BI INTELLIGENCE

BII Internet of Things

THE IoT SECURITY REPORT: Securing new connected devices against cyber attacks

Jonathan Camhi | December 16, 2015

BUSINESS INSIDER

THE IoT SECURITY REPORT: Securing new connected devices against cyber attacks

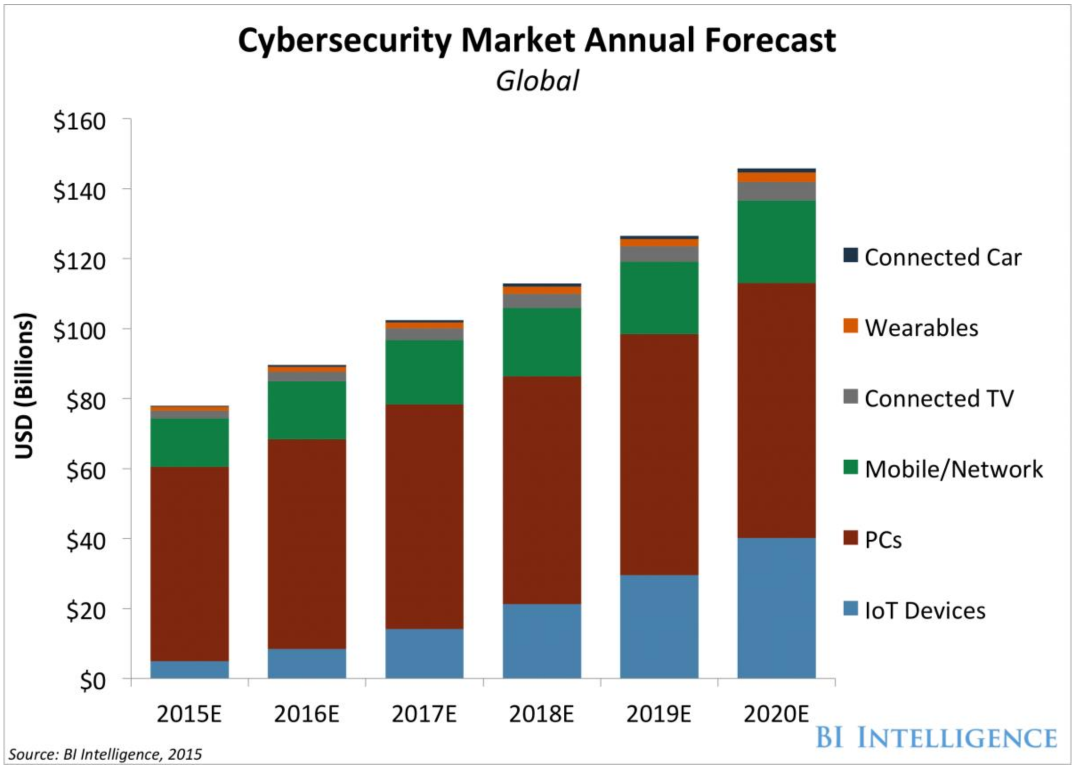
Jonathan Camhi | **December 16, 2015**

KEY POINTS

- **Research has repeatedly shown that many IoT devices currently on the market lack basic security measures like data encryption, which leaves them vulnerable to hackers.**
- **Hackers can leverage compromised IoT devices for an array of criminal acts,** creating a large incentive for hackers to attack these devices as they proliferate.
- **As these new connected devices become more widespread over the next few years, it will lead to increased investment in IoT security.** We predict that $118 billion will be spent on securing IoT devices and systems between 2015 and 2020.
- **A combination of different measures can be used to protect IoT devices from being compromised or used as an entry point to infiltrate government or corporate networks.** The measures are based on the individual device's computing capabilities and the networks it communicates with.

Download the charts and data in Excel »

A new cyber threat



Source: BI Intelligence, 2015

Cybersecurity has become a major concern over the last few years as hackers have penetrated the IT infrastructure of governments and enterprises with increasing frequency and sophistication. The growth of the IoT takes this concern to a whole new level: **When everything is connected to the internet, everything becomes a potential target for hackers.** It means hackers can use newly connected devices to gain entry and take control of government and enterprise networks.

This new problem was brought to the public's attention with a string of connected car hacks this summer. These hacks show how connected devices could be exploited to cause physical damage. In the most highly publicized of these hacks, two security researchers were able to remotely take command of a Jeep's steering and transmission while the car was traveling at 70 miles per hour on the highway.

Beyond these connected car hacks, security researchers have found a wide range of vulnerabilities in other common IoT devices, including wearables and smart home devices. Simply put, IoT device manufacturers and systems providers have too often failed to take the necessary precautions to secure products, despite the high risks in connecting these devices.

In this report, we forecast the size of the market for solutions that help secure IoT devices, and explain why IoT devices are often extremely vulnerable to hackers, why hackers would be motivated to attack IoT devices, and how such attacks can be prevented.

