Announcer (00:02):

You are listening to the Safety Moment Podcast by Utility Safety Partners. Safety is always a good conversation and it's a click away. Here's your host, Mike Sullivan.

Mike Sullivan (00:16):

Today we're talking about cybersecurity. Now it sucks to say this, but we are all at risk of cyber attack, but who's attacking us and why are they doing it? My guest today is Mr. CaSh Wong, CEO of Shing Digital Cash and his team have been utility safety partners, information technology service provider for decades and like others in their field, CaSh has a zero to the ground when it comes to cybersecurity CaSh. Thanks for joining me today. This is looking forward to this one actually. I look forward to all the podcasts, but I was really looking forward to this one because it really applies to everybody.

CaSh Wong (00:49):

Oh, absolutely. Yeah. I

Mike Sullivan (00:50):

Mean, if you don't have a digital footprint today, there are not too many people that don't.

CaSh Wong (00:54):

Oh, absolutely. I mean, God are the days you probably, we can still remember the days where we could run a business without a computer. That's not the case anymore.

Mike Sullivan (01:02):

The cash register, it doesn't exist.

CaSh Wong (01:04):

Exactly, exactly. All your cash registers these days are connected to the internet somehow or another. And it's the same thing with all of our critical infrastructure, not just the IT side. So yeah, it's hugely important.

Mike Sullivan (01:17):

It's scary actually. I mean, we're going to be talking about cyber security, cyber risks, cyber attacks, but what are some of the most common cyber attacks that affect John Q Public?

CaSh Wong (01:29):

I mean, probably one of the biggest things is just the scams going on, and we've been around long enough to, we remember the Prince of Nigeria scams and I mean they still go, I'm still

Mike Sullivan (01:42):

Waiting for my inheritance.

CaSh Wong (01:45):

There's a picture, a vault of a lot of money that the Nigerian prince has, but that goes unclaimed because none of us have made the phone call. But a lot of what we see today is sort of an evolution and

a more dangerous and darker turn of those attacks that we used to see. And I mean, the progression before was a lot of the attacks were against consumers. That was kind of the first big, everybody was not as computer savvy and so much easier to scam a few hundred bucks or a few thousand dollars from the general public. And companies, for the most part, for I would say many, many years, didn't really have to deal with it because they had four walls. They built their fortress around the four walls. And for the most part, most organizations were relatively safe because everybody worked within the four walls. And then of course the pandemic hit and now those four walls got shattered. Everybody went to work from home.

Mike Sullivan (02:49):

It is splintered from everywhere. And that had to be a huge

CaSh Wong (02:52):

Challenge. It was, and we saw a massive increase in the number of tax against organizations. And of course, from the few thousand dollars to maybe even 10 or $20,000 that you can scam out of a consumer, well now you can take hundreds of thousands or millions of dollars from a business. And so it evolved to there and now we are evolving to an even darker side now where a lot of, I think what you talk about a regular basis is more on the utility safety and the click before you dig, call dig. Well now all of that infrastructure is virtually at risk, not just physically at risk.

Mike Sullivan (03:36):

It's susceptible to somebody. Well, ransomware is a big one. Obviously I know of two major utility companies that were attacked in the last 12 months or so and they had to rebuild their entire service.

CaSh Wong (03:52):

Absolutely.

Mike Sullivan (03:53):

And this is becoming more commonplace. This is where it's beyond the annoying. I mean, as you said earlier, the Prince of Nigeria or whatever that was, it was a bit annoying. Or you get these spam phone calls, you've already won a trip or whatever, or Visas calling or Amazon saying your car has been compromised or something like that. It's annoying. You hang up and that's the end of it. But a ransomware, I mean, this is some serious business now. They're asking for a lot of money.

CaSh Wong (04:28):

Absolutely. Yeah. I think one of the, now, and this is a moving target and it's always changed, but some of the biggest ransoms that have been paid over the last few years have been upwards of over $50 million that

Mike Sullivan (04:43):

Actually been paid. They've

CaSh Wong (04:43):

Actually been paid. Now that was negotiated down. I won't mention the company on the podcast, but No, that'd be a good idea. Very prominent

Mike Sullivan (04:52):

Company. And this is our last podcast ever

CaSh Wong (04:54):

Because lawyers are coming to sue us. Yeah, exactly. But the initial ask was, I think it was something like 250 million if they paid within 30 days, and if they didn't pay within 30 days, I think it was like 450 or 500 million that they were asking for. Oh my God. But basically the hackers basically took off with all the crown jewels before they launched the ransomware. And so they had every customer contract, they had every intellectual property, and they, they basically emptied the vault in terms of the information that was there. Now their insurance company got involved and was able to negotiate it down to $50 million. But if you ever imagine, what do hackers do? What they do? Well, 50 million is a pretty big payday, and that's a big,

