The Industrial Internet of Things (IIoT) has introduced unprecedented connectivity and major shifts in the way businesses innovate and operate. To realize the full promise of the IIoT, it is imperative to recognize both the opportunities and the vulnerabilities created by connected technology and take responsibility for securing the IoT landscape.

As the saying goes, the IoT is ‘where bits and bytes meet flesh and blood.’ Software and hyper-connectivity are fueling breathtaking innovations in healthcare, transportation, manufacturing, oil and gas, and an increasing number of safety-critical environments. That same software and hyper-connectivity bring with them new classes of accidents and adversaries.

While the promise has been clear, until recently, the perils were less so. High consequence industrial and safety-critical failures are a new reality, and the stakes are higher than ever. Any single failure could trigger a crisis of confidence in the public – compromising further advancements and opportunities.

"With the convergence of the physical and digital worlds, nearly everything has changed, and each participant in the IIoT value chain must understand their share of the responsibility. Let’s all do our part – starting now.”

Joshua Corman, chief security officer, PTC
Shared Responsibility for Security

Cyber safety and security are now everyone’s responsibility. With the advent of physical digital convergence, this new world requires a fusion of once disparate disciplines – and even new innovation. As with physical safety, everyone will need to do their part. For example, each stakeholder in the IoT ecosystem needs to use best efforts to:

- Developers: Design, develop, and maintain secure, defensible, and supportable products and platforms for use by developers, markets, and end users
- Partners and system integrators: Securely extend, embrace, deploy, harden, and maintain solutions amidst an increasingly dynamic threat landscape
- Customers: Safely and securely operate IoT technologies, while remaining vigilant to emerging threats and responding with speed and agility when required
- Governments and regulators: Incentivize and assist, knowing when to lead, follow, or clear the way for the private sector, with an eye on public good, national security concerns, and the safety of the people affected by the technologies jointly produced

And since “There are things the Public Sector can’t do, but the Private Sector won’t do,”¹ there is significant room for help from philanthropic and civil society to catalyze necessary adaptations as well.

Changing Threat Landscape

1. Predators

Software is not new to safety-critical environments, but the growing levels of remote connectivity are significantly changing the threat models. Systems that once enjoyed air gaps are now deliberately connecting, thus exposing themselves to accidents and adversaries. Systems previously hidden from predators now find themselves unprepared for the significant responsibility that comes with connectivity.

Many attacks are being perpetrated by apex predators, like nation state adversaries, that have significant resources and tenacity. But malicious intent is not a prerequisite to harm. Without intention, the widespread RansomWorm known as WannaCry affected 81 hospitals and their ability to provide patient care and emergency services. It later affected factories for Renault, Honda, and others.

Safety-critical and IIoT environments simultaneously:

- Face some of the most capable and funded adversaries
- Carry relatively higher consequences of failure
- Can be significantly under resourced and unprepared

Below are a few examples of the growing volume and variety of safety critical attacks and failures:

<table>
<thead>
<tr>
<th>ISSUE</th>
<th>AFFECTED</th>
<th>CONSEQUENCES</th>
<th>(ALLEGED) ADVERSARY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stuxnet</td>
<td>Iran’s Nuclear Program</td>
<td>Centrifuge Damage</td>
<td>Two Nations States</td>
</tr>
<tr>
<td>Direct attack</td>
<td>NY Water Reservoir</td>
<td>Opened Slough</td>
<td>Nation State</td>
</tr>
<tr>
<td>CyberCaliphate</td>
<td>Democratized West</td>
<td>Loss of life and a crisis of confidence</td>
<td>Terror Group</td>
</tr>
<tr>
<td>Sam Sam</td>
<td>Hollywood Presbyterian Hospital</td>
<td>Denial of Patient Care</td>
<td>Accident by Ransomware</td>
</tr>
<tr>
<td>WannaCry</td>
<td>Honda Auto Plant</td>
<td>Factory Interruption</td>
<td>Accident by Nation State</td>
</tr>
<tr>
<td>NotPetya</td>
<td>Mersk</td>
<td>Global shipping and trade</td>
<td>Accident by Nation State</td>
</tr>
</tbody>
</table>

¹ Eli Sugarman – The Hewlett Foundation
2. Ourselves

Technology allows us to transform the way we innovate and operate. Yet, most industrial and safety-critical environments are change averse and far from nimble. Therefore, we need to act now to fight the inertia that prevents change.

Ways actions and failure to act jeopardize the promise of IoT:

<table>
<thead>
<tr>
<th>“ADVERSARY”</th>
<th>EXAMPLE</th>
<th>MITIGATIONS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lack of Awareness /Ignorance</td>
<td>“I had no idea those hospital and plant outages were caused by an unpatched vulnerability”</td>
<td>Research and education</td>
</tr>
<tr>
<td>Assumptions</td>
<td>“These devices were approved by IT 5 years ago, so we’re secure.”</td>
<td>Ongoing review of connected device security and implement new mitigations for older devices</td>
</tr>
<tr>
<td>Myths &amp; Dogma</td>
<td>“The FDA won’t let me patch”</td>
<td>Collaborate with industry and other federal government agencies</td>
</tr>
<tr>
<td>Inertia</td>
<td>“This is how we’ve always done it.”</td>
<td>Ongoing research and education</td>
</tr>
<tr>
<td>Insufficient Sharing</td>
<td>Fragmented Information Sharing &amp; Analysis Centers (ISACs)(^1)</td>
<td>Outreach, trials, and pilots</td>
</tr>
<tr>
<td>Complexity</td>
<td>System interdependencies</td>
<td>Reduce system segmentation and isolation</td>
</tr>
</tbody>
</table>

3. The Race to Secure

We are in a race against the clock, as the pace of connectivity accelerates along with the sophistication and evolution of our adversaries. Yet today, the ecosystem and supply chain players are notoriously slow to deploy, change, patch, or update.

