RSAConference2019
San Francisco | March 4–8 | Moscone Center

SESSION ID: MBS-T06

Hindsight and 2020: A Clear-Eyed Look at Shared Responsibil-I-o-T

Joshua Corman
CSO
PTC
@joshcorman

Julie Fitton
VP, Digital Product Security
Stanley Black & Decker

Agenda

- Some Primitives
- Some Threat Context
- 1st movers in Executive & Legislative
- Recent 2018 Actions
- International Actions
- Solution: Shared Responsibil-I-o-T

Hippocratic Oath

Formal Capacities	Plain Speak
1. Cyber Safety by Design	1. Avoid Failure
2. Third-Party Collaboration	2. Engage Allies to Avoid Failure
3. Evidence Capture	3. Learn from Failure
4. Resilience and Containment	4. Isolate Failure
5. Cyber Safety Updates	5. Respond to Failure

www.iamthecavalry.org
@iamthecavalry

New: How IoT is "different"

Aspect	Descriptions
Adversaries	Different adversaries with different motivations and capabilities
Consequences of Failures	Life & Limb, Physical Damage, Market Stability/Confidence, National Security
Context & Environment	Operational contexts can be quite different. Migratory, Perimeter-less, Inaccessible, Difficult to patch/replace
Composition of Goods	Differences in Hardware, Firmware, Software stacks
Economics	Margins, Buyers, Investors, Costs of Goods, etc
Time Scales	Time-to-Live (TTLs), R&D Cycles, Response Times


BlackEnergy cybercrime tool

DEVELOPING NOW

IRANIAN HACKERS TARGETED DAM NEAR NEW YORK CITY

CNN

DOW ▲ 123.07

SITUATION ROOM


EMERGENCY


POISONON


AbuHussainAlBritani
@AbuHussain102
Follow
"Jihad and the rifle alone. NO negotiations, NO conferences and NO dialogues" - (Shaykh Abdullah Azzam, rahimahullah)

Mostly Human: Hacker Down | ISIS' Twitter Star

The story of the first person deemed dangerous enough to kill... because of his ability to tweet. Watch the rest of the episodes on CNNgo via Apple TV, Roku, and Amazon Fire TV. Source: CNNMoney


EMERGENCY

Government is noticing/acting…

Presidential Commission Report

DOC/NTIA Guidance

FDA Guidance

DOJ Work Group

DOD Strategy

EU Guidance

DHS Guidance

FTC Guidelines

HHS Task Force

DOT Principles

NHTSA Guidance

Food and Drug Administration

Postmarket Management of Cybersecurity in Medical Devices

Guidance for Industry and Food and Drug Administration Staff

Document issued on December 28, 2016.

The draft of this document was issued on January 22, 2016.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of the Center Director
Center for Biologics Evaluation and Research

ptc | StanleyBlack&Decker

Department of Homeland Security

STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT)