Mike Sullivan (05:45):

Yeah. Well, who's attacking? Who are these people attacking? So

CaSh Wong (05:49):

Generally speaking, it's been a lot of bad actors that have come from jurisdictions that we can't touch them. Everybody always asks me, we just go after these guys. He goes, well, they reside in jurisdictions like Russia. They reside in jurisdictions like China and Iran, places where there are no extradition treaties in place. We do get lucky sometimes. We've caught a few Russian hackers that have gone for vacation and transited through Europe, and we've caught a couple of them that way. There's been

Mike Sullivan (06:23):

The dumb hackers if there is the dumb hacker.

CaSh Wong (06:26):

Exactly. And there are some, we are starting to see, I guess a few more collaborators that are on shore, and I can kind of go into that more detail, but we've caught some of those folks. But I mean, it's just a drop in the bucket in terms of the hackers that are out there. You just simply can't get to most of them.

Mike Sullivan (06:48):

Well, I mean, as I said earlier, if you have a digital footprint, you're at risk, period. Right, exactly. And everybody, I shouldn't say everybody. Most people today, you're doing your banking online, you send your kid to cuffs up a couple of bucks, you're paying bills, you're doing whatever you're online. And if you're using that device, whether it's your mobile device or your desktop or what have you, it's at risk. So how protected are we? I mean, most of us go through this life blindly not even realizing that these nefarious individuals or organizations, they're waiting for us to trip up.

CaSh Wong (07:29):

Well, I mean, they're just not waiting for you to triple. I mean, there's a few different types of hackers. There are certainly the ones who target specific companies or specific people because there's some sort of set purpose. But the majority of the hackers out there are simply just, you got to imagine they're on a computer. The computer does 99% of the work for them. They hit a button and it sends up millions of pieces of spam every day. And it's constantly probing and testing everything that is connected to the

internet to see whether or not there's a flaw or whether or not there's a way in. And the majority of the time, like I said, it's one click of a button and it's a computer that takes care of all of the rest of it for them. So it's really low cost of labor to get that done.

(08:19):

So they don't even have to be targeting you. They're just casting a really wide net and they're seeing who responds. So even back in the day when we talk about all those spam, I mean, I think most people would take the spam and dismiss it as a whole, but the numbers were that roughly, I think it was like one or 2%. My numbers may be a better around it's been a while, would actually respond. And if you can imagine they can send out five, 10 million pieces of spam, let's just say a day or a week, and that one to 2% becomes a huge number. It does. And so it's the same type of thing with modern hackers when it comes to the consumer side. They're probably not specifically targeting you, but they cast this wide net as to who is willing to fall for it.

Mike Sullivan (09:05):

I mean, I know of two elderly people that, and it has happened a lot, unfortunately, they were victims of spam, and one of them was mid $30,000 that they lost and never got it back. And the other person I know of, they were about to go through with a transaction and they reached out to one of their kids and said, Hey, something fishy here, and just drop it. Forget it. Right? But they're preying on our personality that we want to help or we want to help a family member, whatever it might be. Your grandson is in jail and they need money to get out or something like that. And that's the simple thing, which okay, you can ignore it, just forget it goes away. But then you get into the corporate world, and I mean, even I remember going back could be almost 10 years ago, Alberta one call, we were hit with ransomware, and it was compared to today.

(10:11):

I can only imagine the lack of sophistication back then compared to today. And your team came in and eradicated it within maybe 30 minutes, and we were off and running, but there was never any risk to our members. There was never any risk to anything. But it was an email that came in. It looked identical to whatever it was we were doing, and the person opened it and no fault of their own. And next thing you know, we're getting messages. But today, the ability to make sure that doesn't happen, first of all is pretty good. But the ransomware that does come in, it's got to be so much more sophisticated than it was.

CaSh Wong (11:00):

It's super sophisticated these days. And the scarcity portion is this, back when that incident happened, back then it was just about the ransomware. It was the hackers would get in whichever way, and then as soon as they got in, they would launch the ransomware and you got a message pretty quickly, and it's say you can pay it, or if you're set up correctly, you have a way to restore it. These days, the hackers have learned, now they do what's called a double extortion. So what they do is they dwell inside the network and they steal all the data first. And then once they feel that they've gotten enough data or they feel like if the heat is starting to come on, that's when they launched the ransomware. But by that time, they've gotten enough of information where whether or not you pay the ransom, if you don't pay the ransom, then they're going to threaten to release all of this information that they stole.

