EPISODE 1353

[INTRODUCTION]

[00:00:01] KP: Phishing attacks, malware and ransomware are just some of the major threats everyone connected to the Internet faces. For companies, the stakes are especially high. Setting up secure infrastructure is difficult. Your adversary only needs to find one flaw to get in.

Vancord is a private cyber security company based in Connecticut that was founded and built by security engineers to specialize in incident, resilience and response. In this episode, I interviewed Jason Pufahl and Russell Jancewicz from Vancord.

[INTERVIEW]

[00:00:38] KP: Jason and Russell, welcome to Software Engineering Daily.

[00:00:41] JP: Thanks, Kyle. It's nice to be here.

[00:00:43] KP: Tell me a little bit about your guys work and how you know each other.

[00:00:47] JP: So Vancord is an information security consulting company. Russ and I actually worked together for the past three years here both founders of the company. We also work together for – Oh, I don't know, Russ. I feel like we always make it up ten years at least maybe more?

[00:01:07] RJ: Yeah, about ten years.

[00:01:09] JP: So yeah, we're at the University of Connecticut before that. So kind of always in that security space and peers for a long time.

[00:01:15] KP: And what's Vancord's mission?

[00:01:19] JP: Our focus really is sort of traditional cyber security or information security consulting services really focused on the midmarket. Companies that probably have IT staff likely aren't large enough to really look and hire, say, an information security officer or maybe even a security team. We're a nice fit for sort of augmenting the security responsibilities for companies that just don't have them, right? So vulnerability assessments, pen testing, information security, sort of virtual information security office type services, and then kind of a variety of things around that.

[00:01:55] KP: Well, the modern, I guess, model for a lot of companies to get going is to begin in the startup phase. Maybe you're in a garage and that sort of thing. Probably not a lot of budget and time invested in security. If you're successful though, you need to start taking those things seriously. What's a typical maturity cycle for security look like in a company?

[00:02:18] JP: It's really interesting. It doesn't matter if the company is small or a global company. A lot of times we see some of the same gaps around. So we really talk about the idea of security fundamentals and making sure you're doing some of what we'll call sort of basic blocking and tackling, right? Making sure you've got patches installed, basic vulnerability management. Some security awareness training for employees. Maybe a focus on remote access and some of the restrictions and sort of qualities around securing remote access.

But really, if people deal with those sort of fundamental things, you then start to look at building a more mature program. And maybe that's aligning to a security standard. We're starting to see a lot more now of companies looking to adhere to say NIST 800-171, maybe the cyber security framework, certainly things that move them in a more sort of programmatic direction.

[00:03:13] KP: If an organization decides to adopt some standard or best practices meet some compliance restrictions, is simply being compliant with best practices enough?

[00:03:26] JP: It's interesting. We certainly spoke with clients who feel that they're building a security program solely to meet compliance requirements. In my opinion, that's probably

not the best way to approach it. The reality is a lot of the times that we see that, it's, “Can you do an application pen test for us?” And it's literally a compliance check box, right? So they may not even care that much about the results. And I think what I like to see are organizations that are making good decisions that actually reduce risk in a meaningful way and not just in a way that checks that compliance checkbox, right? Compliance and regulatory requirements, they have a place. And I understand why they exist. And I think, clearly, have to adhere to them. But ultimately, doing things with the spirit of actually reducing risk is what you want to do.

[00:04:16] KP: What's the landscape of threats organizations need to worry about today?

[00:04:21] RJ: Yeah. There's a wide swath of threats, but I think most commonly you're going to see the ransomware crop-up very often nowadays, because it's lucrative. And a lot of those best practices that Jason mentioned just aren't followed and allow for that to happen. But there’re also other attacks that are occurring pretty commonly. You'll see a lot of phishing to get internal access. You'll see corporate espionage. You'll see theft of information. But commonly, it's getting into that environment from some initial vector. And then we're seeing ransomware be the most prevalent thing that's really out there.

[00:05:05] JP: It’s interesting. Yeah, I mean, how often do we refer to ransomware as like the security epidemic, right? Because all the incident response work that we do, what is it? It’d be eight or nine out of every 10 is probably ransomware-based at this point.

[00:05:20] RJ: It's if not ransomware-based, it's definitely on the verge to becoming ransomware. We’re either saying first stage deployed or we're seeing someone preparing to infiltrate a network to perform ransomware.

[00:05:33] JP: Kyle, one of the things you talk about, that maturity landscape. One of the things I hear all the time are people saying, “Well, I don't have data, or my company doesn't have data that any attacker or any cyber actor cares about.” And I think that's such a misconception that they're only looking to take data that might have sort of other value, like personally identifiable information, for example.

The reality is they're looking to disrupt an organization and ultimately either you'll get that ransom paid. Or as a second stage, sort of threaten the release of data and extort money from you. So every company I think is at risk to this. This is why I think it's such a serious threat. And there really are some sort of key things that organizations can do to help protect themselves against it.