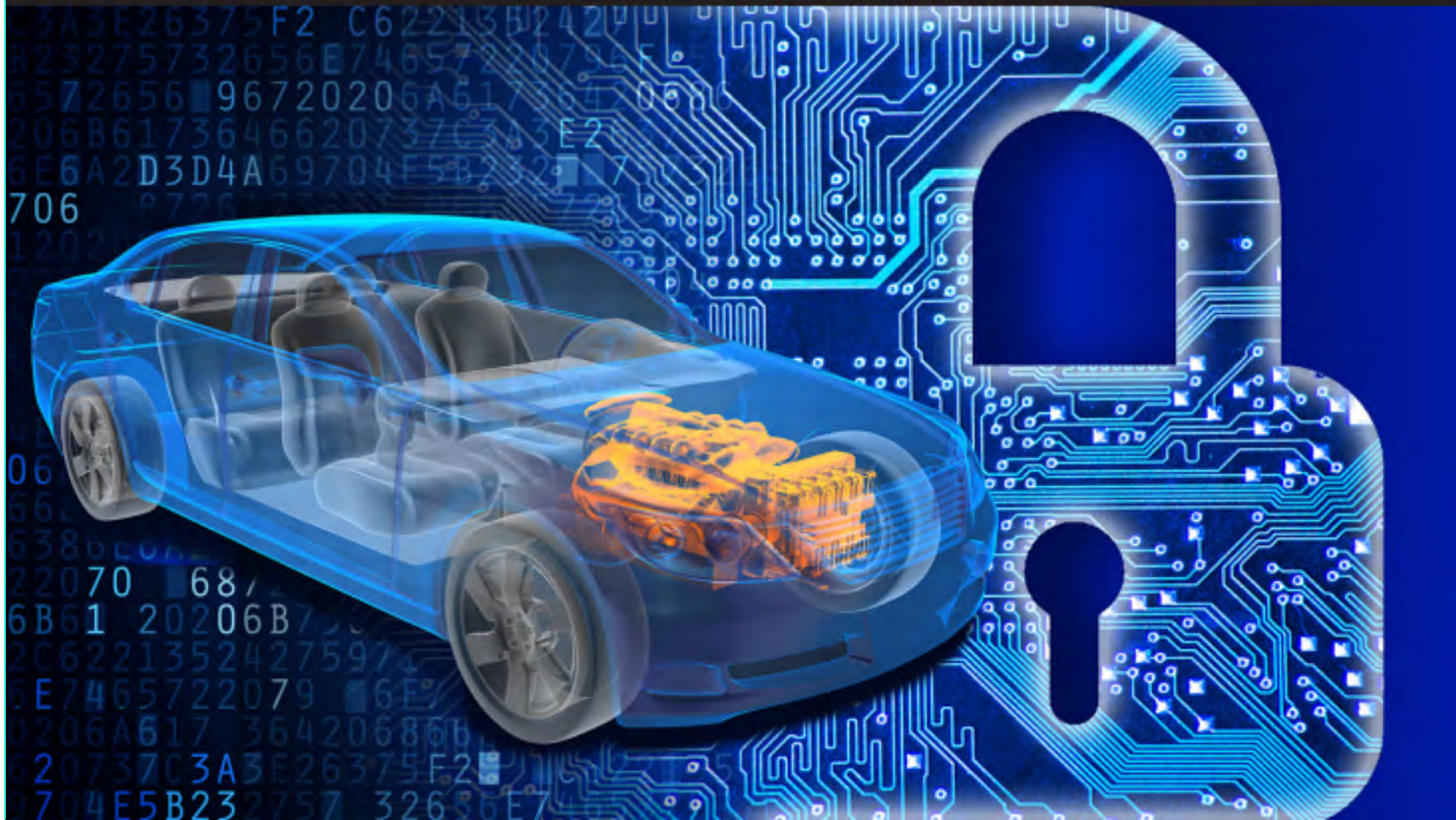
Version 1.0

November 15, 2016

ptc | StanleyBlack&Decker

Department of Transportation

Cybersecurity Best Practices for Modern Vehicles



ptc | StanleyBlack&Decker

Department of Commerce

Multistakeholder Process: Cybersecurity Vulnerabilities

Stakeholder documents

- Deputy Assistant Secretary Angela Simpson's blog post announcing the release of these documents
- Vulnerability Disclosure Attitudes and Actions: A Research Report
- Coordinated Vulnerability Disclosure "Early Stage" Template
- Guidelines and Practices for Multi-party Vulnerability Coordination

Vulnerability Disclosure Attitudes and Actions

A Research Report from the NTIA Awareness and Adoption Group

"Early Stage"
Coordinated Vulnerability Disclosure Template
Version 1.1[1]

NTIA Safety Working Group
December 15, 2016

ptc | StanleyBlack&Decker

Presidential Commission Report

Presidential Commission Report

Action Item 2.1.3: *The Department of Justice should lead an interagency study with the Departments of Commerce and Homeland Security and work with the Federal Trade Commission, the Consumer Product Safety Commission, and interested private-sector parties to assess the current state of the law with regard to liability for harm caused by faulty IoT devices and provide recommendations within 180 days.* (SHORT TERM)

Action Item 3.1.1: *To improve consumers' purchasing decisions, an independent organization should develop the equivalent of a cybersecurity "nutritional label" for technology products and services—ideally linked to a rating system of understandable, impartial, third-party assessment that consumers will intuitively trust and understand.* (SHORT AND MEDIUM TERM)

Presidential Executive Order

(ii) The executive branch has for too long accepted antiquated and difficult-to-defend IT.

(iii) Effective risk management involves more than just protecting IT and data currently in place. It also requires planning so that maintenance, improvements, and modernization occur in a coordinated way and with appropriate regularity.

(iv) Known but unmitigated vulnerabilities are among the highest cybersecurity risks faced by executive departments and agencies (agencies). Known vulnerabilities include using operating systems or hardware beyond the vendor's support lifecycle, declining to implement a vendor's security patch, or failing to execute security-specific configuration guidance.

