MFG Week Webinar Series Transcripts

At The Intersection of Manufacturing and Technology

00:00:06:22 - 00:00:31:17
Unknown
we'll go ahead and just kick this off. My name is Jean price. I'm a partner with Frost Brown. Todd in the Louisville, Kentucky office. I'm joined by Mason clutter. Mason, if you would go ahead and, begin the introductions that I as Jean said, I. Mason clutter. I'm out of Frost Brown Todd's Washington, D.C. office, and I serve as the firm's privacy lead.

00:00:31:19 - 00:01:08:10
Unknown
And, we have pretty strong backgrounds in our respective areas on the cyber security lead. And because, if you think of cyber security, privacy as a Venn diagram, it's like this. We overlap a whole lot. So it's almost a daily occurrence where I'm sitting in Kentucky, Mason sitting in Washington, D.C. we still talk all the time because, while we both dabble in the other's area, we, they overlap so much, it's always good to get a second opinion on stuff or insights that we lack.

00:01:08:15 - 00:01:35:02
Unknown
As far as my background goes. I did not start doing cyber security until right at ten years ago, a little over ten years ago. And that was only because I was, in the Navy Reserve at the time of all things. And I got, involuntarily mobilized to go to the United States 10th Fleet, which is where, which supports United States Cyber Command.

00:01:35:04 - 00:01:56:16
Unknown
And I got thrown into the deep end of the cyber security pool and learned how to swim. And I've been doing it ever since, and I really was gone for several years. All told, about seven years in during that time was involved in hundreds of cyber security incidents of varying degree, some really big, some not so really big and learned a lot.

00:01:56:16 - 00:02:22:20
Unknown
And when I came home, I was volun told to be the cybersecurity lead. And I love it because it's exciting, it's changing. It impacts just about everybody, particularly in manufacturing and technology. So that's my background. Mason. Yeah. So, Dean, you're a little bit modest. He's a very high ranking Navy official and has a significant experience on both the defensive and the offensive side of cyber.

00:02:22:22 - 00:02:53:22
Unknown
So I of course, I'm joining us from Washington, DC, primarily because this is where I live, because prior to joining SVT, I served as the chief privacy officer to the US Department of Homeland Security. And so what

does that really mean? I advised the secretary, the deputy secretary, multiple agency heads on how to operationalize privacy. So how to achieve their missions in a privacy respecting and compliant manner, which is really what I do every day now at SVT with private sector clients.

00:02:53:22 - 00:03:08:16
Unknown
And it really aligns very nicely. Because at the end of the day, there's no one right way to comply from a privacy perspective. I think at times it would be so much easier if the law just said, this is what you need to do, and here's how you do it. And we all just did it the same way.

00:03:08:21 - 00:03:28:01
Unknown
But there's a lot of flexibility built into law that we'll discuss a little bit later. So my focus really is working at the intersection of privacy, technology and security and helping our clients achieve their goals while building and maintaining trust with their own stakeholders. And this, Jeanne said, we work hand in hand. Privacy is a key tenet of security.

00:03:28:01 - 00:03:46:05
Unknown
And likewise security is a key tenet of privacy, so you really cannot have one without the other. Especially from a manufacturing perspective. And I imagine many of you on the call today are thinking privacy. There's not a lot there for me. I only deal in business to business or I don't have consumer data. But we'll also get into that a little bit later.

00:03:46:05 - 00:04:09:02
Unknown
But before we do get into the meat here, I want to turn it back over to Molly, who has been helping, not just helping, but really facilitating the entire SBT Manufacturing League 2025, which is our second annual week. So Jeanne are incredibly excited to be a part of this, but turn it over to her for some housekeeping and for all the important and Kelly related information.

00:04:09:03 - 00:04:38:02
Unknown
Molly. Yes, thank you. Mason. And thank you for that intro. Your your head going everybody up today and I appreciate it. Yes. Just, just a couple of housekeeping items. The first one being, Kelly, I know everybody is, wanting to to make sure they get there. Kelly. So we'll have, additional information. We will be sending a follow up email later this afternoon to everybody who attended, with both Gene and Mason's contact information.

00:04:38:04 - 00:05:00:18
Unknown
The presentation materials, and then also just, a little note about the, Kelly submission. Nothing that anybody on this call needs to do. We will be tracking your attendance, and we will send that into the APA on your behalf. So just be on the lookout for an email from the ABA directly to where you'll fill out the affidavit and get your CLE, accreditation.

00:05:00:20 - 00:05:22:18
Unknown
Also, and just to, you know, facilitate the, the presentation if you have any questions at all during, during the presentation, we have the Q&A box down below. Mason and Jean cannot see, all of you lovely attendees here today, the way we have the webinar set up. So if you have any questions, just type them in the Q&A box.

00:05:22:20 - 00:05:53:22
Unknown
Myself, Jean and Mason will try to, you know, keep an eye on those throughout the presentation and get them answered, you know, as they come in. If not, we will also save a little bit of time at the end for you guys to, you know, to again, ask those questions. Also, we if we don't get to answering your question again, we will have, some, follow up email where either you can reach out directly to Gene or Mason or, you know, we'll have the information on our end of the questions asked.

00:05:53:22 - 00:06:13:21
Unknown
And Mason and Gene will be happy to follow up with you directly as well. I think that was all I had. And I'll turn it back over to, Mason and Gene to kick things off. Thank you everybody. Thanks, Molly. So, here's our agenda highlights. We won't dwell on this too long, but I already mentioned why we're doing this together.

00:06:13:23 - 00:06:40:00
Unknown
And you can see here the impact of emerging technologies, data security and, privacy challenges. You can see how these things dovetail together. Everything that I do concerns Mason and vice versa, as she said. So this is what we're going to cover, strategies, use cases and the future outlook. And let's plow on into it. Can you give me the next slide?