[00:06:19] RJ: More to the point though. Even if the attacker doesn't see the value in the information, if you, the holder of that information, considers it valuable, that inherently makes it valuable to an attacker. Because as soon as you don't have access to it, it now becomes a problem.

[00:06:37] KP: If I had a proper security setup, could I really guarantee that I'm safe from ransomware?

[00:06:43] JP: So you'll never guarantee, right? I mean, that's the challenge of being on the defensive, is you've got these organized entities that are sort of executing or orchestrating these pretty well constructed attacks. And you're trying to some degree position yourself to prevent the known while they're in the position of being able to update and find the unknown.

But the reality is there's things you can do to at least make sure that you can make yourself less of a target, patching systems routinely. Especially when vendors release patches, you want to be early on that. Certainly, you want to make sure you've got good data backups. And I think that really helps in the recovery phase, right? If there was actually a successful attack, you're much less likely to have to pay any kind of ransom if you've got good backups and quality data to recover from.

[00:07:38] RJ: Yeah. And I think the threat actor itself is really the determining factor. So you're not going to stop a nation state. They're going to get in at some point and their means of doing so, they'll find a way. If you are looking to not get hit with ransomware from some attack, make yourself less desirable than the person next to you. And that's probably going to be a big step in avoiding that. Because a lot of time we see basic access as the

first point into a network, and then they'll move through when they'll continue the exploitation.

[00:08:12] KP: So obviously, preventative is the best way if you can get it. What are your thoughts on strategic posturing around, “Okay, we think we've been compromised. What do we do now?”

[00:08:22] JP: Well, you certainly proactively, if you can, right? If you can have an incident response plan to some degree in place, that's always a great first step. And candidly, most folks that we work with probably don't have a plan like that written out. You definitely want a security partner to help you sort of navigate that initial containment and then ultimately through to recovery.

Though in my opinion, one of the worst things that an impacted entity can do is identify that they've got an issue and then sprint to the restoration phase, maybe restoring data or trying to bring systems back online, because the reality is you run the risk of destroying really quality data that'll give you clarity on what the attack was. And maybe even more importantly, what data may have been impacted and which will make it much more challenging to meet your regulatory requirements, right? Notification requirements and things like that.

So it's really important to have a good quality partner, somebody who can help you walk through that incident response. So you don't make any of those sort of critical missteps. And frankly don't land yourself in a position a week or a month from then where you're re-infected and dealing with the same thing again.

[00:09:37] KP: What are some of the common gaps you're seeing that allow people to get in?

[00:09:43] JP: So remote access certainly is always a concern for us. We saw a large exodus from sort of on-prem to home or remote workers through this pandemic, a lot of organizations weren't fully prepared for that and I don't think it had adequate remote access protections in place. So certainly things like port 3389 for remote desktop being open.

That's a really common attack vector that we see. Exploiting users' credentials and accessing a VPN is certainly common. Russ, maybe you want to touch on just the idea of account theft as being one of those critical areas.

[00:10:21] RJ: Yeah. So we see quite a bit of that, so dark web circulating credentials. So you'll have one credential used multiple places. So any sort of reuse, you'll see people using this to get into organizations. The remote access is a big part of it, for sure, through the VPN and through IDP. But we also see phishing, any step to get that initial foot in the door.

Lately, we saw a lot of proxy log on. So a recent attack against Microsoft's exchange on premises, it allowed full access to that server and then a lot of lateral movement occurred there. So we've seen those attacks. I would say anything that is a recent security patch is probably being used right now to gain that initial foothold if it's externally-facing. And it kind of goes back to that thing that you said about fundamentals of patching. If you're patching, you're taking care of a lot of these things. And really that stops that initial vector.

[00:11:21] JP: Yeah, in that same vein, and I don't want to over-generalize. But yeah, I think we have to be mindful of the fact that these are – All these attack activity, it's generally financially motivated. And so ROI is really important for these folks. If they can compromise a company that has poor patch practices, that's an easy target, that's going to be more attractive than somebody who has sort of even the majority of those fundamentals in place. It just makes a little bit more difficult. And they're going to take that easiest path whenever it's practical because it yields the most money in most cases.

[00:11:57] KP: Well, the pandemic has definitely pushed us towards more remote work, a lot more VPN logins and things like that as you'd mentioned. No matter what happens in the future, it's fairly safe to say that we've had a shift towards remote. Maybe we'll shift back a little bit, but it's going to be more prevalent going forward. Have organizations adopted to that yet? Or is the threat greater because this is an opportunity for new styles of work and the attackers could be ahead of the defenders?

[00:12:24] RJ: So the attackers have been ahead for the whole pandemic. The uptick in phishing emails and trusted attacks and attacks into environments, it has been a massive boon for the attackers throughout the pandemic. We started to see some reactionary efforts to protect against these threats that exist. But I would say that we need to do better as a community protecting against remote access attacks and the remote worker, especially when you to have bring your own devices. And now you're bringing your own device, you're connecting it to a remote network, through a VPN. You don't know if your kid is playing on that laptop and maybe they download something that gives access. So there's a lot of stuff with that side of having a device at home. And then just logging into your corporate network, you might have a perfectly secure system. But if your credentials get reused or they're leaked through the dark web in some way, an attacker can get in. To that end, I would obviously recommend compensating controls like multi-factor be applied to some sort of remote access prevent those basic attacks from occurring.