(11:56):

So if you've got a lot of proprietary information, or you have a lot of personal identifiable information like credit cards, driver's, licenses, all the rest of that, well, you can't afford to let that get out. And so

then you're forced to pay the, you're forced to pay the amount, but you're trusting a hacker to delete this data. So imagine that, right? Yeah. You're trusting that you're going to pay a hacker, whatever it is, hundreds of thousands or millions of dollars, and on their good word, that they're going to delete that data and let you give you the key by which you can unencrypt everything.

Mike Sullivan (12:34):

And chances are that data may have been sold, right?

CaSh Wong (12:36):

Oh, absolutely. You take a look at some of the large data breaches, and what they do is they'll promise that they'll delete it, but at the end of the day, they can chop that data up into individual records and sell it individually, and you're never going to be able to trace the source of it. So it's like the gift that keeps on giving for them, they can continue to monetize all of this data that they steal from you. And so that's why there's that double extortion piece now. And again, even more important to sort of put up all of the virtual walls. We don't have physical walls to put up anymore in order to make it as hard as you can for the hackers. One of the things I always tell customers, and anybody that's willing to listen is that we're never going to be able to protect you 100%, but the harder we make it for the hackers, we want them to go look for an easier target. That's not you. So you're never going to be a hundred percent protected. But if we can put up enough walls, if we can put enough barricades in front of the hackers to make them think, you know what? I'm going to go down the street and go bug somebody else. These guys have too many things going on, it's going to take too much work. So

Mike Sullivan (13:51):

How are we protecting ourselves? I mean, as the sophistication of the hacker comes up, well then ours has got to be much stronger. Are we? How better are we today than we were a decade ago?

CaSh Wong (14:04):

I mean, from a technology perspective, we're leaps and bounds ahead of where we were to be able to protect yourself. Now, that being said, the hackers themselves have also gotten we more sophisticated in terms of the technology that they use. So it's a constant cadid mouse game. What keeps me up at night is, oh boy. Yeah. What keeps you up at night? Talk to customers. Oh, we do. Yeah. We have a lot of great customers like utility safety that very much listens to our advice and make sure that the proper systems are put into place to protect your networks, to protect your people. But we have a lot of customers who still don't quite believe that it's that big of a threat that they need to invest in the systems in place to protect them. And that scares me. And I talked to some customers who have, one of the big things coming up is legislation.

(15:02):

So Bill C 27, which is right now in committee, and whether or not it'll get passed this year, I think the chances are low, but I think by next year, as long as it passes before the election changes our entire governance when it comes to data privacy. So that's going to be how companies protect all of your personal information that's going to set a bar much higher. And so a lot of companies who still collect that information still don't take cybersecurity seriously. And if you can imagine when they lose that information, it's your information that they're losing. That's right. So that opens you up personally for identity theft, and you never did anything wrong. You just went and about your business and interacted

with the retailers or the vendors that you typically do. And when they get breached, you are the one that pays the price.

Mike Sullivan (15:57):

So when the legislation, it'll set a new minimum standard, obviously, but anything, there's better practices that a lot of companies employ, and that's why we have people like yourselves and then Shane Digital to help us through that because we don't know, this is not our place. We work in that space, but we don't know that space like you do. What should companies, should individuals be doing? Let's start there. What should individuals be doing? Jack and Jill homeowner, what should they be doing to protect their identity, protect their assets, protect their banking

CaSh Wong (16:35):

As an individual? It's tough. On the corporate side, we have so many options to protect you, right? On the individual side, it's very tough because there aren't a lot of tools. I mean, one of the things is make sure you have a good antivirus. That's number one. That's probably one of the top most important things. And do not just use the free antivirus. So on all the Microsoft platforms, they have their Microsoft, their free version of Microsoft Defender. It is better than nothing, but there are much better programs out there for 50 or $60 a year. You can get a really good application. And I dunno if I should name drop any of those companies here, but I

Mike Sullivan (17:19):

Won't tell.

CaSh Wong (17:20):

You won't tell. Alright. And again, I'm not discriminating from one vendor to another, but Sophos eec, there's a lot of great commercial antivirus and EDR, what are called EDR applications out there for the consumer that they can get and relatively low cost, it's going to be the best 50 or $60 you'll spend for the year. Yeah. Peace of mind, right? Yeah. Well, there's always something to be said about good hygiene in terms of how we deal with email and how we deal with things. But at the end of the day, these hackers are so good that you're going to want something to have your back to. And not that any of those providers are perfect, but they're going to at least provide you with the ability to let you know if something weird is happening. If you've clicked on something and you're starting to see strange things happen to your computer, those applications are going to tell you they won't be able to stop everything. But again, you just want to make it as hard as possible for the hacker so they go somewhere else. That's a really a big, is

Mike Sullivan (18:25):

A desktop computer more at risk than a tablet or your smartphone, or is it all the same?

