HowellCTA Done

Fri, Apr 28, 2023 8:05AM   1:10:18

SUMMARY KEYWORDS

cybercrime, cybersecurity, ransomware, markets, cyber crime, people, hackers, crimes, jose, criminology, cyber attacks, attacks, individuals, question, find, web, podcast, study, extremely, criminologist

SPEAKERS

C. Jordan Howell, Jenn Tostlebe, Jose Sanchez

J Jose Sanchez 00:00

Hey everyone, welcome to The Criminology Academy podcast, where we're criminally academic. My name is Jose Sanchez.

Jenn Tostlebe 00:20

And my name is Jenn Tostlebe.

J Jose Sanchez 00:22

Today we have Professor Jordan Howell on the podcast talk with us about cybercrime, and more specifically, the illicit online supply chain and the way darknet markets enable cyber attacks.

Jenn Tostlebe 00:33

Dr. C. Jordan Howell is an assistant professor in the Department of Criminology at the University of South Florida, and the director of Sarasota cyber security. Prior to these appointments, he was an assistant professor in Intelligence and National Security Studies at the University of Texas at El Paso, and Associate Director of the evidence based cybersecurity Research Laboratory. He received his doctorate in criminology from the University of South Florida in 2021, where he also earned a graduate certificate in digital forensics in 2017, and a master's in criminology in 2016. Dr. Howell's research focuses on the human factor of cybercrime. He employs advanced computer science techniques to gather threat intelligence, which is then used to test social scientific theories, build profiles of active cyber offenders, plot criminal trajectories and disrupt the illicit ecosystem enabling cyber crime incidents.

Jenn Tostlebe 00:35

All right, it's great to have you on the podcast. Jordan, thank you so much for joining us today.

C. Jordan Howell 01:39

Yeah, fantastic to be here. Thanks for having me.

Jose Sanchez 01:43

So just a brief overview of what this episode is going to look like. So we're going to have a general discussion of what is cyber crime. And then we're going to start moving into some of Jordans work on ransomware, illicit supply chain, and hacking. And so with that being said, Jen, why don't you go ahead and get us started?

Jenn Tostlebe 02:02

All right. Thanks, Jose. So to really get the conversation going, as we normally do on this podcast, we're going to start off with a definitional question that may or may not be difficult or too broad to answer. But, Jordan, what is cybercrime?

C. Jordan Howell 02:19

You know, it's really funny. You're starting with this definitional question, because it's something that's so often overlooked by academics, industry, and law enforcement. How can you study cybercrime, investigate cybercrime, or prosecute cybercrime, if you don't know what cybercrime actually is? The laws are extremely vague, academic definitions are extremely vague, and there's really not an agreed upon answer to the question. Cybercrime, at its core is any crime that involves a computer. But what does that mean, right? If I throw a computer at Jose, is that a cyber crime? Maybe. But if I launch a ransomware attack against your podcast, it's certainly a cyber crime. But what differentiates the two? What makes one a cybercrime and one not a cybercrime? And how can you classify these two very different types of behaviors under one umbrella term like cybercrime?

C. Jordan Howell 03:12

So scholars have tried to differentiate it and use terms such as cyber dependent and cyber enabled crimes. So cyber enabled crimes are any crime that existed before the internet that's essentially enabled with the use of computers or network technologies. Fraud, for example, fraud has been committed since I imagined the beginning of time, right. I can picture someone trying to forge the earliest of currencies and that's still being done today. But it's being done using computer and internet technologies. So that's a cyber enabled crime. Where cyber dependent crimes are crimes that exist because of the internet. Right. So if I were to attack your computer system, using my computer system, my computer's the tool and yours is the target. So both of these types of offenses fit under this broad umbrella, but they're often looked at differently. One has more social scientific connotations, whereas the other is often approached using more technical lens. What I'll talk about more throughout the podcast, or at least I hope to, is how both should be studied using a technological and social science framework.

Jenn Tostlebe 04:17

So you already started getting into this a little bit, but for those people who maybe are wondering what exact crimes fit under this umbrella, like in terms that people would understand, what exact types of crimes fall under the Cybercrime umbrella.

C. Jordan Howell 04:35

So many, right so so many crimes that you think of in the physical realm can exist in cyberspace. Harassment, just add the word online to it, and you have online harassment, that's a cybercrime. People often talk about cyber bullying or cyber stalking. You talk about tax fraud that can be committed using the computer making it a cybercrime. So oftentimes, crimes that you think of in the physical world have an online component making get a cybercrime. But then in addition to that you have crimes that exist solely because of the internet exist such as phishing, ransomware, malware distribution, website defacement, right. You know, I can be very upset at you, Jenn, for not coming to USF this year. So, you know, I start attacking your university's website putting USF banners all over it. And that's a cybercrime known as website defacement, because that involves hacking and then defacing a site's content to post content of your own choosing. There's various types of cybercrime, some of which anyone can understand, because maybe they've committed them themselves in the physical world, right. But oftentimes, there's cyber crimes that require those more technical elements. And oftentimes, which again, is something I'll talk about a bit later, there's cyber crimes that have this technical element, right, that exist because technology exists, but also has an overlap with crimes that exist in the physical world. So when you think about Dark Web markets, for example, individuals can go on to these darknet markets, they can buy and sell drugs, right that exists in the physical world, as we all know, but now you're able to use technology to actually buy and sell drugs in an anonymous fashion, using various forms of technology, making even something as simple as drug distribution, a cybercrime.

Jose Sanchez 06:19

Okay, so now we want to go to the other side of the aisle. And so we've been talking about cybercrime. But the other side of this coin is protecting yourself from cybercrime. So, again, with another definition of question, but how would you define cybersecurity?

C. Jordan Howell 06:36

No need to apologize for the definitional questions. This should be what we're talking about, right? Everyone wants to be the expert and talk about how AI informs cybersecurity solutions. But they forget to sit down and think about what cybersecurity actually means. And it's extremely problematic. Maybe even more problematic than the example I gave earlier. About the inability for academics and law enforcement agencies to find cybercrime, let alone study it, investigate it, and prosecute it.

C C. Jordan Howell 07:02

Cybersecurity at its core really is just protecting yourself online, right? It's the acts in which you engage in to protect yourself, your company, or even the nation state you belong to. But what's happening is there's this disconnect between academia and industry, in which academic disciplines have created these silos, right? Everyone starts approaching cybersecurity through these sub disciplinary lenses. You'll talk to a criminologist who only understand social scientific theory, and they'll fixate on the human factor, they'll fixate on the cyber enabled crimes, I talked about in human behavior and decision making. And that's extremely important that is a part of cybersecurity. But they completely ignore or possibly lacked the knowledge to apply some of these technical solutions to build out these more robust security systems. But then conversely, you have computer scientists, engineers, and you know multibillion dollar cybersecurity companies who promise that they've developed, you know, next generation cybersecurity software, just to find out that it was penetrable, right, people were able to actually get into the system and exploit it for their own nefarious purposes. I mean, the Trojan horse, I think, is a good example. Right? It shows that you can have the most impenetrable gates. But if the attacker's let in, or if the attack comes from the inside, right, these physical gates, these impenetrable systems that engineers and companies try to build, they fall because the attacker is already past the impenetrable gate that is the only cybersecurity solution in existence. So I guess to sum up that answer and make it a little more accessible, cybersecurity is not only the act, or acts in which you engage in to protect yourself, but it's the culmination of the human factor. And the technological components required to build up a more robust security posture to mitigate the various types of cyber crimes that we talked about just a second ago.