00:06:40:00 - 00:07:17:02
Unknown
Mason? I'm trying. Thank you. So the impact of emerging technologies on manufacturing and, operations is going to vary person to person, company to company. And there's no way we can cover all of this. Plus, each company, each entity is adopting some of these emerging technologies, at varying speeds. Some are slower, more cautious. Others are sprinting forward, trying to get an edge on the competition.

00:07:17:04 - 00:07:38:02
Unknown
But wherever you are, we hope to cover some of those technologies and how they're emerging and the difficulty it is keeping up with it. I don't know about you all, but I save an hour every day. I try to do at the very beginning, early on, but an hour just to read on what is going on over the last 24 hours.

00:07:38:03 - 00:08:09:12
Unknown
The, these technologies are changing so quickly. Everything from AI to o t to outsourcing third parties. It is very, very busy. So, Mason, tell us about smart manufacturing. Yes, I think what's interesting about, smart manufacturing, and when we think about technology in manufacturing is that sometimes it comes up in

unique ways. So as we see here, there's several examples of what we mean by smart manufacturing and technology and manufacturing.

00:08:09:14 - 00:08:47:22
Unknown
But these are the ones where we see the most significant privacy related and security related concerns. So think about your cloud outsourcing. Anything that you're using as a software, as a service, as a platform, as a service or infrastructure, as a service, these are things that help facilitate, efficiencies, cost efficiencies, reduce operational and infrastructure needs, but also increase risk because information is being shared not just within your organization now, but also with whoever the cloud sourcing provider is or the service as a software, as a service provider is.

00:08:47:23 - 00:09:18:13
Unknown
So this is why we see unique risk in this area. Additionally, the use of sensors and remote monitoring we would call these the Internet of things. So essentially anything that is connected to the internet raises your potential risk from both a privacy perspective, if we're talking about data, information, confidential information, as well as security and safety from the perspective of the actual equipment that may be, in use, as well as the ways in which the manufacturing equipment is connected to other equipment.

00:09:18:13 - 00:09:44:04
Unknown
So think about the concept of critical infrastructure and ways in which bad actors we have seen get into systems, throughout the last few years, sometimes through an eight track system, for example, that can then go through an entire system to wreak havoc on the business. And then lastly, of course, everyone's talking about it. So it's not unique to manufacturing, but artificial intelligence and machine learning, right?

00:09:44:07 - 00:10:18:00
Unknown
In the manufacturing context, we can think about inventory management, supply chain considerations, ways in which I can help you predict or anticipate maintenance needs or get ahead of your support considerations. So there's real potential value in using technology in manufacturing. So obviously we've touched across some of these. But I think in addition to your cost effective solutions, your resources, your efficiencies, the technology also can set you apart in the market.

00:10:18:03 - 00:10:44:10
Unknown
Right? Being innovative, demonstrating to your stakeholders that you are taking advantage of new efficiencies to help keep their costs down, to help provide your products and services to them in a more meaningful, streamlined and efficient way. It's also critically important. But again, with that comes the responsibility to anticipate potential risk in the privacy and security space and mitigate that potential risk as well.

00:10:44:10 - 00:11:14:16
Unknown
So that's what we will focus on today. So from a privacy perspective, we are thinking again about third party related risks. And this is that previous slide. Are you engaging with cloud service providers external vendors or

service providers that are providing software as a service, platforms as a service, or even the use of AI tools? These can inadvertently introduce both security vulnerabilities as well as privacy risks.

00:11:14:16 - 00:11:40:15
Unknown
Because again, data is leaving essentially the four corners of your business and going into the hands of somebody else. So thinking about data handling restrictions that may attach to the data, the confidentiality which we see here on this slide as well, any obligations that you have agreed to with your own stakeholders and customers that may carry over with that data, need to trickle down to your vendors and your cloud service providers.

00:11:40:15 - 00:12:10:11
Unknown
And yes, AI tools from an AI perspective, we're thinking about things like proprietary information, intellectual property information, yes, confidential information and personal information that you may input into a tool that you no longer may have control over. So understanding how the technology works and again, ensuring that you have the appropriate safeguards in place in addition to your legal compliance, is the key way in which you can help address these key privacy challenges.

00:12:10:11 - 00:12:38:14
Unknown
And of course, from a privacy perspective, it really is a never ending game of whack a mole. In addition to international laws, federal regulations, maybe from the Federal Trade Commission, the SEC, etc., we are seeing 19 now, different state privacy laws on the books, and we'll talk a little bit about that. So how do you comply in a patchwork environment can be a real challenge for manufacturers, in this space as well.

00:12:38:20 - 00:12:43:23
Unknown
So change you want to touch on some of the, security challenges.

00:12:43:23 - 00:13:03:01
Unknown
top of the list cyber attacks poll after poll after poll has reported that it is the number one concern in the boardrooms. The SEC has, mandated by rule that, if you're publicly traded, you've got to have somebody with cybersecurity experience on the board.

00:13:03:03 - 00:13:26:18
Unknown
And they don't delineate exactly how robust that, experience needs to be, but it's just proof that it is a extremely large concern. And it's, I think it's wise to just presume that it's not a matter of if you will be hacked, compromised. It's when it will be and how you'll be able to respond to it.

00:13:26:20 - 00:13:58:23
Unknown
So that's obviously number one. Number two, legacy system integration. What that is, is essentially as we're always up operating our operational systems. Microsoft, every time they have a large change like the most

recent ones, Microsoft Office 365, which came with the Windows Defender, things like that, big improvements, wonderful things to see that have really been game changers to a whole lot of issues with cyber security.

00:13:59:00 - 00:14:23:17
Unknown
But sometimes our legacy systems are hardware or the software that we're running in the background is incompatible. Working through that can be very hazardous. And if we don't understand the the gaps that occur when we have a new OS running on a legacy system, it's just an opportunity for the bad guys to get in. And similar to that is the physical and digital convergence.

