IIoT World

Evaluating Risks in the IoT Supply Chain

Originally appeared in IIoT World -
https://iiot-world.com/connected-industry/evaluating-risks-in-the-iot-supply-chain/

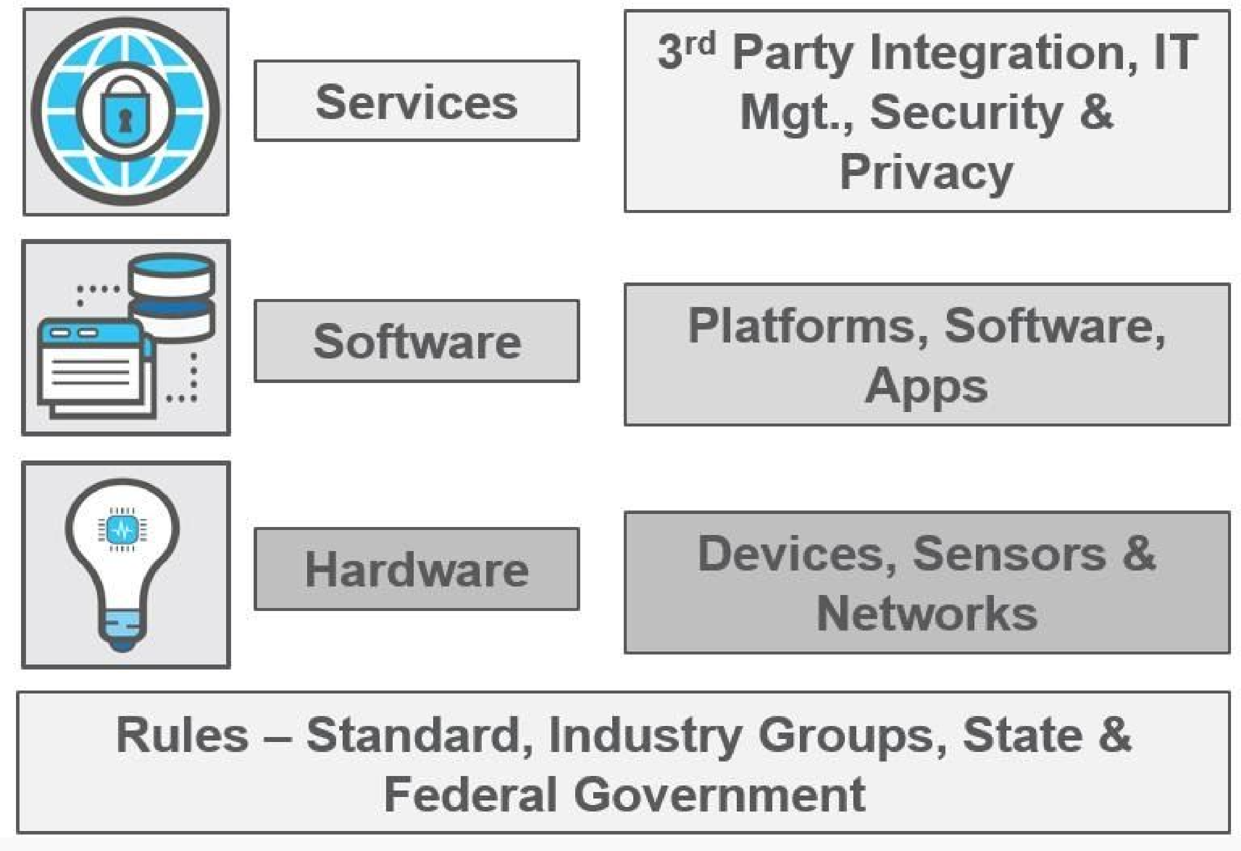
The Internet of Things (IoT) is still at a nascent stage. That, among other things, means significant risk exists in the IoT supply chain – and much of that stems from the software that proliferates in devices, sensors, controllers, networks and other "things."

