Leah Evert-Burks: This is Leah Evert-Burks with the Center for Anti-Counterfeiting and Product Protection @ Michigan State University and *this* is *Brand Protection Stories* - stories about the practice of brand protection by those who live it. In *Brand Protection Stories* we talk to those in the brand protection community about particular cases in their careers. Through some *stranger than fiction* real life scenarios we learn about the practice of brand protection and the challenges faced by brand-owners worldwide.
Josh Mayers: So we had to do the searches not only safely, not only in a way that preserved the digital evidence from any legal attack or challenge, we had to do it in a way that was not alerting to the company because they did have remote access to the wind turbines through internet connections, so we were concerned that they could if they got wind of it, change or put the licensed software back on and take the infringed software off. So, this was all unknown at the time, and we started like we do in any FBI operation: we planned. We gamed it out, you know, first on paper, then we actually went out and practiced and rehearsed, which meant myself and the technical agents with a lot of support from the Boston field office, actually planned and practiced how to climb how to, you know, put on the harness, how to a clip into the ladder inside, how to climb. You climb 80-foot sections and when you get 80 feet, there's a platform you can rest, you can stop.
Leah Evert-Burks: Josh Mayers retired from the FBI in 2018, with 34 years of law enforcement experience. Of those years, he spent 7 years working as a police officer/investigator in New York City and 27 years with the FBI as a Special Agent. With the FBI, Josh worked in most investigative capacities including violent crimes, drugs, gangs, bank robberies, public corruption and fraud cases. He also worked counterterrorism matters for over 10 years, with numerous deployments to the Middle East and Africa. Additionally, he was an FBI Firearms Instructor, Hostage Negotiator, spent 16 years on SWAT, taught interviewing and interrogation, as well as undercover operations to local, state and international law enforcement officers. As we will hear today, Josh was the FBI Case Agent for the 7-year long Sinovel Wind Group investigation and prosecution. Josh is a graduate of the 263rd Session of the FBI National Academy. He earned his B.S. in Criminal Justice from John Jay College of Criminal Justice in New York City in 1985; his J.D. in 1991 from Kent College of Law in Chicago, and an M.S. in Criminal Justice, with a concentration in Cybercrime and Cyber security from Boston University in 2020. Today, Josh is an Assistant Adjunct Professor, in the Center for Law, Society & Justice, Criminal Justice Certificate program at the University of Wisconsin-Madison; he also works as a private investigator and security consultant.
Leah Evert-Burks: Good morning, Josh.
Josh Mayers: Morning, Leah.
Leah Evert-Burks: So, on their paths to growth, many corporations acquire other companies, whether it be to fortify their place in a products category or service category, or to expand and diversify. It's common practice. Due diligence is usually performed as part of mergers and acquisitions, with best practices initiated, which may include things like trademark registrations, status value of other IP, a look at distribution relationships, current employee information, along with reams of spreadsheets and sales and consumer data. But how deep this due diligence should go when acquiring a company? This story, the Sinovel Trade Secret Theft Case, that we'll be talking about today, answers that question. It is the first criminal case against a China Corporation charged and convicted of crimes in the U.S. court of law. So Josh, I'd like to start first with an explanation of what trade secrets are, since this is a little bit of a different subject matter for Brand Protection Stories.

