

# Incorporating the Internet of Things (IoT) in your Strategy



**Michael J. Corby**  
*Executive Consultant*

**40**  
YEARS

**CGI**

Experience the commitment®

# Presentation Overview

The advances in providing internet connectivity to non-traditional devices poses a challenge to all security programs.

Breaches of security have already occurred when a non-traditional device introduces a vulnerability to a previously secured environment.

How can your security program be updated to accommodate connected devices including medical equipment, building environment controls, light bulbs, doorbells, automobiles and just about everything?

This session will present some process recommendations that address the incorporation of these advances in a security strategy.





**The Internet of Things** is a world where smart objects are seamlessly integrated as part of a global network; where smart objects interact with each other or the external environment to deliver new services or improved processes.

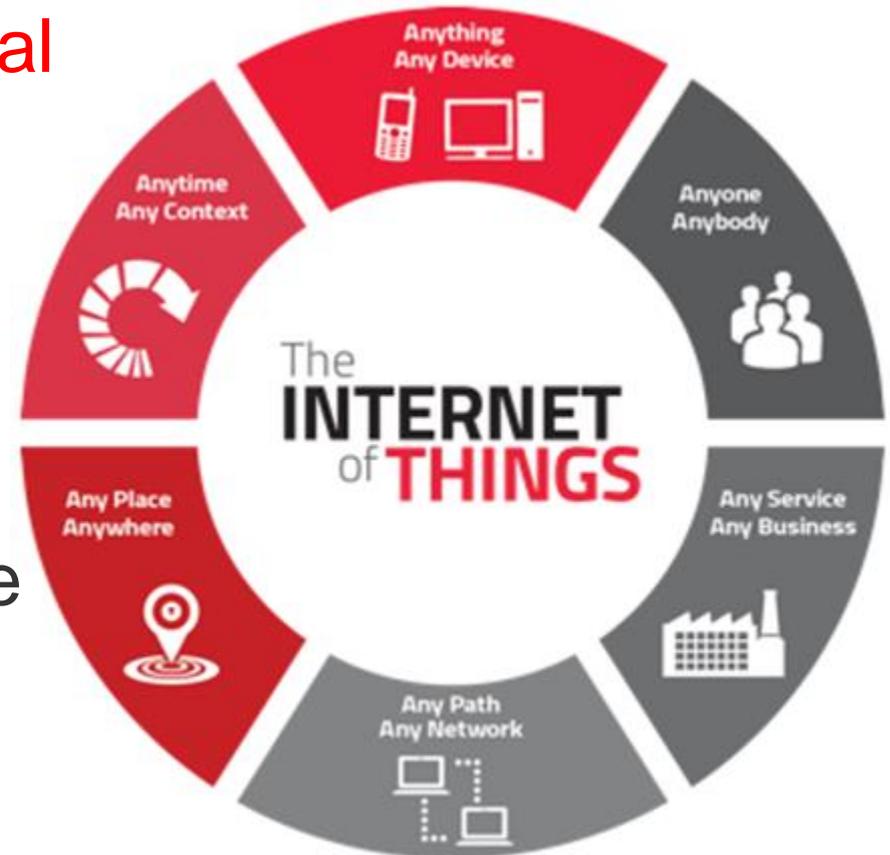
It redefines the way humans and machines interface and the way they interact with the world around them.

# IoT Can Transform Business Operation



# Introduction

- IoT connects the **Physical World** to the Internet
- **Devices** can come in all shapes, sizes and complexities.
- Common link among devices is that they have **program code** and internet **addresses**.