We constantly hear about new startups in the IoT market. Yet, as this market finds its groove, many of these companies will cease to do business, go bankrupt, get acquired, or get out of the IoT space –that's just the nature of emerging markets. *Crunchbase* discusses the massive barriers to entry for IoT companies – from integration to industry consolidation to focus, and *Postscapes* has tracked examples of failed IoT startups as a resource to discover what has worked and what hasn't in the evolution of the IoT. Today's multitude of architectures and standards for IoT products increases the risk to companies deploying IoT projects for their long-term viability and stability often needed to deliver promised return on investments. No one is sure how this will shake out, or if you've placed the right bets.

Don't get me wrong. I truly believe there is tremendous promise in the IoT, consumer and commercial, but in particular in the Industrial Internet of Things (IIoT) sector. However, as you explore the opportunities, I urge you to do so fully aware of where the potential pitfalls lie, and what you can do about them.

Risks in a Typical IoT Ecosystem

First, let's look at a typical IoT ecosystem. This is generally made up of hardware, software and services. Each of these IoT elements require the evaluation of "what if" scenarios if they perform a critical function, are supplied by high risk vendors, or cannot be replaced easily.



Services
3rd Party Integration, IT Mgt., Security & Privacy
Software
Platforms, Software, Apps
Hardware
Devices, Sensors & Networks
Rules – Standard, Industry Groups, State & Federal Government

Figure 1: IoT Ecosystem = Hardware + Software + Services

In this ecosystem, the hardware, software, and services are likely being provided by different vendors with overlapping features and capabilities. As platforms and standards are still not fully developed, the multitude of providers, components, devices, and technology create risk by the simple virtue that over the next five years, many of these companies won't be in business – at least not in the same way they are today. In addition, as more devices are connected and more data is generated, more challenges will become evident not only with the IP but with managing data and privacy and monetization of the data. But how are IoT business and technical owners thinking of the ecosystem and of project continuity and service sustainability?

We'll explain four of the major risk categories that exist in the IoT: security and privacy; software; intellectual property; and data. Of course, some of these categories overlap, so risk mitigation in one area can help others as well.

Security and Privacy Risks and their Implications

One of the most widely discussed risks in IoT is that of security and privacy. There are critical elements in any ecosystem that must be assessed and evaluated for protection against cyberattacks, ransomware, and data breaches.

Ponemon Institute research suggests that IoT providers have a lack of visibility into third-party safeguards and IoT security policies. Safeguards can be used to prevent data breaches and stop ransomware. However, they can be difficult to manage because of complexities of IoT platforms and numbers of vendors. Ponemon reports a "dramatic increase in IoT-related data breaches specifically due to an unsecured IoT device or application – from 15 percent to 26 percent" over three years (FY17 to FY19).

Another study by Altman Vilandrie and Company reported that, "nearly half of all companies in the United States that use an Internet of Things (IoT) network have been affected by a security breach that has hurt annual revenue." They estimate, "the cost of IoT network breaches represented 13.4 percent total revenues for companies with revenues under $5 million annually. For larger firms, the cost could reach tens of millions of dollars. Firms with annual revenues above $2 billion estimated the cost of a single IoT breach at more than $20 million."

The Ponemon study concluded there is a gap between proactive and reactive risk management. They say it's no longer a matter of "if," but "when," organizations will have a security exploit caused by unsecured IoT. As a result, board members of organizations need to pay close attention to the issue of risk when it comes to securing a new generation of IoT devices that have found their way into your network, workplace and supply chain.

The IoT Revolves Around Software – What are the Risks?

At the end of the day, the IoT revolves around software. Because software also constitutes intellectual property (IP) for developers, it carries additional risks. As IoT expert Stacey Higginbotham explains in her post, Sorry, your hardware is all software now, "Once something is connected to the internet it becomes software. We are only just starting to have a conversation about what the implications of that are for the everyday goods around us."

She continues, "Smart products behave more like software than hardware. Confusion and drama over software changes that fundamentally break smart home hardware are not uncommon. There are dozens of companies that have built products only to go under and subsequently see the physical hardware they made turn into a brick. … So, companies building connected devices need to get ahead of this trend; they need to both help educate consumers and build tools that offer continuous value over the life of a connected product."