CC : From: http://www.flickr.com/photos/maiabee/2760312781/

HEALTH CARE INDUSTRY CYBERSECURITY TASK FORCE

June 2017

REPORT ON IMPROVING CYBERSECURITY IN THE HEALTH CARE INDUSTRY

HEALTHCARE CYBERSECURITY IS IN CRITICAL CONDITION

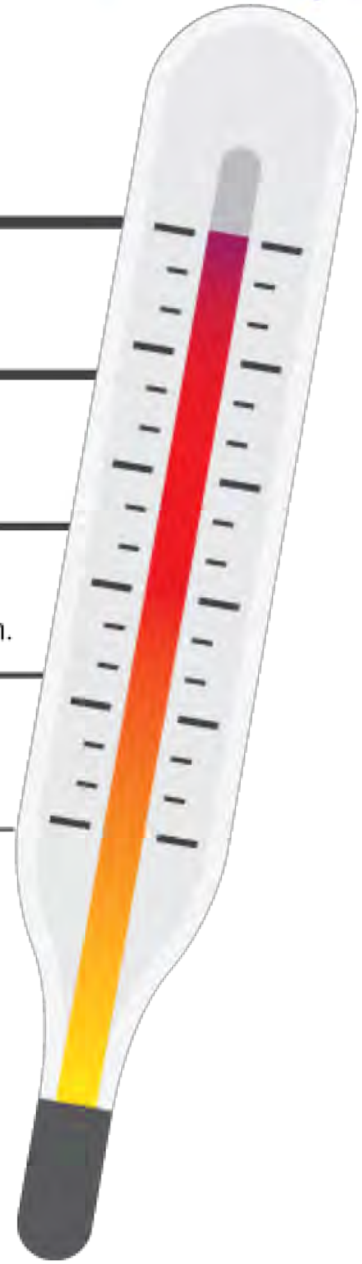
Severe Lack of Security Talent
The majority of health delivery orgs lack full-time, qualified security personnel

Legacy Equipment
Equipment is running on old, unsupported, and vulnerable operating systems.

Premature/Over-Connectivity
'Meaningful Use' requirements drove hyper-connectivity without secure design & implementation.

Vulnerabilities Impact Patient Care
One security compromise shut down patient care at Hollywood Presbyterian and UK Hospitals

Known Vulnerabilities Epidemic
One legacy, medical technology had over 1,400 vulnerabilities



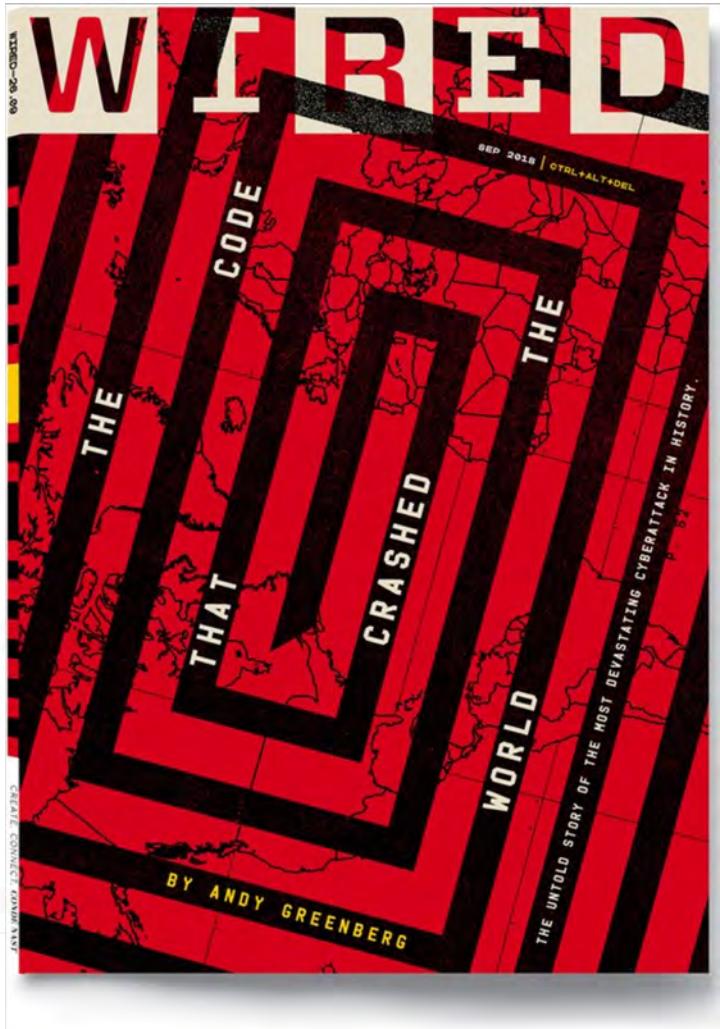

Ooops, your files have been encrypted!
English
What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.
Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.
How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am
Payment will be raised on
5/15/2017 14:57:41
Time Left
02:23:59:02
Your files will be lost on
5/19/2017 14:57:41
Time Left
06:23:59:02
About bitcoin
How to buy bitcoins?
Contact Us
bitcoin
ACCEPTED HERE
Send $300 worth of bitcoin to this address:
115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn
Copy
Check Payment

ANDY GREENBERG SECURITY 08.22.18 05:00 AM

THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY

IT WAS A perfect sunny summer afternoon in Copenhagen when the world's largest shipping conglomerate began to lose its mind.