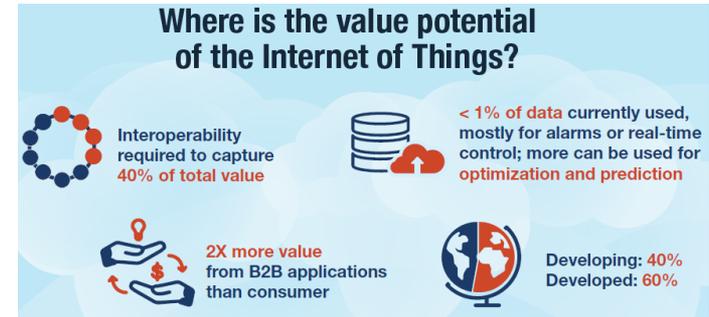
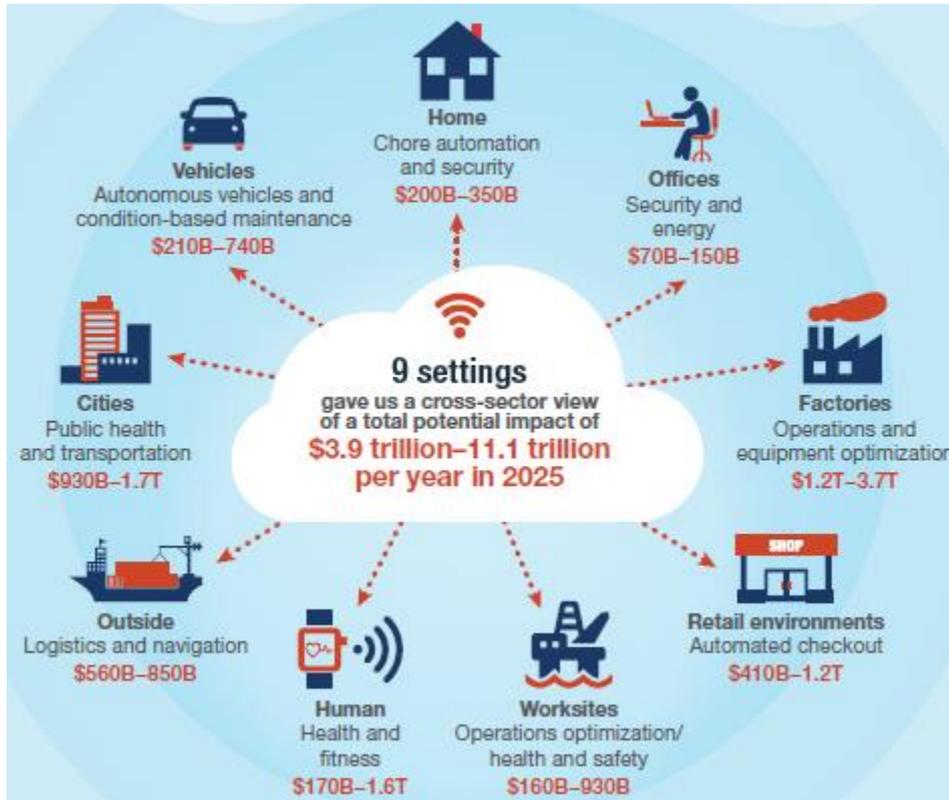
# Predictions of Growth Driven by Business Needs



“IOT PROVIDES THE DATA NEEDED FOR THESE GOALS”