CaSh Wong (18:35):

I'm going to say that a computer is going to be more at risk than your tablet or your phone. That doesn't mean that there aren't at attacks against those devices. So you should always be cautious, but there's going to be a lot more attacks against your computer just because the device itself is more sophisticated. As an example, if you have an Apple device, apple does a really good job of locking down their device. So again, not that it's impossible, but it makes it very difficult for hackers to attack, right?

Android phones a little bit more open and a little bit more susceptible to attacks, but your Windows computer is very sophisticated and they don't lock you down as much as those devices. And so you're way more susceptible to any kind of attack that might happen. And there will be people out there that goes, well, I run an Apple, I'm perfectly fine. He goes, well, no, no, you're not. The Apple are listed in terms of, are listed in the top 10 in terms of the most vulnerabilities that are out there. The only reason why you don't hear about Mac attacks quite as much is because they only own something like 8% of the market. And so you're not going to hear about it as much as the Windows side, which I think owns something like 70, 75% of the market. I

Mike Sullivan (20:00):

Was an avid Blackberry user when they were out, and that was the thing. Now, I seem to remember President Obama that he had that Blackberry welded to his hand. He didn't want to part with it. But is it true that Blackberry operating system was superior to apples as well in security?

CaSh Wong (20:21):

I would say yes at one point in time, absolutely. Yeah, not, but with the market changes and with Apple sort of winning over all that marketing share and Blackberry where it is, Blackberry also had to transition over to the Android platform as well. So their proprietary platform that they use is still around, but they now use that platform in the automotive world. So a lot of cars run off of what the bringing systems that used to run off your Blackberry,

Mike Sullivan (20:52):

Run your

CaSh Wong (20:52):

Blackberry. But absolutely a blackberry back in the day was the gold standard. But of

Mike Sullivan (21:02):

Course, I seem to remember that, and it's been a long time since I owned a Blackberry, but they were great when they were out.

CaSh Wong (21:07):

Oh, absolutely. Absolutely. That being said, back then, the type of attacks and the sophistication of the attacks are not at the same level either. Rights.

Mike Sullivan (21:17):

That's true. That's right. So we talked about Jack and Jill homeowner and what they can do. Then you move into a medium-sized business like a family business and maybe an accounting firm or something like that. What are they looking at? What are their costs of maintaining some kind of security?

CaSh Wong (21:37):

I mean, it depends on what you're looking at. For small business, they say you should be spending somewhere between eight to 10% of your revenue on it and security. How many organizations actually reached that level? We certainly have some, and they have everything in the correct things in place, but even if you don't spend that amount, it's about spending it in the right places sometimes is more

important. So it's about assessing your risk, assessing your budget, what you can spend on. So again, one of the things is the same kind of advice that we have for the homeowners. Make sure you have, now we get start getting a little bit more sophisticated in terms of the tools. Now instead of just wanting an antivirus, we want, our industry loves acronyms and they love the fancy things up. Ours too. Yeah, exactly. What

Mike Sullivan (22:31):

Is the acronym for acronym anyway?

CaSh Wong (22:34):

The acronym for acronym.

Mike Sullivan (22:37):

Okay. Nevermind. I'll

CaSh Wong (22:38):

Have to look that one up.

Mike Sullivan (22:39):

I don't know either.

CaSh Wong (22:41):

But the industry, so from a corporate perspective, we start moving off to things that we call EPP or endpoint protection, which is just a fancy way of saying it's a new version of the antivirus that has a lot more AI and machine learning built into it so that it can better detect attacks that haven't been seen before. Traditional antivirus has always been, we catch a piece of malware, we identify it, and we come up a way to identify it in the future, and then we add it to the program to look for that specific signature. Well, that doesn't work so well anymore. That only protects you against roughly about 40% of the threats that are in the wild today. So you have 60% of these threats that have never been seen before. And so you have to have what call the new EPP. Sometimes we call it next Gen antivirus, but they're just a lot smarter and use AI or machine learning to adapt and understand how an application is supposed to work, and it doesn't work that way and is doing something weird and nefarious. You want to be able to stop it.

Mike Sullivan (23:51):

And that's interesting. So artificial intelligence is improving the way we can defend ourselves from attacks, and yet AI is got to be doing the exact same thing for the Yeah, exactly. For the bad guys.