00:14:23:19 - 00:14:57:12
Unknown
This gets into the operational technologies, that we'll be talking more about, but actually having software run flows, think water, electricity, anything. And, you know, utility. If you are in a manufacturing entity, it can be your operations, how you put together things to sell, to take to the market. And as this physical meets the digital, it also creates gaps and seams that have to be thought of, and also the safety aspects.

00:14:57:14 - 00:15:30:09
Unknown
And finally, insider threats. And, I'm going to throw a curveball at you here. When I think of insider threats, it's not that much, although it's a concern somebody's behaving badly taking information they should not. I've got a couple of matters on that right now, but far bigger than that is the insider threat that you don't know who it is, and it is that person who isn't paying attention during October when they do their cybersecurity training and they are not getting it.

00:15:30:09 - 00:15:52:06
Unknown
And when they get first, they are just curious. They want to see what's going on. And then they click on an executable without meaning to, and they're hacked and they don't even know it. So these are the kind of challenges that your OT, your IT director, CTO or wrestling with on a daily basis. And we'll dig in more to that.

00:15:52:07 - 00:16:11:17
Unknown
Yeah. And I think what's so interesting here, Jane, when you're talking about insider threat, is that for years you hear about cyber hygiene. And it really does come back to that over and over and over again. You can have all of the systems in place. Right. But if you're if the folks on the inside are clicking on links, they shouldn't be clicking on, will there go your defenses.

00:16:11:17 - 00:16:34:05
Unknown
So it really is a signif. It's it remains a significant issue given all that we still know about cyber attacks today. So the silly part of is why you are here. We want to make sure we cover that as well. So these links should be, active and you should be able to access the relevant laws that are on regulations that are on this page, as well as some of the upcoming cases.

00:16:34:11 - 00:16:58:05
Unknown
As Molly said, if you need additional information afterwards, please don't hesitate to let us know. But talking about that patchwork of international and domestic, so international and U.S privacy laws and regulations, I'm sure we've all heard about the GDPR, the EU General Data Protection Regulation and its recitals. The reason we all know about this was because it was the game changer.

00:16:58:05 - 00:17:22:14
Unknown
It was the first such comprehensive regulation in the European Union that also applies extraterritorial. If individuals are directing their business activities to individuals in the EU, or gathering information about individuals in the EU, and it remains the baseline for privacy and data protection in the EU. Since its passage in about 20, I think it was 17 or 18.

00:17:22:18 - 00:17:49:21
Unknown
We've seen more, regulation in the European Union targeted at specific activities, including the EU, AI act and of course, the EU Eprivacy directive. That was long before the GDPR. But that is what is responsible for a lot of those cookie banners that we see, right, requiring consent to collect information about individuals online. One thing on a flag is to keep an eye out on what is happening in the EU.

00:17:50:01 - 00:18:15:07
Unknown
We're seeing a lot of conversation, especially in the AI space, and we hear a lot of this chatter in the United States as well about innovation balanced against regulation. And what we're hearing in the EU is that they're starting to reconsider, really take seriously this balancing approach in that perhaps, their regulations have gone a little too far on the pendulum.

00:18:15:07 - 00:18:45:19
Unknown
So keep an eye out for whether we will see the regulations change, whether from the GDPR perspective or even from the EU AI perspective. So that brings us to California and certainly in California, being one of the largest state was informed by the GDPR. And they passed both the California consumer Privacy Act, or CcpA, followed by the California Privacy Rights Act, which are both implemented by implementing regulations.

00:18:45:24 - 00:19:21:22
Unknown
California clearly is a key player in the United States. It was the first. It is unique in that its law applies not just to, consumers, which are really just defined as residents of California, but it also applies in the business to business and the employment context. So you want to keep that in mind. So when you think you don't have any privacy related issues in manufacturing, it is likely to come up in the context of your online activities, your employment activities, and including the information that you may be collecting from your business contacts who are California residents.

00:19:21:24 - 00:20:07:18
Unknown
But while California is incredibly important, and I do not mean to dismiss it, it is no longer the standard bearer. We have 19 other scandals comprehensive consumer privacy laws in the United States, three of which have yet to come into effect and will come into effect in 2026. So, what is important to know about these laws is that they each have a threshold for applicability, meaning do you meet the standards for covered entities and all but two Nebraska and Texas have thresholds for the amount of personal information you collect, the number of citizens or residents of a particular particular state on whom you have personal information, and the ways in which you use that

00:20:07:18 - 00:20:45:12
Unknown
personal information to enhance your gross revenue. The exceptions are Nebraska and Texas, which do not have threshold applicability. Other than that you conduct business in the state and that you have information about a Texas owner or Nebraska resident. Interestingly, however, because of that low threshold, Nebraska and Texas did implement a small business exception to the law. So if you meet the definition of a small business under the SBA's definition, then you may be exempt from those laws, except when it comes to what is called sensitive personal information.

00:20:45:12 - 00:21:09:21
Unknown
And and disclosing and sharing that information. California also has a threshold applicability standard of over $26 million if your annual gross revenue is over $26 million, you are covered by that law and will need to comply. One thing I wanted to flag before we move on is watch out for the newest player, Maryland. Maryland's data privacy law came into effect on October 1st.

00:21:09:23 - 00:21:36:20
Unknown
It is an outlier. It has lower threshold applicability standards given the population of Maryland, as well as stricter what we call data minimization standards, meaning the standards for the information that you can collect and how you can use it are much stricter than what you see in other states. So if you operate in Maryland, please, please, please be aware that there are new laws in effect.

00:21:37:00 - 00:22:02:04
Unknown
And if you have questions about that later, we can go into much more detail. But do take a look at it from definitions of biometric information, minors information meaning under the age of 18, sensitive information and consent. Maryland is an outliner, meaning that if you want to collect information about a Maryland resident in the course of your business, even if you don't need it for your business, and they say, okay, you still can't collect it.

00:22:02:04 - 00:22:28:09
Unknown
Consent is not a viable reason to collect information you do not need in Maryland. Add to that the Federal Trade Commission, with its unfair and deceptive trade practices, authorities as well as other international laws

like India that has been passed but is not yet in fact, again, this can be very overwhelming and very complex given the nature of your business and where you do your business.