# McKinsey (and other analysts) Forecast the Internet of Things will Drive significant Value

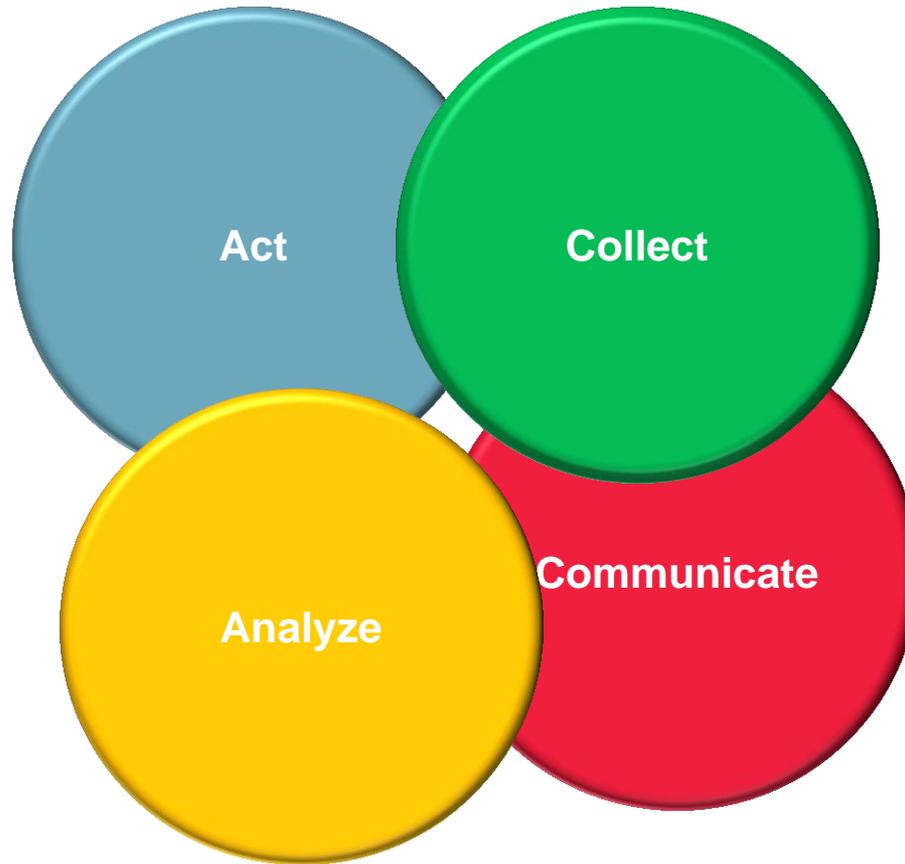


**This amounts to a projected 11% of the global economy for 2025**



Source: McKinsey Global Institute, 2015: Unlocking of the potential of the Internet of Things

# IoT Can Offer Several Solutions



Success requires integration of diverse environments



# So if the IoT makes good business sense, what are the risks?



40  
YEARS

**CGI**

Experience the commitment®

# Eight “Big” IoT Business and Technology Risks

1. Devices may have been developed using obsolete, obscure or untrusted O/S and program languages
2. Actions can happen offline independent of connectivity (confounding any attempts to monitor operation).
3. Devices can be purchased outside of the customary IT controls.
4. Devices can be cloned or added to an existing network.
5. Data can be redirected to unauthorized locations.
6. Activities on IoT devices can affect the entire network and infrastructure.
7. Program code can be deleted or altered without authority.
8. Devices can be operated by users with limited skills and abilities



# Obsolete or non traditional architecture - Items 1 & 2



- Devices may have been developed using obsolete, obscure or untrusted O/S and program languages
- Actions can happen offline independent of connectivity (confounding any attempts to monitor operation).

# Operational Environment

## Development = Operating Environment

Old versions of Linux, Windows, Android, “phone”, etc.

## Other untraditional IoT Operating Systems

 RIOT	 GOOGLE BRILLO OS	 CONTIKI	 APPLE HOMEKIT
 ARM MBED	 THINGSQUARE	 TINY OS	 PARTICLE

Experience in applying Patches and Fixes?



# Part-Time Connectivity

- One major benefit of IoT is that the devices contain programmed intelligence capable of operating without connection.
- This benefit comes with the risk of the device doing something incorrect/improper, or even to stop operating entirely.
  - Cause could be purposeful or malicious
  - Could be an undiagnosed “bug” or equipment error
- Configuration and communications changes are more complicated and must be coordinated over a wider range of components.



# Options for Risk Remediation

1. Determine the Operating Environment best suited for IoT devices.
  - Set technology limits or create “approved IoT infrastructure” standard
  - Program language and coding standards
  - Define and enforce operational logs (i.e. on/off times, data transfer volumes, actions taken, etc.)
2. Review all IoT components and replace/upgrade/convert to set of accepted technology standards.
3. Require each device have a periodic connection for upgrades, operation validation, error/bug remediation, operating statistics, patches and software upgrades



# Acquisition channel not accustomed to operational risk – Item 3



- Devices can be purchased outside of the customary IT controls.