Josh Mayers: Thank you, Leah. I'm so glad to talk with you today about this case, and you're right--the discussion should start with understanding what a trade secret is. And the law is governed by the Economic Espionage Act of 1996, and a good source of information for listeners might be the U.S. Patent and Trademark Office which talks about trade secrets, and a trade secret is any information that has either actual or potential independent economic value, by virtue of it not being generally known. So again, it can be actual or potential economic value, as long as it's not generally known to the public. It has two other critical elements: all three are necessary. The trade secret must have value to others who cannot legitimately obtain the information, and is subject to reasonable efforts, or reasonable measures as the statute says to maintain its secrecy. You must have all three elements for there to be a trade secret.
Leah Evert-Burks: Okay, interesting. And it is intellectual property, correct?
Josh Mayers: Yes, that's right, and intellectual property comes in many forms as you know. It can be an idea, it can be a blueprint, it can be a design or an invention. In our case, it was software. It was software that was researched and developed by very smart engineers working as a team, who were able to develop software that helped when turbines operate efficiently and stay connected to the grid. And in this case, particularly important to the Chinese customer Sinovel was when there's grid instability, when there's a sag, you know we've all had that happen, maybe when we've been in a rainstorm and the lights in our homes dim. Well, that's a temporary sag in the power grid. That's the case here. The software was the trade secret that was developed by American Superconductor, the victim company.
Leah Evert-Burks: Right. And so those smart individuals were AMSC, and that was an energy technology company that was founded by MIT graduates.
Josh Mayers: That's right. American Superconductor is still a publicly traded company on the U.S. stock exchange. It was created by three MIT grads in the 80s, and they have a lot of different products, but the product here was wind turbine technology, primarily software that was used to keep wind turbines running and functioning online, and they had offices in Massachusetts, they had two offices in Wisconsin, which are relevant to this case, they had a large office in China, and an office in Klagenfurt, Austria, which is where the subsidiary Windtec was that they acquired which your setup alluded to. They did acquire an Austrian company called Windtec, and that's where really the team of software engineers in collaboration with U.S. engineers work to develop this wind turbine technology.
Leah Evert-Burks: So, that was in 2006 where they saw that growth opportunity potential for an acquisition of Windtec and of expanding some of their product offerings into the renewable energy market, which of course is and was a big business.
Josh Mayers: Yes, that's exactly right, and they were growing very quickly, so acquiring Windtec helped give them additional both human capital as well as an expertise in this niche of developing wind turbine software, which helped in grid stability something called *low voltage ride through technology*. LVRT was very important and was valuable and was something that AMSC was working with Sinovel with their largest client in China to develop this technology for Sinovel so that it would not only help the wind turbines operate efficiently but also retrofit thousands of wind turbines in China to modernize as part of the Chinese grid code stabilization that was going on in China in the late 2009-2010 timeframe.
Leah Evert-Burks: Okay. So, when AMSC acquired Windtec, they acquired their customers. They acquired the relationships licensee/licensor or relationship that existed with Sinovel, which as you indicated was a large company in the wind turbine business. I think they were third ranking at that time with aspirations to be the leading in the world. And as you said, there was some motivation for them if we look back at this trade secret

theft that occurred. As you indicated, there was an initiative to reduce air pollution and dependence on coal fired plants in China, so retrofitting of the software was required to meet the Chinese government standards. And as you said, prevent shortages and blackouts and the like. But license agreements can be expensive and so, Sinovel was looking at that expense that they were incurring with licensing the technology.
Josh Mayers: Yes, that's exactly right, Leah. It was expensive. Part of it is supply and demand. AMSC provided a unique product for Sinovel, and they had been working collaboratively with Sinovel for a number of years to try and meet their needs both retrofitting old wind turbines that were already online and operational and needed the software retrofit, as well as Sinovel's expansion, they were trying to be number one in the world for wind turbine manufacturing and so Sinovel was trying to expand outside of China. They were building wind turbines in various parts of the country and in fact, ultimately, they got a contract to build four wind turbines in Massachusetts, so Sinovel was in a large growth posture. AMSC was meeting that demand with not only quality electronics, support hardware, and then software but also servicing the wind turbines in China with employees of the American Superconductor and Windtec, and that involved one of our protagonists in the story. One of our defendants that was ultimately indicted and charged Dejan Karabasevic, he was a young Serbian national, an engineering student who Windtec sponsored to come live in Klagenfurt, Austria to work at Windtec, and he was a rising star in the company. He was very smart, liked being in China, liked climbing wind turbines and servicing them and working with his Chinese counterparts. So, then Karabasevic was helping Windtec and then AMSC initially to grow the demand for their clients Sinovel; however, ultimately, that relationship soured as we'll explain.
Leah Evert-Burks: IP assets can be monetisized to provide revenue through the licensing of proprietary rights – such as the use of a trademark by a company outside a goods category to expand the reach of the brand, a song, images or an invention, these are examples of what can be licensed to a third party with their payment of royalties to the IP owner. For many inventors and/or companies that own innovative technology such as software, this can be their main source of revenue - and therefore something that needs to be aggressively protected.
Leah Evert-Burks: Instead of licensing the software, they decided to steal it and Dejan, I think he was also known as D.K., was a good candidate to kind of pull into the fold with the CEO of Sinovel. You mentioned certain aspects of his character, but were there other aspects that made him susceptible or a good candidate to be involved in this theft?
Josh Mayers: Yes, there was. You know, we always want, in the FBI when we're investigating crimes, we always want to try and understand the motive of the people who we believe are allegedly committing crimes, so we always look to motive and look to, you know, why did someone do something not just what happened, and so in this case, we really have to go back to the beginning, and that starts in the late summer and early fall of 2010. Windtec sent some engineers out to western China to the Gobi Desert to check on some Sinovel wind turbines that they were servicing and running tests on, and they noticed when they got to the wind turbine that there were some anomalies and that the wind turbine was running on software that appeared to be altered or different in some way from the license software that Sinovel was paying AMSC for. And they did some checks and they made some screenshots, which they took back to their lab in Klagenfurt, and ultimately, the engineers determined that there had been a breach, or a hack, if you will, into the wind turbine software. And so, they didn't necessarily know who had done this, but I think they suspected Sinovel being responsible at the time. However, as you said, Sinovel was a large customer of theirs, and they didn't want to offend them or hurt their business relationship, so they did, they took some protective measures as a company to protect their trade secret, to protect their software which they