CaSh Wong (24:07):

So I'll give you a couple of examples of how the bad guys are using AI back to our Prince of Nigeria sort of example. One of the ways you can always identify those type of emails was usually the spelling was bad, the grammar was bad, right?

(24:22):

Well, now the hackers just go to chat g PT and say, Hey, write me something. And then GPT chat, GPT, writes it in perfect English exactly how, and they can even ask for a tone goes, I want it in this tone, and it will write that email for them. So you can't even identify it that way anymore. That's a really simple example. Now, a more sophisticated example is this. We've always had malware that we call 'em polymorphic malware in that every single single time they infect the computer, they change their code slightly. So that way it looks different every single time,

Mike Sullivan (25:05):

Right? Makes sense.

CaSh Wong (25:07):

But it required really smart programmers to program that type of malware. So now the next generation of that is that the guys writing the malware have embedded the ability for that malware to call out to chat GPT. And so every single time it infects a computer, it calls out to chat GPT and says, I need to rewrite this portion of my code. Can you do that for me? And so chat, GPT goes and changes it, downloads it, and now you have what looks like a brand new piece of malware.

Mike Sullivan (25:41):

This is a great conversation, by the way, but the more we talk about it, the more terrifying it actually is and what's going on. We just live our lives in this thinking, everything's fine, but what's going on around us? I mean, we are susceptible to anything. And I use my device for, I don't ever carry cash. I don't ever carry any physical money on me, and when I do, I never use it. It just sits in my pocket anyway. So I just always use my device to pay for something. But every now and then I go online. I look at, wait a minute, how come it's not, there's something missing here and it's just updating or whatever, but you do worry. Am I being hacked or something like that? What's going on? And it happens. So what are our banking systems, things like that. What is our government doing? What's the military doing? We talked about the homeowner, the small business. What are these major establishments doing to protect themselves and protect us?

CaSh Wong (26:44):

Well, part of that is some of the legislation that is coming out. Unfortunately, some industries won't take concrete steps until there's legislation, right? Live

Mike Sullivan (26:58):

Business.

CaSh Wong (26:58):

Exactly. So if we take a look at oil and gas, oil and gas is a perfect example. There's a lot of regulations around oil and gas. However, one of the things that we see on the ground with oil and gas companies that have significant assets like SD facilities, refineries, those types of things, we see a bit of a dichotomy from the corporate IT side. They follow all the regulations in terms of what they should be putting in place for cybersecurity programs, and they invest quite a lot in that side. However, then we flip over to the operational side of the business and we see that a lot of those same controls and a lot of those same systems are not in place. Part of that is a bit of a mindset change for the industry in that you not only have to protect the corporate side, but you also have to protect the operational side as well.

(27:55):

Now, where this has to be a big mindset changes this, and again, this isn't the case with every company, but a lot of the companies that we've interacted with, the operational side is the side that makes the money. And so they also tend to be the ones that can kind of dictate what happens on their side of the business as well. And so we have to make sure that the people who are running the operation side are comfortable with the cybersecurity systems that are put into place because a much different calculus from an operational side, from an IT side, and I know some IT guys will get mad at me, but if things break, it's an inconvenience. We can certainly get it back up and running and people will be mad at us. They'll be twirling their thumbs because they have nothing to do, but at the end of the day, it's not life and death.

(28:46):

Now you take that to the operational side. Now it's a very different calculus now. It is about safety. It is about life or death. And so the systems that we're putting in place to protect these systems can be seen as intrusive. And so the care that we have to take in designing and implementing those same kind of security and controls on the operations side have that much more urgency and that much more, we have to give it that much more thought to make sure that gets implemented properly. So that's why from a regulation perspective, again, another bill working its way through committee right now at the federal level is Bill C 26, which today it's for critical industries. So that's going to be a lot of your power generation, power transmission, transportation, like airlines, and then for pipeline companies that are either run pipelines, provincially, or internationally into the us.

(29:50):

So it directly affects those companies today. However, that being said, that's just a starting point. They could at any time, add in additional industries to make them a critical industry as well that have to meet this new regulation. And so we're starting to see a lot of resource companies now sort of getting ahead of the game and starting to put all of these cyber programs and cyber measures protection measures in place at the operational level because they know legislation is coming. The US is well ahead of us in terms of legislation and regulation for their critical infrastructure. And a lot of that spawned out of what happened with Colonial Pipelines in 2021. But the US moves at a speed, which I don't think we Canadians understand.

