Shared Responsibility: IoT Cyber Safety & Security

Foreword

The Internet of Things (IoT) has introduced unprecedented connectivity and major shifts in the way businesses innovate and operate. To realize the full promise of IoT, we must all acknowledge the peril connected technology presents and each take responsibility for securing the IoT landscape. We must band together.

As our Chief Security Officer is fond of saying, the Internet of Things (IoT) is "*Where Bits & Bytes, meet Flesh & Blood*". Software and hyper-connectivity are fueling breathtaking innovations in healthcare, transportation, manufacturing, oil & gas, and an increasing number of safety critical environments. That same software and hyper-connectivity bring with them new classes of accidents and adversaries. Our adversaries include nation states and extremists who are organized and relentless. While the promise has been clear, until recently, the perils were less so. High consequence industrial and safety critical failures are now upon us. If we're cavalier about the perils, a single exotic failure could trigger a crisis of confidence in the public to trust such innovations - postponing otherwise superior advances and opportunities.

> At PTC, we have taken a fresh look at IoT security principles to help each participant in the IoT value chain understand their share of the responsibility. As we begin this journey, our initial adversaries will include ignorance, inertia, and time. With the convergence of the Physical and Digital realms... nearly everything has changed... which means we, too, must change. Let's all do our part – starting now.
>
> Jim Heppelmann, President & CEO
> Joshua Corman, SVP & CSO

Shared Responsibility for Security

Cyber safety and security are everyone's responsibility. With the advent of physical digital convergence, now that bits & bytes meet flesh & blood, 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:

- The developer of industrial innovation platforms needs to use best efforts to design, develop, and maintain secure, defensible and supportable products and platforms for use by the developers, markets, and end users we serve.
- The partners and system integrators in the rich and growing ecosystem of Industrial IoT need to use best efforts to securely extend, embrace, deploy, harden, and maintain these solutions amidst an increasingly dynamic threat landscape.
- The customers of these technologies need to safely and securely operate these innovations while remaining vigilant to emerging threats – and increase their ability to affect prompt and agile responses when required.
- Governments and regulators will need to incentivize and assist in the necessary transformations – knowing when to lead, follow, or clear the way for the private sector – ever with an eye on public good, national security concerns, and the safety of the people affected by the technologies we jointly produce.
- 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.

Changing Threat Landscape

1. Predators

Software is not new to Safety Critical environments, but the growing levels of remote connectivity is changing our threat models – significantly. Systems which once enjoyed air gaps are now deliberately connecting and exposing themselves to myriad accidents and adversaries. Systems which enjoyed relative obscurity from predators now find themselves both prone and prey – unprepared for the significant responsibility that comes with connectivity. Worse, many of these attacks are being perpetrated by apex predators like nation state adversaries – with significant resources and tenacity. And perhaps even worse, malicious intent is not a prerequisite to harm. Without intention, the mass infecting RansomWorm known as WannaCry affected 81 hospitals severely affecting availability of patient care delivery and emergency services. It later affected factories for Renault, Honda, and others.

Safety Critical and Industrial IoT environments simultaneously:

- Face some of our most capable and funded adversaries
- Carry relatively higher consequences of failure
- Can be significantly under resourced and immature with regard to cyber hygiene

[1] Eli Sugarman – The Hewlett Foundation

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

ISSUE	AFFECTED	CONSEQUENCES	(ALLEGED) ADVERSARY
Stuxnet	Iran's Nuclear Program	Centrifuge Damage	2 Nations States
Direct attack	Ukraine Power Grids (x2)	Power Outages	Nation State
Direct attack	NY Water Reservoir	Opened Slough	Nation State
CyberCaliphate	Democratized West	Terror Loss of Life Crisis of Confidence	Terror Group
Sam Sam	Hollywood Presbyterian Hospital	Denial of Patient Care	Accident by Ransomware
WannaCry	81 UK Hospitals (> 40% capacity)	Denial of Patient Care	Accident by Nation State
WannaCry	Renault Auto Plant	Factory Interruption	Accident by Nation State
WannaCry	Honda Auto Plant	Factory Interruption	Accident by Nation State
NotPetya	Merck Pharmaceutical	>$300M & Vaccine Production	Accident by Nation State
NotPetya	Mersk Shipping	Global Shipping/Trade	Accident by Nation State
NotPetya	Nuance	Delayed/degraded patient care	Accident by Nation State

2. Ourselves

Most Industrial and Safety Critical environments are change averse - and far from nimble. As W. Edwards Deming said: ***"It is not necessary to change. Survival is not mandatory."*** But we choose not only survival, but the transformation of the way we innovate and operate. Therefore, we need to act now to fight the inertia that prevents change.

