forbes.com

Investing In The Internet Of Things Security

Jayshree Pandya

9–11 minutes

Investing In the internet of things (IoT) security

Getty

Since security has immediate and future

consequences, what is the real cost of solving — or not solving — the internet of things security problems?

Introduction

Security is a complex challenge. As the smart, autonomous future dawns upon us, the security risks for the rapidly growing intrinsic web of connected things across cyberspace, aquaspace, geospace, and space (CAGS) are becoming complex.

As the number of things and devices being added to the internet of things (IoT) increases every day, so does the potential security threats. It is no longer only about the nature of connected things and the connectivity of an enterprise or critical infrastructure; the reality today is that the internet of things is now connecting everyone and everything. As a result, everyone is vulnerable to security threats. This changes everything, as hackers can now gain access to anyone's networks through either a thermostat, digital locks, refrigerators, baby monitors, light bulbs, smart

meters and so much more. It is no brainer that securing the IoT is fundamental to the well-being, privacy, data security, personal safety, and security of everyone and everything across nations.

This is mainly because the connected devices commonly use tiny processors for embedded functions. While these processors are cost-effective and efficient, these devices do not have the necessary computing and memory power to incorporate the current security solutions to be resilient. Nor can they be upgraded when new information becomes available on any emerging security threat from cyberspace or beyond. Moreover, in the absence of global standards, interoperability and integration are getting complex. Also, the low cost of things (devices) and the resulting mass production makes it impossible to keep track of.

This is primarily a cause of concern because while we are still struggling to manage the security risks from cyberspace, security is becoming even more challenging as everyone and everything is getting

connected across CAGS. As Jeff Williams of Bain Capital says in this Risk Roundup, “The adversaries have now moved towards going after these devices because it’s easy access to the network we’ve all spending so much money and time protecting.” Now, when quantum computing is well on its way to becoming a reality, solving the already complex problem of the internet of things is getting even harder.

So, as we evaluate the overall IoT security vulnerabilities and needs, it is crucial to understand what is required for meeting the security challenges. What kind of innovations are needed for IoT security? How do we build connected things that can be secured adequately? Where is the investment going?

Acknowledging this emerging reality, Risk Group initiated a much-needed discussion on Investing in the Internet of Things Security with Jeff Williams from Bain Capital based in the USA on Risk Roundup.

Disclosure: I am the CEO of Risk Group LLC.

Risk Roundup Webcast: Investing In The Internet Of Things Security

Risk Group discusses Investing in the Internet of Things Security with Jeff Williams, a Partner at Bain Capital Ventures, based in the United States.

To solve the integrated security problem, there is a need to understand each part of the IoT ecosystem. It is crucial to understand and evaluate the cyber-security integration points to know where the security risks are emerging in the connected CAGS ecosystem.

Digital Data

As we evaluate IoT technologies, applications, and platforms, it is becoming clear that there are many layers to IoT security. Perhaps the most critical layer is the data security layer. While digital data is the driving force of a digital global age, the ever-increasing data breaches have already become a growing problem for each individual and entity across nations: its government, industries, organizations, and academia (NGIOA). From the small breaches to the significant ones, from low-

profile attacks to high profile attacks, data breaches, data theft, and data manipulation are practically becoming an everyday affair across nations. As of today, there doesn't appear to be an easy way to halt this growing surge of cyber-attacks from anywhere. As a result, irrespective of personal data, corporate data, government data, big data, or IoT data, no individual or entity seems to be immune to data security challenges.

Nations today face data destruction, deletion, and manipulation threats. The cyber-criminals and attackers don’t just steal data, but they also delete it or manipulate it. This is a critical risk facing any individual or entity within any NGIOA. Amidst the interconnectedness and inter-dependencies of a digital global age, the boundaries between personal data, corporate data, consumer data, citizen data, national security data, big data, and IoT Data are blurring. That brings us to an important question: *Amidst this complex interconnectedness and inter-dependencies, who is accountable for data security? How do we*

manage the security risks at all integration points? What tools are available, and what tools are necessary?

Data security is a complex challenge. With new security threats appearing at a rapidly increasing pace, each individual and entity across NGIOA are facing data security risks. While there is an on-going effort to secure data, it is essential to evaluate if we have the right approach to data security and whether we have sufficient technology and process frameworks that would allow us to manage data security risks effectively.

Encryption Keys

Traditionally, the proprietary, private, and treasured data of individuals and entities across NGIOA were generally protected by encryption keys, which are transmitted between a sender and receiver from point A to point B. These secret encryption keys, however, can be intercepted, corrupted, and exposed if a malicious hacker eavesdrops on these keys during transmission.

The reality today is that the encryption technology

is commoditized. While entities across NGIOA can choose to encrypt data at the application level, the database level, the storage level, or the network level, it is essential to understand the differences between encrypting at different levels and what parameters should decide this choice. It is also important to know whether all data needs to be secured in the same manner and how integrated security networks will evolve.

While not all data needs the same level of security, the interconnectedness of data and the blurring boundaries of individual security, physical security, network security, and device security necessitate an integrated approach to ensure the security of data at all levels to prevent unauthorized access, changes to data, disclosure, or destruction of data. *That brings us to an important question: Do we have the necessary technological and process solutions capability with the current encryption technology?*

It seems that while encryption can be applied in many ways to protect a wide variety of data types,

it is not a full proof security solution for protecting data in all states. Moreover, while there is a lot of focus on encryption keys, key management — where many vulnerabilities originate — is mostly ignored. And as a result, criminals tend to target the encryption keys and processes that are used to manage them. *That brings us to important questions: In addition to problematic potential backdoors, what are other specific technological and process problems with current encryption technology? What makes them vulnerable?*

Complex Challenges

The internet of things (IoT) ecosystem is facing many complex security challenges. To begin with, the security perimeter is porous and can be easily penetrated, disabled, or manipulated. Since the internet of things (IoT) is connected via the internet, many of these systems thought to be safe are still vulnerable from both outside the perimeter and inside. Second, while IoTs have critical functionality, the devices are produced in masses, and many of them are disposable.

Moreover, the security assumptions that are generally made about the devices do not consider all the parameters to meet the needs of the current and future security ecosystem. Additionally, most IoT devices cannot be easily patched or upgraded and have a long-life cycle. Third, securing IoT will also need an increase in computational power, which is currently an issue. *While these are just a few challenges facing IoT security, it is crucial to understand and evaluate what new tools, technology, and procedures need to be developed for securing IoT systems in the coming years.*

What Next?

The spending on the IoT rises steadily and is expected to hit trillions of dollars in the coming years. It is an understatement that IoT requires stronger endpoint security that can withstand not only cyber warfare but also EMP warfare. Not only does the safety of humans depend on the secure operation of endpoints and of the IoT ecosystem as a whole, but also the very survival, security, and sustainability of nations and the future of humanity

rely on it.

NEVER MISS ANY OF DR. PANDYA'S POSTS

Join here for a regular update.