00:22:28:11 - 00:22:59:01
Unknown
But there are key similarities and differences across the jurisdictions. So considering the scope of the application, whether they have extraterritorial reach, right? For instance, in the United States, are you doing business in that particular, state and in EU, or are you doing business in or targeting your business activities to individuals in the EU? Again, I flagged this difference between business to business versus business to consumer and application to application employees.

00:22:59:03 - 00:23:22:22
Unknown
Generally speaking, GDPR in California apply in a business to business context, in a consumer to business context, and in an employment context. Whereas in many of the other US states do not. So understanding from who you are, getting your data and for what purposes is critically important in understanding how it needs to be handled. Same thing. Consent requirements and definitions.

00:23:23:02 - 00:23:49:05
Unknown
Those are somewhat similar but sometimes different. So you need to know about, those requirements. User access rights. We've become very familiar with these. Whether it's access to my information, the right to know what you have about me, the right to delete my information, the right to correct it, the right to opt out of use of my information for advertising, or for drawing of inferences.

00:23:49:05 - 00:24:13:08
Unknown
Right. We see a lot of similarities, even though they may be somewhat unique. If you can familiarize yourself with some of these key some similarities, it really does give you a good foundation for how to approach your data privacy program at your respective business. One public service announcement I wanted to make is about data broker laws. In this question of are you a data broker?

00:24:13:14 - 00:24:39:05
Unknown
Especially in California. Late last year, California revised its, regulations with respect to data brokers and a lot of businesses overnight became data brokers that never would have thought that they were a data broker. And this is because traditionally, data brokers are considered to be entities that gather or sell, use information of individuals with whom they do not have a direct relationship.

00:24:39:07 - 00:25:01:19
Unknown
California, yes, follows that definition, but also says if you as a business had a direct relationship with an individual but haven't engaged meaningfully with that individual in the last three years, and you still use their information, then you may be a data broker, which means that you have to follow the registration requirements, which is a fee, and subject to fines if you don't do it.

00:25:01:19 - 00:25:17:21
Unknown
So keeping that in the back of your mind again, the ways in which you use data, where you got it from, how you use it in Y can really impact and trigger other laws. So, Molly, do we have any questions yet?

00:25:17:23 - 00:25:39:14
Unknown
None at the moment. Okay, great. So please do not hesitate to throw them out there. We will we will pause and address those. So here are some recent enforcement examples. Even if you're not in the privacy space, I'm sure you're familiar with the matter of Facebook. Fine. In the EU this was again for online lawful behavioral advertising, €1.2 billion.

00:25:39:14 - 00:26:05:20
Unknown
So Europe means what they say. In the United States we're seeing significant enforcement activity, obviously out of California, who just last month, entered into its largest settlement to date against the company Tractor Supply. You'll see some similarities here on this slide between Tractor Supply and Honda and even the Todd Snyder case out of California. These are, very unique businesses, right?

00:26:05:20 - 00:26:47:22
Unknown
Honda is a different type of business than Tractor Supply is. But the reasons in which they found themselves within the crosshairs of the California Privacy Protection Agency are not that unique and really do apply to really any business, that does business online, right? If you have a website, if you have an app, pay close attention. So these companies, entered into settlements with the California Privacy Protection Agency because the agency alleged that their privacy policy in the Tractor Supply case failed to notify consumers of their data subject access rights, those delete, correct.

00:26:47:24 - 00:27:08:14
Unknown
Access rights, opt out rights. They failed to notify California job applicants of their privacy rights and how to apply them. Again, California applies to applicants and employees in ways that other states may not. They failed to give you an effective mechanism to opt out of selling and sharing of personal information. Again, you see this come up a lot in the context of cookie banners.

00:27:08:14 - 00:27:33:00
Unknown
But that's not the only ways in which you may engage individuals. Now there is something called a universal opt out mechanism, or an opt out signal that browsers can send to businesses automatically, and that covered entities must recognize to opt out individuals from collecting and selling of their information. Again, I could be an individual with whom I don't have a business relationship with your manufacturing company yet.

00:27:33:06 - 00:27:57:02
Unknown
Nonetheless, I come to your website and you may collect my information. You have privacy obligations, or you may have privacy obligations related to users of your website. Honda, similarly, was was deemed for data

subject access right and making it easy for individuals to implement those in proper use of a privacy management tool. This is your cookie banner, right?

00:27:57:02 - 00:28:23:07
Unknown
We see a lot of companies that offer privacy compliance tools online. The gist here is that irrespective, it is still your responsibility to ensure that those tools and those companies are doing what they say they are doing and working correctly. So it's not one and done. Yes, sometimes you can throw money at the problem, but you do have to stay on top of the compliance mechanisms you are using and make sure they are effective and meaningful.

00:28:23:13 - 00:28:47:13
Unknown
And then I cited a few other cases here that you may want to take a look at. Obviously, we're not talking about the health care context today, but those are good, cases for you to be aware of, to understand the ways in which the federal government is looking at the improper use of pixels online. So, again, here we are on, identifying risks online.

00:28:47:13 - 00:29:10:22
Unknown
And I raised this because in my work I have been with manufacturing clients. This is where I see most of the risk or privacy issues come up. Do you have a website and or do you have an app? Right. So again, we've seen a lot of regulatory focus on digital tracking tools that enable advertising online. I know what you're going to say.

00:29:10:22 - 00:29:31:15
Unknown
Everybody does it. Yes they do. And sometimes this can be considered a cost of doing business, but nonetheless it can be an expensive cost of doing business if you're not doing it. The right way and an enforcement authority comes around again. We see this in the context of third party cookies, tracking pixels and mobile SDKs and fingerprinting tools.

00:29:31:17 - 00:29:52:06
Unknown
Symmetry in your opt out versus opt in. And if you are a frequent web user like I am, I'm sure you've started to notice cookie banners that previously said accept or learn more. Now they are starting to say accept all, reject all, or manage. What this means is that you must have symmetry and opt out versus opt in.