C C. Jordan Howell 07:02

Yeah, it's interesting thinking about cybersecurity. So whenever I think of cybersecurity, I just, every year, my computer sends me this alert, like, Hey, your antivirus is about to expire, it's time to renew. I pop in my credit card information. And it's like, okay, you're good for another 365 days. And like, that's as far as I get. Or I'll hear, like on the news, like, US Bank was just hacked and all your banking information might be at risk. Shouldn't the bank have like, the most top notch security system? Like I know, I don't have a lot of money in there, but I'd like my couple $100 to be safe.

C C. Jordan Howell 09:39

Yeah, that's exactly right. And we always talk about cybersecurity and you always hear these buzzwords, right. All these companies are talking about next generation AI right, you know, purchase this product in order to blah, blah, blah, blah, blah. But it's never evidence based. Right? And that kind of gets back to the disconnect I was talking about before. I can easily come up with a cybersecurity solution. I'm doing air quotes for those listening, you know, audio only. But at the end of the day, I can tell you one thing, and if it's not effective, who cares, right? I'm a cybersecurity company. I'm the fat cat, I already made a billion dollars off promising false protection. So I'm not sure if real cybersecurity solutions exist currently. But I think there's a step forward. Right. I think that, you know, once we bridge that disconnect, and we start approaching cybersecurity as a scientific discipline, and we start ensuring that the cybersecurity solutions that we implement and charge people for are based on science and tested using rigorous methodology, I think will be one step closer to having true cybersecurity that can protect the couple 100 bucks in Jose's accounts.

Jenn Tostlebe 10:49

Yeah, for sure. I know, I always get those alerts on my computer too. And I'm like, Yeah, but I know people who have paid for that, and they've still gotten hacked, or still have viruses. So you know, I think that exactly points to what you were saying, Jordan about this disconnect.

C

C. Jordan Howell 11:05

Exactly.

Jenn Tostlebe 11:06

Yeah. So a cyber criminology as a sub discipline of criminology has, I think, really been growing over time. And I've been hearing more and more about it, especially in more recent years. And so when did attention really start being given to cybercrime as a discipline or as a thing to study?

C

C. Jordan Howell 11:28

It's a great question. And I want to preface it by saying that my opinion and thoughts here are not going to be generalizable to the larger cyber criminological community. I find that I'm often the outcast with these ideas and thoughts. It doesn't mean I'm wrong, right? It just means that my opinion disaligns with the masses here. So bear with me, and I hope I don't upset anyone who's listening to this episode.

C

C. Jordan Howell 11:54

So cybercrime has been part of criminology since the 1990s. You have some early scholars such as Peter Grabowski and David wall, who were talking about cybercrime before the year 2000, mid to late 1990s. And they were doing really good theoretical work talking about criminology's importance in understanding cyber criminal behavior. And it was foundational work, it was extremely important. And early on, they showed criminology is relevant in this umbrella term, cybercrime, cybersecurity, which I believe to be extremely interdisciplinary, right. Cybersecurity cannot be owned and operated by a singular academic discipline or industry. It requires collaboration, stakeholders. And scholars such as you know, Grabowski and Wall showed that criminology deserves a seat at the table. In the early 2000s, you found more scholars engaged in empirical tests relating to cybercrime, or cyber criminal behavior. And you know, some of the bigger names I guess, would be, you know, Tom Holt and Adam Bosler. And a lot of these studies, again, extremely foundational and it led us to be able to conduct the work we're doing today, involved survey designs, samples of college students, to better understand perceptions and self reported victimization. Again, extremely important showed the relevance of criminological theory and perspectives in providing a more robust cybersecurity framework.

C

C. Jordan Howell 13:29

In my opinion, this is where I really disalign and will upset some listeners, right. I think cyber crime and cybersecurity really took off in criminology around 2010. I'd like to take credit and say I spearheaded that, but that's simply not true. I think some of the more instrumental scholars would be David Decary and David Maimon, who were doing work with active offenders, right. They were going on to hacking forums, Dark Web markets, extracting this data to analyze what they were doing in their natural habitat. David Decary he was big on one of the, maybe the first in criminology, I'm not sure, but definitely one of the most well known to start studying the original Silk Road, right. So when we're all kind of awestruck by, you know, David Decary had the insight to go on and actually assess individuals behavior while on the market through a criminological lens. So kudos to him for that. David Maimon similarly, right, rather than just asking students like, Hey, if you were a hacker, would you hack Jose's bank account and why? Which I find to be problematic. You know, David setup the first honeypot in criminology, David Maimon, which essentially allowed his research team to trap hackers in this virtual environment and study what it is they were doing once they've infiltrated the system. Again, really cool. Kudos to David Maimon for that and that was 2012/2014 and that's actually how I got involved in cybercrime cybersecurity. I started working with David Maimon along with other prominent cybercrime cybersecurity scholars. And it was the work I wanted to do. But I wanted to take it to the next level.

C

C. Jordan Howell 15:07

I think since 2017/18, or really, maybe 2020 even, we've really taken that to the next level. And we've started using the criminological perspective to study active offender data. Again, similar to what David Decary, David Maimon did, but we're doing so by advancing the cyber intelligence, and even Information Security literature. So rather than just assessing one market, right, like David Decary did, we actually have a database now, which maybe I'll have a chance to talk about later, in which we've identified over 75 Dark Web markets from which we're extracting active offender data from to build out a more ecosystem based model, right? So instead of knowing what people are doing in the one tiny Walmart in your hometown, right? We want to know what people are doing it all Walmart's across the world. So we take it to the next level by improving our cyber intelligence capabilities. But in addition to that, right, we're actually building up our technical capabilities as well. So we're building out Python scrapers and parsers to extract more data, right to analyze it for trends. So not only can we understand what the current environment looks like, which was the work in 2010, but we're able to actually forecast future cybersecurity trends. So that's when all these machine learning AI algorithms come into play.

C

C. Jordan Howell 16:25

Because at the end of the day, one thing that really bothers me about academia, and maybe cybercrime, too, definitely cybercrime, the cybercrime literature as well, is by the time we start assessing data, nobody cares. It doesn't matter, right? Like by the time we're publishing on something, the data is obsolete and the threat landscape has changed. So it's irrelevant, we do nothing to improve policy. So if you're talking about what's happening currently, by the time anyone's reading it, you're talking about historical events. And we're not historians were scholars, right? We're on the verge of creating policies that can mitigate cyber attacks. So one of the things we're really working on now, and I think it's going to take the cybercriminological cybersecurity literature, the next level, is while gathering these data using the cyber intelligence capabilities I talked about, we're actually using it to build out these deep learning models to predict future trends and patterns that can actually have an impact on mitigating threats to be.