The headquarters of A.P. Møller-Maersk sits beside the breezy, cobblestoned esplanade of Copenhagen's harbor. A ship's mast carrying the Danish flag is planted by the building's northeastern corner, and six stories of blue-tinted windows look out over the water, facing a dock where the Danish royal family parks its yacht. In the building's basement, employees can browse a corporate gift shop, stocked with Maersk-branded bags and ties, and even a rare



Government is noticing/acting…

Presidential Commission Report

DOC/NTIA Guidance

FDA Guidance

DOJ Work Group

DOD Strategy

EU Guidance

DHS Guidance

FTC Guidelines

HHS Task Force

DOT Principles

NHTSA Guidance

Bi-Partisan Bill(s)

https://www.scribd.com/document/355269230/Internet-of-Things-Cybersecurity-Improvement-Act-of-2017

ALB17666 S.L.C.

115TH CONGRESS
1ST SESSION

S. _____

To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agencies, and for other purposes.

IN THE SENATE OF THE UNITED STATES

Mr. WARNER (for himself, Mr. GARDNER, Mr. WYDEN, and Mr. DAINES) introduced the following bill; which was read twice and referred to the Committee on _____

A BILL

To provide minimal cybersecurity operational standards for Internet-connected devices purchased by Federal agen-

Internet of Things

Cybersecurity Improvement Act of 2017

Senators Mark Warner, Cory Gardner, Ron Wyden, and Steve Daines

FACT SHEET:

While 'Internet of Things' (IoT) devices and the data they transmit present enormous benefits to consumers, the relative insecurity of many devices presents enormous challenges. Thus far, there has been a significant market failure in the security of these devices.

Sometimes shipped with factory-set, hard-coded passwords and oftentimes unable to be updated or patched, IoT devices can represent a weak point in a network's security, leaving the rest of the network vulnerable to attack. Additionally, the sheer number of IoT devices – expected to exceed 20 billion devices by 2020 – has enabled bad actors to launch devastating Distributed Denial of Service (DDoS) attacks. **This legislation is aimed at addressing the market failure by establishing minimum security requirements for federal procurements of connected devices.**

The legislation requires vendor commitments:

- That their IoT devices are patchable.
- That the devices don't contain known vulnerabilities.
  - If a vendor identifies vulnerabilities, it must disclose them to an agency, with an explanation of why the device can be considered secure notwithstanding the vulnerability and a description of any compensating controls employed to limit the exploitability/impact of the vulnerability.
  - Based on this information, an agency CIO could issue a waiver to purchase the device.
- That the devices rely on standard protocols.
  - Outside experts emphasize the importance of having the vendor disclose what network protocols are in use, for instance to assist Department of Homeland Security (DHS)'s Einstein program.
- That the devices don't contain hard-coded passwords.

Recognizing that it may be infeasible for certain devices to meet those requirements, and in consideration of network-based technologies that can help manage risks from insecure devices:

https://oversight.house.gov/hearing/cybersecurity-internet-things/

CYBERSECURITY OF THE INTERNET OF THINGS

Subcommittee on Information Technology

SUBCOMMITTEE ON INFORMATION TECHNOLOGY

HEARING DATE: OCTOBER 3, 2017 2:00 PM | 2247 RAYBURN HOB

*House Oversight and Government Reform – hearing panelists

RELATED UPDATES

INNOVATIONS IN SECURITY: EXAMINING THE USE OF CANINES

EXAMINING AMERICA'S NUCLEAR WASTE MANAGEMENT AND STORAGE

PRESS RELEASE

Walden Asks HHS to Convene Sector-Wide Effort to Develop Software Bill of Materials for Health Care Technologies

11.16.17

OVERSIGHT AND INVESTIGATIONS

WASHINGTON, DC – Energy and Commerce Committee Chairman Greg Walden (R-OR) today sent a letter to the Department of Health and Human Services (HHS) requesting they convene a sector-wide effort to establish a plan of action for creating, deploying, and leveraging software bill of materials (SBOM) for health care technologies. The request follows a recent #SubOversight hearing examining HHS' role in health care cybersecurity, and letters on outbreaks like NotPetya.

Department of Commerce

National Telecommunications and Information Administration
United States Department of Commerce

Newsroom | Publications | Blog | Offices | About

Home » Publications » Other Publications » 2018

Topics

- Spectrum Management
- Broadband
- Internet Policy
- Domain Name System
- Public Safety
- Grants
- Institute for Telecommunication Sciences
- Data Central

NTIA Software Component Transparency

Topics:
Internet Policy | Internet Policy Task Force | Cybersecurity | Internet of Things

Printer-friendly version

Date:
October 30, 2018

Upcoming meeting:

The next meeting will be held on November 6, 2018, from 10:00 a.m. to 4:00 p.m., EST.