thought had been had been perhaps intruded on and so they put on some encryption, they put a timing limitation, which would have the software shut off if they weren't paying, and then they continue with the relationship so that it's sort of like a chess game, Leah if you think about it, so you know, Sinovel took one action, then AMSC and Windtec took sort of a response protective measure, then Sinovel who still didn't want to pay for what they'd been paying a lot of money for made a business decision. We learned ultimately they decided to recruit an insider. And as we know in other cases, insider threats are real and are significant. They've happened in government, they've happened in the private sector, and so, an insider who's not identified as being a risk or a threat to a company can cause great harm. And that change, caused Sinovel to look for an insider, and they came upon Dejan Karabasevic--D.K. we call him. And just as you said, D.K. was right for the picking. He was somewhat disgruntled, although he had been helped by Windtec and rose quickly in the company. He, we learned, had a fairly big ego, he had appetites for expensive living, for having many girlfriends, and he was frustrated because Windtec wanted to bring him back to the headquarters in Klagenfurt and participate as a manager in a managerial role. He wanted to be in the field in China, having girlfriends and adventures and climbing wind turbines and working with his Chinese counterparts, so there became a rift or a conflict between the employee and the company. And as you also very adroitly have pointed out early, Windtec and AMSC didn't recognize this disgruntled employee. They didn't really understand or see the depth of his frustrations and anger at the company. And so as early as the fall of 2010, Dejan Karabasevic with Sinovel's help and support and encouragement began talking and planning on stealing technology, on hurting Windtec, which was clearly part of his goal, and on helping Sinovel and hopefully he wanted a job with Sinovel and a career with them, so those plans started shortly after the hack in the Gobi Desert was identified, and it took six or seven months for Sinovel and D.K. to complete the theft of the trade secrets which we'll explain in more detail, but that started the ball rolling towards the crime that ultimately the FBI and my team investigated and successfully prosecuted, but it took seven years, and it was a long, long haul. There was evidence on three continents. A lot of complex legal challenges in this case, as in any case with this type of complexity.

Leah Evert-Burks: As you indicated, this was insider theft, which when you look at the cases involving theft of trade secrets and other IP, many times it's from insiders. And this was an insider that was acquired, so he came over to AMSC through the Windtec acquisition. So, again, looking at mergers and acquisitions, when companies are acquiring other entities, it's important to know who they're acquiring and the characters, the nature of the characters, of those employees.

Josh Mayers: That's right. You're not just acquiring a company, right. You're acquiring the human capital, the most important part of a company.

Leah Evert-Burks: Right. You're acquiring people that may be just disgruntled, as you said.

Josh Mayers: That's right.

Leah Evert-Burks: Now to do the hacking of the software for the wind turbines, as I understand, Sinovel moved D.K. into a safe house. Can you tell us a little bit about that?

Josh Mayers: Yeah, exactly. So what happened was, as I said, they started planning in the fall of 2010. By March of 2011, D.K. had put in his papers to resign. Austrian law had a unique feature in that he could take what's called *garden leave* which means he had three months of leave stored up, and instead of like a U.S. company where they would pay you out for that leave or, you know, you might stay on the books for your health care but you wouldn't have access to the crown jewels and all the valuable information in the company, in Austria, he was permitted to continue to have access, and he used some

