Podcasts

Regulating the Internet of Things

June 2021

Thousands of devices connected to the internet - the Internet of Things - may help streamline operations, improve productivity for manufacturers, but IoT is not without risk. Recent federal and state laws will influence the controls needed to minimize business interruption, workplace safety and data breaches.

Jackson Lewis P.C. · Regulating the Internet of Things

- Apple Podcasts
- Google Play
- LibSyn
- Pandora
- SoundCloud
- Spotify
- Stitcher

Host

Joseph J. Lazzarotti

Principal
Berkeley Heights 908-795-5205
Email

Practices

International Employment
Litigation
Privacy, Data and Cybersecurity

Services

California Consumer Privacy Act

Takeaways

Regulating the Internet of Things and Implications for Advanced Manufacturing

Thousands of devices connected to the internet - the Internet of Things (IOT) - may help streamline operations, improve productivity for manufacturers. Think of sensors that can share information throughout the control system to ensure processing maintains quality standards. But, IoT is not without risk. Recent federal and state laws, including the Internet of Things Cybersecurity Improvement Act of 2020, will influence the controls needed to minimize business interruption, workplace safety, and data breaches.

What Manufacturers Need to Know

- The National Institutes of Standards and Technology (NIST), defines the IOT as a device that has a network port and either a sensor or an actuator or both—something that is connected to the network, but also is either affecting or detecting something else. It is that connectivity that contributes substantially to overall risk.
- McKinsey & Co. estimates about 43 billion additional IOT devices will be connected to the internet by 2023. These devices connect the physical world to the digital world, bridging the divide between information technology (IT) with operational technology (OT).
- According to Deloitte, 83% of manufacturers today believe that by 2025, their production will be transformed by this technology.

- Why would IOT be a risk?
    - The IOT has seen 300% growth in the last five years, 80% of which is in the industrial space. The sheer number of devices makes them a bigger target for threat actors.

- There are several enterprise risks for manufacturing organizations as a result of an IOT type attack.
    - Data security risks, where compromised IOT systems connect to the company's information systems.
    - Compromising a sensor resulting in the shutdown of operations with potential ripple effects including supply chains disruption, unexpected equipment shutdowns jeopardized worker safety, contractual obligations being unmet and the cost of restarting operations.
    - Compromised working conditions could influence labor negotiations.
- The planning and resources needed to mitigate risk go beyond the factory floor and should involve senior management, risk management and human resources.
- Manufacturers need to keep security in mind when designing devices, not just asking the question, what must we do, but should we do. Who should have access? How are we protecting it? Where are we storing data?
- Users of IoT need to keep good data security hygiene to keep the network secure.
- The Internet of Things Cybersecurity Improvement Act of 2020 directs NIST to provide guidelines for securing IOT devices. The law is limited to the federal government's use of IOT technology. However, it is likely that NIST standards for federal agencies will have a significant influence on the private sector as well. Additionally, several states are establishing reasonable security requirements for IOT devices: laws in California and Oregon have already passed laws to this effect.
- Data security best practices generally follow three key tenets: confidentiality, integrity and accessibility. These should be considered when developing any set of system controls.
- Following NIST is not an exact science. Businesses need to consider risks involved with the kind of data maintained in addition to the anticipated guidance. Cybersecurity, accessibility, data integrity, privacy and other considerations should factor into decisions on the actual controls to implement.

Transcript

Lara (00:06):

Welcome to Jackson Lewis's podcast We get work™, focused solely on workplace issues everywhere and under any circumstances. It is our job to help employers develop proactive strategies, strong policies, and business oriented solutions to cultivate a workforce that is engaged, stable, and diverse. Our podcast identifies the issues dominating the workplace and its continuing evolution and helps answer the question on every employer's mind. How will my business be impacted? Smart medical sensors, door locks, and washing machines are examples of just some of the thousands of devices connecting to the internet every second. And that make up the internet of things or IOT. This technology serves not only consumers, but businesses seeking to streamline operations and improve productivity, particularly manufacturers. The advantages of IOT are not without risks. Notably, cybersecurity risks. Recent federal and state laws are sure to influence the controls needed and expected to minimize those risks, which include business interruption, workplace safety, and data breaches.