Mike Sullivan (30:37):

No, not at all of this legislation, all of this work. And then to bring the standards up to the new level of legislation, that new minimum standard, all of that costs a lot of money. There's no question about it. There's a huge amount of money that is going to be required to do this resources. But on the opposite side, cyber attacks is big business. Is that generating, how much wealth is that generating annually?

CaSh Wong (31:04):

Oh, the numbers are absolutely crazy. So I usually always have a slide out in terms of the amount of estimated revenue from a worldwide for cybercrime, right? And usually my chart starts off in around 2018 where worldwide cybercrime revenue was about a trillion dollars a year. Now that's a lot of money. That's a lot of

Mike Sullivan (31:29):

Money.

CaSh Wong (31:31):

But back then, ransomware was actually a very small portion of that trillion dollars. A lot of that back then was stealing corporate data and trading it and selling it on black markets. So that was a lot of the trillion dollars. But as ransomware has gained prominence, now, it's a much larger piece of it. And so for 2024, well, 2023 estimated worldwide cyber crown revenue is $8 trillion,

Mike Sullivan (32:00):

$8 trillion. I mean, that is incredible. And obviously it's not all off of Jack and Jill homeowner here. This is coming off major industry, and as you said earlier, some company had to pay or they negotiated down to a $50 million ransom. That is phenomenal. And then knowing full well, like you said earlier, knowing full well that all of that data, oh, sure, we're going to delete it. We're going to give it back to you. It's out there. Exactly. If you said it could be in bits and bites and chopped up, but it's out there.

CaSh Wong (32:34):

Absolutely. Absolutely.

Mike Sullivan (32:36):

That is incredible amount of money.

CaSh Wong (32:38):

Well, and just to kind of put it into perspective, right, Canada's GDP today is $1.8 trillion. Yeah.

Mike Sullivan (32:45):

Oh, I know, right?

CaSh Wong (32:46):

Yeah.

Mike Sullivan (32:47):

Maybe we should get into that business and solve our No, I can't do that. That's

CaSh Wong (32:50):

A side conversation. You and I will have,

Mike Sullivan (32:52):

Mike. We'll have to do that.

CaSh Wong (32:53):

We don't want this recorded. No,

Mike Sullivan (32:55):

No, no. That would not that part. No, we're not doing that if you're listening government of Canada. But when this amount of wealth that is incomprehensible, that amount of wealth is going to these nefarious

people or individuals or organizations, and your guess is maybe as good as mine, but probably better. What is that funding?

CaSh Wong (33:23):

I can guarantee you it doesn't fund anything good, because this amount of money is not just so somebody can buy a bigger mansion. Right.

Mike Sullivan (33:31):

Although I'm sure they do.

CaSh Wong (33:33):

I'm sure they do. Yeah. But I'm sure this funds a lot of other criminal enterprises that we don't even want to think about. Right? Back in the day, when you take a look at these cartels that were moving illegal drugs from South America through Central America and up, and they always tell you that by participating in purchasing these drugs, you're funding a lot of their activities that cost human lives and that put entire countries at risk. And I would say that a lot of the revenue that goes into these criminals, I think a lot of that because now you're starting to see a lot of these criminal gangs have crossed over now to the cyber side because of the money that's there. I mean, it's hard to ignore 8 trillion a year, right? Oh, you can't. In what other business organization, enterprise, can you generate that amount of revenue without ever leaving your basement?

Mike Sullivan (34:35):

That's incredible.

CaSh Wong (34:36):

And you don't need an army of people, although they have those too. And so these are funding things that now a lot of these gangs are, again, in jurisdictions that are sanctioned by the us, by Canada, by other countries in the world, and there's a good reason for it. So now, when ransoms are paid to a lot of these gangs in those jurisdictions, even the FBI ceases some of, maybe I won't put words in their mouth, but they've allowed companies to pay these ransoms because they know that they need to continue to do business.

Mike Sullivan (35:20):

And what are the choices they have? They had no other choice. They're shut down. They're done.

CaSh Wong (35:24):

Exactly. One of the stats, which I wish we could find that is very hard to find out there, is how many businesses actually can stay afloat after a cyber incident?

Mike Sullivan (35:38):

Well, I mean, just the integrity of the organization has been depleted. I mean, they don't tell anybody, obviously then, Hey, guess what? We were attacked. This is stuff that people just don't know about and they won't broadcast it for the most part. I can't see. Well, sometimes they do. They're forced to, but in order to keep doing business, I mean, how could you be public about it?

