Transcript Episode 16 Craig Zawada

Ron Kruzeniski:

Today, I have the pleasure of talking to Craig Zawada. Craig is a practicing lawyer in the city of Saskatoon. He's a past president of the Law Society of Saskatchewan. Currently, he does a video cast called Bite Size CPD that is available on the Law Society website, and checking yesterday, he had done 79 different editions. So Craig, welcome, and first of all, please tell us a bit about yourself, all the things that I missed out that I should have mentioned.

Craig Zawada:

Thanks, Ron. Great to be with you. Yeah, I'm a lawyer. I've been a lawyer for over 35 years, mostly in Saskatchewan. And also, my undergrad was computer science so I have a way too unhealthy relationship with computers and tech. It's continued to be a hobby and interest of mine. Also did work both in terms of administering our own networks at various law firms and advising clients on problems after breaches, so I've started to have this passion for security of data and protecting it, especially in the legal realm.

Ron Kruzeniski:

I am particularly interested in the issue of security of data and that's why I called you to see if you do this podcast. Before we get into specifics, are there any basic principles which we should keep in mind as we look at the whole issue of data security?

Craig Zawada:

Yeah, there's a few that I think inform what you do later on. I think the first one is it's not a question of will you be hacked, but when. A lot of people criticize me and say, "Well, that's a bit pessimistic, isn't it?"

But if you adopt the mindset that you will be hacked, first off, if you aren't, then all the better, but you'll prepare much better and you'll follow good practices throughout.

Second is what I call the, I call it the mediaeval castle theory. When you look at what castles were like 500 years ago, kings and queens were trying to protect their people and their property. Their defenses had to be perfect. They had to have everything in place to stop the invaders, but the hordes only had to find one flaw. That's the same thing with IT security is that you can have 99.9% perfect security, but if you've forgotten or missed one thing, it's as if you had nothing there. So you always have to keep that in mind, and some would say that's unfair, but that's the way it is.

Then the final principle that often comes into play is the dichotomy between security and convenience, and you can't have all of one without giving up all of the other. Let's say I want to have some materials that are completely impervious to attack. Well, I could lock them in a safe and wrap chains around that and drop it at the bottom of the ocean. That would be pretty secure. Nobody would be able to get at that, but it's not very convenient.

We see this all the time with people that fail to put pins or passwords on their phones. They don't like the extra three seconds it takes to enter in their pin on their phone, so they just don't have one and they just swipe to get in. Well, that's super convenient, of course, but not very secure. So the whole trick in security planning is to get an appropriate level of security for the level of convenience that you want to obtain, and it's not going to be the same for all information. Certain sensitive information needs higher security, whereas you might be able to get away with more convenience on something that's less important.

Ron Kruzeniski:

You give a lot of your advice to lawyers and law firms like Bite Size CPD. My audience is different, it's more a privacy, data protection, data security, but do you think the advice you give to law firms really applies to just about any organization that holds a lot of sensitive data?

Craig Zawada:

Absolutely. Yes, lawyers have special considerations and special rules and special expectations around the information that they contain because they are information managers, but we all are information managers. Now, business, individuals, doesn't matter. There are few organizations or businesses that can afford to ignore these principles, particularly if you're holding a lot of personal data. Retail organizations for example, have all kinds of customer data that has been entrusted to them. It's just a matter of fact now that all of our information is basically in a form that can be attacked from anywhere in the world, whereas it used to be the case that people have to literally break into your building and be on premises. Now, it's a completely different world, but it applies just as much to butchers and bakers and everybody else as lawyers.

Ron Kruzeniski:

So, you and I know, and I would say most clients expect that when dealing with their lawyer, that information will be kept confidential. And that means to me that if I'm consulting a client, I shouldn't go to the coffee shop and talk about the client's affairs. But do you think that confidential obligation extends to protecting information, protecting data, keeping it secure? These are different words, but in your mind, does it all add up to the same thing?