sleight of hand, he used a deception and a lie to the human resources person, so again, not checking fully his story, he was allowed to--he manipulated the human resource system--to permit him to still have access during this three month period, and he lied to his co-workers and said he was going to be traveling and taking vacation, when in fact, just as you said, he very quickly after downloading the software from Austria, which was on a server in Wisconsin, that's how we get Wisconsin in the mix, you know, you have to have jurisdiction for a federal crime, and jurisdiction fell in the Western District of Wisconsin, the federal district where the AMSC office was that held the server that contained the software D.K. stole. So, he stole it from his Klagenfurt office, he downloaded all of the crown jewels, the actual source code for the software, so that once you have the source code, you can change and manipulate the software at will, and then instead of his three month vacation, he quickly went to Beijing, where he was in fact, put in a very luxurious two story apartment, safe house that Sinovel set him up in, and they also set him up with a test bench which was replicating the components, the two primary pieces of hardware in the wind turbine, which are called the PLC, the *programmable logic controller* at the base of the wind turbine, and then the power module at the top of the wind turbine, the nacelle, those two pieces of hardware have software on them that the AMSC developed was their trade secret, and those two pieces of hardware and software talk to each other in milliseconds to keep the wind turbine running, converting the spinning of the blades to electricity which then pushes it out to the grid, so he stole a very critical component, critical software in the functionality and operation of the wind turbine.

Leah Evert-Burks: Yeah, it's really the brains of the wind turbine.

Josh Mayers: That's right.

Leah Evert-Burks: So, how did the FBI become involved?

Josh Mayers: So interestingly, this crime occurred, well was committed in March of 2011, D.K. returned to Austria briefly in late June and early July to see his daughter, young daughter, who remained back in Klagenfurt with his ex wife, and when he came back, the Austrian police arrested him with the complaint filed by Windtec and American Superconductor. The FBI was not involved at this point. This was at first thought to be strictly a European crime, a crime occurring in Austria, and unfortunately the trade secret laws are fairly weak in Austria, so ultimately, D.K. was only, he was convicted of stealing the software in Austria, but he received a nine month sentence of basically home detention. He would be out working during the day, and then he would go at night into an incarceration facility, but very, you know, very minimal punishment. They just don't have the current laws caught up with trade secret theft like we have developed in the U.S. So, he went through that legal process, and then the FBI has a program called the legal attache' program where we've got FBI agents stationed all over the world in U.S. Embassies. They're overtly declared to the host country, and they're there to help facilitate U.S. cases and interest and also to help facilitate the host country interest when appropriate. So, in this case, the FBI legal attache' was an excellent agent. Steve Paulson who had worked with actually ironically in the same office in Wisconsin, and he called and said, "Hey, the ambassador just came down the hall and said that there's a company with the U.S. headquarters that's been a victim of a theft of technology. Can you help us?" So, that started the ball rolling in Wisconsin, and we began. I opened the case in November 2011, and we began working with the victim company, and this is a critical part of the story in that, in this case, and in any trade secret theft cases, particularly ones that last as long as this one, the relationship between law enforcement the FBI, and the private company is critical. So we worked very hard cultivating that relationship, treating them as a true victim, and working with them very closely from start to finish. It was really critical to the success of this case. So, companies who are out

there who are reluctant to report crimes like this, I hope are reassured that, you know, the government and the FBI in particular work very hard to protect victims of crimes like this and to help them through these things and to not further injure them, to not further expose their trade secrets if litigation happens. As in this case, we took Sinovel to court. We prosecuted them in open court.

Leah Evert-Burks: The FBI as with other U.S. federal agencies, employs attaches' who are dispatched to foreign locations to assist in the monitoring and protection of U.S. interests, including intellectual property. In the first edition of The Brand Protection Professional we explored the USPTO's program with the Director, of the Intellectual Property Attache' Program and their Attorney-Advisor, from the China and Enforcement Team in the Office of Policy and International Affairs.

Leah Evert-Burks: So, a number, I am assuming that in your long career in law enforcement, you've served a number of search warrants for various locations, maybe some barns in Wisconsin and other other type of buildings, but for this case, you actually served and searched a wind turbine Can you tell us about that unique experience?