The meeting will be held at the American Institute of Architects, 1735 New York Ave., N.W., Washington, DC 20006. It will also be webcast (link coming soon), with a call bridge for remote participation.

Toll free call bridge: 877-939-1574 Passphrase: NTIA
Toll and international dial-in: +1-517-308-9330 Passphrase: NTIA

- 11/06/2018 Meeting Webcast
- *Federal Registe*

Working Groups

October 1 update

At the July 19 kick

Date: July 19, 2018

- Agenda
- Webcast Archive
- Notes from stakeholder discussions
- Presentations from the Perspective Sharing session
  - Art Manion, Senior Vulnerability Analyst, CERT/CC
  - Bruce Lowenthal, Senior Director, Oracle Security Alerts Group
  - Jim Jacobson, Chief Product Security Officer, Siemens Healthineers
  - Chris Wysopal, Chief Technology Officer, CA Veracode
  - Josh Corman, Chief Security Officer, PTC
  - Jennings Aske, VP & CISO, New York Presbyterian

ptc | StanleyBlack&Decker

Food and Drug Administration

Contains Nonbinding Recommendations

Draft – Not for Implementation

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Draft Guidance for Industry and Food and Drug Administration Staff

DRAFT GUIDANCE

This draft guidance document is being distributed for comment purposes only.

Document issued on October 18, 2018.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of the Center Director
Center for Biologics Evaluation and Research

ptc | StanleyBlack&Decker

Contains Nonbinding Recommendations

Draft – Not for Implementation

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices

Draft Guidance for Industry and Food and Drug Administration Staff

12. A CBOM including but not limited to a list of commercial, open source, and off-the-shelf software and hardware components to enable device users (including patients, providers, and healthcare delivery organizations (HDOs)) to effectively manage their assets, to understand the potential impact of identified vulnerabilities to the device (and the connected system), and to deploy countermeasures to maintain the device's essential performance.

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Office of the Center Director
Center for Biologics Evaluation and Research

FDA U.S. FOOD & DRUG ADMINISTRATION
CENTER FOR DEVICES & RADIOLOGICAL HEALTH

ptc | StanleyBlack&Decker

The aim of this Code of Practice is to support all parties involved in
manufacturing and retail of consumer IoT with a set of guidelines to
products are secure by design and to make it easier for people to st
world.

The Code of Practice brings together, in thirteen outcome-focused
widely considered good practice in IoT security. It has been develop
Department for Digital, Culture, Media and Sport (DCMS), in conju
National Cyber Security Centre (NCSC), and follows engagement
consumer associations and academia. The Code was first published in draft in March
2018 as part of the Secure by Design report.

Introduction

The Internet of Things (IoT) brings great opportunities for people. But a significant number of devices on the market today have been found to lack basic security measures. People should be able to benefit from connected technologies safely, confident that adequate security and privacy measures are in place to protect their online activity.

This Code of Practice sets out practical steps for IoT manufacturers and other industry stakeholders to improve the security of consumer IoT products and associated services. Implementing its thirteen guidelines will contribute to protecting consumers' privacy

Senate Bill No. 327

CHAPTER 886

An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy.

[Approved by Governor September 28, 2018. Filed with Secretary of State September 28, 2018.]

LEGISLATIVE COUNSEL'S DIGEST

SB 327, Jackson. Information privacy: connected devices.

Existing law requires a business to take all reasonable steps to dispose of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable. Existing law also requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Existing law authorizes a customer injured by a violation of these provisions to institute a civil action to recover damages.

This bill, beginning on January 1, 2020, would require a manufacturer of a connected device, as those terms are defined, to equip the device with a reasonable security feature or features that are appropriate to the nature and function of the device, appropriate to the information it may collect, contain, or transmit, and designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure, as specified.

This bill would become operative only if AB 1906 of the 2017–18 Regular Session is enacted and becomes effective.

Vote: majority Appropriation: no Fiscal Committee: yes Local Program: no

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1. Title 1.81.26 (commencing with Section 1798.91.04) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.26. Security of Connected Devices

1798.91.04. (a) A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:

(1) Appropriate to the nature and function of the device.

Senate Bill No. 327

CHAPTER 886

An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy.

[Approved by Governor September 28, 2018. Filed with Secretary of State September 28, 2018.]

SECTION 1. Title 1.81.26 (commencing with Section 1798.91.04) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.26. Security of Connected Devices

1798.91.04. (a) A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:

(1) Appropriate to the nature and function of the device.

(2) Appropriate to the information it may collect, contain, or transmit.

(3) Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure.

(b) Subject to all of the requirements of subdivision (a), if a connected device is equipped with a means for authentication outside a local area network, it shall be deemed a reasonable security feature under subdivision (a) if either of the following requirements are met:

(1) The preprogrammed password is unique to each device manufactured.