Jenn Tostlebe 17:25

Wow, yeah, that's really cool. And I feel like maybe especially with cybercrime, that it's like changing very, very rapidly.

C. Jordan Howell 17:33

Everyday.

Jenn Tostlebe 17:33

And so I could see the need for this right? For sure. One question that I had, because you mentioned how cybercrime is pretty interdisciplinary. Do you do a lot of work with, like information scientists and people from other fields?

C. Jordan Howell 17:49

Yeah, of course, of course. Again, I don't know who your listener base is, at least one person is going to ever be like, I hate that Jordan guy. He's cocky. He talks so much. And they're right. Those are probably true, but I do it because I want to advance the discipline, right? I don't want to just stick within this sub disciplinary silo that the gatekeepers have built and tried to keep us in. Yeah, right. I work with few criminologists at this point, I find myself working more and more with people from other fields, who can bring these other perspectives and skill sets that allow us to conduct better research to promote holistic cybersecurity solutions. So in academia, we find people just like ourselves, right? The exact same background, the same PhD, right, the same statistical modeling techniques, and we work together but why? I think it's better to find someone who shares the same interest but brings another perspective. And then when you work together and collaborate, you're able to take into account like I was saying earlier, the human component, the technical component, using active offender data, and you know, cyber intelligence, which I believe--this is where I get disagreement--is the only way to advance the Cybercrime cybersecurity discipline and promote holistic cybersecurity solutions that have a real world impact. Criminology by itself will never do an adequate job assessing cybercrime and cybersecurity. So when I see teams of scholars who are only criminologists, only using criminology perspectives, I don't respect it. Criminology has a seat at the table, but they don't own the table. So interdisciplinary collaboration and translational research, as well, working directly with the stakeholders is of the utmost importance, in my opinion.

Jose Sanchez 19:35

Okay, so, either based on research or official reports, which I'm going to take a wild guess here and say that this is probably gonna be a little hard to answer. Do we have any estimate the number of cyber crimes that actually happen each year like even like the faintest idea?

C. Jordan Howell 19:52

We have lots of estimates. How good the estimates are is an estimate in itself right? You'll find reports saying that there are billions of cyber attacks that occur annually, leading to I think I saw one statistic earlier today or yesterday, saying cyber crime attacks costs like $8.4 billion to the global economy or something along those lines. But how is it operationalized? What's a cyber attack? There are so many questions, it makes the numbers and statistics, in my opinion, almost useless. Right? So say, you know, the bank that you go to Jose, right, say, it's what bank do you use? Do you mind saying in your podcast?

Jose Sanchez 20:30

Well, I already mentioned it earlier, US Bank.

C. Jordan Howell 20:33

So US Bank, right. So if US Bank is compromised, and as a result, your credit card number's stolen? But so to are a hundred other 1000 customers? Is that one cyber attack or 100,000? And that's always gonna be classified differently, right? Because it's one data breach with 100,000 identity theft victims, resulting from said data breach. But there's an FBI Director once stated, I'm going to completely butcher the quote, but it'll be close enough, is you've either been the victim of a cyber attack or don't know you've been the victim of a cyber attack. So a lot, I think is the best way to answer your question. There's a lot of cyber attacks that lead to a lot of financial loss.

Jose Sanchez 21:14

Yeah, definitely. It reminds me of many, many, many years ago, I think cyber anything was kind of started to creep into like the mainstream. And I was getting these notifications on my cell phone, which still had physical keyboards, or had a physical keyboard at that time, saying, Hey, you just ordered $150 worth of pizza in Iowa. I'm like, Iowa? I'm in Los Angeles. So I was like, what is happening here?

Jenn Tostlebe 21:42

Jenn Tostlebe 21:42

It was me! I'm just kidding.

Jose Sanchez 21:44

Now I know it was Jenn hacking my bank. Like, yeah, me and banks have had a very tumultuous relationship.

C. Jordan Howell 21:51

So I guess one thing I want to add to that, right. It's loosely relevant to your question, but I think it is important, right? Because you're talking about estimates and the number of cyber attacks and you know, the amount of financial loss that occurs as a result of the cyber attacks. One of the, no the most prominent self reporting, I'm doing air quotes again, self reporting system is the IC3. Right? It's owned and operated by the FBI, each year, they will produce an annual report. So essentially, what happens is, you know, Jose, like US Bank is compromised, you lose your couple 100 bucks. You know, you call the police. The police are like, sorry, Jose, we can't help you, you know, figure it out. They send you to the FBI to report the cyber attack. Maybe you do it, maybe you don't. I wouldn't, but I'm a skeptic. But you do you go through, you fill out the form. And then it's logged into their database for researchers to make these estimates down the road. And when we look at this database, it's riddled with underreporting, and leaves a lot to the imagination. A lot of people don't know they're the victims of cybercrime. If they do know, they're not likely to report it to this institution that promises nothing in return for reporting it. Sorry, you lost 200 bucks, can you fill out this form that's going to take more of your time. No, thank you. Unless you're gonna give me my money back. I'm not gonna fill this form. But I can say it's a drastic underestimate. Because when looking at those numbers, we can look at the number of identity thefts, for example, when that's again, the most "robust" cyber crime victimization database in existence, or at least in the US. And my team, which is comprised of a handful of PhD and graduate students, were able to identify more identity theft victims in like one month than was reported to the FBI's database. So it just shows that the databases that scholars are using to talk about cybercrime are riddled with inaccuracies, and does little to nothing to help our understanding of cybercrime, the frequency of occurrence, or the resulting impact.

Jenn Tostlebe 24:05

So, we're talking a little bit about, like specialized groups that have been created either report or combat cyber crime. And we imagine this is probably pretty difficult to do as well. But exactly how difficult or is it even possible to effectively police cyber spaces for crimes that are occurring or have occurred?

C. Jordan Howell 24:30

Yeah, well it depends. It's a really good question. And what you find in these conversations is you get this dichotomy, right, where people are super pro law enforcement, you know, this is how good we are, or they're super anti law enforcement, like they suck, they can't do anything.

And I don't think either of those are really true. I think it really depends on the type of cybercrime that we're interested in, first of all. Like if I send Jose a really mean message after this from an anonymous account and he reports it the FBI, they're gonna hang up on Jose, right. Whereas if I'm, you know, the kingpin of the dark web, and I'm selling billions of dollars of fentanyl, they're gonna care a lot, right? And they're going to invest a lot of resources in ensuring that I'm no longer doing that. So it really depends.