This episode of We get work™ discusses IOT related risks for manufacturers along with best practices and recommendations when adding IOT to their systems. Our host today are Joe Lazzarotti of Jackson Lewis, co-leader of the firm's privacy data and cybersecurity practice group. Joe is joined today by our special guest, Doug Heim, a cybersecurity technology expert with Tracepoint. Having worked together on data breaches and other projects, Joe and Doug will discuss this emerging technology along with its cybersecurity challenges. Joe and Doug, the question on everyone's mind today is, what can I do to ensure my organization understands what the IOT is and how we can use it in our processes, the compliance requirements for doing so, and if I do use the IOT, how will that impact my business?

Joe Lazzarotti (02:12):

Absolutely. Thank you, Lara. Doug, thanks for joining us today to talk about these issues. We work a lot with Tracepoint and we appreciate them giving you some time with us.

Doug Heim (02:24):

Thanks so much for having me.

Joe Lazzarotti (02:25):

You bet. So, when we use the word smart to describe a new or an old gadget, it usually means that the gadget can now do some really neat stuff, smart washing machines, smart TVs, smart cameras. We may not realize just how ubiquitous these devices are, and they're not just new toys for consumers. By some estimates I've seen we're introducing thousands of smart devices every day to the internet. Part of a technology that we generally refer to as Internet Of Things or IOT. Consulting firm, McKinsey estimates about adding 43 billion IOT devices will be connected to the internet in 2023. And these devices really at a high level, connect the physical world to the digital world or the electronic world bridging the divide between what we think about is information technology or IT, with operational technology or OT. IOT is what enables autonomous driving. It's what empowers Alexa. And it's also what helps manufacturers bring efficiencies, improved safety, and also cost savings to the manufacturing process. According to Deloitte, 83% of manufacturers today believe that by 2025, their production will be transformed by this technology.

So you consider like, IOT sensors that can track heat and humidity and other elements for equipment that might help to reduce maintenance efforts, reducing downtime, fewer injuries might result, and your equipment might last longer. There's also wearable devices that can detect hazardous conditions and warn employees, and also shut down equipment automatically, which may help keep employees safe. Connected devices can also allow a manager to be remote when overseeing operations, something that might come in really important during pandemics like we've been through and also improve safety and reduce costs. So with all this good stuff, what's the downside? So like more traditional information systems, and networks, and laptops that connect to the internet, IOT tends to expose to the internet formerly closed control systems, which manufacturers tended to rely on. But before we get into those risks, let's get a better handle on just what IOT really is. So Doug, maybe you can help us out with that.

Doug Heim (04:53):

Sure. There are a lot of definitions, a lot of different marketing people use to talk about what IOT is. I've standardized on what NIST uses. NIST is the National Institutes of Standards and Technology, which we'll talk a good bit about today, I believe. Anything that is a device that has a network port and either a sensor or an actuator or both. So it's something that's connected to the network, but also is either affecting something else or detecting something else. You brought up operational technology earlier, Joe. Operational technology versus information technology. Everyone knows about IT. That's what you use at the office. Documents you send, emails, that's all administrative tasks, what's known as information technology. Operational technology is really that realm where the IOT devices sit. It's that area where they're connected both to the network and then to whatever they're monitoring.

IOT applications come in many different formats. We look at commercial devices like your personal trackers, your Fitbits, smart homes that have thermostats and climate controls and even doorbells that will show you who's at your door while you're sitting in the office. And those being the simple ones that I think we see all the time, but also there's a large amount of IOT in industry, medical devices, imaging and monitoring tools that are saving lives every day. And then within manufacturing, we see the use of what we call Industrial Control Systems or ICSs that allow the control of machines, the quality control of what's produced by those machines and keeps everything safe. Where we really see growth in the industrial devices is where they're improving and making things more efficient by detecting minor failures or just moving the process along. It gives us much more control of what we're doing.