Let’s look at the current race statistics between vulnerability exploitation and vulnerability remediation. When a new publicly known security vulnerability known as Common Vulnerabilities and Exposures (CVE) is published, we’re now seeing the attackers’ mean-time-to-exploitation of that vulnerability compressing down to days. In stark contrast, the defenders mean-time-to-remediation or mean-time-to-patch is holding still at months to years.

For example, Microsoft provided patches for their OpenSMB flaw, but WannaCry impacted over a third of UK hospitals capacity. In the aftermath of this worldwide RansomWorm, there were about 500,000 exposed, unpatched systems discoverable on the Internet. On the one-year anniversary of the attack, there were still about 500,000 exposed, unpatched systems vulnerable to another predator.

Delays in any part of the value chain or poorly executed hand-offs among stakeholders enables accidents and creates opportunities for adversaries to cause significant cyber physical...
harm. Stakeholders, such as regulators, auditors, and certification authorities, can unintentionally contribute to and perpetuate the collective inertia. All too often, a security fix or patch in one “leg” of the IoT landscape is supplied, but downstream players delay its implementation. To remove any obstacles, be sure to identify and involve all stakeholders.

PTC Commits to Industry Best Practices and Collaboration

Yesterday’s best practices are best no longer. We collectively need to pioneer new ways to address today’s dynamic threat environment.

As the provider of a leading Industrial Innovation Platform, PTC sits at the foundation of many of the world’s safety-critical systems. We recognize the responsibility that comes with this foundational role and are committed to doing our part. Now, PTC is calling on partners and customers to work together with PTC to optimize IIoT security by taking responsibility for the components in their control.

PTC is continually enhancing security best practices, especially in key maturity areas such as Secure Software Development Lifecycle (SDLC), Operational and Infrastructure Security, and Security Response Capabilities (both on the incident response and vulnerability remediation side). Below are some of the best practices PTC is introducing:

Third-Party Collaboration

• Launch of a Coordinated Vulnerability Disclosure (CVD) Program
• Greater engagement with IoT and security solution providers
• Partnership with academia

Leadership of Public Policy, Regulatory, Standards, and Industry Initiatives

• Leadership in IIoT standards bodies and working groups
• Prominent engagement in legislative and executive branch activity
• Participation in information sharing groups such as ISACs
• Creation and/or support of working groups to improve security for safety critical sub-sectors

Many of these actions and investments have corresponding parallels and hand-offs for developer ecosystems, system integrators, professional service partners, downstream operators, and relevant policy makers, auditors, etc.

"Through our over dependence on undependable IT, we have created the conditions such that the actions of any single outlier can have a profound and asymmetric impact on human life, the economy, and national security.”  


When you’re over dependent on undependable things, you have two choices: make the things more dependable or become less dependent on them. In the race toward the promise of connected technology, we have focused on reaping the benefits, but have yet to fully internalize the cost of managing the security threats lurking beneath them. Often the focus is on the initial deployment of new technology, and security becomes an afterthought.
In this shared responsibility model, if a party is not prepared to do their part, they have a choice to make: If you can't afford to protect it, then you can't afford to connect it.”

At a high level, our responsibilities are shared and extend our spheres of control and influence. We seek to develop more specific responsibilities with our ecosystem teammates.

**Shared Responsibilities Stack**

PTC seeks partners who are committed to owning their share of responsibility for creating a secure environment. For those who are up to the task but don’t know where to start, we’ll help get you on the path to be race-ready:

- Always update software to the latest release and deploy patches in a timely manner
- Ensure system deployments embed security best practices from design to implementation
- Train personnel to ensure all critical actions are performed with security and safety in mind
- Take responsibility and hold others responsible and accountable
- Challenge and revisit your assumptions

**Summary**

Cyber safety and security must be a shared responsibility for IIoT environments. At PTC, we're dedicated to working together with our customers and partners to develop and deploy secure IoT platform and product lifecycle solutions. With PTC, global manufacturers and an ecosystem of partners and developers can capitalize on the promise of the IoT today and drive the future of innovation.

For more information, please visit [www.PTC.com/security](http://www.PTC.com/security).

---

1) Joshua Corman (2017) with regards to the Healthcare Cybersecurity Task Force Report and WannaCry attacks on UK Hospitals


© 2018, PTC Inc. (PTC). All rights reserved. Information described herein is furnished for informational use only, is subject to change without notice, and should not be taken as a guarantee, commitment, or offer by PTC.

PTC, the PTC logo, and all PTC product names and logos are trademarks or registered trademarks of PTC and/or its subsidiaries in the United States and other countries. All other product or company names are property of their respective owners. The timing of any product release, including any features or functionality, is subject to change at PTC’s discretion