00:29:52:08 - 00:30:12:12
Unknown
So if it only takes you one step to opt in, it can only take the individual one step to opt out. They cannot be required to click multiple times and go down a rabbit hole to opt out. So are your cookie banners compliant? That's a first kind of shot across the bow to an enforcement agency that you may not be compliant in your privacy practices.

00:30:12:14 - 00:30:40:11

Unknown
We already talked about the universal opt out mechanisms, and if you're interested and think this may apply to you, I urge you to look up global privacy control. It's the most widely used, mechanism. And they have a lot of great information for those who are implementing and receiving the signals. And then finally here another side note if you have a website, you may be at risk of what are called California Invasion of Privacy Act claims.

00:30:40:13 - 00:31:04:24
Unknown
We're also seeing these come up at the federal level under the Electronic Communication Privacy Act. In short, it is a very, unique interpretation of the law that collecting information about individuals on your website without their consent and sharing it with third parties, like for instance, meta, Facebook, Google Analytics, etc., somehow invades privacy. These are nuisance claims.

00:31:04:24 - 00:31:27:12
Unknown
They can be very expensive to settle. And so it's really a matter of timing of when those cookies and tracking technologies are firing on your website. So all of this is to say, again, in the manufacturing context, even if you find that you do not carry a lot of personal information, in your day to day activities, if you have a website or app, these laws may apply to you.

00:31:27:14 - 00:31:59:04
Unknown
So over time, okay, little color commentary, just to put emphasis on what Mason saying from a litigation point of view, I've handled dozens of these cases. The California invasion of Privacy Act and it's, it's irritating. It's frustrating. But if we end up having clients, that get sued and they've got pixels running on their website, they had no idea were there.

00:31:59:06 - 00:32:24:18
Unknown
I had one last week where someone, just came to us and said, hey, we need to check out our own website. We're not sure what's there, but here's what we think's running. And they add about ten different third party cookies on it. We ran the analytics on it. We found 76. So, if you don't know what's running on your website, a lot of it can get you in trouble.

00:32:24:20 - 00:32:52:06
Unknown
So just take a quick look at that. Have your, it people do some analytics and you might be surprised at what you're running. So enough of that. What manufacturers are up against from a cybersecurity point of view, I'm just want to give you a lay of the land going on right now with manufacturing, in cybersecurity, the global medium dwell time, that's a fancy word, fancy phrase.

00:32:52:06 - 00:33:20:15
Unknown
For how long are the bad guys in your network before you know it? From whichever way, it used to be in, measured in months and it has plummeted down. It's gotten a lot better. But they're still in networks for way

too long. The global media. And according to Mandiant, one of the most authoritative sources for information is 11 days for external notice.

00:33:20:17 - 00:33:46:06
Unknown
And that is where, someone, a third party comes in and says, hey, you've got a problem here. It could be the federal government, law enforcement, a lot of different things. It's ten days for internal notice. That's where somebody on the inside in your company realizes we've got an anomaly or something's not running right. And they do an investigation, and they realize there's bad guys in the network.

00:33:46:08 - 00:34:10:12
Unknown
And then five days from the cyber attackers themselves, those. And these are typically the guys who just want a quick payoff. They dry out as soon as they get in. They will, file transfer protocol as quickly as they can. Some of your sensitive data, if they can find where it is. And once they get that downloaded, they'll make themselves known.

00:34:10:12 - 00:34:33:01
Unknown
And frequently they will encrypt a whole big part of your network. But that just makes the point that bad guys can be in your network, and you won't even know it for a while for a lot of different reasons. Phishing emails. This, fascinating statistic about a third of all phishing emails are open by the recipients. That sounds good.

00:34:33:03 - 00:35:03:10
Unknown
But, you know, we're getting it down because it used to be all of us were opening these things, but now we got it down to a third. But that 30% leads to 91% of all cyber attacks, according to analysis done by VentureBeat. So what that is driving is we've really got to do a better job of educating our people and then testing them, finding out if they can really hold up to a very convincing email, a phishing email.

00:35:03:12 - 00:35:23:23
Unknown
I have done that kind of training before, and we do it here at our firm at Frost Brown. Todd and I kind of boasted a little bit that, you know, I've seen I've seen everything. And then I got an email from my daughter, or so I thought. It was the guys who had heard. Oh, yeah, this guy thinks he's immune.

00:35:24:00 - 00:35:46:20
Unknown
And so they sent me a phishing email. You know, the good guys did it, and I fell for it because it was tailored, socially engineered to me. So I say that just because all of us are susceptible to these things and we're never going to eliminate it, but we can still train it down to the greatest extent possible.

00:35:46:22 - 00:36:14:12
Unknown

The number of espionage motivated cyber attacks, appears to be, driven a whole lot by the Chinese. And I'm going to talk about that in the next slide. Actually, this next slide here. And that is, when I say the Chinese, the People's Republic of China, the Ministry of State Security sitting in Beijing, and they there's three different groups that work there that are really starting to get into our networks.

00:36:14:14 - 00:36:42:24
Unknown
The one that's the scariest is the one that's gunning for you, is the one that's coming after manufacturers and utilities, and that is Volt Typhoon, according to the FBI. And I would just say that there's not a doubt in my mind, based upon my prior experience in Fort Meade, that it's the People's Republic. And what they are doing is, they are laying in malware in places where you would not expect to see it.

00:36:43:02 - 00:37:05:19
Unknown
Maybe it's running in memory in what's called a Mimi cat attack, which and I want to get technical, but it's basically living off the land. They are so good at what they do that they embed malware into your network. And you have you really can't find it unless you're using all kinds of sophisticated juristic to see trend lines and things like that.

00:37:05:21 - 00:37:32:23
Unknown
The goal is to bring is to bring your network down if they ever need to. And that is typically oriented toward, Taiwan. If there's a war over Taiwan, they don't want the United States to come to Taiwan's aid. And this is coming from the FBI. And what they will do is go after your network at that point, they will activate, the malware and bring everything to a halt.