Joe Lazzarotti (06:52):

Okay. So that's really helpful, Doug, but our firms have worked together on a lot of different incidents, data incidents, right? Ransomware attacks, business email compromise cases, insider threats, stealing company data, a garden variety of employee error resulting in disclosures of personal data, usually.

In the news, we hear about compromises to massive amounts of credit card data resulting from perhaps a skimmer installed by bad guys or phishing attacks, perhaps even a website might've been configured and properly exposing personal information of thousands of individuals. And it seems like it makes sense, right? That bad guys are going to try to access this data because they can then use it either to commit identity theft, or they might seek a ransom from the victim company. And so isn't that really what's driving a lot of the data breaches. So why would IOT be a risk? Why does a hacker really care about accessing a sensor that detects the heat that a machine is generating or a camera that sees movement and moves to that movement or moves to sound that it hears? What is it about the factory floor that makes IOT and manufacturing a target?

Doug Heim (08:08):

Well, the first thing we see Joe, is that these devices are just growing by leaps and bounds. So just the virtual fact that they exist and they're growing where we've seen about 300% growth in the last five years, 80% of which is in the industrial space. So just the sheer number of devices makes them a bigger target for threat actors, as we call them to attack them. You'll see that those are being used and they're growing because they're making things more efficient. They're making the factories more efficient. They're allowing us to track machines and do predictive maintenance to them so that we have less downtime and increase just the work that's being done.

One of the things we with that though, is that security just has to improve. And we know that we need to improve it because we see where these devices are being hacked. There's been multiple new malware attacks and variants that specifically addressed ICS, Industrial Control Systems like we talked about. Particularly there's one came out a couple of years ago called Triton, also known as Trisis that went into specific industrial control systems and pulled information from them, added controls that you didn't necessarily want to have, and just generally wreak havoc with that system.

There's also a fairly well known attack vector known as Mirai, which takes IOT devices that are running Linux, which a large percentage of them are, and can turn them in to a dedicated denial of service and distributed denial of service bot net so that you can attack a victim from a bunch of devices that you don't even own just by virtue of using this attack.

I think one of the things we've all heard of recently is the Colonial Pipeline. And although operational technology was not the target, concerns with that spreading is what caused the shutdown. And something we're seeing in the environment as we look around from trace point, that there are threat actors that are becoming mercenaries and offering ransomware as a service. So if you have an organization that you think is behaving inappropriately and get some friends who are threat actors, they will either for a fee or just because they agree with you, we'll carry out these kinds of attacks.

Joe Lazzarotti (10:27):

Yeah, that's real interesting Doug, because I think, for manufacturers, this really has some significant implications and in any other organization that incorporates IOT into their business practices, but particularly for manufacturers. I mean, given what you said, tell me if you think I'm wrong, but I can envision that there might be several enterprise risks for manufacturing organizations as a result of an internet of things type attack.

Doug Heim (10:57):

Definitely.

Joe Lazzarotti (10:58):

Of course. Right. So we can think of like data security risks, where IOT is compromised and those systems might be able to, which they would normally be set up to connect to the company's information systems. So an attack hitting a device could result in a compromise to personal data, right? Sensitive personal information in some cases. Classified information for example, if a manufacturer is doing something for the federal government. But I think, and again, tell me what you think, but the risks might go further than that. So for example, you might have a compromise to a sensor that results in the shutdown of operations. And that could have ripple effects. Supply chains could be disrupted, unexpected equipment shutdowns could jeopardize worker safety, contractual obligations can go unmet, and the cost of restarting operations I assume, could be pretty significant.

You also might think about it and say, inadequate security could raise worker safety issues that might find its way into labor negotiation. So, clearly the risks and the planning and resources needed to mitigate, I would think go way beyond the factory floor and might also reach senior management, risk management, and also human resources. So thinking about that and knowing that that hackers have IOT in mind, internet of things in mind, as you mentioned from some of the variants you've talked about, I think for years, businesses have been struggling to kind of enhance the controls that they have and maintain over their information systems, their IT. Right. And so we've heard a lot about international, federal, state, local laws that are emerging rapidly to help organizations identify areas of vulnerability and how they can mitigate these risks.