The current landscape

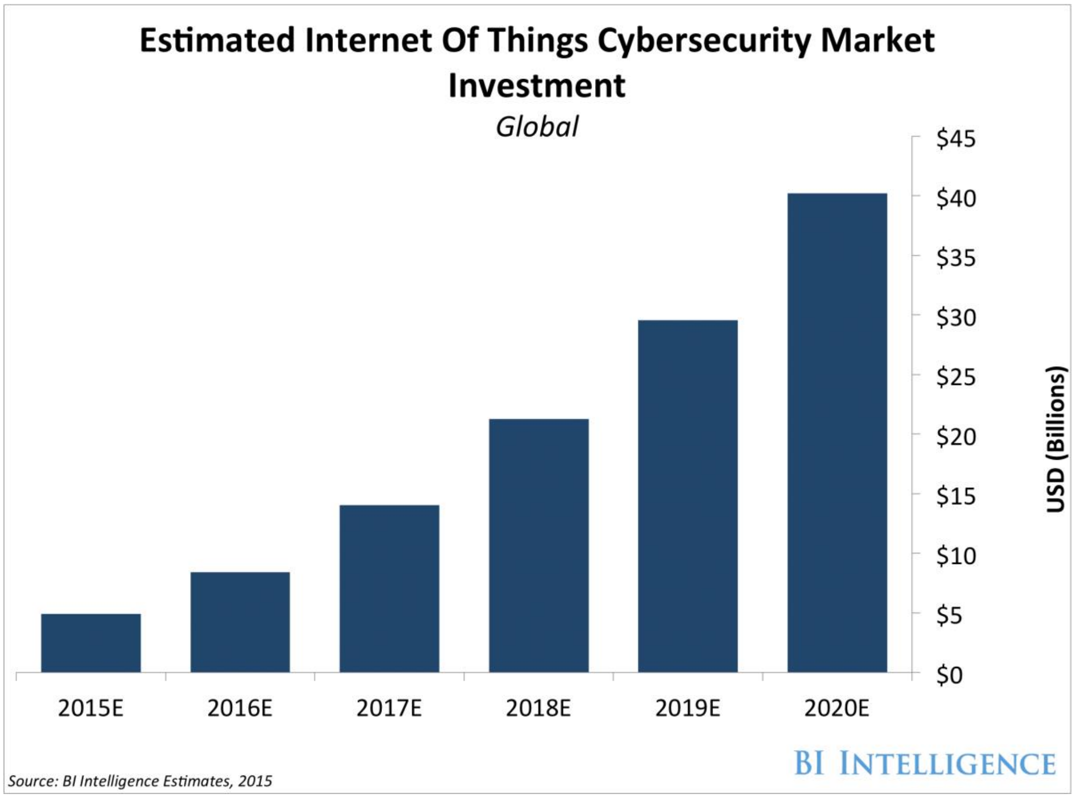
The past year of hacks and studies has shown that IoT devices often have little-to-no protection against intrusions by hackers. For example, one study earlier this year conducted by security firm Veracode looked at six smart home devices currently on the market. Five of the six devices failed to require strong passwords or use authenticated encryption to keep hackers from intercepting data sent by the devices, according to the study. **The study indicated that the devices typically lacked these basic protections because IoT device manufacturers often rush their products to market, so they don't take the time to implement security protections.**

This problem is common across many different segments of the IoT. Since the IoT is in its infancy in terms of adoption, device manufacturers want to rush their products to market to get ahead of the accelerating adoption of IoT devices that everyone expects in the years to come. Testing new products for security vulnerabilities and implementing necessary protections take time and money, so IoT device manufacturers often skip security entirely. Many IoT devices are made by startups, particularly in the smart home market, and many of these startups don't have any security professionals on staff to test and secure their products.

Another systemic reason for security vulnerabilities in IoT devices is that so many companies in the IoT lack cybersecurity experience. Many established companies in the automotive, manufacturing, and mining sectors that have traditionally produced or dealt with nonconnected machines now face serious cybersecurity threats as those machines are connected to the internet. However, few of them have experience with security practices, like network monitoring and penetration testing, that are common in the banking and technology industries.