00:37:33:00 - 00:37:59:02
Unknown
Now, that might be in your IT network. It might be in your own network. But either way, it's just sitting there and it could be there for years. In the FBI and the, Cybersecurity and Critical Infrastructure Agency, are both saying that we don't know how pervasive this is. So the best thing we can do is really double down on, your mistakes.

00:37:59:02 - 00:38:29:09
Unknown
And looking at things, in our networks, whether it's operational or it. And find out what's going on. Saul. Typhoon is related. It's just as bad, but it's more at the, internet service providers, cell phones. And they, have gotten in to a lot of communications. And there were news reports that the highest levels of the federal government, people using their personal cell phones, were infiltrated by the Chinese through Salt Typhoon.

00:38:29:11 - 00:38:51:24
Unknown
So they and this is true according to CrowdStrike. So you can see that this is a insidious problem, but the one that we really have to be concerned about in manufacturing is Volt Typhoon, 60% of file sharing phishing attacks, which is kind of technical. I'll save you the explanation. But they have gotten so good the bad guys have.

00:38:51:24 - 00:39:24:03
Unknown
And these are typically Russian gangs that they use legitimate sending domains and leverage that to steal login credentials, of various types in MFA, the whole bit. And then finally, from the time that ChatGPT four was, debuted in November of 2023, the bad guys started leveraging it. And you can see this the abnormal report is, quoted here, but you can see just about anywhere in that six months.

00:39:24:05 - 00:39:42:23
Unknown
Gen AI tools, increase the number of cyber attacks by 50%. And I've read in some places that it's now over 150% from that November timeframe. So give me the next slide, please. Mason.

00:39:43:00 - 00:40:12:00
Unknown
Okay. Incident reporting a critical infrastructure, manufacturing is considered by the federal government to be a critical infrastructure. Most of you probably know that, two days after Russia invaded, Ukraine, Congress passed this law. They had been going back and forth with it for years, literally. It was strongly recommended by the federal government under both the Trump administration and the Biden administration.

00:40:12:06 - 00:40:50:17
Unknown
But Congress, for various reasons, never enacted it. It just took, 48 to 72 hours for them to pass it after that invasion. So the key to all of this is when they're going to read the slide to you. You can see what, what it covers. But the key is the regulations that are going to enable the 72 hour reporting that you have to do as a manufacturer if you are hacked in a covered cyber incident, covered entity wasn't defined, covered cyber incident wasn't defined.

00:40:50:19 - 00:41:25:17
Unknown
Preservation of data was not defined. So we've all been waiting for those regulations to hit. And they finally came out in April of this year. And they were, while a step in the right direction from my point of view, from the manufacturing, the collectives, like, all the, manufacturer association of manufacturers across the United States were critical of it, and they were so critical because the, what is a cyber incident was extremely broad.

00:41:25:19 - 00:41:51:11
Unknown
The 72 hours, okay. Starting when? Because you can be hacked and you don't know what you've been hacked in, you don't know what to report, you don't know hardly anything. So that was that was criticized and, covered entities. Okay. We're in manufacturing, but there's nothing critical about us. We make baby wipes, you know, whatever it might be.

00:41:51:13 - 00:42:14:19
Unknown
It was a little bit too broad. So Cisa has taken those regulations, those comments to heart, and they have delayed the implementation by a full year. They are going to roll out the revised, hopefully heavily revised,

regulations and that those will come out in the year. I believe it's going to be a year after the initial publication.

00:42:14:19 - 00:42:38:09
Unknown
And at last I saw that was April of next year. So, Mason, if you give me the next slide, I want to make sure we, we have 16 minutes. So I'm going to move a little bit faster here. Most of you manufacturing have operational technology networks. Those are your industrial control systems your programable logic controller data systems in electricity.

00:42:38:11 - 00:43:03:12
Unknown
And these are what make our, your businesses run. An IoT network can go down and you're going to keep on ticking. It's going to be a hassle. There's going to be people upset. There might be people fired, but typically the company is going to continue forward. But if your operational technology network goes down, everything grinds to a halt.

00:43:03:14 - 00:43:25:08
Unknown
The most well known, operational technology network actually was an IT attack. And that was the Colonial Pipeline attack back in 2019, 2020. And I remember that vividly because I was in the Pentagon. I was on duty at the time, and I had an aide walked in and said, sir, do you have you up if you build your tank with gas?

00:43:25:10 - 00:43:44:10
Unknown
And I thought, that is a very weird thing to be asking me. Why are you asking if she pointed to the window to where the Pentagon's gas station used to be, and it was lined up for as far as you could see over a mile? And I said, what's going on? And she said, Colonial Pipeline has shut down all the pipes.

00:43:44:12 - 00:43:53:05
Unknown
There's no gas flowing anywhere. So whatever's at the gas stations is all we're going to get. So everyone was lining up to fill up.

00:43:53:07 - 00:44:21:01
Unknown
That really was an IT attack. And this is a very important point to understand. Colonial Pipeline shut down everything because they had an I.T. attack and they were ransomed by, the, Russian gang. And when they were ransom, that means everything was encrypted. And suddenly they could no longer see what they were selling. All that gas going out was unmeasured, and it was unknowable.

00:44:21:03 - 00:44:50:06
Unknown
So in order to save the company, they had to shut everything down. And that's what led to this, this panic on the East Coast, which was the genesis of, sir, see this statute we just looked at. Now, your own network

doesn't use words. It uses values and commands. It, doesn't have a whole lot of privacy concerns because privacy data is not there, but it the network availability is has to be high.

00:44:50:06 - 00:45:23:03
Unknown
It has to be on all the time. But yet it's very fragile. So Ferc, the electronic the Federal Electronic Regulatory Commission has been very concerned about the bulk electric systems at the utilities, which go to support manufacturers everywhere. And this is a harbinger of things to come. They recently mandated internal network security monitoring, commonly called NSN, for certain systems on the OT side.