So for example, in the US, there are several statutes that have been passed. We hear about the New York SHIELD Act and the CCPA, the California Consumer Privacy Act, the Massachusetts data security regulations that went into effect in 2010. There's a whole bevy of state laws that address this. And so there are of course these statutes establish administrative physical and technical controls to protect information system. So, can't we just apply these frameworks that are in place already to IOT? What is it about these devices that may make the current approach for information systems different?

Doug Heim (13:35):

Well you're right, Joe, ideally we would just apply these controls that have been established for IT over time to OT. The challenges with that is that the early industrial control systems never were intended to be networked. They sat on their own, you push buttons to control them. They did what they do and move on. You could pull information from them, such as reports, but over time industries have wanted to improve that process to make those devices more efficient. And the easiest way to do that is to analyze the data that they provide. And it's next to impossible to take that much data manually and move it from a control device into an IT type device. So you didn't have that plan for security. And I think as we see new devices hit the market, we are going to see that and we're going to need to see security be a key concern as you're developing these things.

One of the biggest issues with these devices is, they are computers. Yes, just like any other computer, but they don't have the wide ranging operating systems that you see where you can do antivirus on a PC, a laptop, desktop to protect you from malicious tools. You could install that on something like the machine, but usually they have limited memory and it makes it very challenging to do that. And one of the goals we're seeing and one of the benefits we're going to realize is to take these devices and make them part of a system. So you have networks of firewalls and intrusion detection devices, and what have you, around them so that it's not just, this is my IOT device, come and hack at it. But its part of a system that's protected by other what we would call compensating controls.

Joe Lazzarotti (15:26):

Okay. So that makes sense because at the end of the Trump administration, Congress passed and the former president signed the Internet of Things Cybersecurity Improvement Act of 2020. In short, the law directs the National Institute of Standards and Technology known as NIST to provide guidelines for securing IOT devices. The law is limited though, to the federal government's use of IOT technology, but considering the size of the federal government, it is likely that NIST standards for federal agencies to follow when procuring IT will have a significant influence on the private sector as well. We also have seen laws in California and Oregon that have established reasonable security requirements for IOT devices and other states, several of them are considering similar measures. So I know you mentioned NIST earlier, but Doug in general terms without getting too technical and to try to stay conceptual on this, what can you tell us about how NIST guidance might affect implementation of IOT for a manufacturing business?

Doug Heim (16:33):

Well, sure, Joe, first we need to look at NIST as a whole and understand what it does. It is part of the federal government that provides guidance and standards for technology as the name would imply, for the federal government. How do the federal organizations track and handle several different things, but computer security being one of them. There are three tenants that NIST works on and what's known as CIA, Confidentiality, Integrity, and Accessibility. And their goal is to maintain those three in all situations. They have generally broken out controls and control is just a method to maintain your CIA. And they break it up into several subject areas. Some examples would be access control, the lock on the front door, incident response, what do you do when someone breaks the lock on your front door? And configuration management, how many locks do you have on your front door? Just areas that are used within the control structure that NIST maintains.

The core document that's been used for security and compliance individuals for years is special publication, 800-53. And that provides guidance for all kinds of security controls. Specifically the IOT guidance has just kind of occurred naturally. They started developing some documentation early on. That was the NIST inner agency report, 82 59. And the number is going to be as detailed as I get on these for you all. But that guidance talks about what the internet of things is and how we need to improve it. Now that movement was pushed along significantly by the law that Joe referred to, the Internet of Things, Cybersecurity Improvement Act. So that requires NIST to develop federal guidance, which they were already in the process of doing, as well as prohibits procurement of IOT devices that are not meeting that guidance starting December 5th, 2022, that's two years after it was released.