Josh Mayers: Yeah, it really was, and you're right. You know, the FBI is pretty good at searching things. We can search houses and cars and garages and yes, barns occasionally in Wisconsin, but in this case, we started investigating, we had a great team of prosecutors, three amazing prosecutors, two from Wisconsin and one from Washington, DC, from the Computer Crime Intellectual Property Section, and so what we learned as we did our investigation was that the purpose of the theft was really two-fold. It was as I said earlier to retrofit thousands of wind turbines in China that needed upgrades to their technology, to their software to become compliant with the change in Chinese grid code specifications. That was critical to Sinovel to have. The second thing they were doing was exporting wind turbines which they manufactured in China, and when they exported the wind turbines, they used the hardware and software from other countries, so they used hardware and software from the AMSC for those exported wind turbines, so we began to suspect, or theorize at least, that the stolen source code was also being used to export wind turbines around the world. And so when we learned in 2012 that Massachusetts had provided both stimulus funding, green energy, green technology stimulus funding to Sinovel and they had obtained a waiver for a non-U.S. wind turbine manufacturer to be able to export wind turbines into the United States, so they both got funding and a waiver and part of the justification was that they were using the hardware and software of a local Massachusetts company, AMSC, and therefore, they got a priority in their export license, and so we learn in 2012 that Sinovel was in the process of constructing four wind turbines in Massachusetts: one in Charleston, one in Scituate, and two in Fairhaven. And so we went to the owner/operators of those wind turbine projects, who we also by the way viewed as victims. They were not witting to the stolen software. They had no idea what they were developing and importing in their mind and they contracted for was licensed legal software that the Sinovel wind turbines would contain, and then we went to them, we asked them for cooperation. The FBI can't do many things in their investigations without the public support and cooperation. We depend on it. It's critical. And it was certainly critical in this case, so we went to them, and they were very helpful and cooperative. We always treated them as victims also because they also suffered economic harm ultimately because you're right, we did do searches of four wind turbines and as you can imagine, FBI headquarters, the supervisors, and management were a little nervous at first when we proposed this. It had never been done before. And they didn't want us to break them. They're expensive. They have a lot of electricity running through them. They can be dangerous and so it became quite an adventure to both plan and prepare and train with our technical agent, how to do this safely and how to gather evidence in a way that would preserve the

evidence to be useful in court, if in fact, we found stolen infringed on software running on the Massachusetts turbine, so that's what we undertook was a nine month project to do for searches.
Leah Evert-Burks: Wow, wow, up on those wind turbines.
Josh Mayers: Yeah, and covertly because they're part of Sinovel agreement with the owner operators and Massachusetts was a two-year, kind of warranty if you will, so they brought Sinovel engineers over to Massachusetts, they were living in a home, they were servicing the wind turbines if a problem happened, they would do patches and upgrades, they were there legitimately to serve these wind turbines and service them as part of a service agreement, so we had to do the searches not only safely, not only in a way that preserved the digital evidence from any legal attack or challenge, we had to do it in a way that was not alerting to the company because they did have remote access to the wind turbines through internet connections, so we were concerned that they could if they got wind of it, change or put the licensed software back on and take the infringe software off. So, this was all unknown at the time, and we started like we do in any FBI operation: we planned. We planned it out, you know, first on paper, then we actually went out and practiced and rehearsed, which meant myself and the technical agents with a lot of support from the Boston field office, actually planned and practiced how to climb how to, you know, put on the harness, how to a clip into the ladder inside, how to climb. You climb 80 foot sections and when you get 80 feet, there's a platform you can rest, you can stop and then you get to the very top that sort of big square thing you see at the top of most wind turbine which is called nacelle that's really like a control room. You can fit five or six people up there. There's a large generator which is connected to the blades within gears which are turning the generator that helps convert the turning blades to electricity, and then there are electrical control cabinets up in the nacelle which contain the hardware, the components--in this case the power module--which holds the software which was running the wind turbines, and that's what we need to get access to in order to image or copy the software, you know, in a digitally sound manner, so it's not been altered, it's not been changed, it's preserved. And then we compared it with the licensed software from AMSC and we also compared it to other evidence we had from the D.K. theft, so we knew what D.K. stole. We knew what he--we knew what the license version looked like, and we also knew what D.K. changed because we had access to some of the computers and information from the Beijing safe house. We were able to get some evidence from the Beijing safe house ultimately, so we had good comparisons. We had our original evidence, and then we had good things to compare it to. And we were able to establish that the Massachusetts wind turbines were running the stolen modified software that D.K. took and changed at Sinovel's request. Quite exciting.
Leah Evert-Burks: Wow. Well, the first thing I think of is thank goodness you don't have a fear of heights.
Josh Mayers: That's right. Well, you know, you're inside, so you don't really see out, but I will tell you, you know, you still feel like you're going up in the air, and when it's windy, you can feel that the top, you can feel it sway a couple inches. It's a little unnerving because when you're up there you can actually feel it moving a little. So yeah, you don't really need, it's not so much a fear of heights it's just it's a little claustrophobic, and it's a little unnerving because you're just climbing and climbing up this ladder. It seems forever, and the thing is shifting and moving a little bit, but we had great help. We had great instructors teaching us, and nobody got hurt and we, you know, most importantly we're able to seize evidence, in this case, not only seize it in a way that was usable in court but also show very definitively that not only had Sinovel stolen the software and used it in China, but here they'd had the audacity really to come back and use it in

American Superconductor's front yard, which is just sort of outrageous if you think about it.