00:45:23:05 - 00:45:43:15
Unknown
Now you prob you're probably thinking if you know much about your own LTE network, well, there's an air gap they can't get in. Well we seen the Russians do it. Now the Russians have gotten into some OT networks that were air gapped and, didn't happen in the United States, but there have been some very suspicious things happen here.

00:45:43:17 - 00:46:11:23
Unknown
The well, I won't go into them in the interest of time, but this, internal network security monitoring is probably going to be coming to other OT networks as things mature. And it's just a good thing to be familiar with the fact that we already are having to do this with our electrical utilities. It's going to be a bigger thing for, operational, technology networks as we move forward.

00:46:12:00 - 00:46:35:15
Unknown
So next slide please. Mason. So how about we jump Gene to one of the use cases folks will have, this but we could quickly go through some of the I, I use case. I think that could be helpful in our last few minutes. Yeah. Let's back up one though, just so we understand what the risks are.

00:46:35:17 - 00:47:05:12
Unknown
These are the things that you have to worry about from a legal point of view. If you're going to use AI in your operations. Worst you can see, AI is being sold it, gene. AI primarily. And that's the low hanging fruit for AI. As it gets better and, and improves, you're going to see more and more artificial intelligence running operational networks, which means you're going to have to integrate your IT with your AI in most instances.

00:47:05:14 - 00:47:33:06
Unknown
So that introduces IP problems, privacy problems. And you I'm not going to read all these. Please take a look at them. But these are the eight main areas where you have to be concerned with legal risks. If someone comes to you with a great idea, pull this out and take a look at it. And this is what you should be taking into consideration from an AI governance legal risk, perspective.

00:47:33:09 - 00:47:57:16
Unknown

So next slide please. And remember those vendors we were talking about earlier. We see so many vendor agreements that include the use of AI for no purpose. Right. And so essentially, you know, the supports the person receiving the service. So essentially they're taking data and training on it and learning from it. And so you really want to be aware of that in your contract negotiations.

00:47:57:18 - 00:48:23:08
Unknown
So I won't give you use cases on all of these. We'll just use a couple. I already covered electricity, but using, operational technology, your wrist sticks to monitor for for threats. Now, normally, your instincts aren't good. They are, you know, bias and things like that in the human mind. But in technology, a juristic is a rule.

00:48:23:10 - 00:48:55:06
Unknown
And so you want ot your ot your wrist to monitor flows in just about anything. Now, that's not just electricity. It can be water. It can be your production line. It can be just about anything. And the OT can be used, bringing the it in, from a is there a threat here? Are we looking at things correctly in a AI running in the background to instantaneously figure out what's going on?

00:48:55:08 - 00:49:26:03
Unknown
Looking at the cross sector predictive maintenance, I have a client right now who's looking at unloading, AI into their networks. On the IT side to do some, predictive maintenance, not just look at the, you know, okay, we've been doing this many hours on this network, but I actually understand from the flows, the values, the the protection emphasis, the delay impact and things like that to keep up with everything.

00:49:26:05 - 00:49:49:16
Unknown
And you take the humans out of the loop. So each one of these is a specified area where you will be able to punch above your weight in the legal department just by asking those questions. If you combine this with the previous slide, thinking about AI governance, you will be ahead of the game. So, Mason, I think we have about nine minutes left.

00:49:49:18 - 00:50:09:20
Unknown
Yeah. So we'll jump in here very quick into why does this really matter and what should you be doing next. So I know that was a lie. I know it can be very scary and so very overwhelming. And some of the privacy perspective, I think there's a couple things to keep in mind. Again, as I said at the top, there's no one way to comply.

00:50:09:21 - 00:50:39:13
Unknown
Right. And so really being specific to the ways in which you do your business, the ways in which you engage with your customers and using those, advantages and the flexibilities in the law can really, to really help distinguish yourself in the marketplace and build and maintain trust with your stakeholders. This not only gives you a competitive advantage, in, you know, today's time, but it can also help you when it comes to mergers and acquisitions later.

00:50:39:13 - 00:51:12:15
Unknown
If you want to sell your business, ensuring that you are compliant with data security and privacy requirements and practices are key considerations in M&A. We have seen significant deals fall through or significant costs on the other side of a deal because security vulnerabilities were not appropriately patched, because privacy considerations were not appropriately considered. So it is important from the beginning of starting a project to the end of selling a business, that these considerations flow through throughout your process.

00:51:12:17 - 00:51:32:20
Unknown
And again, what can we do? So Gina and I will jump in here together. But what you should be looking at is James, at one hour a day, he spends reading continuously, keeping up with the global legislative changes and assessing whether and how they may apply to you is a good place to start thinking about privacy and security by design.

00:51:32:20 - 00:51:58:00
Unknown
And what do we mean by this? We mean by having the right folks in the room at the front end. If any time you are thinking about doing a new project activity, solution that involves technology, making sure that you have your IT folks, your privacy folks, your counsel, right? All of the all of the stakeholders within the company at the table when decisions are being made.

00:51:58:00 - 00:52:20:17
Unknown
This will help you build in efficiencies and safeguards along the way, which will only help you, save money and time on the back end. I think privacy has security folks, especially privacy folks, get a bad rap. As you know, we're slowing things down. We're constantly saying no. I would say about 85% of the time if that's because we're brought in at the last minute.

00:52:20:23 - 00:52:47:13
Unknown
Right. And so change is critical. Changes need to be made which can slow down a project which can cost more money and time and resources. So if we're part of the conversation on the front end, this only helps you on the back end. Awareness and accountability. Again, this comes from the top down. This comes from leadership establishing that these are our core, principles and priorities training, anticipating security incidents.