Software comes into play with unique devices manufactured for specific use cases that contain software, algorithms and firmware or customized applications that process critical functions.

People and businesses increasingly rely on IoT devices full of software. Therefore, it’s essential to think about and build upon proven, best-practice software protection strategies to extend that protection to the supply chain. As IoT enables monitoring and optimization at the device level, it will be important for the software in the individual devices to be able to talk to each other for higher-level digital transformation.

Risks of Intellectual Property throughout the IoT Ecosystem

As you consider what unique IP lives in your IoT ecosystem, think about the impact if it is compromised.   This could cause revenue loss, impact your customers, or even inflict reputational and brand damage as a result of bad press. Healthcare technology is one example, as explained in this Politico article, "As more and more medical devices get Internet enabled, they're going to have more complex software code. We're seeing the risks increasing day by day."

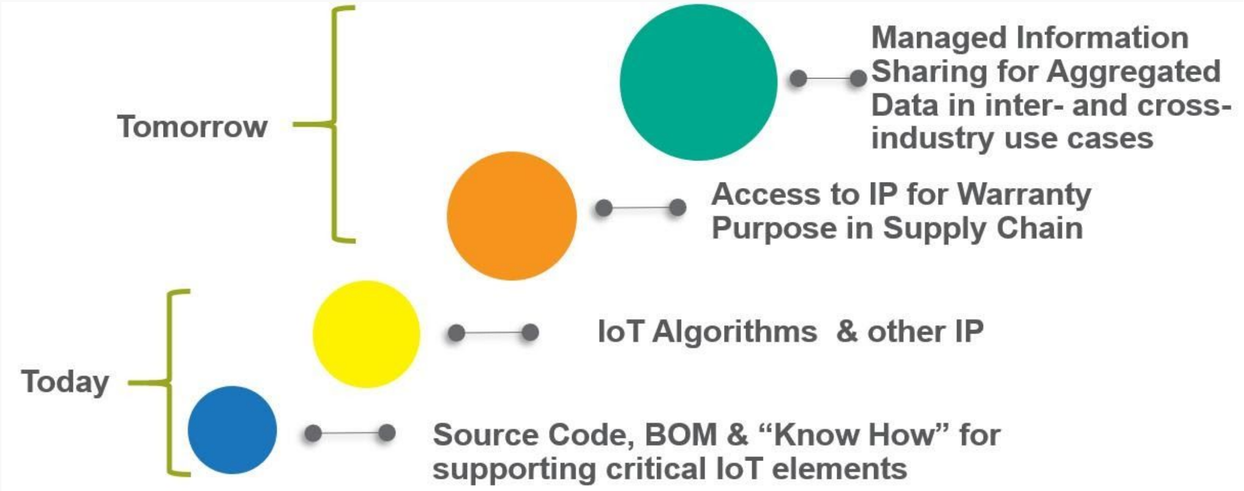

Tomorrow
Managed Information Sharing for Aggregated Data in inter- and cross-industry use cases
Access to IP for Warranty Purpose in Supply Chain
Today
IoT Algorithms & other IP
Source Code, BOM & “Know How” for supporting critical IoT elements

Figure 2: Intellectual Property Assets in the IoT Supply Chain

Today, we see companies assessing things like source code, bills of materials (BOM) for manufacturing, algorithms, and other IP to determine if legal covenants suffice to protect them. Or, is access to the IP necessary to ensure sustainability of the project for the intended timeline?

In the future, we see the need for a registry of IoT devices – an idea put forward by Vint Cerf, chief internet evangelist for Google. Think of this registry like code that has been sun-setted and is placed into the open source repositories. A registry of IoT devices would work in a similar way, so that “know-how” of no longer supported IoT products could be maintained.

In an EE Times article, Cerf explains, “We should be extremely thoughtful about the quality of IoT software. People are relying on these things to work autonomously, and these days, almost anything can become a programmable, communicating device because the chips are so inexpensive.” He believes the Internet of Things won’t live up to its promise unless engineers redouble their efforts to develop high-quality, secure, and interoperable software. Even then, new programming techniques and even legislation may be needed.