Craig Zawada:

Yeah, I think they are just different ways of talking about the same thing. Let's consider when everything was on paper in law firms say 50 years ago or even less long ago in many cases, but we couldn't validly claim as lawyers that we could just carelessly toss these papers around or leave them visible on a coffee shop table or on desks where clients could see them or anything like that. That was definitely within our confidentiality obligations, and I don't think any lawyer would argue with that. The medium is different now, of course, but it's beyond obvious that lawyers and anyone storing private information has a duty to keep it as safe as reasonably possible, particularly electronic data where it can be attacked from just about anywhere.

Ron Kruzeniski:

Last week I attended a session where a presenter listed off 29 different steps that one can take to protect security. I thought just for the length of this podcast, I would say, what do you think are the five most important things a lawyer could do, or any organization could do to keep its information secure?

Craig Zawada:

Yeah, it wouldn't be hard to come up with 29, but you're right, I will keep it to five. First is passwords. Passwords are a pain. We hate passwords, they're a pain to manage, but they are a major form of protection and probably the major form that we have. You need to treat them like you would a key to your most valuable property because literally what it is when you're looking at things like online banking. There's a whole bunch of hygiene tips that you need to have around passwords, but number one, never reuse a password. We all have these favourite passwords and we think, oh, it's something I came up with, it'll never be guessed, so I may as well use it everywhere. Well, just remember that when

organizations are hacked, and they do get hacked, the first thing that the hackers will do with the credentials that they get will take that user ID and password and try it at all at the other big sites like the Googles, like the banks, like Microsoft, and if you've reused your password, then they've instantly got in there, so you cannot reuse passwords.

Other thing is we all hear the jokes about using the word password or your dog's name or your birthdate as a password, and we should know better than that. The best passwords are long strings of random characters, at least 12 characters, probably 16 or more is better. And of course, you can't remember all of those different passwords, so you need to have a password manager, which is just a database that encrypts all your passwords and keeps them safe. So passwords generally is the first thing that you need to do to keep your information secure.

Number two, which is related to the first, is to use multifactor authentication or two-factor authentication whenever you can. Two-factor authentication, you've probably seen it or used it where you enter a password and then immediately something will be texted to your phone or you might get an email with a six digit code that you enter in, so it's basically a second password. Sometimes you'll have an app on your phone, an authenticator app, which will generate these constantly changing codes. Two-factor authentication is incredibly powerful in terms of protecting your information because if somebody does happen to guess or get your password, they still need to have your phone or access to your email or whatever your second factor is in order to get through. All of the big sites, Google, Microsoft, Twitter, Facebook, they all offer 2FA in some fashion. And if you haven't already set it up, do so, especially for valuable information like banking information.

Thing that I would say in that list would be take a long hard look at the information you store and this goes back. If your assumption is that you will be hacked, you want the criminals to have access to as little as possible. And for lawyers, that's tough because we tend to have a bit of a hoarding mentality. We're information managers, so more information must be better, but if you don't need information, delete it, or give it back to the client, or just don't hold it because having that information in your systems is a huge amount of risk for you and your clients and everybody else that it relates to.

Yeah, it's convenient to store a credit card number for then you can charge your client the next month, but it's a huge risk, and that's the kind of information that hackers are looking for. So if it's far better to just call the client every month than say, "Can I have your credit card number again?"

They might be annoyed until you explain to them why you're doing it, but they'll understand that you're only doing it to protect their information. The compartmentalization and deletion of information that you don't need is something that is just key to privacy.

Fourth thing is backups, and again, this comes from a hacking is inevitable mindset. You must, must, must have backups of information. Suitably protected and locked down of course, because if you are hacked, say a ransomware attack comes in, locks on all your computers, you want to be able to go and find that information in a non-compromised way hopefully so that you can continue on with business. One model that I recommend often is a 3, 2, 1 model, which means that you should have at least three copies of information, two of which are in different formats, so maybe one on your hard drive, one in the cloud or something like that, and one of them offsite. That's really important because we often have backup systems that are sitting by our servers and we're backing up.