C. Jordan Howell 25:18

A lot of the lower level cyber enabled crimes, they don't receive attention. Law enforcement has expressed, they've expressed a lack of interest in investigating them, they feel like it shouldn't be their responsibility to do so. And there's tons of jurisdictional issues, right. So say, Jenn, you actually did in fact order pizzas, using Jose's credit card to Iowa, right? And Jose is in Los Angeles, who investigates the crime? Is it the Los Angeles PD or the PD in your current location? So it becomes extremely problematic. And that's with us still talking about crimes within the United States. A lot of crimes that occur online are nation state actors, or at least foreign actors, who are actually attacking US citizens, businesses, or government agencies from abroad. So how do you investigate that? Right, especially if you're working to investigate a crime that's occurring in a country that isn't a US ally? Right, that we don't have friendly relationships with them, it becomes extremely problematic if not impossible. But in addition to jurisdictional issues and definitional issues, or I'm sorry, in addition to jurisdictional issues, there's these definitional issues. So whose responsibility is it to investigate certain types of crimes, and it has to hit a certain dollar amount and be deemed as it depends on dollar amount, right? So if the crime is costing millions of dollars, or is attacking critical infrastructure, the FBI is going to be at your doorstep immediately because they're going to be invested in it. But if you're just sending out mean messages online, it's not going to happen, right? There's tons of issues related to law as well, because we only can investigate and prosecute acts that violate certain laws. But since the Cybercrime threat landscape is continually evolving, oftentimes the laws we had in the 1980s simply aren't relevant or robust enough to cover the crimes people are committing in 2023. So it becomes extremely problematic, which I think law enforcement alone can't handle the investigation and prosecution of cybercrime. It requires the collaboration with industry and academics as well.

Jenn Tostlebe 27:31

Yeah, for sure. And I can see how it would take specialized training to police these types of crimes as well, for just you know, your typical police officer. So there's probably also that issue as well.

C. Jordan Howell 27:45

That's exactly right. I mean, if you think about forensics, for example. I have a background in digital forensics. And this is a joke, kind of, the main thing I learned in like years of studying digital forensics is that I never want to work in digital forensics. It's my number one takeaway because it's such a specialized skill set, it's extremely tedious, labor intensive work. And oftentimes, you're investigating child pornography. And that was something I knew I couldn't do. I mean, mad respect for the people that do, right, they're angels, they're saints, we need those individuals out there ensuring that children are protected. But I certainly couldn't do it. So I've used those skill sets to create a whole new research agenda that gathers digital artifacts using forensic techniques. But it's hard to teach someone who just wanted to be a cop, to be a cybersecurity professional, which is ultimately what's needed to investigate these types of crimes.

Jose Sanchez 28:43

Well, I think we can start moving into discussing some of the work that you've done. And so today, we are going to be discussing a variety of projects that Jordan has worked on, including two reports, the first one, which was co authored with Lauren Tremblay, and it's titled, â€œAn assessment of ransomware distribution on darknet markets." And a second report titled, â€œPredicting which hackers will become persistent threats.â€ We'll also be discussing information from a piece Jordan co-authored with David Maimon in The Conversation titled, â€œDarknet markets generate millions in revenue selling stolen personal data, supply chain study finds.â€ In many of the pieces we'll be discussing today, we used a variety of terminology that people may be familiar with, but not necessarily know how to define. And people that listen to us consistently know that we are very big on definitions here. And so this is not new to them. So let's start with more definitions. And this time, we would like you to define what is ransomware and how does it work?

C. Jordan Howell 29:53

Yeah, absolutely. So the reports that you're discussing, or I guess I'll be discussing are published in AT&T cybersecurity. I just want to talk about that very briefly before we move into some of the details because, you know, I've become friends with or at least colleagues, I guess is a better word with the editor of AT&T cybersecurity. And we agreed that it was extremely important to disseminate the type of research that we're conducting here at the University of South Florida, specifically Sarasota Cybersecurity Lab, to a more generalized audience, right. Oftentimes, an academic publication, you know, you spend three, four or five months publishing it for it to go through a review process that can take anywhere from a couple of weeks to a couple of years, right, I've had some pretty bad experiences. But when you're conducting research on current threat landscapes, and you're trying to predict trends, you need to disseminate that work ASAP. Because it's the only way it gets into the hands of policymakers, practitioners, and non academics who have an invested interest in creating a safer cyberspace. And the reason we worked on the ransomware piece, which is what I'm about to define, is because ransomware was defined as the greatest cybersecurity threat in 2023, based off of the number, I guess I should say the the frequency and severity of attacks that happened in 2021 to 2022.

C. Jordan Howell 31:16

So ransomware has actually been around for over 40 years. So why now is it's the greatest cybersecurity threat? Ransomware at its core is simply malware that is installed on your computer that encrypts your files, and asks for a ransom in order to allow you access to your files, computer, network, whatever it is that's encrypted. So it's essentially just a form of malicious software that embeds your system and requires that you pay a set amount of cash in order to allow you to access your system again, that's the definition of ransomware. Sorry, for the long winded answer.

Jenn Tostlebe 31:59

No, it's good. You actually led into our next question. You're talking about how this is considered the greatest cybersecurity threat today, and how it's been around, I think in one of the reports, you mentioned the earliest recorded case of ransomware was released in the late 1980s. And so just what exactly has changed to make this become such a prominent threat or concern?

C

C. Jordan Howell 32:27

Yeah, it's a really good question. And I hate answering it in a matter of fact, type way because it's an empirical question at the end of the day. There are lots of hypotheses that could be given for that, you know. One that I have in my mind, is cybercrime has exacerbated since the COVID-19 pandemic. We actually published a different piece in The Conversation about that. So it could be that financial forms of cybercrime, such as ransomware, right, which again, forces you to make a payment in order to use your computer or access your files, maybe these types of crimes have exploded because COVID-19, o I guess I should say, the response to COVID-19 pushed so many people into poverty, right? All of a sudden, small businesses are closed, individuals aren't able to work. Inflation has skyrocketed. So is there really any surprise that people with the technical know how are engaged in financial types of cybercrime such as ransomware, fraud, identity theft, which are also on the rise by the way. That's a hypothesis, right? Maybe that's the motivation that has led to this increase. But motivation alone doesn't lead to the increase, right? Motivation is the motivation, right? But you also need to be enabled, you need the mechanisms, the tools, the skills to do it. And in the AT&T cybersecurity paper, we posit that the increase in ransomware, and the reason it's became the greatest cybersecurity threat is because it's enabled by Dark Web markets. So individuals have the motivation, right, they want to purchase and use ransomware. Thus, there's demand. And these dark web markets are able to supply. So it's simple supply and demand. So individuals like myself, right, who are technical enough, but I probably couldn't develop an extremely sophisticated form of ransomware. Could go on one of these dark web markets, I could purchase ransomware, and then I could launch the ransomware against Jose. I could be like Jose, I need that couple 100 bucks in your bank account otherwise, I'm locking up the dissertation and you're not going to graduate and Jose's gonna freak out, right? And there's going to be this risk reward calculus, and he's gonna say, you know, that's a couple 100 bucks, but like, I really want to get out of school, right? So he's probably going to send me the couple 100 bucks, because as we talked about earlier, law enforcement simply is not going to be able to investigat it in a timely manner. And you probably have a lot of deadlines with your prospectus and diss defense.