Leah Evert-Burks: Right, right. Yeah, and thinking about how you set that up, and as you said, there were Sinovel employees in the location. They were monitoring the systems. So, you had to be careful not to be physically and electronically or through cyber detected that you were doing something. Were you posing as AMSC employees?

Josh Mayers: We use just sort of a light cover of doing a grid inspection, so we didn't, you know, provide a lot of detail, but we did give notice to Sinovel that there was going to be a time when the wind turbine is offline, and we just tried to make it seem like a normal routine maintenance thing that they were notified of but frankly didn't need them on site, and they accepted it. They didn't question. I suppose they could have, you know, we had some contingencies in place if they did show up and we would address that but sometimes simple is the best way we just kept it simple. We kept it, we did the muscle in the middle of the night, so we did it off hours, which always helps a little bit, and we had plans to intercept them if they had decided to drive out and poke their nose around and see what was happening, but we felt pretty comfortable actually that in this instance they were, they accepted what we told them through sort of third parties, and they didn't seem any the wiser. So, sometimes it's better to be lucky than good. I suppose so we were a little bit lucky too. Yeah, but we were really concerned at the time of being discovered because we were mostly concerned, not for our safety but just that if they realized that we were on to them then they could change or manipulate the software remotely, and we'd not have a way to preserve the evidence if it was in fact stolen, you know infringed on software. So, that's always the concern, you know, your main job as a law enforcement officer in a search is to preserve evidence. That's your goal and your purpose, and it was no different here.

Leah Evert-Burks: So, you were able to gather and maintain that evidence, and that was in Massachusetts. Of course AMSC was officed out of Wisconsin, so then you gather the evidence it was adequate to bring an action against Sinovel, and that was brought in the Western District of Wisconsin.

Josh Mayers: That's right. In June of 2013, so we finished our searches in 2012. We gathered the evidence. It took a few months to both analyze and compare the evidence, so we, you know, we had to be sure, obviously, we were guessing here that the evidence was in fact proof of the theft and the modifications to the source code. We had to be sure of that, so we had to be sure both that the evidence was intact and preserved and that, you know, we had a good examples and that we could in fact prove beyond reasonable doubt that this was stolen, infringed software. So, that took a little time, couple months, some very smart computer scientists, and computer response agents worked on that very hard with the prosecutors, and ultimately, by June of 2013, we indicted in the Western District in Federal Court. We indicted Karabasevic who did the theft. He himself stole the software. We indicted his two primary handlers:
Zhao Haichun and Su Li Ying. These are two upper level managers in the R&D department (Research and Development Department) of Sinovel in Beijing, in the Beijing office, who were decay coworkers but also became his handlers, and they helped recruit him and manipulated him to steal the software on Sinovel's behalf. So, those are the three people who were indicted. Unusual are unique in this case, Leah, was that we indicted a corporation. You don't often think about a corporation being something you can charge with a crime, but in fact, you can charge a corporation with a crime in federal court if you can show that their agents of the company or the employees and agents acting on behalf and at the direction of the company committed the crime, and that's in fact what we alleged that Su and Zhao as agents or employee of Sinovel, at Sinovel's direction recruited and used D.K. to steal the software to transmit it to them after making

modifications or changes to it, so we indicted the company which was a big deal to indict a Chinese Corporation and, you know, U.S. Federal Court, like you said is a big deal and was the first time this had happened, and that set in motion a long legal dispute. There were legal challenges to our service. We served Sinovel in their Houston office. There were legal arguments. You know, they hired two large well known law firms in the U.S., Sinovel did, and litigated the case even, you know, before it went to trial, and so unfortunately, it took some time. This went up to the Seventh Circuit Court of Appeals, where we persevered, we prevailed, we won, but it took two years just on the service issue, whether or not we properly served a foreign corporation in the U.S., and therefore, they be subject to U.S. law, and the Seventh Circuit agreed with us and agreed with our prosecutors who argued, and so then the case was set for trial, but it wasn't until January of 2018, that we had a jury trial, a 11 day jury trial in Madison, Wisconsin in Federal Court, and at the end of that, Sinovel was convicted, but we brought in American Superconductor and Windtec witnesses, we brought in the engineers who wrote the software, the Austrian engineers who had worked with D.K. very closely, which really brought the case to life for the jury I think, we brought in a mockup of a wind turbine, we brought in the actual piece of hardware, the power module which weighs about five or six hundred pounds, we brought that into the courtroom to show the jury, and we explained and we walked them through, just as we have here, how the case started, how we gathered evidence, we presented the evidence from the searches in Massachusetts of the wind turbines, and we were able to establish beyond reasonable doubt that Sinovel had in fact recruited and hired D.K. to steal and modify the trade secret, and it caused tremendous harm. It caused American Superconductor to lose, you know, hundreds of millions of dollars, and ultimately, the jury found in our favor and awarded AMSC 54, almost 56 million, in restitution and then $850,000 in restitution to the Massachusetts wind turbine operators who were also, as I said earlier, victims in this case.

