Be in a defensible position.

Be cyber resilient.
Agenda

• Why Are We Here?
• Introduction to Internet of Things (IoT)
• IoT Risks
• Fun Facts
• IoT Hacking
• What can be done?
• Questions???
Why Are We Here

- IoT is already an immense footprint with billions of points of presence on the Internet and it is only expected to grow at an ever increasing rate

- Organizations not always aware of what is on their own networks; people not always aware of use in daily life

- Leading to an equally immense potential attack surface as many of these devices are unsecured out-of-the-box

- Little to no regulation but awareness is growing
  - How can we address the security risks IoT devices represent
  - What can we do to drive towards a better IoT future
What is the Internet of Things (IoT)?

Everyday devices and systems (i.e., things) are connected to the internet through low-cost sensors. Devices can autonomously take action based on real-time data, processes, and information. Interconnected devices collect environmental and behavioral data that can help generate timely business decisions and improve customer interactions.
IoT (by the numbers)

2025 IoT Usage Forecast:
- More company revenue from sales of services than products
- Over 10% of electricity will be micro-generated by consumers and contributed to the Smart Grid.
- At least 5 countries will target “zero road fatalities,” relying on connected cars and smart road infrastructure to prevent accidents.

Mobile Devices

2015: 13B
2020: >34B*

Connected Automobiles

2015: 370M
2020: 3.5B*

Connected Wearables

2020: >43 Million
2020: 2 to 6

Smart Homes

2015: 300M
2020: 1B*


*Analyst forecasts vary significantly in methodology and IoT definition
IoT (by the numbers)

- The IoT ecosystem has more stakeholders than traditional products.
- Each stakeholder has a specific perspective paired with a cost/benefit.
- Who is focused on the bigger picture? Who is following the life of the data?
- Is anyone focused on building consumer trust through security, safety, and privacy?

Focus Areas
- Product functionality
- Design and consumer engagement
- Product adoption and platform promotion / preservation
- Telematics architecture
- Availability and connectivity
- Cost-focused service offerings and infrastructure management
- Product reliability and usability
- Dynamic user experience
- Privacy of personal information
- Brand loyalty and trust

Creator
Consumer
Enabler

© 2017 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.
IoT Public Sector

- Why would the public sector want to invest in IoT?
  - Create cleaner cities
  - Deliver better healthcare
  - Make transportation systems safer
  - Conserve water
  - Boost productivity
  - Have IoT work for the everyday citizen

*Analyst forecasts vary significantly in methodology and IoT definition

- KPMG’s IoT Security survey demonstrated increased focus and concern from Boards of Directors
- Emphasis on foundational Security/Privacy by Design; layered throughout product lifecycle
- Third-party risk management viewed as largest threat to IoT ecosystem

IoT users and their boards are becoming increasingly concerned about the risk of cyber attack on their IoT solutions

Source: KPMG cyber security and IoT Survey

How concerned is your firm’s board about the threat of cyber-attacks involving your IoT solutions?
Stakeholder perspectives

– The IoT ecosystem has more stakeholders than traditional products
– Each stakeholder has a **specific perspective** paired with a **cost/benefit**
– Who is focused on the bigger picture? Who **is following the life of the data**?
– Is anyone focused on building **consumer trust** through security, safety, and privacy?

---

**Creator**

- Product functionality
- Design and consumer engagement
- Product adoption and platform promotion / preservation

**Enabler**

- Telematics architecture
- Availability and connectivity
- Cost-focused service offerings and infrastructure management

**Consumer**

- Product reliability and usability
- Dynamic user experience
- Privacy of personal information
- Brand loyalty and trust
IoT introduces new risks

- The exponentially growing connected ecosystem is creating new challenges for organizations to manage
- Market innovation continues to invent new ways for devices, people, and the cloud to talk to one another, creating a moving target for developers, and security and risk professionals
- IoT has impacts on various risk domains, notably security, privacy and safety, which all impact trust

