

Securing Enterprise Data in the Ever Connected Internet of Things



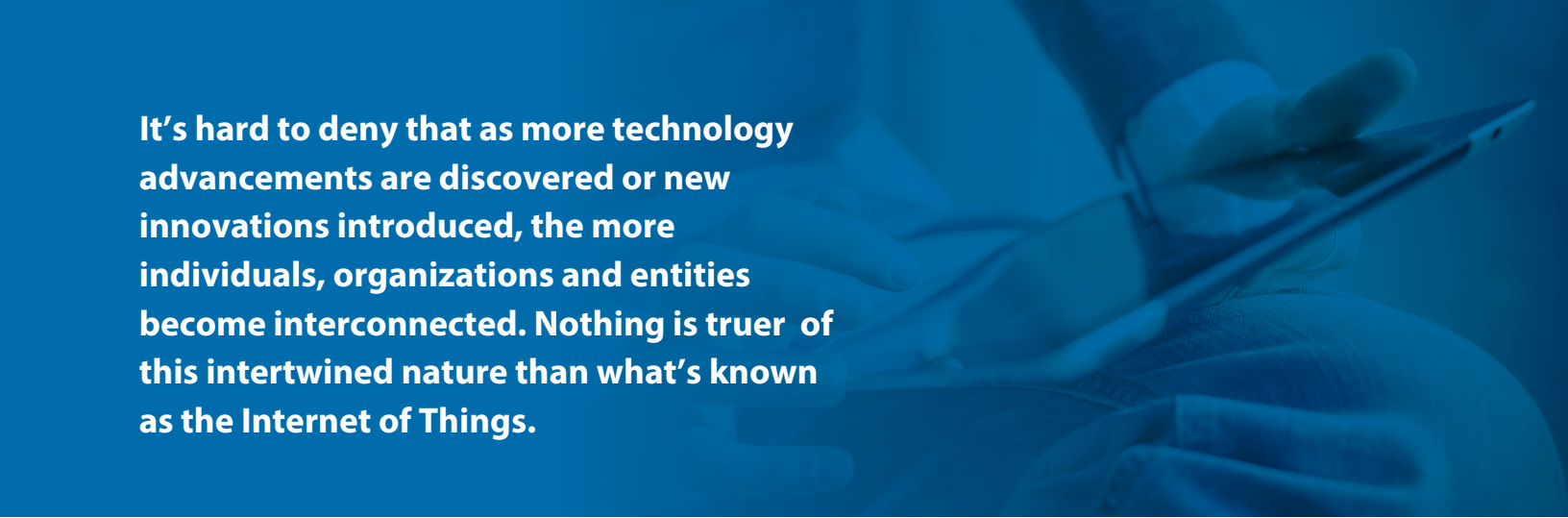
TABLE OF CONTENTS

Security Concerns with IoT3

4 Stages of IoT Data and its Movement5

Checklist for Minimizing Vulnerabilities Created by IoT Devices6

What’s Next for Data and IoT?6



It's hard to deny that as more technology advancements are discovered or new innovations introduced, the more individuals, organizations and entities become interconnected. Nothing is truer of this intertwined nature than what's known as the Internet of Things.

According to Gartner, the Internet of Things (IoT) is defined as “the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment.”

More often than not, IoT is thought of as a fitness tracker like a Fitbit or voice connected assistant devices like Amazon's Echo. While a number of early “things” are consumer devices, the potential impact on the enterprise is quickly becoming apparent. Let's take a look at some of the staggering numbers around IoT:

Research firm IDC expects global wearable device shipments to surge from 76.1 million in 2015 to 173.4 million units by 2019.

According to Intel, by 2025, the total global worth of IoT technology could be as much as \$6.2 trillion—most of that value coming from devices in healthcare (\$2.5 trillion) and manufacturing (\$2.3 trillion).

Cisco estimates that the number of connected devices worldwide will rise from 15 billion today to 50 billion by 2020. Intel is even more bullish, claiming that over 200 billion devices will be connected by 2020.

By 2020, 90% of cars will be online, compared with just 2% in 2012, according to Spanish telecom provider Telefonica.

And these are just some of the numbers as research and market projections are ever changing on one of technology's newest industries.

SECURITY CONCERNS WITH IOT

IoT involves the increasing prevalence of objects and entities provided with unique identifiers and the ability to automatically transfer data over a network. Much of the increase in IoT communication comes from devices and embedded sensor systems used in industrial machine-to-machine (M2M) communication, smart energy grids, home and building automation, vehicle to vehicle communication and wearable computing devices.