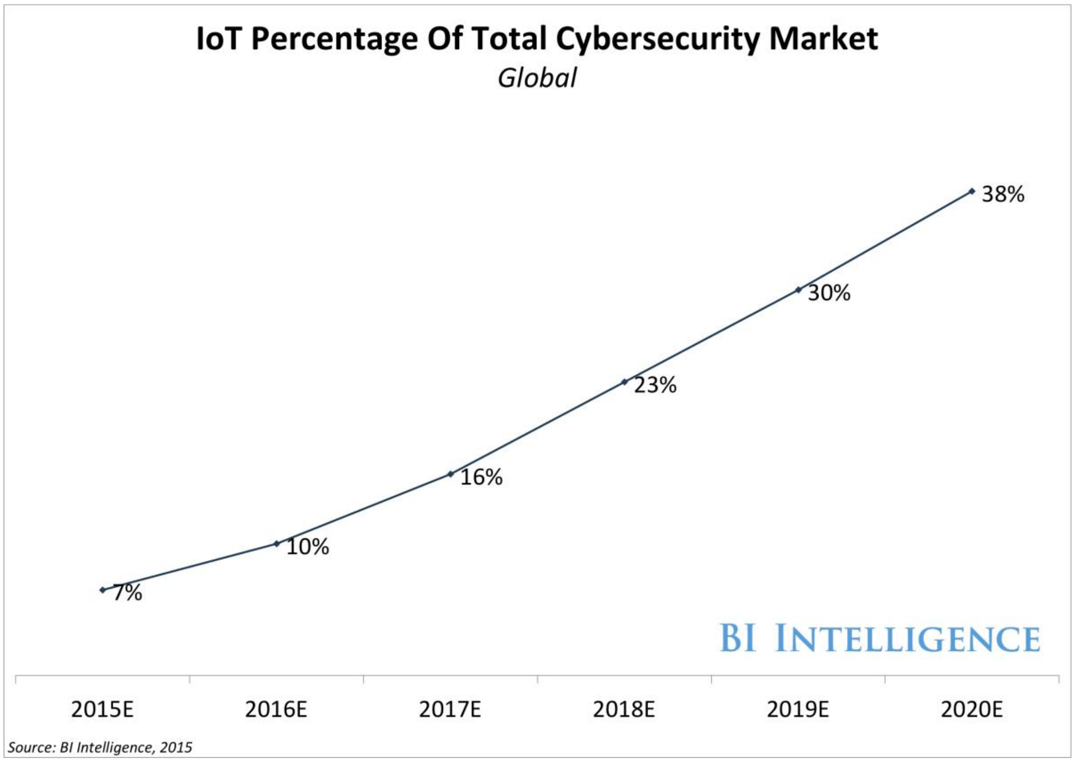
Despite the widespread vulnerabilities that have been found in IoT devices, there have been few attacks conducted by bad actors against IoT devices. Right now the vast majority of spending on cybersecurity is dedicated to securing traditional PCs and servers, as these are the most common vectors of attack for today's cyber criminals. We expect this will change soon: As billions of IoT devices are connected to the internet, hackers will take notice of the opportunities that those billions of new entry points represent. When hackers do take notice, device manufacturers and end users will respond by increasing their investment in securing IoT devices.

We forecast that investment in cybersecurity for IoT devices will increase from $5 billion in 2015 to $40 billion in 2020. That means $118 billion will be spent cumulatively between 2015 and 2020 on securing IoT devices against hackers.



Source: BI Intelligence Estimates, 2015

PCs will continue to receive the most cybersecurity spending of any device category, but IoT devices will grow to become the second-largest device category in terms of cybersecurity investment by 2017. **We expect that total cybersecurity spending will reach $140 billion in 2020, with 38% of that spend dedicated to securing IoT devices and systems.**



Source: BI Intelligence, 2015

Why hackers will target IoT devices

Research has shown that IoT devices are low-hanging fruit in terms of how vulnerable they are to common hacking methods. However, there is still a significant technical barrier to hackers exploiting IoT devices. Hackers have tailored their attacks for years to exploit systems commonly running on PCs and servers. They will need to tweak or tailor those attack methods to go after IoT devices since they often run on different systems than PCs or servers. For instance, a malware program designed specifically to attack computers running Microsoft Windows would likely have to be changed to exploit the operating systems on IoT devices.

So far hackers haven't had the incentive to do this: They are having plenty of success attacking traditional PCs and servers with proven attack methods.

However, as more IoT devices are connected throughout the world, we believe hackers won't be able to pass up the opportunities that these vulnerable devices offer them. Different types of hackers will be able to take advantage of vulnerable IoT devices in different ways to attain their objectives:

- **Hackers backed by nation-states have a clear motivation to exploit IoT devices.** If they learn how to exploit these devices, they could shut down an enemy country's infrastructure through a cyber attack. For example, if a state-backed hacker group can hack a smart meter, then they could potentially use that as an entry point to take down an entire electricity grid. Connected devices could be used to attack other types of infrastructure too: Connected manufacturing equipment or oil wells could be exploited to shut down factories and extraction sites. For instance, a cyber attack last year caused crippling damage to a blast furnace at a German steel factory. A nation with these types of attacks in its arsenal would have a distinct advantage over one without them. Cybersecurity experts we have spoken to suspect that most of the world's major countries are already working to acquire the knowledge to conduct such attacks. As damaging as an attack that targets critical infrastructure could be, it is also extremely unlikely that we will see such an attack on a large scale any time soon. A large-scale cyber attack on a country's critical infrastructure would likely be considered an act of war by the victim nation, putting the attacking nation at risk of a major armed conflict.