00:52:47:13 - 00:53:11:20
Unknown
Like Jeanne said, it's not a matter of if but when doing those tabletop exercises, having those incident response plans and policies in place, practicing to mitigate your potential risk is key. And something that you can certainly wrap your arms around and do. Responsible use of AI, right? Ensuring that you actually have a specific use case for AI, not just from the top down.

00:53:11:20 - 00:53:39:24

Unknown
Everybody needs to be using AI. We come across this a lot with our clients, and it's a really great mandate, especially from an efficiency perspective. We are leaning into the use of AI, as, as well, but being very clear about why you want to use it, for what purposes, how it's going to help you achieve your goals and then putting around those use cases, the specific guardrails that are unique to the data that's issue, the security implications at issue.

00:53:40:04 - 00:54:05:06
Unknown
This is what we mean by data governance. Right. Putting in place the appropriate mitigation measures because at the end of the day, again, security and privacy is not a risk elimination business. It is a risk mitigation business. You have to be able to still run your company and do your business. You just have to anticipate the most likely risks and mitigate those.

00:54:05:06 - 00:54:39:03
Unknown
And I would, suggest that this conversation about innovation, versus privacy and security and regulation is kind of a false start, right? These things are not mutually exclusive. You can have good innovation while still ensuring that you're doing it the right way. So a privacy and security perspective. And then, of course, one of the things I found for my particular clients in the privacy space is that having good privacy practices and being transparent about what you do and saying what you do and doing what you say are critically important, right?

00:54:39:03 - 00:55:05:19
Unknown
Each of us has received a cyber security letter in the mail. Our data has been breached. We've been through that. We know how it works. So some companies have been able to distinguish themselves in the marketplace because of their privacy safeguards. Right. Individuals are savvy new generation of users. Tech users are very savvy. They are making choices about which companies they engage based on sometimes their privacy practices.

00:55:05:21 - 00:55:38:06
Unknown
One thing I failed to mention earlier, and then I'll turn it back over to Jeanne in the context of vendors, any obligations you have from a cybersecurity perspective or a privacy perspective, carry through with your work with vendors and service providers and third parties who help you do your business. So if you have made, for instance, representations to individuals about how you will handle their information or the appropriate security, protections that you put in place, you need to make sure that your vendors are subject to those same requirements, too.

00:55:38:08 - 00:56:00:10
Unknown
And in those cases, I previously showed you with Honda and Tractor Supply as examples, those were also critical enforcement actions that they faced in California for failing to ensure that they had the appropriate contracts in place with their vendors and service providers. So we really cannot stress enough, be sure that you know what is in those agreements and negotiate to the extent you can.

00:56:00:12 - 00:56:33:04
Unknown
Sometimes you're going to have to make hard decisions about the vendors you work with because of their privacy and security practices, which will only set you up, in a more favorable position down the line. So, Jane, any last thoughts here? Yeah. Let me hit two things. First, we've mentioned, governance a couple of times. And when Mason and I have worked, with clients before on governance, sometimes even in the legal office, you can see the fog come in, the eyes glaze over is like, why are we doing this?

00:56:33:06 - 00:57:00:07
Unknown
It's absolutely essential if you're going to have, a really good plan to get after all the stuff Mason just talked about, to have a, a governance plan and simplified. It's just understand mapping your network for privacy for, the risks and understanding what your data is, what kind of data you have. Is it encrypted? Yes. Just map your data.

00:57:00:09 - 00:57:29:06
Unknown
And then what's the risks there? Identify them and then try to mitigate them. And if you can't mitigate them, then manage them. And then finally integrate all that into your operations. That's really all governance is, is just to simplify it. So strongly encourage you if you don't have a strong governance program, to take a good, hard look at it, because it will save, a lot of headache, maybe heartache down the road.

00:57:29:08 - 00:57:56:02
Unknown
Finally, for me, I think everybody here is probably seeing the Big Bang Theory. And I use that because everyone's seen it. There's a point here. Schrodinger's cat comes up all the time in Big Bang. Sheldon loves that conundrum. And that is simply where this physicist, German physicist, conceptualize is putting a cat into a box, closing the box up.

00:57:56:04 - 00:58:21:22
Unknown
And then is the cat alive or dead? I don't know, I won't know until I open it up. Okay. That's how you need. Seriously, you need to think about your network the same way you think about Schrodinger's cat. And if you have a thought about Schrödinger's cat, then let's think about your network. You don't know if it's there's bad guys in it at any one time or not.

00:58:21:24 - 00:58:47:15
Unknown
You simply do not know in your IT, people will not be able to say with 100% assurance whether or not that is true. So you have to be resilient. That whole concept leads, inevitably to can I recover quickly? What is it that's going to allow me to get right back up on my feet? So resilience is the name of the game in cybersecurity.

00:58:47:19 - 00:59:03:22
Unknown

Presume that you're going to be hacked or you have been hacked. Now what am I going to do to get on my feet? So I think we're just about we are out of time. I think, I think you can see the conclusions there. Any other any questions?

00:59:03:24 - 00:59:34:24
Unknown
None at the moment. No. Well, as we said at the top, here's our contact information. And in case anything comes up related to the project or on or to the presentation or unrelated, really, at the end of the day, I know again, this was a lot. What we focused on is operationalizing these things right? These these are, privacy and security really are a of a complete part of the package that can help you achieve your goals in a responsible way and mitigate risk.

00:59:34:24 - 00:59:59:10
Unknown
Right. They aren't necessarily barriers. They really do help build your relationships with stakeholders. They help keep your relationship intact. They help you on the back end when you're ready to sell or merge, right? They are key considerations, but they shouldn't be viewed as hurdles. They really are opportunities. And there's a lot of unique approaches to achieve compliance as well as to mitigate risk.

00:59:59:10 - 01:00:17:14
Unknown
And that's really what Gina and I try to focus on, even if that isn't what the presentation of the takeaways were, the presentation was a little scary. Things are out there, but there's a lot of flexibility and there's there's more than one way to skin this cat. And we're always happy to help, with that as well.

01:00:17:16 - 01:00:19:07
Unknown
Thank you all.