Jenn Tostlebe 34:57

Interesting.

C. Jordan Howell 34:57

That's my theory, and we find some support for that right. We find a growing market for it. And we find that's extremely accessible and cost effective.

Jenn Tostlebe 35:06

For people who maybe have heard the term but don't know what it is. Can you talk about what the dark web is? Dark net?

C. Jordan Howell 35:14

Yeah! Of course. One of my favorite topics. So the dark well, let me talk about the surface web first, right. So if you're listening this podcast, you're on the surface web. You're on, where to most people stream the podcast from?

Jenn Tostlebe 35:27

Probably Apple Podcasts or Spotify.

C. Jordan Howell 35:31

Perfect example. That's the surface web, someone goes to Apple podcast, or Spotify, and you're on what's referred to as the surface web. Also, on the surface web will be popular sites such as Google, my labs website Sarasotacyber.com, and sites that you visit on a daily basis, Facebook, Twitter, etc. But the surface web only consists of roughly 5% of the internet, whereas the Deep Web is the other 95%. So these are things that aren't indexed, right? Google is indexed, right, you can type in Google and Google comes up, you can type in Apple podcasts and Apple podcasts come up.

C. Jordan Howell 36:11

So essentially, a dark web market is a market that exists on the dark web. And the dark web essentially means that it's not indexed and can't be accessed via the surface web without the specialized software, Tor. So they're essentially hidden illicit markets that you have to use specialized software to access. So once you go on Tor, you can find all these hidden wikis and different... The more you get embedded, the more ways you learn to find Dark Web markets. And then you go on these dark web markets. And it's very similar to Amazon or eBay, or whatever your favorite retailer is Jenn, and I'm not entirely sure.

C. Jordan Howell 36:11

You can't simply go into Google and find the most prominent Dark Web market today. Instead, you need a specialized search engine, right. And that's oftentimes Tor, but there are others as well, such as I2P, and a few others that are less often used. So I'm gonna focus on Tor because it's by far the most popular. So Tor is very similar to Google Chrome, it's a search engine that you can download by going to torproject.org, you download it, just like you download Google Chrome, and boom, you have this browser. But the browser, again, is a specialized software that allows you to search for websites that exist on The Onion Router (Tor), right? Meaning they're not indexed. They're not on the surface web. And that's where all of these dark web markets exist.

Jenn Tostlebe 37:37

I use Amazon a lot.

C. Jordan Howell 37:38

Amazon is perfect. So if I go on Amazon, and I'm looking for, I just bought new Airpods, right. If I go on to Amazon and I want air pods, I type in, you know, headphones, or air pods specifically. And then it gives me, you know, a whole list of options from which I can purchase. It's the same on the dark web markets, right. So you find a dark web market using Tor. Maybe you're interested in buying cocaine, or fentanyl, or maybe you're interested in buying Jose's credit card number. So you just type in that keyword, right credit card numbers, fentanyl, cocaine, etc, into the market. And then boom, a whole list of options appears and you the customer can just browse at your convenience sitting at your computer, and purchase, essentially whatever it is you want and have it delivered to your doorstep.

Jenn Tostlebe 38:26

So wild to think about being able to go on to a website and just browse for all these things.

C. Jordan Howell 38:33

I can show you one day. Maybe there's some collaboration.

Jenn Tostlebe 38:36

Yeah.

Jose Sanchez 38:38

So you recently conducted a study that investigates the prevalence of ransomware on the dark net. Can you tell us a little bit about what you found in this study?

C. Jordan Howell 38:49

Yeah, absolutely. So firstly, we recently started this study less than a year ago. And the first step was to engage in various forms of cyber intelligence gathering, right. We first needed to identify dark net markets from which the ransomware was being sold. And in doing so, we gathered or compiled is a better word, the largest dark net market database in existence, we found over 70 markets. Most scholarly articles will publish on one, five is typically kind of a higher number. The highest amount ever published on was a study I published this past year, and I think we only included 32. Government reports usually have around 20, 30, 40 markets. So we identified seventy markets, which is big, right? But importantly, we think this is just the tip of the iceberg, right? We think we've only scratched the surface. And with the appropriate collaborations and the right expansions, we'll be able to find more sophisticated markets and markets catering to a more sophisticated clientele. So identified over 70 markets selling ransomware products. And on these markets, we find, I mean, 1000s of vendors, not every vendor of course sells ransomware. But we find multiple vendors selling ransomware. And we find that it's extremely accessible. And interestingly, vendors sell ransomware on multiple markets, right? So it's not like if I were a ransomware vendor, right, and I'm gonna use physical markets as an example. If I'm selling ransomware, I'm not just selling it on Amazon, right? I'm selling it on eBay as well, and probably Walmart, because if eBay, Amazon, or Walmart go down, I still have my market, I can still make money, right? Amazon's aren't going anywhere. But Dark Web markets are much more volatile, right? They're constantly being attacked by hackers. They're constantly under investigation trying to be shut down by law enforcement operations. And oftentimes, they exist on less than secure servers in like some dudes basement. So they're not as stable as the servers that you know, Amazon and eBay, or the online version of Walmart exist on.

C. Jordan Howell 41:04

So these vendors actually set up shop across markets, selling products, which is extremely important from threat intelligence standpoint because it creates this interconnected ecosystem, right. So we found 70 markets, and the current law enforcement approach is identify a market, spend a bunch of money to try to shut the market down. Who cares? Right, you shut down market one, there's 69 other markets in existence in which these vendors already have stock it. So it doesn't do anything. So it essentially creates this resilient ransomware distribution hub that allows individuals to continue buying and selling ransomware despite law enforcement operations. In addition to that, right, we find it's actually extremely affordable, accessible, and we have reason to believe based on reviews and prior tests that it does, in fact, work, right? We're actually working on a study now we're going to purchase a lot of the ransomware and start launching attacks against ourselves to find out what products are the best how we can predict the quality and essentially come up with better solutions, once someone is infected with ransomware, that doesn't require them paying the ransom.

Jenn Tostlebe 42:16

That's cool.

Jose Sanchez 42:17

So in another study, you investigated stolen data markets to better understand the size and scope of the illicit online ecosystem. Based on these findings, how often or how much stolen scope of the illicit online ecosystem. Based on these findings, how often or how much stolen information gets sold to other individuals?