# Separation from Company Policy

1. After many years and countless heated discussions, I/T devices and software has commanded a specialty within purchasing.
    - Price is not the only differentiator
    - IT components require maintenance/upgrades
    - Self-modification may be limited
    - Liability may be very limited
  2. IoT components may not be recognized as I/T based
    - Data collectors, infusers/injectors/adjustors, notifiers are often “stealthy” computers
- Solution to #1 is to include IT in the purchase decisions
  - Can I/T respond with knowledge to items in #2?

# Options for Risk Remediation

1. Create a sub-department of Purchasing/Acquisition to determine if a device is internet capable based on product specifications
2. Educate I/T research or technical staff on the specifics of determining whether the prospective vendor uses good practice for device programming, maintenance and error reporting/resolution
3. Update purchasing Standard Terms and Conditions to identify IoT device impact and remove liability limitations



# Integration of IoT into a semi-stable environment – Items 4, 5, & 6



- Devices can be cloned or added to an existing network.
- Data can be redirected to unauthorized locations.
- Activities on IoT devices can affect the entire network and infrastructure.

# The Cost of Failure

- The device fails
  - Someone dies or is physically harmed (i.e. Heart Pacemaker)
  - An error condition is missed and corrective response is absent (i.e. Trains on collision course)
  - A process is aborted (i.e. a “domino” is misplaced and the reaction stops)
- The rest of the infrastructure is compromised
  - The device has security weaknesses and introduces compromise (i.e. “smart” doorbell)
  - The device explicitly connects to other infrastructure components and contaminates secure operation (i.e. HVAC monitors inject Credit Card data skim & export)
  - Errors in the device overrun network performance (i.e. verbose loop in set-up or diagnostic code)



# Options for Risk Remediation

1. Make certain that version of software code is validated as often as feasible.
2. Utilize a “heartbeat” process to assure that continuously operating devices do not shut down
3. Run an activity log to determine if device is being used, and for infrequent use, initiate a “wakeup and check” feature.
4. Consider only acquiring devices that are physically tamper-proof (disabled if seal is broken) and demand encrypted independent channel transfer of command sequences.
5. Be able to immediately find, stop, & disconnect rogue devices via an alternate channel.
6. Number all messages to that out of sequence or missing numbers can be investigated.



# Operation beyond the bounds of IT management – Items 7 & 8



- Program code can be deleted or altered without authority.
- Devices can be operated by users with limited skills and abilities

# Operation (or modification) by a novice/nobody

Recent Facebook story on a diabetes patient that hacked their monitor:

<http://motherboard.vice.com/read/this-diabetes-activist-hacked-her-medical-device-and-made-an-artificial-pancreas>

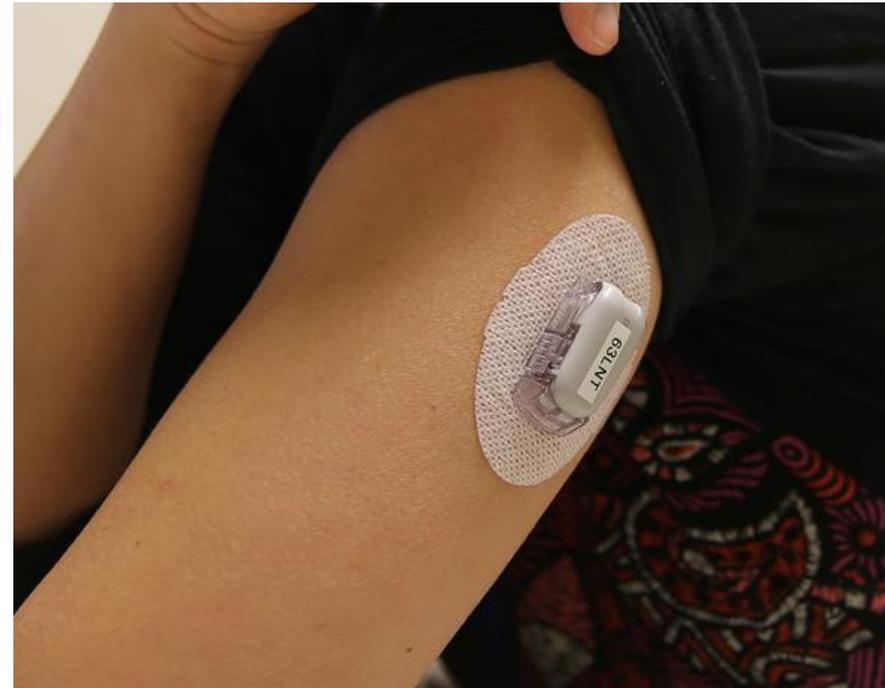
#medicaldevice #security #privacy #health