### Examples of IoT Impacts on Risk Domains

<table>
<thead>
<tr>
<th>Security</th>
<th>Privacy</th>
<th>Safety</th>
</tr>
</thead>
<tbody>
<tr>
<td>— Denial of service attack,</td>
<td>— Release of location history</td>
<td>— GPS location tampering to facilitate robbery,</td>
</tr>
<tr>
<td>causing disruption of communications</td>
<td>— Release of personal data stored on a device or in</td>
<td>ambush, etc.</td>
</tr>
<tr>
<td>— Spoofing a device to take</td>
<td>the cloud, with the potential for blackmail</td>
<td>— Medical device tampering, causing negative</td>
</tr>
<tr>
<td>control or exfiltrate data.</td>
<td>— Release of corporate data/trade secrets</td>
<td>impact to health/life.</td>
</tr>
<tr>
<td>— Theft of device to gain foothold</td>
<td></td>
<td>— Sensor tampering, causing vehicle crash,</td>
</tr>
<tr>
<td>into an IoT ecosystem</td>
<td></td>
<td>robot malfunction, nuclear accident, etc.</td>
</tr>
</tbody>
</table>

### Examples of IoT Incidents

| — Vehicle remotely controlled        | — Iran’s nuclear program damaged by Stuxnet       |
| — German steel mill boiler damaged  | — DDoS caused by IoT botnet                        |
| — DDoS caused by IoT botnet          | — Credit cards breached via HVAC                  |
KPMG’s understanding of IoT risks

• Our approach to understanding IoT risk is to evaluate devices and their interconnections within, their ecosystem based on the risk domains of security, privacy, trust, and safety. When assessing an IoT device from these four domains, we identify risks from three perspectives:

  – Device: Is it a smart device? Or is it simple? Is the device able to perform complex tasks and provide data? Does the device perform automated tasks, based on sensor data?

  – Ecosystem: Is the device part of an open standard? Does it work with multiple types of systems? Does it need to interact with third parties? Is the network isolated?

  – Environment: Is the device used in a consumer, industrial, or enterprise context? Is the device mobile? Is it required to be in a public area to record data?

• By considering these perspectives, KPMG is able to form a threat landscape specific to an IoT product, enabling further evaluation of risks and controls within an organization’s IoT program.

SPST = Security, Privacy, Safety and Trust
Simply Put: People are worried about IoT

- ...and they should be – the security track record for IoT devices is horrendous
- Convenience leads to compromising the security of more critical systems
- The people building these devices – don’t know how they’re hacked.

### Americans Concern For Smart Home Device Data Breaches

Q: How concerned are you about the possibility of a smart home data breach and your information getting stolen?

- Very Concerned
- Somewhat Concerned

<table>
<thead>
<tr>
<th>Age Group</th>
<th>Very Concerned (%)</th>
<th>Somewhat Concerned (%)</th>
</tr>
</thead>
<tbody>
<tr>
<td>All Americans</td>
<td>71</td>
<td>44</td>
</tr>
<tr>
<td>25-34</td>
<td>69</td>
<td>39</td>
</tr>
<tr>
<td>35-44</td>
<td>71</td>
<td>39</td>
</tr>
<tr>
<td>45-54</td>
<td>73</td>
<td>45</td>
</tr>
<tr>
<td>55-64</td>
<td>82</td>
<td>51</td>
</tr>
<tr>
<td>65+</td>
<td>68</td>
<td>46</td>
</tr>
</tbody>
</table>

Source: Icontrol State Of The Smart Home, 2015
Why attack systems that have security – if there’s tons without?

- PC’s have security software, does your thermostat or car?
- IoT: Small system – less ability to update
- No commitment to patching
- Do you know what data is leaking out
If security vendors can’t get it right, what makes IoT vendors think they can?

- IoT vendors shouldn’t build things without first understanding how they can be broken into
- What risk are you bringing into your organization?

If security vendors can’t get it right, what makes IoT vendors think they can?

– BTW – that’s a Raspberry Pi in there... (>_<)
Getting Intel – IoT Scanning Tools
KPMG thought leadership

Additional IoT related resources available for download at KPMG Global

KPMG Connected Devices Portal

Security and the IoT ecosystem

Automotive

Your connected car is talking. Who’s listening?

Test-driving vehicle cybersecurity

Healthcare

The time to address medical device cybersecurity is now
Questions?
Thank you

KPMG’s Cyber Team works with organizations to prevent, detect and respond to cyber threats.

We can help your organization be cyber resilient in the face of challenging conditions.

• Contact us

Manager, Cyber Security
T: 250 589 2538
E: grosario@kpmg.ca