- **Cyber criminals** will likely use IoT devices as a new avenue to infiltrate IT networks and infrastructure to steal data that they can profit from. If a cyber criminal can hack a smart home device, they could then use that device to gain access to the home network and intercept data sent over that network, such as the homeowner's financial information. Similarly, a criminal could hack a connected device on a company's assembly line and then infiltrate the company's internal networks and databases to steal corporate data like intellectual property or customer information. In this way, IoT devices could be used to conduct major data breaches, like the Target and Home Depot attacks in recent years.

- **Hacktivists**, hackers who conduct cyber attacks to promote political or social causes, could also exploit IoT devices to cause physical damage or steal data. A cyber attack that shuts down a factory or disables an electricity grid would draw a great deal of media attention, and hacktivists are constantly looking to draw public attention to their causes. For instance, environmental hacktivists might look to damage or disable connected oil wells at an oil field to both damage production and garner headlines. Hacktivists could also gain public attention by using IoT devices to steal data from corporate or government entities that they're opposed to, and then publicly expose that data.

Securing IoT devices against attacks

A number of different measures can be employed separately or in unison to secure IoT devices based on where they are deployed, what other devices and systems they are connected to, and what kind of computing capabilities and memory they have to run security functions. For example, there is much greater risk for physical damage if a hacker takes control of a connected car than a smart meter, so connected cars need to have more safeguards in place to prevent hacking attempts. Here's an overview of the different aspects to device security that need to be considered when deploying IoT devices:

- **Hardening the device** — keeping the device itself free from malicious infections — starts with a secure boot. That means that when a device is opened and starts up for the first time, it should scan for possible viruses or malware before it starts communicating with the network it's connected to. Another useful device-hardening measure is a hypervisor, which segments different operating systems on a device, allowing a single device to simultaneously run multiple systems. So if a hacker gains access to a device, the hypervisor could prevent them from taking control of the device's different functions.

- **Data encryption** is obviously a core tenet of IT security, and any data stored on an IoT device needs to be encrypted to protect it from hackers. Device end users also need to ensure that the encryption keys for that data are hidden, so if a hacker gains access to a device he won't have the tools to access the data.
- **End users should also be able to filter and monitor the device's communications**. Filtering means they can set parameters around what other devices a given device can communicate with. That can block any attempt from a hacker's computer to communicate with the device. End users should also be able to monitor the traffic on the device, so if a device suddenly gets flooded with activity for no reason, it can be investigated.
- **Device management and visibility tools** enable companies to set security policies for their devices and remotely inspect them for possible intrusions.

Network monitoring and segmentation will also be crucial to stopping attacks that target IoT devices. That is because some IoT devices, particularly small, low-power devices like sensors and smart lights, don't have any memory or computing power to run any security measures on the device itself.

When the device itself can't be secured, measures need to be taken to ensure that a hacker can't use the vulnerable device to steal data by infiltrating networks that connect the device to crucial assets like databases that hold financial data. Any network that connects vulnerable IoT devices should be segmented off from such critical assets. Network segmentation segregates a network into sub-networks, allowing security controls to be implemented that prevent unauthorized individuals from moving between the sub-networks.

In addition to segmentation, governments and enterprises should also carefully monitor the traffic that comes from their networks that connect to vulnerable IoT devices. Traditionally, organizations have hired staff to keep an eye on their network traffic, but this role is increasingly performed by automated network monitoring software. Network monitoring allows an organization to spot strange activity on its networks that could indicate a breach. For instance, if an industrial control network in a factory starts communicating with the enterprise's IT network in an unusual pattern, the organization's security team can be alerted to investigate.

THE BOTTOM LINE

- **IoT device manufacturers are too often ignoring security to rush their products to market to cash in on the growth everyone expects in IoT adoption.**
- **IoT devices increase the risk associated with cyber attacks, as hackers could use them to cause new damage including destroying physical infrastructure.**
- **The diversity of IoT devices means that there is no one-size-fits-all solution to IoT security, as different devices will require different security measures.**
- **IoT security goes beyond securing the devices themselves — networks the devices communicate with must be monitored and segmented to thwart hackers.**

About BI Intelligence
BI Intelligence, a research service from Business Insider, provides in-depth insight, data, and analysis of everything digital. Our research is fast and nimble, reflecting the speed of change in today's business. We give you actionable insights that enable smarter and better-informed decision-making. We publish in-depth reports, news, and an exhaustive library of charts and data focusing on key areas of tech: mobile, e-commerce, digital media, payments, the Internet of Things, and more.

To learn more please visit: intelligence.businessinsider.com.