(2) The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time.

Vote: majority Appropriation: no Fiscal Committee: yes Local Program: no

THE PEOPLE OF THE STATE OF CALIFORNIA DO ENACT AS FOLLOWS:

SECTION 1. Title 1.81.26 (commencing with Section 1798.91.04) is added to Part 4 of Division 3 of the Civil Code, to read:

TITLE 1.81.26. Security of Connected Devices

1798.91.04. (a) A manufacturer of a connected device shall equip the device with a reasonable security feature or features that are all of the following:

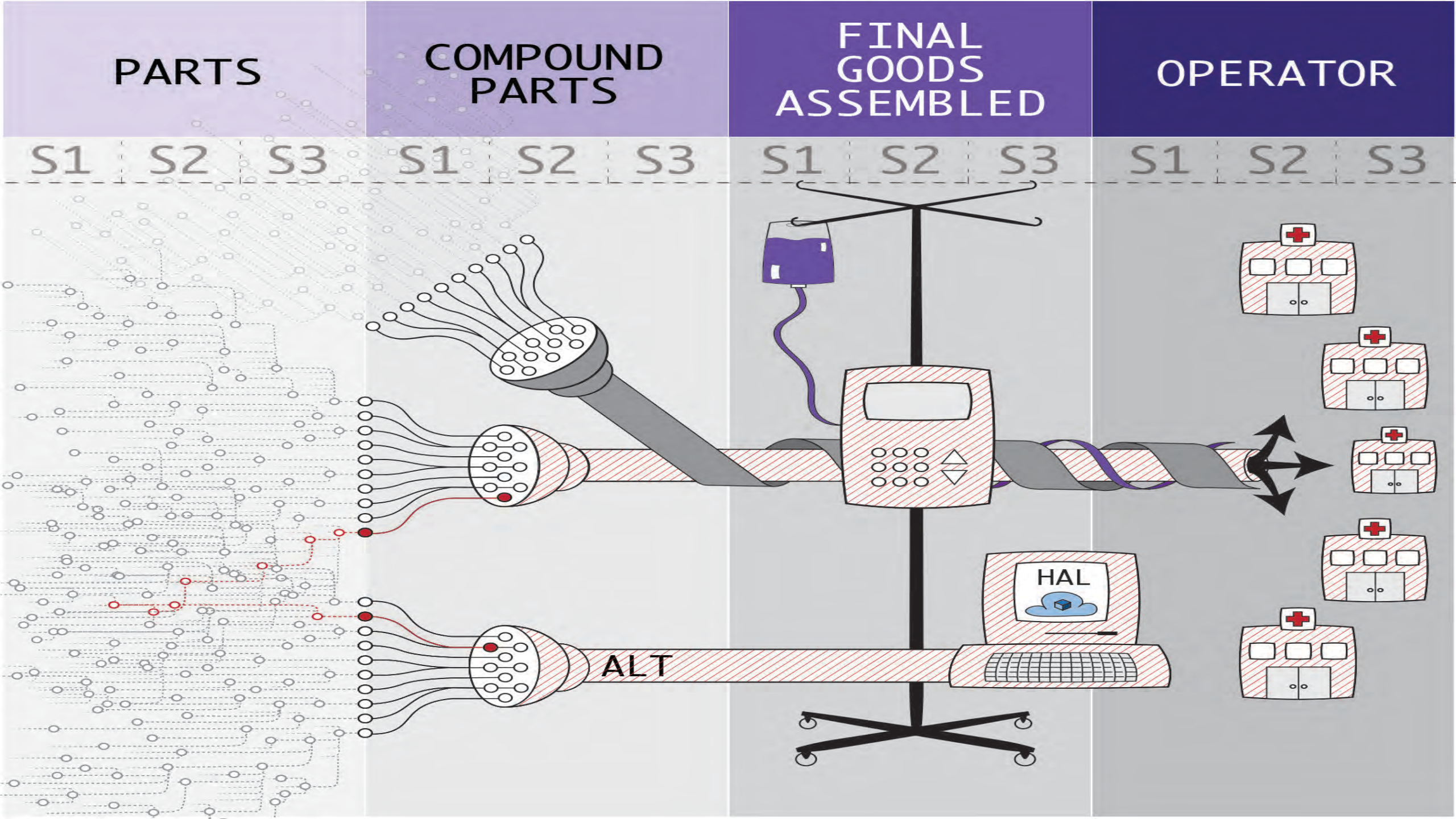
(1) Appropriate to the nature and function of the device.