The main problem is that because the idea of networking appliances and other objects is relatively new, security is not always considered when the products are designed – first to market is more important. IoT devices can be sold with old and/or unpatched operating systems and software. Additionally, purchasers of these devices often fail to change the default passwords on the devices. Beyond the traditional security concerns with unpatched systems and poor password behavior,

IoT is becoming an increasing gold mine of data for cybercriminal activity.

Through always-on sensors that are waiting for motion or voice controls to smartphone-controlled thermostats, the more data collected and analyzed, the more vulnerable to exploit IoT is by malicious actors. IoT devices can also act as the gateway to accessing more precious data stockpiles like an organization's intellectual property, employee personal identifiable information or customer payment details.

High profile cybersecurity incidents like those that hit Dyn in 2016 and brought down the entire U.S. East Coast's internet connectivity for several hours are perfect examples of how IoT security issues can no longer be ignored.

Hacked Cameras, sDVRs Powered Today's Massive Internet Outage – An excerpt from
KrebsonSecurity.com, October 21, 2016

"A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

Earlier today cyber criminals began training their attack cannons on Dyn, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.

At first, it was unclear who or what was behind the attack on Dyn. But over the past few hours, at least one computer security firm has come out saying the attack involved Mirai, the same malware strain that was used in the record 620 Gpbs attack on my site last month. At the end September 2016, the hacker responsible for creating the Mirai malware released the source code for it, effectively letting anyone build their own attack army using Mirai.

Mirai scours the Web for IoT devices protected by little more than factory-default usernames and passwords, and then enlists the devices in attacks that hurl junk traffic at an online target until it can no longer accommodate legitimate visitors or users."

Incidents like this should cause an organization to pause and ask: **how can we protect our data from falling into the wrong hands?**



*"Data breaches are becoming more complex and are no longer confined to just the IT department, but are now affecting every department within an organization," according to the Verizon 2016 Data Breach Investigations Report (DBIR).
– [HelpNetSecurity](#)*

4 STAGES OF IOT DATA AND ITS MOVEMENT

Pull quote/data point: The global economic impact of the Internet of Things (IoT) is estimated to be \$2 trillion by 2020, with more than 21 billion connected “things.” (source: Gartner)

Before protections can be put in place or vulnerabilities patched, it's important to understand how IoT data moves and any potential missteps or red flags along the way. Here are four stages of IoT data and its movement.

Stage 1: The creation of the device

It's important to understand that IoT data's journey doesn't start at the point when the data is sent or received – or even when the device is turned on. Data is embedded within a smart devices – whether through protocols used to create the hardware, the various sensors built into the device to capture anything from voice to movement or the software developed to respond and react. While the device itself is considered an “endpoint” that would need to be protected, how the device is built and the standards used to create the hardware and software can impact how to protect the data collected and shared.

One other thing to consider is that IoT devices typically are small and their sensors or parts have to be designed at a cost that individuals would invest into the product. Therefore, the protections that are built into the manufacturing of consumer devices may not be feasible to implement in early IoT products due to economies of scale. It's important not to assume that any manufacturer has pre-built protections in place since IoT is still very early in its technology lifecycle.

Additionally, since the IoT ecosystem is still in the early phases of development, there are not common standards that manufacturers use to build or develop against. There are a number of industry organizations popping up to address industry-wide standards or agreed upon best practices, but it's still early on in the introduction of IoT.

Stage 2: The device is activated

Once a device has been created and purchased, a user must activate it. This is another important stage in the creation, sharing and dissemination of data. As a device is activated, a user's preferences, account information, authentication and sometimes payment details, location and behaviors are stored with the service provider. This is also the point in the device's lifecycle where it's connected to the Internet, adding a gateway to the service provider and the consumer of the “thing.” Once the device is activated, the flow of information can begin.

Stage 3: Data is sent/received, processed and stored

Now that the device is set up and activated, it will begin to react to user commands or automated sensors. Consider an Amazon Echo or Google Home device, the voice command prompts the device to begin to execute your request, whether that's answering a question, ordering takeout, calling for an Uber or turning on your iTunes or Spotify accounts. The creation of data and flow of information increases exponentially – creating a broader amount of potentially sensitive data for a malicious attacker to seek out and exploit.

Stage 4: Data continuously flows back and forth

Even if there is only one IoT device, consumer or enterprise grade, there's an interconnectedness to devices, the network, third party services, etc. As one piece of information is shared from point A to point B, it might continue to be shared, stored or access with a number of other services, networks or tools.