C. Jordan Howell 42:33

Yes, great question. These are technically separate studies, the one you're referring to now, which was published in The Conversation rather than AT&T Cybersecurity was funded by DHS. And up until my current project, which we gathered 70 markets was the largest systematic assessment of Dark Web markets to date. But they're not really mutually exclusive. Because in both projects, we're looking at this dark net ecosystem that enables the distribution of hacking products and services, including stolen identities. So what I really liked about that study and ecosystem approach as a whole is oftentimes on the news, you know, you'll hear of, you know, US Bank, right being hacked, you know, a couple 100,000 accounts being compromised. And that's really the end of the story. Right? That's what you hear. You don't hear anything else. Maybe if you're Jose, you receive, you know, a credit card in the mail, because yours has been compromised and they want to prevent it from being used, but the public doesn't get a lot more. What we find is that's actually the first of many stages in the supply chain. Right. So once the hacker attacks the bank, steals or compromises the accounts, what they do is they actually, they become the producer in the supply chain. And the next step is they often send the data to a wholesaler, or they could also be the wholesaler in some situations, where the wholesaler provides the data on these dark web markets for sell. And that's what an end user comes in purchased as a data to actually engage in the nefarious act against Jose specifically, right? So the hacker attacks the bank, steals all the credit card numbers, either gives it to a wholesaler or becomes the wholesaler, and that's all these dark wet markets, and then from the dark web markets an end user, you know, the fraudster, purchases the data, and then uses it to launch an attack, engage in identity theft, commit fraud, etc. And all that's enabled by the existence of these dark web markets.

Jenn Tostlebe 44:43

Is that a quick process? Do we know? It seems like it would be relatively like fast that all of these things would happen within a very short span of time?

C. Jordan Howell 44:53

Extremely, extremely fast. Which is why most cybersecurity solutions are so obsolete, right? Every one will wait until the data is like already in the hands of the cybercriminal, who's going to use it for identity theft and fraud before they start trying to address the issue, but you really have to go upstream. Because the second that data is compromised, it's almost immediately sold on these dark web markets. And within days, it's being used for nefarious purposes. So if the attack goes unnoticed, and the data reaches the end user, then the Cybercrime has occurred, right. So now it goes from one cyber attack against US Bank to hundreds of 1000s of attacks against all of US bank's customers, which is much more problematic, especially for everyday internet users. And in our experience, we're able to gather the data upstream. So we're able to actually identify the stolen credit card numbers, the stolen bank accounts, before it's used by the end user. And we're working on different solutions in order to inject various interventions into the supply chain to keep it from going from the hacker to the end user. We want to keep it in the hands of the hacker or intercept it before it's used nefariously.

Jose Sanchez 46:08

So something that we found interesting was, you're finding that only a handful of the markets were responsible for trafficking most of the stolen data products. And it reminded us of the Wolfgang and colleagues study from 1972, where they found that only about 6% of delinquents accounted for the majority of offenses, but of course, not all of them. What did the revenue look like for these large markets? And how does it compare to companies in the US that are operating legally? And I say that with a little bit of skepticism, but for these purposes, let's say legally.

C. Jordan Howell 46:52

Yeah, it's a good question. Right? So again, I and this is how we differ, my research team, differs from most scholars studying the dark web is we don't look at Dark Web markets, we look at an entire ecosystem. And when you take a step back and look at the ecosystem as a whole, you see that not everyone has the same role in that ecosystem. So if we think about your example of licit, legal markets, not every markets equally successful, right. So we used some really good examples earlier, I think with Amazon and eBay, they dominate the market, walmart.com, those three dominate the market. I can't think of another retailer that competes with these three. Maybe you guys can, maybe there's a fourth, but they definitely take up the lion's share of traffic and distribute the most legal products, right. And the same exists in the dark web, right? Not all markets are going to be equally successful. So we find that there are some markets that within an eight month timeframe make almost $100 million, it was $91 million. In eight months. In eight months, these markets made $91 million selling nothing was stolen data products. If we would have taken into account drugs and guns and other types of products and services, that number would have been much, much larger because at the end of the day, stolen data products aren't the most sought after commodity on the dark web. Spoiler alert: drugs are the most sought after product on the dark web. So three markets really dominated the ecosystem, were making millions of dollars, and were each the size of a mid sized US company within an eight month timespan, whereas other markets made substantially less right. So markets made, you know, still hundreds of 1000s dollars, right? Not a bad side gig, right? If you're the administrator of that market. Other markets made $0 Right? So we find that it parallels almost perfectly what you see in the legal business community did air quotes again.

Jenn Tostlebe 48:57

Air quotes. Alright, so so far, you know, we're gonna kind of circle back to the top of the podcast when you were talking about definitions. But so far, we really mostly focused on the actual act of the cybercrime, specifically ransomware. But there's another component which you've mentioned, which is the offender and kind of their motivation for actually engaging in cybercrime. And so we're assuming that as with all crime, the motivation likely differs from person to person, but is there any specific motivation that stands out above all the rest for why people commit cybercrime? Is it money? Is it something else? Do we know?

C. Jordan Howell 49:41

It's a fantastic question. And if I can answer it perfectly, then I'm not entirely sure criminology would exist anymore, because what would be the point right? I have a philosophical belief that may actually be more upsetting to your listeners than some of my earlier statements about cybercrime. Motivation is simple, right? Between stimuli and action comes a choice. Right? So everyone has that choice, right? So at the end of the day, crime, like all other actions are in some part rational. They're bounded, right? It's bounded rationality because you can't possibly predict all future risks/rewards associated with the decision. So I operate on the assumption that cybercriminals, like everyone else, are rational actors who attempt to maximize rewards while minimizing pain. And these individuals are often highly skilled individuals, who, as we discussed earlier, lack fear of law enforcement intervention because law enforcement struggles to police cybercrime. So for these individuals, I've talked to a lot of them personally, I actually have a decent amount of report in some different hacking communities, and ultimately, the same thing, they're like, dude, I'm not even living in the US, like, what is the FBI gonna do to me? Like, they can't, right? There's too many jurisdictional issues. And oftentimes, I'm like, Okay, well, what if, and they're like, Dude, it doesn't matter. There's no What if. They say, even if they could investigate this, they would never find out who I am because I'm using the correct techniques, software's, and anonymizing technologies to evade capture. So for these individuals, their perceived reward is often monetary. Right, they can make money by selling or using ransomware, whereas their risk is low, right? They believe that they are undetectable. So I think this is a classic example of the utility of the rational choice perspective, and shows that if an individual doesn't fear sanction or punishment and believes they can walk away with, you know, Jose's few $100, they're going to do so. So to change that calculus, we need to do one of two things, right, we need to either disincentivize cybercrime, I'm not entirely sure to do that, right, that would make me a Nobel Prize winner, or we need to find ways to increase the probability of identifying the individuals behind the keyboard. I guess really importantly, this is gonna get way too theoretical and kind of off topic. But I think it's important, right? Because you're asking about motivation. And Jenn, I think you're going to disagree with me, I've read some of your work, right? So even though between stimuli and action comes a choice, right? So at the end of the day, that's the direct effect, right? An individual makes a choice. The calculations vary, right? Everyone has a different perspective, based on their risk tolerance, etc. But that choice, of course, is going to be influenced by circumstance. So we find a lot of these individuals are involved in hacking teams so we could think about social learning theory, right? These individuals have this differential association and reinforcement that leads them to believe that cybercrime is the right choice. Oftentimes, these hackers are from third world countries, and this is way more profitable than whatever they would be doing if they had to work a nine to five, right? So then you could take into account strain theory, or maybe that's just rational choice as well. But morale of my story here, right, is that all models, all theoretical models that posit a direct relationship between anything and crime, suffer from Omitted Variable bias there misspecified models because the end of the day, all of these different factors that we call criminological theories, they don't predict crime, they don't predict the outcome. They simply predict choices and preferences, and that preference is what leads to the act. I'd love to hear your thoughts on this, though.