CaSh Wong (36:00):

Yeah, exactly. For companies who don't put all of the systems in place by which to protect all of their data and be able to recover, they're pretty much done. Once all of your data is encrypted. And if you don't have insurance, and again, even for a small company, they're not asking, we had a client of ours hit with ransomware probably a good seven years ago. And seven years ago, the ask from the hackers was about $40,000. And that happened before the hack against the UFC. And UFCI think paid 25 grand. And at that time it was an outrageous amount, right? So now companies would drop a

Mike Sullivan (36:47):

Bucket

CaSh Wong (36:48):

Drop in a bucket compared to how much they're asking for now. So even a small company, they're asking for, I think the average in Canada is just over $200,000 is the average ransom in Canada. How many small organizations can afford to pay that?

Mike Sullivan (37:02):

Not very many. And how many of these are happening every day? You think?

CaSh Wong (37:06):

Oh,

Mike Sullivan (37:07):

In Canada,

CaSh Wong (37:09):

I'm sure there's a number out there, but I think some of the numbers in terms of small businesses, something like 60% of small businesses surveyed in Canada have been hit by some sort of cyber incidents. Could be minor, it could be major, but 60%, it's a big number.

Mike Sullivan (37:25):

Yeah. No, cyber insurance is obviously you have that much of a risk in terms of your financial loss. There's insurance for it, but those costs are escalating. We're seeing it. Everybody is seeing it. Where is all this going to go? I mean, 8 trillion in annual sales, if you want to call it that. I mean, I can't think of any insurance that can protect you from something like that.

CaSh Wong (37:55):

And insurance companies have been trying to, well, we'll take this back a few years. A few years ago, cyber insurance was a new product, and insurance companies and brokers were bundling it in with your general liability, giving you a million dollars, but they didn't assess the risk. Now, with that being said, Canadian companies as a whole, on a per capita basis, are the best cyber insured in the world.

Mike Sullivan (38:25):

Well, that's good to hear.

CaSh Wong (38:27):

But that also leads to the hackers know they're going to get paid when they come after Canadian

Mike Sullivan (38:31):

Companies. Oh, that's true. Yeah, because the insurance will cover it.

CaSh Wong (38:34):

Exactly. Even if we compare the number of cyber attacks in North America, well North America, excluding Mexico, their numbers are harder to find on a per capita basis. We face more cyber attacks than our US counterparts. And for that very reason, we're better insured,

Mike Sullivan (38:52):

Better insured. They know they'll get paid. Never thought of it that way. But yeah, that makes a heck of a lot of sense. Unfortunately, it really does. So where do you think all of this is taking us? I mean, we talked about roughly 10 years ago when the Prince of Nigeria and those annoying emails became a bit of the joke that around the water cooler. And today it's very sophisticated. And where is this taking us? Where are we going with this?

CaSh Wong (39:24):

I mean, the attacks are going to continue to get more and more sophisticated if cybersecurity isn't top of mind. And if you're not setting aside budget by which to invest in it, staying in business is going to be very tough. It's just a fact of life. You have insurance companies that are actively shedding policies from their books because of how much they've paid out over the last few years. And then of course, you have the flip side. If you are a large organization that's even looking for funding, a lot of the large banks now require you to have cyber insurance before they'll fund you because it's a risk, right? Because it's just another calculus in their risk calculation. So we're sort of caught in this rock and a hard place where we have to put all of these systems in place, but at the end of the day, everything else, we still want insurance in case something happens. But the insurance companies are making much harder and setting the bar higher and higher every single year.

Mike Sullivan (40:28):

Do the insurance companies in Canada realize that they're kind of part of the problem and that they exist and the insurance policies are so good that they're going to be guaranteeing payout?

CaSh Wong (40:41):

Well, and I think that's one of the reasons why they're making it harder to get the insurance itself. They realize there's still a market. They realize there's still money to be made, but they can't just hand it out like candy anymore. Right? Now, they have to scrutinize.

Mike Sullivan (40:55):

Well, the legislation that is being crafted and in committee right now, is it contemplating this insurance piece?

CaSh Wong (41:04):

It is not. What they're focusing on is the tactical and the governance pieces that organizations have to put into place so that they can be better protected. And again, part of that reason was because there was this split of between it and the operational side, or we call that ot, where companies were really putting in two separate systems and one was not adequate enough to protect the critical systems. So legislation is going to mandate that they bring those two together.

Mike Sullivan (41:39):

When we started our discussion here in the top of the episode, you had said that things have gotten dark. It's not no longer just that annoying email. Things have gotten. And you're right. Holy crap, as we talk about this, I just feel this like the world could be caving out us here. It is dark. I guess with the question I have is with this legislation, is there some light that we see? Is this going to be this horrible demon of a beast that we're going to have to just live with?