OWASP 2018
Internet of Things Top 10

I1	**Weak, Guessable, or Hardcoded Passwords**	Use of easily bruteforced, hardcoded, publicly available, and/or unchangable passwords in client-side software/firmware that can grant unauthorized access to deployed systems.
I2	**Insecure Network Services / Protocols**	Unneeded and/or insecure listening/active network services—especially those exposed to the internet—that compromise confidentiality, integrity, or availability/authenticity of information or allow unauthorized remote remote control, e.g., Telnet, WiFi, ZigBee, Bluetooth, FTP, SSH, UPnP, etc.
I3	**Insecure Access Interfaces**	Insecure web, backend API, cloud, or mobile interfaces that allow compromise of the product and/or its ecosystem. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.
I4	**Use of Insecure or Outdated Components**	Use of deprecated and insecure software components/libraries. Insecure customization of operating systems, and use of third-party software or hardware components from compromised supply chain.
I5	**Lack of Secure Update Mechanism**	Lack of ability to securely update the device/ecosystem, lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anit-rollback mechanisms, lack of notifications of security changes due to updates.
I6	**Insufficient Privacy Protection**	User's personal information stored insecurely on device, is used insecurely, improperly, and/or without permission in logs and other artifacts, is transmitted insecurely over the network or the internet, or the system lacks adequate privacy disclosure before usage.
I7	**Insecure Data Transfer and Storage**	Lack of security of sensitive data at rest, in transit, or during processing e.g., weak or lacking cryptography, mismanagement of keys, inefficient platform access controls, insufficient key rotation, absence of secure hardware backed storage.
I8	**Lack of Physical Hardening**	Lack of physical anti-tampering defenses and/or lack of system integrity checking that allows potential attackers to gain sensitive information that can help with a future remote attack.
I9	**Insufficient Security Configurability**	A lack of vendor-provided product features to help the user secure the device through configuration, e.g., stronger authentication, logging and monitoring, encryption strength management, granular policy management, etc.
I10	**Lack of Device Management**	Lack of security support on existing devices deployed in production, including asset management, update management, and secure decommissioning.

I1	**Weak, Guessable, or Hardcoded Passwords**	Use of easily bruteforced, hardcoded, publicly available, and/or unchangable passwords in client-side software/firmware that can grant unauthorized access to deployed systems.
I2	**Insecure Network Services / Protocols**	Unneeded and/or insecure listening/active network services—especially those exposed to the internet—that compromise confidentiality, integrity, or availability/authenticity of information or allow unauthorized remote remote control, e.g., Telnet, WiFi, ZigBee, Bluetooth, FTP, SSH, UPnP, etc.
I3	**Insecure Access Interfaces**	Insecure web, backend API, cloud, or mobile interfaces that allow compromise of the product and/or its ecosystem. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.
I4	**Use of Insecure or Outdated Components**	Use of deprecated and insecure software components/libraries. Insecure customization of operating systems, and use of third-party software or hardware components from compromised supply chain.
I5	**Lack of Secure Update Mechanism**	Lack of ability to securely update the device/ecosystem, lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anit-rollback mechanisms, lack of notifications of security changes due to updates.
I6	**Insufficient Privacy Protection**	User's personal information stored insecurely on device, is used insecurely, improperly, and/or without permission in logs and other artifacts, is transmitted insecurely over the network or the internet, or the

I5	**Lack of Secure Update Mechanism**	Lack of ability to securely update the device/ecosystem, lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anit-rollback mechanisms, lack of notifications of security changes due to updates.
I6	**Insufficient Privacy Protection**	User's personal information stored insecurely on device, is used insecurely, improperly, and/or without permission in logs and other artifacts, is transmitted insecurely over the network or the internet, or the system lacks adequate privacy disclosure before usage.
I7	**Insecure Data Transfer and Storage**	Lack of security of sensitive data at rest, in transit, or during processing e.g., weak or lacking cryptography, mismanagement of keys, inefficient platform access controls, insufficient key rotation, absence of secure hardware backed storage.
I8	**Lack of Physical Hardening**	Lack of physical anti-tampering defenses and/or lack of system integrity checking that allows potential attackers to gain sensitive information that can help with a future remote attack.
I9	**Insufficient Security Configurability**	A lack of vendor-provided product features to help the user secure the device through configuration, e.g., stronger authentication, logging and monitoring, encryption strength management, granular policy management, etc.
I10	**Lack of Device Management**	Lack of security support on existing devices deployed in production, including asset management, update management, and secure decommissioning.


