Cyber in the C-Suite: Industrial

Today’s industrial manufacturing landscape is being disrupted in a hurry. The opportunities for business are tremendous: Increasingly dynamic products create deeper and more profitable customer relationships. But anything that’s connected can be hacked, and insecure infrastructure and products can undermine the platform for future growth. In this era of increasingly “smart” manufacturing and connected products, cyber security is no longer optional. Leaders face a two-fold responsibility: Internally, you must protect the integrity of your supply chain and products; and, externally, you must protect your customers and brand.

YOU'RE NOT ALONE

As a business leader, harnessing opportunity and protecting your enterprise from emerging cyber threats can seem overwhelming, and finding a starting point can be daunting. You'll need to cast a net wider than ever before, taking a full-value-chain perspective on the challenge. Today, you need to think much more broadly than back office IT. The new world connects everything: R&D, supply chain, manufacturing, and customer services.

One unique challenge faced by manufacturers is how to handle the factory environment, where businesses cannot afford unplanned disruptions and downtime. Traditional Information Technology (IT) security approaches rarely translate into the Operational Technology (OT) environment, where core manufacturing processes occur. These environments can’t be easily updated and rebooted like systems on a corporate network.

GET AHEAD ON CYBER

Industrial manufacturers require an actionable strategy for securing product lines and customer relationships. That means product cyber security requires executive attention. The good news is that it’s not too late to act.

Through our work with manufacturing clients, we have identified the five big moves you can make to ensure your organization has a cyber security strategy that protects and enables your growth.

1. Treat your business as a fully connected ecosystem.

What was once considered an impossibility is now reality: There are countless examples of hackers jumping from IT networks into the production environment. They gain access through the supply chain’s many touchpoints, via routine maintenance interactions, and because of internal process breakdowns. A single point of weakness exposes risk across your business. Treating the factory separately is no longer an option; effective cyber security requires a strong security posture across all environments, including supply chain, O&M, the factory floor, and supplier communities. You need a single strategy that adapts appropriately for each operating environment yet integrates a set of core principles.

2. Establish a single point of accountability.

The reality of today’s cyber risk is that the operational environment is now vulnerable to attack. That means you need a role or function with cross-organizational authority. Today’s leading organizations are appointing a single entity with overall responsibility for securing the full ecosystem. This business leader articulates a clear strategy, builds organizational consensus, seizes value-add opportunities, and manages overall risk.

3. Ensure business unit leaders are responsible for cyber.

In the end, your company is in business to generate revenue and grow customer relationships. Cyber security must be viewed as key discipline at every level of the business—not an add-on cost or impediment. While you need a singular leader to drive overall
Cyber isn’t just part of doing business today: It’s how you’ll win the future.

cyber strategy, actions to mitigate the risk must extend beyond the “security” box on your organizational chart. Make cyber security an accountable activity: Build relevant metrics into your business leaders’ performance goals, along with traditional targets like revenue and headcount. Business units should be responsible for operational downtime no matter what the cause, even cyber.

4. Embed cyber security into product development.
You must embed security at the start of the product development lifecycle, so you don’t generate downstream risk in this highly interconnected ecosystem. Do this by embedding a group of diverse cyber experts into key parts of your business. Guided centrally, yet co-located with various business functions, these individuals can tailor policies, standards, and approaches to meet your unique organizational needs. This will do more than secure your business; it will protect the intimate customer interactions—with real-time data sharing and highly customized products and services—that will be a key driver for growth. Security is an important pillar for deep and sustainable customer relationships.

5. Embrace the cultural transformation.
With the rise of connected technologies, your organization is undergoing a fundamental change. There’s new opportunity, new customer expectations, and new risk. Cyber security is an important part of this change, and an enterprise-wide approach to security needs to be on your agenda. But this is about more than compliance. It is about protecting the promise of new business opportunities in our increasingly connected world.

Organizations that find the creativity and flexibility to tackle cyber in this new way will be best positioned to keep pace with the speed of innovation and competition in the connected era. The “smart factory”—connected, automated, and optimized—is a huge opportunity for the manufacturing industry. A cyber security program that maintains trust with customers and reinforces brand quality helps make sure these opportunities are realized.

Now is the time to act!

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

**Sedar M.T. LaBarre**  
Vice President  
labarre_sedar@bah.com  
+ 202-346-9201

**Matt Doan**  
Senior Associate  
doan_matthew@bah.com  
+ 703-377-8860

**Pranav Saha**  
Lead Associate  
saha_pranav@bah.com  
+ 410-684-6628

To learn more, visit www.boozallen.com. (NYSE: BAH)