Jenn Tostlebe 53:48

I mean, I don't know exactly why you think I would disagree with you?

C. Jordan Howell 53:52

Because you're the psychological researcher, you have to. It's in your nation, right?

Jenn Tostlebe 53:56

I mean, I suppose. I do stuff in psychology, but also I'm trained in sociology, right.

C. Jordan Howell 54:02

Sociologists also hate the rational choice perspective. So another reason you would disagree with me.

Jenn Tostlebe 54:07

Okay, well, we have Kyle Thomas as one of our professors, who is a rational choice theorist, and maybe he's had some influence. And I think Jose would say that Jenn is the control theorist.

Jose Sanchez 54:22

I would.

Jenn Tostlebe 54:24

I think it's interesting. I don't wholeheartedly disagree with you. Although I would probably stay away from the strain perspective. I'm not a big strain theorist.

Jose Sanchez 54:35

I think we're about to lose our strain theory fans but yeah, not we're not strain proponents. Sorry Kendra. But actually, Jenn and I are going to be working on a rational choice gang membership paper.

Jenn Tostlebe 54:51

This was proposed to me to work on, so we'll see how it goes.

Jose Sanchez 54:56

Yeah, I kinda roped Jenn into it. It really wasn't a choice that I gave her.

Jenn Tostlebe 55:02

It was not rational.

C. Jordan Howell 55:05

What are the odds that I'm in a room with two of the only rational choice people left in our field. So I didn't expect that. I'm happy about it.

Jenn Tostlebe 55:14

No, that's fair, especially two people who are in a sociology program.

Jose Sanchez 55:19

I'm not going apologize to the sociologists listening to this, get it together. Okay, so our next question is, how often do hackers engage in cyber crime, because if you go off of like TV shows, it'll go from, this is what they do all day, every day. And this is just some 15 year old kid in high school, like, just like, hit enter, and his computer is just running some program, while he's in third period, math or whatever. So do you know how often like they actually just engage in this behavior?

C. Jordan Howell 55:56

No. Right, it's a good question. Because I guess Let me twist the question around ask you, Jose, like, do you know, how many crimes the average criminal engages in? Right? It's impossible to answer because there's so much variation between the different types of cyber crimes, and the individuals that commit them as well. And you brought up the Wolfgang's study earlier, which was interesting because it was something I was recently thinking about for a different study. I think it really applies here. There are individuals that are extremely prolific. I mean, it's insane, right? We do a lot of open source Intel. And these guys, or gals are attacking computers constantly. I mean, it's insane. I don't know if they have any free time, like they're acting as if it's a full time job. And they're working overtime, every single week. And there are other hackers, or just cyber criminals more generally, I guess, who will appear in our database, and we won't see them for an extended period of time. And then they'll just pop back up, right? Almost as if, like, they just do it because they're bored every now and then like, the way I play basketball, right? Like, you know, every six months, I'll go into the local LA Fitness and shoot, right, but that's certainly not representative to everyone there who play daily, right, or weekly or monthly. So there's a lot of variation in the number of attacks each hacker or cybercriminal generates, and the severity of those attacks as well, right? Everyone differs in skill level, motivations vary, age varies, right? So there's really not this stereotypical image of a cybercriminal. It's often portrayed by media, that you're probably imagining when you give the examples of the 15 year old kid. But we did conduct a study, I believe I published it with George Burruss and maybe David Maimon, in which we collected a lot of active offender data. And were able to actually calculate how many attacks each of the hackers generated over the course of maybe a year, I don't remember the specifics. This was a few years ago, and we ran a latent class analysis, you know, based on the frequency of its acts, and we found that there really are these two different groups, right, the people who were really prolific and people who are kind of just, you know, show up every now and then, you know, shot basketball, or, you know, launching attack, and kind of just disappear for a while. So a lot of variation that makes that question hard to answer.

J Jose Sanchez 58:20

Yeah, and I guess it kind of ties into just like normal people as well, like, you know, your life changes. Like, there's hobbies that I used to do, like, all day, every day, from what it seemed like, and then I got married, I had a kid, and I just don't really get to do those things as much anymore, or at all, you know, like, life trajectories just kind of go all over the place.

C C. Jordan Howell 58:45

Trajectories. I think that's the best word for it, right? Because we see that a lot as well. And I'm pretty sure that we're about to head into this direction. So I'm really sorry if I'm kind of jumping the gun. But it's just a perfect segue, right? Because you used to have all these hobbies that you did daily, you got married, you had kids, right? You're in a Ph. D program. And all of a sudden, you don't have time to go to LA Fitness to play basketball every day, right? Like your priorities have changed. And we see the same thing in cyberspace as well. Again, one things I alluded to, or maybe directly stated, I'm not entirely sure is that a lot of the Cybercrime research is really bad, because they don't gather active vendor data. They'll talk to college students, if you could do this, would you and why? Whereas we're taking to the next level by actually extracting actionable intelligence on active offenders. And we're often able to find out some of these turning points, right, we're able to gather open source Intel and use different forensic techniques to maybe not perfectly capture but provide a proxy for different types of turning points and we see that their trajectories much like yours changes with time, right? You may be extremely active in the hacking community when you're 15 and 16. And then you get a girlfriend and she's like, yo, let's go to the movies instead. And like, you know, that's two hours that you would have just been attacking sites. And now, you know, you're sitting, watching whatever movie that your girlfriend want to see, because obviously she picked.

J Jose Sanchez 1:00:17

Given all this, is it possible to predict who will become a persistent threat?

C C. Jordan Howell 1:00:23

I think so. We just published a report in AT&T Cybersecurity, that attempted to do that. It was the most recent report we published. And we were able to find that digital artifacts extracted using open source intelligence, were predictive of criminal trajectory. So there are things that hackers can do early on in their career that are correlated with future attack trends. Right? So one example is we found a large number of political hackers, hackers who were outraged by, you know, the political climate, right, hacktivist, if you will. And at the onset of their career, they were extremely active, right, attacking websites daily to spread their political message, just very involved in that community. And then with time, you just see them naturally decline absent intervention, right? They're no longer the active hacktivists they were before. So maybe like activists in the real world, they were just virtue signaling that's possible. Or it's possible that whatever they were upset about changed the time, right, maybe they were upset about something and a policy was introduced to change to something that upset them. Or maybe they just stopped caring, right, time heals all wounds, I imagine it heals political wounds as well. But we find people who start their careers because of the specific political, ideological, religious reasons just fade with time. Conversely, which is interesting, we find that people who join teams, and are very vocal and active on social media sites actually engage in more attacks as time progresses, showing that they're going to be either persistent threats or, you know, continued threats. I mean, I could create some ad hoc hypotheses around that. But it makes sense to me, right? These individuals are trying to gain a reputation within their community, right, they start getting attention from their friends, their peers, their networks, the last thing that they can do or should do, if they actually care about their reputation is cool down, right? Instead, you need to continue to use your newly acquired skills to show what you've learned, why you belong, and, you know, prove yourself.