CaSh Wong (42:16):

It is going to have to be one of the things, those things that we're going to have to live with. Now, that being said, all of the large organizations that provide a lot of our software are hardware now have it top of mind. So there's a lot more focus on making sure that the quality of the product that they're putting out is a lot more secure. You see that from Microsoft's perspective, Microsoft is from a security spend perspective, one of the largest companies in the world in terms of what they spend on security. But even then recently, they were slapped on the hand in terms of some that in certain instances, they still weren't providing or they still weren't following some of the best security practices. So Microsoft has now added into all of their KPIs for all of their executives and leadership group that security is a piece of their key performance indicators.

(43:13):

They have to make sure that it's top of mind on everything that they do. And then we're starting to see that from on the industrial control side as an example, Rockwell, Honeywell, all of these manufacturers now realize how vulnerable all of the equipment that they put in the field is. And so I think Rockwell just put up some guidance, like if you're running these models or families of some of our controllers, that you should make sure that they're not exposed to the internet and because they have some of those critical vulnerabilities in it. So now you're seeing a lot of the controls companies, again, are taking this a lot more seriously now. And so the good part is that now it's an industry. You've got some of the big players like the 40 Nets and the Palo Altos and all of these guys, big security companies who create firewalls and all of these devices and software to do all these protections. Now they have a focus on the operational technology side. So this way, there are solutions out there to properly protect all of these critical infrastructure while at the same time not disrupting the key business that produces, they're the golden goose of most organizations. So

Mike Sullivan (44:36):

It sounds like obviously we're in a better place and we're moving to a better place than we are now. The legislation will be in place at some point, maybe this time next year and before the next election, let's hope. But this is a nonpartisan thing. So I mean, all parties want this. It's not going to get bogged down, I doubt anyway. And those industries that provide us with a software, we so desperately need to manage our businesses, they're pulling up their socks too. So that's a good thing. So maybe we're in a better place, but at the same time, this is a bit of a reciprocating issue. The higher one goes, the higher the other goes, and Sophist occasion just continues to build. The part that I found somewhat fascinating in a spooky kind of way is the AI influence that is, I never even thought of that. And I'm sure if somebody

wanted to go online and Google what's the best software, I can pull off the web to start attacking, they could probably do that too, which is

CaSh Wong (45:37):

Oh, absolutely.

Mike Sullivan (45:38):

People like you and I, well, I don't think like that, but you're paid to think that way. But I mean, I don't think that way, but people out there do. And if they have nefarious desires, I guess they can. Fascinating stuff. CaSh. You've given some presentations at, I know at some of our events, and I know you've given some on your own as well, obviously in your line of business, this is a topic that's not going away, and I'm sure we'll have opportunities to discuss this further. Hopefully that legislation has been passed, we're better protected. This is no longer the risk it was, but I have a feeling it's always going to be there.

CaSh Wong (46:18):

It is, it is. And hopefully legislating. For us, it's all about organizations taking it seriously, because one of the things we always want to do is look after our customers, make sure that they stay in business because without them being in business, I think we've got so many great customers that I would hate to see any of them lose their business because they didn't have the right protections in place by which to sort of fight off all of these bad guys. And like I said, $8 trillion. And I think the estimate for 2025 is 10 and a half. They're financially motivated, right? They're financially motivated to come after you. Oh my God.

Mike Sullivan (46:55):

Yeah. And just where that eight to $10 trillion is being funneled, that's what scares me the most. That really does. I mean, that has got some very, very dark, as you said earlier, very dark connotations around this cash. Thanks so much for joining me today. I sincerely appreciate it. Fascinating discussion. You guys. Shing Digital does a great job for Utility Safety partners. We have been doing the business for a couple of decades. Very much. I since really appreciate everything you do to keep us and our members and our users secure us. Sincerely appreciate it. Thank you.

CaSh Wong (47:31):

Awesome. Thank you for having me, and this was great.

Mike Sullivan (47:35):

I want to thank our producers stories and strategies, and I hope you choose to follow this podcast on any directory you're listening on. Please do leave a reading. We appreciate it. You can follow us on Twitter or now X at Utility Safety. We're also on Instagram and Facebook, and you'll find these episodes on LinkedIn as well. If you'd like to send us note, maybe you have an episode idea, you can email us at info@utilitysafety.ca and put podcast in the subject header. And here's something new. Maybe you'd like to sponsor the Safety moment. If you want to do that, you can reach us by email as well. I'm Mike Sullivan, president of Utility Safety Partners. Click to know what's above and below. One click costs you nothing and not clicking. Well, that could cost you everything.