Ways our actions and failure to act imperil the promise of IoT:

"ADVERSARY"	EXAMPLE	MITIGATIONS
Lack of Awareness /Ignorance	"I had no idea those hospital and plant outages were caused by an unpatched vulnerability"	Research & Education "Safety Critical Mass" Working Groups
Assumptions	"All our devices sit behind the firewall and are therefore secure."; "These devices were approved by IT 5 years ago, so we're secure."	Ensure ongoing review of connected device security, and implement new mitigations for older devices. Embed a thorough understanding of unique needs for connected device security.
Myths & Dogma	"The FDA won't let me patch" False; In fact, a failure to patch may cause a recall or regulatory action. [2]	Critical Thinking Myth Busting Campaigns Explainers
Inertia	"This is how we've always done it." "We can't touch certified environments." Less/Indefensible legacy w/long lifespans	Critical Thinking Myth Busting Campaigns Explainers
Insufficient Sharing	Fragmented ISACs* w/ low participation *Information Sharing & Analysis Center [3]	Outreach, Trials, & Pilots
Complexity	Elective Attack Surfaces Interdependencies / Entanglement Compounding "Technical Debt"	System Reduction Segmentation & Isolation Paying Down Technical Debt

[2] FDA Post Market Guidance: https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf
See also FDA FACT SHEET (Dispelling Myths): https://www.fda.gov/downloads/MedicalDevices/Digital_Health/UCM544684.pdf

[3] Full list of ISACs can be found here: https://www.nationalisacs.org

3. The Relay Race

We are in a complex relay race against the clock, which is perhaps our greatest challenge. The pace of connectivity continues to accelerate and the sophistication of our adversaries is evolving rapidly. But today, the ecosystem and supply chain players are notoriously slow to deploy, change, or patch/update.

As an example of how we are losing the race against the clock, let's take a look at the current race statistics between vulnerability exploitation and vulnerability remediation. When a new CVE (Common Vulnerabilities and Exposures; publicly known security vulnerabilities) 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-years**. In the case of WannaCry, Microsoft had provided patches for their OpenSMB flaw; WannaCry hit UK hospitals in less than two months later – affecting over a third of their national healthcare 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 are still about 500,000 exposed, unpatched systems just waiting for another predator to pounce.

A brief example of some stakeholders in our Ecosystems and Relay Races:

PTC OFFERING	DEVELOPER/OEM	OPERATOR	AFFECTED GROUPS	GOVERNMENT
Axeda	MedDevice Maker	Hospital	Patients	HHS
Kepware	System Integrator	Power Plant	Plant Workers/Citizens	DOE/DHS
ThingWorx	Manufacturer IT	Auto Parts Maker	Auto Makers	DOT

Delays in any leg of this relay race or poorly executed hand-offs of the baton among stakeholders enables accidents and creates opportunities for adversaries to cause significant cyber physical harm.

- It's not enough to supply a security fix or patch in one "leg" of the IoT landscape if downstream players introduce or allow elective or egregious delay.
- It's not enough for fixes to get to the last mile only for operators to wait for another six months or a year to enhance the security of their operations.

Compression and streamlining must occur not only at each leg of this relay race, but also with an eye toward how change flows throughout the entire ecosystem to achieve the ultimate desired result. All stakeholders should be considered and brought to the table to remove obstacles. This includes regulators, auditors, certification authorities, and the like who (with the best of intentions) can contribute to and perpetuate our collective inertia.

PTC Is Making Changes

Yesterday's "best practices" are "best" no longer. We collectively need to pioneer new ways to address the dynamic threat environment we exist in today.

As a leading provider of Industrial Innovation Platforms, 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 will do our part. **Now, PTC is calling for our partners and customers to work together with PTC on optimizing security in IoT by taking responsibility for the IoT implementation components in their control.**

PTC is continually enhancing security best practices, especially in key maturity areas like Secure Software Development Lifecycle (SDLC), Operational and Infrastructure Security and Security Response Capabilities (both on the incident response and vulnerability remediation side). What follows are samples of some new changes PTC is making to introduce best practices for today's world:

3rd Party Collaboration

- Launch of a Coordinated Vulnerability Disclosure Program
- Greater engagement with IoT & security solution providers
- Partnership w/ academia

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

- Leadership in IIoT / IoT Standards bodies and working groups
- Prominent engagement in Legislative and Executive branch activity
- Participation in Information sharing groups like ISACs (Information Sharing and Analysis Centers) for sectors we serve
- Creation and/or support of working groups to get safety critical sub-sectors from Current State to Desired State
- Sector Education – E.g. "Safety Critical Mass" and our Cyber Safety Village at LiveWorx

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

> 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, economic, and national security." [4]

When you're over dependent on undependable things, you have two avenues: make the things more dependable or depend upon them less. In the race toward the promise of connected technology, we have focused on reaping the benefits, but have yet to fully internalize the costs of managing the security threats lurking in these benefits. All too often, the eyes are on the initial deployment of the hot new technology, and security becomes an afterthought and bolt-on despite past major failures with this approach. In this shared responsibility model, if a party is not prepared to do their part, they have a choice to make:

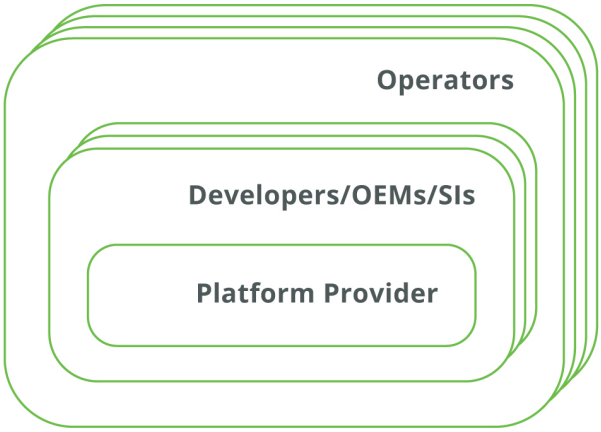
> "If you can't afford to protect it, then you can't afford to connect it." [5]

[4] Congressional Testimony (Corman) 2017 IoT Cybersecurity: https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm482022.pdf

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

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



The promise of IoT is too vital and the safety critical risks too devastating to connect without protecting. In the IoT relay race, we only want partners who are committed to owning their share of responsibility for creating a secure environment. If this is more than you are willing to do, in some cases, we may need to part ways. For those of you who are up to the task but just don't know where to start, we'll help get you on the path and 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 your personnel to ensure all critical actions are performed with security and safety in mind
- Take responsibility, and hold others responsible and accountable
- Challenge/revisit your assumptions....

Public Policy and Regulatory Activity

Public Policy makers (US and international) are taking action to adapt their postures and guidance to the new realities of hyper-connected innovations. These adaptations are not evenly distributed, but below are a few already in effect – and others in process.

AGENCY	POLICY/REPORT	SAMPLE DETAILS
US FDA	2014 Pre-Market Guidance [6]	Threat Modeling, Risk Assessments, Secure By Design
US DHS	2016 Strategic Principles for Securing IoT [7]	Security by Design Patchable Technologies SW BoMs Coordinated Vulnerability Disclosure
US Commerce NTIA	2016 Coordinated Vulnerability Disclosure [8]	Early Stage Template for Safety Critical Industries [9]
US FDA	2016 Post-Market Guidance [10]	E.g. If you have a Coordinated Vulnerability Disclosure program, mitigate flaws w/in 30 days, & fix them w/ 60 days you can avoid regulatory action/recall
US White House	2016 Presidential Commission on Enhancing National Cybersecurity [11]	An exploration for the state of the law regarding liability with regard to software and IoT
US White House	2017 Executive Order: Cybersecurity for Critical Infrastructure [12]	"for too long accepted antiquated and difficult-to-defend IT" "Known but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies" "attacks that could reasonably result in catastrophic regional or national effects on public health or safety"

[6] FDA Pre-Market Guidance for Connected Medical Devices: https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

[7] JDHS Strategic Principles for Critical Infrastructure: https://www.dhs.gov/news/2016/11/15/dhs-releases-strategic-principles-securing-internet-things

[8] NTIA Multi-stakeholder Process: https://www.ntia.doc.gov/other-publication/2016/multistakeholder-process-cybersecurity-vulnerabilities

[9] NTIA Coordinated Vulnerability Disclosure Template: https://www.ntia.doc.gov/files/ntia/publications/ntia_vuln_disclosure_early_stage_template.pdf

[10] NTIA Coordinated Vulnerability Disclosure Template: https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM356190.pdf

[11] Presidential Commission: https://www.nist.gov/cybercommission

[12] Presidential EO : https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/

US Congress	2017 Healthcare Industry Cybersecurity Task Force [13]	Legacy Technology Risks & Mitigations Known Vulnerabilities Epidemic Call for a Software Bill of Materials
US Congress	2017 Internet of Things (IoT) Cybersecurity Improvement Act of 2017 [14]	Avoid Known Vulnerabilities Must be Patchable Avoid Fixed Credentials Use Standards-based Encryption & Protocols Coordinated Vulnerability Disclosure Program
UK NCSC	Secure by Design & Code of Practice for IoT [15]	Avoid default passwords Patchable & Patching Vulnerability Disclosure Programs Attack Surface Reduction … (13 total)

Summary

Cyber Safety & Security are necessarily a shared responsibility for IoT environments. We at PTC are committed to doing our part and to helping you to do yours. We are excited about the promise of hyper-connectivity and industrial IoT Innovation and vigilant to the peril. We're eager to join forces with you to share the responsibility for securing the IoT ecosystem so that collectively all stakeholders can participate in the promise of this transformative opportunity.

For more information, please visit www.PTC.com/security.

[13] HHS / Congressional Task Force on Healthcare Cybersecurity: https://www.phe.gov/Preparedness/planning/CyberTF/Documents/report2017.pdf

[14] Senators Warner & Gardner IoT Bill : https://www.congress.gov/bill/115th-congress/senate-bill/1691/text

[15] UK Secure By Design for IoT (and Code of Practice): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/686089/Secure_by_Design_Report_.pdf

SharedResponsibility:IoTCyberSafety&Security–EN–2018