Leah Evert-Burks: Right, and I think one of the quotes that came out of that trial was, “This was nothing short of corporate homicide.”

Josh Mayers: Yes, that's right. That’s exactly right.

Leah Evert-Burks: So, when you talk about theft of trade secrets, the damage runs deep. As you related, approximately, you know, billions of dollars were lost, jobs were lost, and, yeah, so it's interesting too that this was a jury trial.

Josh Mayers: Yes, and we really tried to bring that to light. We brought in, for example, we had testified for the government, the human resources manager at American Superconductor who had to personally fire hundreds of employees because of this theft, and then she herself, she fired herself on her last day. Dan McGann, the CEO, ultimately talked to her, and it was understood that even she was going to have to go, so this company lost you know, this is about people. When, you know, we think of sort of a theft of a trade secret, it sounds sort of sterile and impersonal and you know, it's a crime that, you know, affects a company or effects technology, but this really affected human beings. The Madison office, for example, closed. When I would go there initially to meet with some of the engineers, there were, you know, hundreds of desks and employees and bustling office, when at the end, the office was empty, and they closed. You actually saw in really stark terms, the effect on human beings. The human resource officer who testified brought to life how many people she had to personally let go and how hard that was emotionally for her and her co-workers. So, there’s the human cost of this. It’s not just economics, but it did cost AMSC, was estimated with their stock loss and all the other revenue, lost about 1.2 billion, with a B, and hundreds of millions of dollars in lost contracts that Sinovel had agreed to and had signed, you know, an expectation of

paying that they reneged on, so real human cost here. A lot of people, 600 people or so, lost their jobs permanently because of this theft. A real impact.
Leah Evert-Burks: I think that's so important to bring up, Josh, that the economic loss is really a human loss. And, again, when we're talking about some of the dangers of mergers and acquisitions, specifically due to lack of due diligence when you're acquiring employees such as D.K., those that are easily lured into illicit work have skills to carry out the damage. It's also important to research who your new customers are that you're acquiring, and in this situation too there was a general disrespect or lack of respect of intellectual property. As I recall, there was kind of a degrading of the value of the software, referred to as cabbage.
Josh Mayers: That's right, yeah.
Leah Evert-Burks: To make the theft, not so distasteful, though, you know, obviously it was the opposite of that. This was extremely valuable property, but there were attempts to make it degrade the value of the software to, I think, allow people to proceed with the theft.
Josh Mayers: Yes. That's exactly right. It's a good memory. The cabbage term, we heard was was from Mr. Han, the CEO of Sinovel, had made a disparaging comment that “it’s just software, you know, even if it was taken, it's only software. It has no value. It's like cabbage,” he said, so this sort of a became a moniker for us or a sort of thing to just keep in the back of our heads, and that's right. The people who did this crime didn't feel there was any risk in doing it. They did it with impunity, they did it with an arrogance, and yeah, they did it with a real degrading of the value of the trade secret of all the hard work that went into developing that software, and you know, human beings spent thousands of hours and time and effort and their brainpower on developing software and making it work so that there could be clean energy. And so, that was a critical piece of this, sort of the arrogance of the defendants here who just felt like they could run roughshod over the AMSC, and AMSC didn't go in with blinders on. They had been doing business in China. They understood some of the challenges unique to U.S. companies doing business abroad. This is not unique, by the way, just to China. This happens in many countries where U.S. companies are trying to do business, and there are some challenges in working with other countries laws, other countries culture. And so, this is something AMSC actually had thought through and was good at. They just, I don't think, realize that their best customer was going to, on the one hand, pay them a lot of money and seem to be a great business partner, but on the other hand, were really plotting their demise. They were really, as you said, corporate homicide. They really tried to kill AMSC and almost did. They almost succeeded, but AMSC, thanks to good leadership and some, you know, just amazing employees who were able to stick around, they've been able to rebound and recover from this, and I think we helped. We always viewed our role in the government as trying to, we always try and help victims of crime, no matter who the victim is, whether it's an individual human being or a company. They're still a victim of a crime. They have rights, and we really kept that at the forefront of this investigation the whole time. Very important to us.
Leah Evert-Burks: Well, thinking about this case, this story, which was seven years of your life, a hard task here, if you could select one word to describe the case, what would that be?
Josh Mayers: You know, for us it was perseverance. We really tried to stick in there with our victims, to hang in there, to encourage them to hang in there, and it really became a matter of perseverance. You know, you can, you take all the twists and turns a case takes you on, and you know, off of the FBI we were all replaceable, right? If I had, you know, gotten off the case or gone and done something else in the fourth year mark or fifth year mark, I'd be replaced the next day. There'd be as equally good or