PARTS
COMPOUND PARTS
FINAL GOODS ASSEMBLED
OPERATOR
S1
S2
S3
S1
S2
S3
S1
S2
S3
S1
S2
S3
HAL
ALT

SHARED RESPONSIBILTIY MODEL

WHITE PAPER

ptc

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

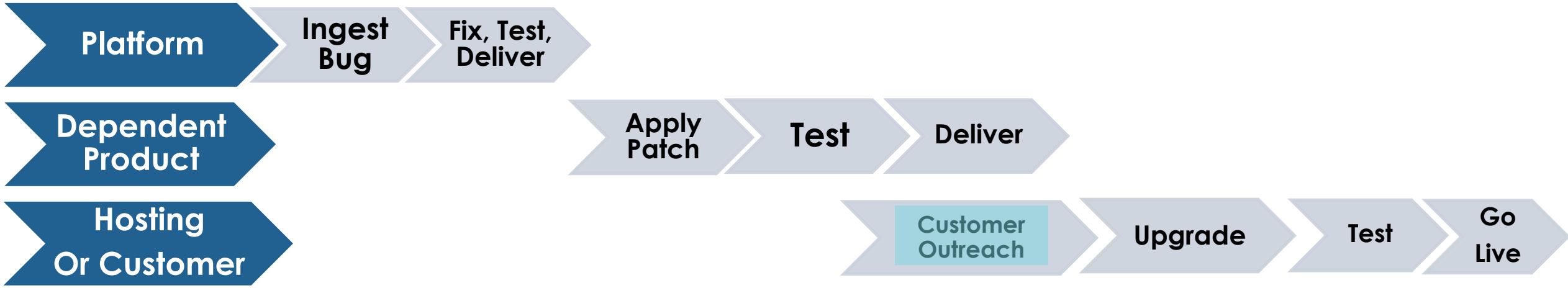
Page 1 of 9 | White Paper

ptc.com

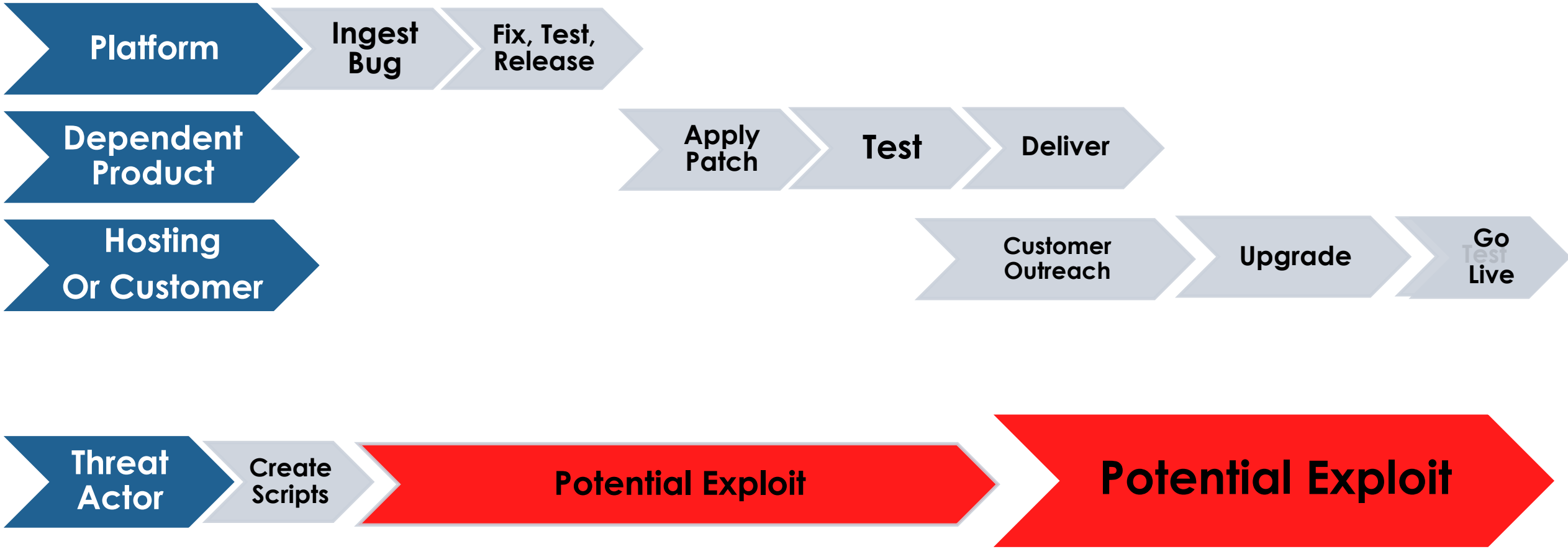
ptc | StanleyBlack&Decker

RSAConference2019

RACE TO A FIX


Platform
Ingest Bug
Fix, Test, Deliver
Dependent Product
Apply Patch
Test
Deliver
Hosting Or Customer
Customer Outreach
Upgrade
Test
Go Live

ADVERSARY


Platform
Ingest Bug
Fix, Test, Release
Dependent Product
Apply Patch
Test
Deliver
Hosting Or Customer
Customer Outreach
Upgrade
Go Live
Test
Threat Actor
Create Scripts
Potential Exploit
Potential Exploit


121
SKANSKA
BLOUP