Who’s Protecting Your IoT Data?

As more devices are connected, more data is generated, and more challenges will become evident, not only with the IP, but with the monetization of data.

Data is rapidly becoming as valuable commodity as companies like Netflix, Uber, and Airbnb, add value is based upon their skill at gathering, interpreting and acting upon data. Even brick-and-mortar companies will benefit from having access to detailed data about their customers and markets. Organizations will need the means to buy and sell data in the same way they do goods and services today. New mechanisms must ensure that those transactions are tracked, documented and audited in the same way that cash transactions are tracked by a bank.

Central to these relationships is data integrity, security, and accountability. Few organizations have the skills or desire to build the sophisticated mechanisms to handle these demands. Most will use trusted third parties. Today, conflicts over data access are delaying business return on investment.

We are in the early stages of understanding how these relationships will work, but we can expect that many organizations will need trusted agents to collect and validate data to protect it against misuse or exploitation. Parties in a data exchange will want verification of authenticity and proof of ownership, and new standards will evolve to establish intellectual property rights. There are companies already emerging in the market to assist with these issues and risks.

Control the Future of your IoT Ecosystem

As the market continues to establish itself, the fate of many IoT suppliers will end with bankruptcy, merger, or divestiture. We've seen multiple examples of this such as Twitter's acquisition of online trust and safety startup Smyte, Centralite's Chapter 7 filing, and Lowe's getting out of its Iris smart home business.

Ultimately, you want the ability to control your future. By this, I mean you want to minimize the risk of being forced to "rip and replace" any part of your IoT ecosystem if uncontrollable events take place. For some organizations, this may be an acceptable for building a knowledgebase and experience, however, this won't fly on fully funded efforts with big promises and ROI expectations. The worst-case scenario would be if the failures from third-party risk ended in litigation or brand damage.

Eventually, you will need to satisfy internal governance, as well as state and federal compliance requirements. Compliance requirements at the state and federal level will force us to pay more attention to how companies' contract, deploy, and manage these elements of the ecosystem. NIST (the National Institute of Standards and Technology), along with the states of California, Illinois, and others are already passing guidance and laws around IoT devices.

You want contractual leverage to have a fair seat at the table. Said simply, as an organization you want to have a say in the usage of the technology you deploy. And, if you are an IoT provider, you want a simple way to engender trust and address real concerns for our customers.

IoT IP Risk Mitigation Steps

Here are the strategies we see companies focusing on as they work on mitigating these risks:

- Identify critical points in your IoT ecosystem = It’s key to identify connected devices, along with knowing the function of those devices, and if (and how) data is collected and transmitted.
- Define where proprietary code, algorithms, intelligence, and data exist in the ecosystem.
- Structure a risk assessment and evaluation - Many companies are creating a discrete function within Enterprise Risk Management for the IoT discipline -- and then deciding how best to evaluate what is deployed.
- Develop contingencies in your critical supply chain that include alternate providers as well as taking over the responsibility to maintain.
- Collaborate with Legal and Risk Management to assure contract terms and address known risks.
- Decide if your access to “know how,” source code, IP, and other forms of trade secrets give you leverage. If it does, establish a way to access this information in case of contingencies. If something ultimately does go wrong, you’ll have the right to step in and either maintain that technology yourself or find someone that can.
- With an escrow-like solution to risk mitigation, determine how you can validate/verify the intellectual property, not just have access to it.
- As your IoT efforts evolve, review and evaluate your contingency and risk mitigation approaches.

The IoT offers tremendous opportunity to help companies improve quality and/or performance, improve decision making, and lower operational cost, regardless of whether your endeavor is consumer-based or industrial.

Understand your risk, where the unique IP lies, and what the impact may be to your organization. This will help drive decisions to develop the right contingencies and access to source code or IP that will enable you to support your technology for as long needed to address stability and continuity concerns.

This article was written by John Boruvka. He is vice president for Iron Mountain’s Intellectual Property Management group. John has been involved in the technology escrow and intellectual property management field for more than 32 years. His focus is on helping companies create solutions relating to protecting intellectual property assets.