better agent taking my place. So, you know, that's the strength of the FBI is we have a lot of depth and a lot of really great smart people, but we stuck with it, and not only the FBI but the partnership with the prosecutors. We had three amazing prosecutors who are just brilliant and great litigators, and they stuck it out for the seven years, so if they stuck it out, I stuck it out, and we really did it because we got to know the victims, and we got to really care about the victims not the corporation per se but the people, like you said, the human beings behind the company who we got to know, and we respected them. They didn't deserve this. They didn't do anything to cause this, and so we felt our obligation to the victims of this pretty serious crime to hang in there, so perseverance on all fronts was the moniker. The word for this case I think.
Leah Evert-Burks: Absolutely because when you go into investigation and prosecution on a case like this, you know that it's going to be a long haul.
Josh Mayers: Yes.
Leah Evert-Burks: There's going to be legal challenges, as you indicated, there were challenges with respect to service to a foreign entity. Those are almost a given, and you know, there's going to be challenges with gathering evidence and pursuing the case at every step, so perseverance certainly is a good word to capture this.
Josh Mayers: Right, for sure.
Leah Evert-Burks: So Josh, I want to thank you for joining us here today at Brand Protection Stories and just thank you for doing the hard work.
Josh Mayers: Thanks, Leah. It was my pleasure. I really enjoyed talking with you today.
Leah Evert-Burks: This story provides some valuable take-aways for companies looking to do mergers or acquisitions. Including - doing background checks on employees and truly understanding your new customers' motivations as part of your standard due diligence. Companies spend money and resources protecting their property, constructing perimeter fencing, installing security systems, entry restrictions, employing guards, and building firewalls into their information systems, but at times companies may not think about protecting their intangible assets such as intellectual property. 85% of trade secret thefts are by someone familiar with the owner - a business associate, a customer, an employee... As important as your physical perimeter is, the one around your innovation and IP is of equal or greater importance.
Leah Evert-Burks: If you're interested in sponsoring episodes of Brand Protection Stories, please contact A-CAPP Assistant Director Kari Kammel at kkammel@msu.edu.
Leah Evert-Burks: In the next episode, meet a man in the shadows, U.S. Federal Undercover Agent Bobby Sherman. Bobby connected the dots of a wide scale pharmaceutical counterfeit operation that penetrated the UK supply chain down to healthcare facilities and pharmacies. He did this through keen deduction of the motivations and vulnerabilities of the parties involved and brought the savvy manufacturer of the counterfeit therapeutic drugs to justice in the U.S., and assisted the U.K. authorities in putting the wealthy, ruthless kingpin behind bars.
Leah Evert-Burks: Thanks for joining us today for this edition of *Brand Protection Stories*, produced by the Center for Anti-Counterfeiting and Product Protection (or A-CAPP) @ Michigan State University in East Lansing, MI. Please visit us @ a-capp.msu.edu. A-CAPP is a non-profit organization founded in 2009. It is the first and only academic body focusing upon the complex global issues of anti-counterfeiting and product protection of all products, across all industries, in all markets. In addition to this series, we offer certificate courses in brand protection, applied education and academic courses, executive education, student internships, live summits and virtual events, ground-breaking research, and publish the quarterly digital industry journal, *The Brand Protection Professional*.

Leah Evert-Burks: This is Leah Evert-Burks with A-CAPP. Until our next session, keep protecting your brands, and the world's consumers. Keep it real.