But if there's a fair flood there, that's not going to help. In fact, the director, Francis Ford Coppola, he had a burglar break into his place, I think it is in Brazil or something several years back. He had all of his scripts from The Godfather and Apocalypse Now and everything like that on his computer. He was backing them up to an external hard drive, but that external hard drive was sitting beside his computer and the burglars took that too, so it has to be offsite. The cloud is a great solution with appropriate

encryption and protection that way, but at least then it's impervious to floods and other natural disasters that you'll have at your business.

And then the final point that I would mention to keep your information secure is education. Keep yourself up to date and keep your staff up to date on what is happening. A lot of them will have seen the standard phishing and Nigerian prince things, but you have to impress upon them constantly and remind yourself constantly of the risk and do lots of training. Sometimes organizations will do penetration testing.

An organization I belong to will send out periodic fake phishing emails. They look legitimate like they're from Amazon or something like that, but if you happen to click on the link, it goes back to the penetration tester and then they send you a message saying, "Ah, no, you shouldn't have done that. Here's why."

So it's a bit of education that goes into it, and if you report it properly, then you get a bit of a reward sometimes. But overall, making sure that everybody is up-to-date on this kind of stuff because it's always evolving is really important.

Ron Kruzeniski:

For the sake of time in drafting these questions, I started with five, but is there anything on your list that just almost made the top five, but you think are pretty important that law firms or any organization with data ought to also do?

Craig Zawada:

I think one and maybe could probably go into the top five is make sure you have a breach incident plan prepared. Some legislation like PIPEDA, the federal Personal Information Protection Electronic Documents Act, and the new replacement for that, which will likely come this year, the Canada Privacy Protection Act, they both require notifications of a breach, both to the Privacy Commissioner and to affected individuals. But your incident plan should include that, but more, there's lots more to be done. How are you going to keep operations going? Who else do you have to report to? Who is the point person that's going to be managing all of this? Remember that when there's a breach, there's going to be a level of panic, and you want something that you can just refer to and go down a checklist so that the emotion gets out of the way of following best practices. So breach incident plan is absolutely mandatory I think for any business law firms included.

Another thing is constantly staying up to date on your malware protection and good practices. We're all pretty aware that we should have antivirus and similar stuff and most operating systems like Windows have it built in now, but remember that the criminals are only getting better. Everything that has happened in the past, they've figured out why it didn't work, and so they add onto that and so you can never be static on this kind of thing. Some businesses consider insurance, and there is cyber insurance available, although it's getting more expensive with the prevalence of these attacks. I would recommend having insurance. Some lawyers do have a bit of insurance through the SLIA insurance that we have in Saskatchewan, but it's definitely not a first line defense. Insurance isn't going to get back a whole bunch of things that you lost, and so insurance is part of the plan, but you want to do it.

And the final thing on all of this advising is, I don't know if it's advice or not, but some things are outside your control. You can do everything perfectly, but you are going to be involved in some kind of scam. We had an example where hackers literally copied our entire firm website and just changed the URL slightly because they couldn't get our URL and changed the phone numbers and email addresses in that to point to them. But everything else was identical, lawyer pictures, everything else like that. And then they started faxing people.

I only learned about it because I started getting these emails from people all over North America saying, "Got this fax from you," and it was along the lines of a Nigerian prince, I'm holding 80 million in an estate for you.

And then that fax pointed it to this fake website and people would go on there and it looks legitimate. But lots of them contacted me to say, "This doesn't sound right."

And I'd tell them, "Yeah, it's not right." It was nothing I could really do other than just tell them not to go to the site, but you wonder how many people did go there and whether anybody was trapped by it. As much as you can protect yourself and do the things right, there's just crime around and you're going to have to deal with that.

Ron Kruzeniski:

So, as you and I know, some lawyers practice all alone and some lawyers get together in groups of four or eight, and some are involved in larger firms. The sole practitioner certainly might say some of the things that the experts recommend we do are just too expensive. So what advice do you have for the sole practitioner?