C. Jordan Howell 1:02:40

So we find that there's ways to predict it using cyber intelligence. And we have multiple studies right now using active offender populations that are going to allow us to assess some of the more traditional criminological turning points because I'm personally really interested in seeing if getting married, having a girlfriend or boyfriend, having a child deters you, right? Because you can't it's rational, right? Like you have more to lose. You know, Jenn, you're the control theorist, right? You have these attachments to society and family, these bonds that you don't want to break. And we're actually working on a project now, where it's gonna be the first large scale survey of verified active malicious hackers. I know that's an absolute mouthful, but each of those words are important. Because if you look at the criminological literature, and you just read the abstract or title, you be like, Oh, my God, so many people have surveyed hackers. And then you read like the actual study, right? And it's like, well, we asked people, like, if they could hack would they or we asked people if they've ever used someone's Netflix account or something like that? Right? They're not real hackers, right? Like, there's obvious differences, both observed and unobserved between the two groups. So this would be the first time anyone's ever been able to ensure that the hackers were verified, and truly malicious, active hackers. And we're going to ask them these types of questions right, about their attack frequencies, their motivations, getting back to one of your questions earlier. And their turning points, right, both previous and perceived. Because maybe you if you were a hacker, Jose or Jenn, right. Maybe you're like, yeah, like if I got married, I would have to stop doing this. Maybe you already know before it even occurs.

C. Jordan Howell 1:02:40

Very cool. I'll be interested to see what you find.

C. Jordan Howell 1:02:41

If you want to add questions to my survey, let me know I think they can land really need outlets across disciplines.

Jenn Tostlebe 1:04:33

Yeah, for sure. All right. I know we're over time, but we have one last question for you if you have time?

C C. Jordan Howell 1:04:39

Of course.

Jenn Tostlebe 1:04:40

Okay. So given everything as a whole that we've discussed, and I know we covered quite a bit of ground here. What are the implications of your work for research and then policy and practice?

C C. Jordan Howell 1:04:54

Yeah, I think that's the second most important question after the definition ones you asked early on. Right now there's a huge disconnect. And I've used that word multiple times, because it's really the best way to describe what's happening between academia and industry. Academics approach cybersecurity as criminologists, or as computer scientists or as blah, blah, blah, blah, blah, blah, we can go on forever and ever, right? But scientific innovation, it can't occur in a vacuum, right? We can continue to test control theory or social learning theory in cyberspace. And that's cool, right? Like, maybe you guys will cite it one day. And ultimately, that's all that'll happen. I find that to be extremely problematic. At the end of the day, if the research that you're conducting doesn't have immediate benefits for policymakers and society as a whole, you're wasting taxpayers money. So the work we're doing really takes the human element from the social sciences, including criminology combines it with innovations in cyber intelligence, while including these technical components to build out holistic solutions, right. So we, informed by theories of human behavior, extract, actionable Intel, which is then used to build out systems that are more robust, right? Because they take into account the person behind the keyboard, right, the person at the main, they take into account end user who may completely ignore the policies and protocols that were implemented by a computer scientist who only thought about the technical components. And I think it's important and when we work with the financial sector, we have lots of partners in the financial sector in the cybersecurity industry as well. What we find is they really want this paradigm shift. They really want to see this interdisciplinary research that takes into account all these different disciplines and offers holistic solutions. But academics are just so resilient to it, because it's not in their best interest, right? If you're a criminologist, and you've been a criminologist for life, and now you want to make a little money by calling yourself a cyber criminologist, the last thing you want, is some guy coming in and telling you like, hey, this actually isn't cybersecurity. It just criminology poured into a new bottle with a new label, right. So the innovation in our research is that we take tried and true concepts from across disciplines to ensure that we're able to provide a more comprehensive understanding of the current landscape in order to predict future trends and prevent cyber attacks. And hopefully, if I ever appear on the podcast, again, Jose, when you asked me about the number of cyber attacks, I'll be like, less than last year, right. That's the goal. And that's what we hope that our research can accomplish for policymakers and the nation as a whole.

Jenn Tostlebe 1:07:46

Very cool.

J Jose Sanchez 1:07:47

Yeah, that's awesome. And we're looking forward to those results. But those are all the questions that we have for you today. Thank you so much for joining us. We really appreciate you taking time out of your day to talk with us. Is there, besides what we just talked about, anything else you'd like to plug that we should be on the lookout for?

C C. Jordan Howell 1:08:04

No, but all of your listeners should follow me on Twitter @Dr_cybercrime. And I chose that handle specifically because of academia doesn't work out, I want to be a Spiderman villain. I got an additional graduate degree so I can fit in with the rest of his enemies.

J Jose Sanchez 1:08:23

Awesome. Yeah, man, that's you just stopped me? Because my next question was gonna be where can people find you?

Jenn Tostlebe 1:08:30

Predicting the future.

J Jose Sanchez 1:08:31

And yeah, you guys are

C C. Jordan Howell 1:08:33

I can say my twitter handle again because I'm trying to gain the followers. Maybe this will give people incentives to follow me. John Cena just followed me on Twitter.

Jenn Tostlebe 1:08:45

I saw that. Did you post something about that?

C. Jordan Howell 1:08:49

Yeah, it was pretty awesome. He is one of my childhood heros. It was unfortunate though, cuz he followed me and I was like, I can't see him, you know?

J Jose Sanchez 1:08:57

I was gonna make that you can't see me.

C. Jordan Howell 1:09:01

Low hanging fruit, right. I mean, you have to, but he lives in Tampa. Who knows? Maybe we'll collaborate on projects. podcast.

Jenn Tostlebe 1:09:10

Yeah. If nothing else, you can go get drinks with them. Hang out. Well, thank you again.

C. Jordan Howell 1:09:22

Yeah. Thank you so much for having me. I really enjoyed chatting with you about cybercrime, cybersecurity, and all of my controversial views on the topics.

Jenn Tostlebe 1:09:33

Hey, thanks for listening.

Jose Sanchez 1:09:35

Don't forget to leave us a review on Apple podcasts or iTunes. Or let us know what you think of the episode by leaving us a comment on our website, thecriminologyacademy.com.

Jenn Tostlebe 1:09:45

You can also follow us on Twitter, Instagram, and Facebook @TheCrimAcademy.

Jose Sanchez 1:09:56

Or email us at thecrimacademy@gmaill.com. See you next time!