**This Diabetes Activist Hacked her Medical Device and Made an Artificial Pancreas**

Activists are hacking medical devices to free the data.

MOTHERBOARD.VICE.COM



# Options for Risk Remediation

1. Harden the device environment so that modifications and rogue “enhancements” are limited.
2. Develop awareness training materials, video, printed, etc. at 3 levels:
  - End User
  - Customer Support (Help Desk)
  - Core Development and Operations

Purpose is to educate and inform how to use/operate and more importantly, how to recognize and respond to incidents.

3. Solicit customer/user suggestions and offer incentives to assist in device and service improvements and simplify user operations.



# Summary of Solutions to Explore



40  
YEARS

**CGI**

Experience the commitment®

# Technology/Infrastructure

1. Determine the Operating Environment best suited for IoT devices.
  - Set technology limits or create “approved IoT infrastructure” standard
  - Program language and coding standards
  - Define and enforce operational logs (i.e. on/off times, data transfer volumes, actions taken, etc.)
2. Review all IoT components and replace/upgrade/convert to set of accepted technology standards.
3. Require each device have a periodic connection for upgrades, operation validation, error/bug remediation, operating statistics, patches and software upgrades



# Acquisition

1. Create a sub-department of Purchasing/Acquisition to determine if a device is internet capable based on product specifications
2. Educate I/T research or technical staff on the specifics of determining whether the prospective vendor uses good practice for device programming, maintenance and error reporting/resolution
3. Update purchasing Standard Terms and Conditions to identify IoT device impact and remove liability limitations



# Operations Monitoring

1. Make certain that version of software code is validated as often as feasible.
2. Utilize a “heartbeat” process to assure that continuously operating devices do not shut down
3. Run an activity log to determine if device is being used, and for infrequent use, initiate a “wakeup and check” feature.
4. Consider only acquiring devices that are physically tamper-proof (disabled if seal is broken) and demand encrypted independent channel transfer of command sequences.
5. Be able to immediately find, stop, & disconnect rogue devices via an alternate channel.
6. Number all messages to that out of sequence or missing numbers can be investigated.

# Awareness and Training

1. Harden the device environment so that modifications and rogue “enhancements” are limited.
2. Develop awareness training materials, video, printed, etc. at 3 levels:
  - End User
  - Customer Support (Help Desk)
  - Core Development and Operations

Purpose is to educate and inform how to use/operate and more importantly, how to recognize and respond to incidents.

3. Solicit customer/user suggestions and offer incentives to assist in device and service improvements and simplify user operations.



# Other General Recommendations

## Environment for Testing

- The IoT test environment is similar to the BYOD test environment. A robust and “deep” test environment with a solid sandbox for investigating issues and conducting research.
- Be prepared to act quickly on device updates and recalls, if necessary, when (not if) issues occur or problems persist.

## Incident Response

- Because of the severity of risks that can be exploited, incident reporting, containment and response has an extraordinarily high priority. The best way to improve incident response is to conduct frequent training and practice, practice, practice. Look at the rigorous emergency response simulation models that have been effective in airports, fire departments, civil defense, law enforcement communities.



# Comments, Questions, Challenges



40  
YEARS

**CGI**

Experience the commitment®

# Placing IoT at the Center of Digital Transformation



Contact:



**Michael J. Corby, CCP, CISSP, CBCP, PMP, SAFe**  
Executive Consultant

[Michael.Corby@cgi.com](mailto:Michael.Corby@cgi.com)

+1 508-892-2980