Craig Zawada:

First off, I'd say it's not that expensive, especially if you're building good practices from the start. There's very little extra cost to the things I've mentioned already, like backups. Okay, get a NAS for a few hundred dollars and you can be backing things up, or use the cloud for a couple dollars a month and literally back up there. So that's not expensive. Good passwords don't cost you anything. Education, that stuff is available online for free. It's just a matter of going around and looking for it. So you can get people selling you all kinds of fancy firewalls and things like that, but most basic routers provide enough firewall protection as long as they're configured properly. So it's not expensive to start with, but more importantly, there's no comparison between the cost of protection and the cost of an incident.

Businesses literally go broke from this stuff. The best case scenario if you are hacked is lost business, perhaps lost clients, loss of reputation, but that's the best case. And you don't want to be worrying and laying awake at night if you can carry on or waiting for the lawsuits or the class actions that apply or that appear. Really, the cost of this, it's like a lot of things that we don't see a big benefit from right away like insurance, but we realize that we've got to have insurance.

The other thing too is that you don't have to spend zillions of dollars, and I refer to what the poppy principle, that is, the highest poppies always get cut off. What that means in this context is that hackers got lots of targets and they're going to look for the easiest ones. If they start seeing that you've got various protections or hard ways of breaking in or things that are slowing them down, they'll move on to an easier target and that's really what you want to do. I'm not wishing bad on those who are the easier targets, but the fact is, if I can just make it a little bit harder to get into my systems, chances are they'll move on and the cost of that is really very little.

Ron Kruzeniski:

As a result of, I'm going to say COVID but obviously advancing technology, and I do believe COVID sped it up, lawyers can work from home, in the office, in the airport, in the taxi, wherever. Do you have any advice for them in terms of additional security protections?

Craig Zawada:

Yeah, a couple of things, I guess. One is to be mobile aware. By definition, mobile devices are small and easily lost or easily pilfered, so that means that you need to have good passwords and security. If you don't have your PIN or password or even just fingerprint or facial recognition to protect your device, you got to do that right now because it just takes one little slip or you leave it in a taxi somewhere and then people can be browsing through all of your information and taking advantage of all your accounts and stuff like that. So have that security.

Also, guard your devices. Don't even get up to go to the counter at the coffee shop by leaving your laptop there because you just don't know what people could do in just a few seconds. Speaking of coffee shops and mobile, we all like to use Wi-Fi and public Wi-Fi whenever we can in coffee shops or hotels. Never, ever connect to those onto a site without using a virtual private network or a VPN. VPNs, we could have a whole podcast on that. But essentially what a VPN does is creates this secure tunnel between you and your destination that nobody can see the data that's in there. The Wi-Fi at coffee shops and hotels is completely out in the open. If you're not using a VPN, gosh, there's no way you should be visiting your bank or any other valuable site because there's a chance that criminals could be sniffing the traffic going and seeing passwords and other ways of getting in. So always use the VPN if you're working remotely, especially on Wi-Fi.

You mentioned the COVID lockdown. Mobile is a vector for criminals to take advantage of some things that happened from that. If I was back pre-lockdown, if I got this weird email from my business partner, I would just yell down the hallway, "Hey, Sue, did you just send me this email?"

And she would say, "No," and we'd be okay. But when Sue is working at home and I'm working at home and we can't really just talk to each other, we don't have that extra bandwidth for communication. You have to be more careful when you're dealing remotely or at least can't check these kinds of things because that's what the criminals prey upon is this asymmetry of information that they have or you don't have. And if you don't set up your things properly with lots of protections and vigilance, you can run into problems.

Ron Kruzeniski:

Well, Craig, I’m gonna say thank you very much. Many of the things that you have talked about I completely agree with, and they're good advice to law firms, they're good advice to basically any organization. As more and more data are sitting on our servers wherever they are, we just need to be conscious of all the things you've mentioned. Thanks for taking this time out of your busy practice, and I'll be looking for version 80 of your next video cast, so thanks again.

Craig Zawada:

Pleasure, Ron. Great to be with you.