So the general structure of that guidance is to look at that device as part of a larger system, as we just discussed. And look at the controls that have already been put out there as part of SP 800-53, and make sure that they're being addressed as an effective method against, or to protect IOT. There are several documents that come out of it in the 82 59 family, but basically they are just listing capabilities, both technical and non-technical, how to you use them, and what profiles to use them in profile, just being a collection of those capabilities. And then the final document is just talking about how to build your profile. What is my profile as a manufacturer of cars is going to be substantially different than someone who is making paint as an example, just maybe more moving parts, more components that you need to consider, and maybe even more robotic controls.

Joe Lazzarotti (19:36):

Okay. So it sounds like one of the things that comes out of this is there's going to be a lot of common threads among various profiles that we'll see based upon 853 and the general controls that we would expect. But following NIST is not an exact science. As a business, you need to consider your risks, the kind of data you maintain. And that cybersecurity is not the only thing we're thinking about. We're thinking about, as you mentioned, accessibility, data integrity, but also privacy and other considerations that have to go into what are the actual controls that you might want to maintain. And so with that in the time we have left Doug, maybe just give us what are three popular or really fundamental controls that you would recommend anyone who's really thinking about implementing IOT into their environment, that they have?

Doug Heim (20:27):

Sure, I would recommend you kind of split up these requirements. So you look at what manufacturers are doing in building devices, and then what users are implementing them. From a manufacturing perspective, we definitely need to make sure we have security in mind when we're designing these devices, not just asking the question, what can we do, but should we do. Who should have access? How are we protecting it? Where are we storing data, those kinds of items. And when you have that mindset then updates are frequently needed. You need to address new security and privacy concerns. As a law, like the New York SHIELD law comes out, there are going to need to be changes to devices that are recording and gathering data in the home, in the industry, and what have you. So I think from a manufacturing perspective, that's key. Make sure you're keeping up to date and moving forward and have a mind towards security.

From a user perspective, it's just generally keeping good security hygiene as we call it in the business. Making sure that, you don't write your passwords down and stick them on a sticky note on the side of your monitor, keeping your password or key in a secure place, you don't leave things laying around. So to that end, a couple of key things are just making sure your networks are segregated and protected. If you have an IOT device that's on your network, make sure you have a firewall in front of it. You're protecting it from all the ports that can be used to access it. That you're just making sure that as best you can, that device is not available to Joe off the street, pardon the name use. And then within that segregation also, you want to make sure you are keeping your devices up to date. As the manufacturers are putting out patches and updates, make sure that you're getting them implemented as quickly as possible just to keep your whole environment safe. And that's a good practice across the board from a cybersecurity perspective.

Joe Lazzarotti (22:22):

That's great. And thanks for those reminders. I'm removing my post-it note with password right now. But as you noted manufacturers and all organizations need to consider the threats and vulnerabilities for their particular environments and operations. And establishing a risk management plan for their information technology, as well as operational technology, as we talked about. And so with smart devices continuing to proliferate, as we mentioned in the commercial and industrial space, Doug and I hope that this program has helped to spur and encourage additional thinking around what you can do in your organizations to address the emerging risks, which threatened not only production activities, but also the company's workplace and its financial position. If anyone has any questions, feel free to reach out to Doug or me, including if you want access to some of the NIST publications that were mentioned. Doug, thanks so much again for joining us. We really appreciate. It was great. Thanks a lot.

Doug Heim (23:19):

Thank you. Thanks so much for having me.

Lara (23:20):

Thank you for joining us on We get work™. Please tune into our next program where we will continue to tell you not only what's legal, but what is effective. We get work™ is available to stream and subscribe on Apple Podcasts, Google Podcasts, Lisbon, Pandora, SoundCloud, Spotify, Stitcher, and YouTube. For more on today's topic, our presenters and other Jackson Lewis resources visit jacksonlewis.com. As a reminder, this material is provided for informational purposes only. It is not intended to constitute legal advice nor does it create a client lawyer relationship between Jackson Lewis and any recipient.

Transcript provided by Rev.com