders should take heed. The hype surrounding IoT is creating heightened expectations and a mad rush to capture share. IoT is in the midst of a Technology Hype Cycle[1]: The speed to market and desire to push further will soon reveal cyber security challenges that force companies to evaluate their approach or run the risk of substantial losses.

IoT is in the midst of a Technology Hype Cycle that will soon reveal costly cyber security challenges.

Learning from Automakers

We see this reassessment taking place already in the automotive space. Nearly 10 years ago, when connectivity first began to enter vehicles in the form of embedded phone capabilities, the market responded with demands for even more.

Automakers rushed to influx their vehicle fleets with everything from GPS systems to Wi-Fi. As early adopters of IoT, automakers were faced with the need to integrate traditional back office IT and IoT concepts to be competitive. In the race to build connected vehicles, elements—like security—that were viewed as a detriment to cost, agility, or customer demands were deprioritized.

Fast forward to the present, and we see automakers coping with the impact of those decisions. From the Markey Report to media headlines, government and consumers now view information and vehicle safety as paramount to our connected vehicles. Automakers are left struggling to retrofit their facilities and products with this new expectation in mind.

The cost of going back may well outweigh the initial gain from speed to market. And some may never recover.

Leaders in other industries can learn from the automotive sector. The same demand for security and privacy of information will soon be paralleled for all smart, connected devices. And Cisco projects that, by 2020, the number of connected devices is estimated to grow to 50 billion[2]. Companies that want to remain relevant in the long term, not just the present, must build their infrastructures and products from the beginning with sustainable security in mind.

[1]Gartner Technology Hype Cycle, 2014
[2]Cisco, "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything," 2011

Companies must evaluate their approach to IoT or run the risk of substantial losses.

Profit from Process

Businesses that want to compete in the converging, connected market must remain agile by approaching this race as a marathon versus a sprint, with a few smart maneuvers up front.

1. Make ecosystem cyber security a C-suite priority.
By now, most executives recognize that cyber matters; the world of IT in the background is gone. Smart, connected products underline this imperative, because anything that is connected can be compromised. Without understanding cyber risk across your entire business ecosystem, your products can pose a threat to your company as well as your customers. IoT demands that leaders expand their cyber security worldview and work to spawn people, process, and technology solutions that address the expanding cyber security challenge at an organizational level. This isn't just about technology; this is about engendering a culture that understands the connection between security and the bottom line.

2. Create a competitive advantage by embedding security from the start.
If we've learned anything from recent breaches, it's that the cost of fixing an issue after the fact greatly exceeds that of building in security from the start. Moreover, the current practice of identifying—rather than preventing—intrusions relies substantially on expensive human capital. The sheer scale of IoT significantly drives up the need for expensive analysts to identify intrusions. At the same time, the cost of embedded security is decreasing. Clearly, the economics are changing. Early adopters of embedded security can achieve lower overall lifecycle costs when compared to those who drive down initial cost by ignoring security.

3. Build solutions with dynamic security.
Security for IoT is not solely associated with devices or IT networks; it might not even be a technology issue. Remaining secure in a connected society requires a dynamic cyber strategy that is pervasive across all things important to IoT—from the supply chain to manufacturing operations, from enterprise IT to insider threats. It must be an active part of all elements that matter to your business, extending to the direct customer interface. To be successful, businesses must shift the focus from traditional, static methods of security and instead focus on building a flexible, agile, and transparent environment where everyone understands the challenge and their part in the solution.

4. Know your priorities, and focus on them.
Today's companies operate with sprawling infrastructures. There's no way you can feasibly secure it all, nor is it logical to do so. Instead, leaders must step back from cyber security and agree on the "crown jewels" that drive their business model. Is it a specific manufacturing site? Certain automated processes that derive important customer intelligence? Whatever it is, agree to a manageable set of items that truly matter within your ecosystem. From there, you can take intelligent steps to implement an optimal blend of security measures that keep your business moving faster and with more confidence.

Reputation is the currency of the digital age. Companies like Apple have built empires by focusing on the needs of customers rather than simply market competition. This model holds true across sectors. It's hard to recover from launching an insecure product into the market. And it can be hard to convince organizations in the early stages of a market opportunity to integrate security; it's tempting to do things quickly rather than properly. But those who succeed long term will do so by avoiding risk and creating a trusted brand experience that sets the foundation for new revenue streams and higher margins. With a strategic view of cyber security, smart leaders can turn the problem with IoT into their competitive advantage.

Innovate Forward

To learn how Booz Allen Hamilton can help your business thrive, contact:

Bill Stewart
Executive Vice President
stewart_william@bah.com
Tel +410-684-6473

Walton Smith
Principal
smith_walton@bah.com
Tel +703-902-4165

Matthew Doan
Senior Associate
doan_matthew@bah.com
Tel +703-377-8950

www.boozallen.com/cyber

Booz | Allen | Hamilton