In fact, data might be shared back and forth, depending on the set up of a service provider or a service contacted via the IoT device. Even prior to the proliferation of IoT devices, data moved between a variety of stakeholders and technology services. Now, more data than ever is created, shared and stored – and the flow is continuous.

That continuous flow makes it difficult to protect the sensitive data created by a device or the direct or indirect connections that a device might have to an enterprise.

So what's an organization to do? Keep reading for our checklist on minimizing security vulnerabilities created by IoT devices.

CHECKLIST FOR MINIMIZING VULNERABILITIES CREATED BY IOT DEVICES

"Forrester predicts that in 2017, more than 500,000 IoT devices will suffer a compromise — dwarfing Heartbleed. Heartbleed demonstrated the danger inherent in using open source components. Today, firms are developing IoT firmware with open source components in a rush to market." – Forrester

The journey of IoT data may seem ominous, making you ask yourself, how in the world would you protect so much data?

What's important to remember is that today's security challenges provide a blueprint for proactive steps that can be used to minimize the flow of sensitive data that moves outside of your protective net. It's also critical that IT admins consider the following actions or points of vulnerability, since even a consumer-connected device could be used to infiltrate an organization's network. Here are eight critical steps that any IT admin or security professional can take to lock down or protect IoT data.

1. **Practice** good security hygiene: Patch systems regularly & avoid weak passwords
2. **Review** privacy policies from providers to better understand what they will or won't do with your data
3. **Don't overwhelm or overstretch** your computing power or memory when you need the power to run security tools
4. **Review** all Internet-connected systems and devices to better understand your potential attack surface
5. **Implement** authentication across services
6. **Encrypt** all sensitive data, to avoid it being targeted while in transit
7. **Avoid** critical dependencies on one system (or set of systems)
8. **Consider** data management tools like a managed file transfer (MFT) solution or data loss protection (DLP) services to ensure the secure transfer of data –and to proactively watch how data flows in and out of your organization

End users can play an equally important role in preventing a data breach or data loss. They can assist IT by following these five easy steps to ensuring the highest level of data security:

1. **Enact** smart password practices - do not use the same passwords for devices or services
2. **Check policies** and EULAs with device manufacturers or service providers to better understand what they will or won't do with your data
3. **Monitor** which applications and programs have access to the data on your IoT connected devices, restricting access when an application or program is no longer needed
4. **Only allow access** when you know and trust the third-party vendor
5. **Assume** there are a number of adversaries out there at any time, and do not share data unless you are comfortable with it getting into another person's hands

What's the bottom line? For both the IT team and individual users it's important to be aware and be vigilant. It's essential to understand what is going on with your data and Internet-connected devices, and ultimately how it can affect you or your organization.

WHAT'S NEXT FOR DATA AND IOT?

"By 2020, more than half of all business processes and systems will incorporate data from connected systems built around Internet of Things (IoT)-enabled devices, according to technology analyst Gartner."

– [Samsung](#)

As IoT evolves as an industry and larger ecosystem of connected devices, organizations and individuals will need to wade through the hype to discern what advancements are real. Other factors that are becoming more mainstream which may also impact the overall vulnerability of data include things like dark data, which is the data that's stored but not accessed for analysis, or behavioral analytics that are reviewed by cognitive or artificial intelligence technologies. The world of technology will only continue to advance and systems will only become more interconnected. That continued interconnectedness will put data at risk of being lost or breached.

What is important to remember is as IoT becomes more mainstream, regulations and standards will surface that assist in the protection and privacy of data. In fact, this is a critical point where more security and IT influencers can provide their own suggestions and recommendations for these standards by participating in regular industry events or making their perspectives known to regulators. As an IT leader, it's essential that defenses and proactive steps are taken or put in place to prepare for the uncertain and often overwhelming reality that is IoT. No one organization or individual can be discounted when working to protect sensitive data.

Gartner predicts there will be several significant IoT product recalls that could cost up to \$1 billion due to faulty IoT implementations by 2022 – Gartner



For more information
please [visit our
website today.](#)

The best thing you can do is to understand the challenges and start taking action. Whether that's creating policies and procedures to protect your organization, educating your employees on how their IoT devices might impact the company, or monitoring and managing a company's IoT footprint.

Historic security incidents can also go a long way in providing a guide on to how to protect data, systems and organizations from larger breaches or other cybersecurity attacks. Learning from the past will be important to protecting the future, in a world of things.