[00:13:38] JP: And companies really need to recognize that many employees may return, but the reality is, to Kyle's point, we're not going to shift fully back, right? And so we need to start building the security models around understanding that a large portion of employers are going to be remote. Getting visibility into those users workstations, understand what your data flows are, generally positioning yourself to protect workstations that aren't going to be sort of in the four walls of whatever corporate headquarters might be, right?

And I think a lot of folks just didn't recognize that. We talked to people who had systems configured to collect patches from on-prem servers when none of their hosts ever came back to the office. And so you had organizations that probably had decent security practices in place that just sort of fell apart once their workforce went remote. And you really need to think through how you're protecting the data, how you're protecting your sort of mobile or your remote workforce really in a different format. And a lot of companies just have not done that.

[00:14:49] KP: Well, I'm wondering if we can put ourselves in the shoes of a software engineer, someone who's technically proficient. Probably has the best intentions of pushing features out there. Maybe some goals of getting their code to be beautiful and stuff like

that. They're not against security, but they're not a security professional. What types of mistakes does a person like that tend to make that might be avoidable?

[00:15:15] RJ: So there's a lot to unpack there. So I would say the basic vulnerabilities that we've seen for the past 20 years are still appearing in code today, and kind of SQL injection, your cross-site scripting, cross-site request forgeries, a lot of web attacks predominantly, because that's externally facing from an environment. You're going to see that. But any hosted service, memory corruption. And, honestly, there's the same attacks repeated over and over and over. And I think it's because we've not kind of focused on security from a software development standpoint. And I really do think security needs to be more forefront in developers' minds.

And you're starting to see a turn toward this even at the programming language level. So we're seeing Rust and Go have compiler level and support for memory safety for type safety, thread safety. And these things are preventing some of the attacks that we've seen historically. But it doesn't stop everything. We're still having those low-hanging SQL injection attacks all across the net. And I've seen recent code myself when I was doing reviews where a naive developer has best intentions. They want to accept a file and process it. And they pass it off to a system shell without handling the input for standardization. So now I have direct access to that machine can run anything as the account that I'm working on.

So in terms of developers, it's the same problems. And you'll even see this in the GitHub's AI system that they just released, the Copilot. If you go through some of the examples, it generates code with these errors in them and with the same problems. So bringing in an understanding and a knowledge of these problems I think really comes back to like software development and computer science education. It needs to really kind of be a forefront of a developer's mind even if other developers, the people who are smarter than myself designing these languages are trying to put the safety mechanisms in place, they're not going to be able to stop everything.

[00:17:41] JP: So Russ, we sometimes get folks saying, "Well, I don't want to implement security controls because it slows things down." However you want to interpret that

statement. Or the security is an impediment to sort of the business practices that we put into place. Is there any reasonable argument to be made that in software or application development you're implementing security controls or doing input validation and things like that substantively slows the process? Or is that something you just debunk?

[00:18:17] RJ: So there are cases depending on your data sets where things will be slowed down, for sure. But I would say it's probably less often and less severe than most people would assume. It's one of those don't optimize before the problem is solved. So there is a case for it, but I would say solve the problem. Try to do it the best way possible, review it. And if you need to take some optimization, then apply it.

For example, I had a colleague who at one point did not want to enable full disk encryption because they claimed it would slow down their computer until I showed them that the speed of the code processor doing the decryption was faster than their disks read-write access and they're like, “Oh, okay, I understand now.”

So there's definitely places where you might have to deal with that as a contention, but I would say, generally, that's not the case. You should probably try to be doing the correct validation when you need to be doing that validation.

[00:19:19] KP: Where do you think the impetus should come from for that in an organization? Is this top-down that you need executives really trumpeting the security first principles? Or should you hire and take a bottoms-up approach?

[00:19:35] RJ: So I think our kind of internal philosophy is security is everyone's responsibility. And I think from a development standpoint that remains the same. So your executives and your high-ups, they should probably care about security. But the reason that they care is most likely the bottom line that they're trying to optimize, your developers should care about security because the cost and time that they're going to spend addressing issues is going to be painful for them.

Across the board though, I’d say you probably – If you're going through an iterative development process and you're releasing some software, you have your core development

team who is focused primarily on the application logic and any code that you're dealing with, then you'd probably have a separate security team if you're really having a robust review process. And at that code review you have someone who is specifically looking for these security issues. They might not necessarily fix them. They might pass them back to the original developers and kind of inform them about what's going on. But it's all the way through the chain of employees. Everyone kind of needs to have their hand in it at some point and be aware of what they're doing.

[00:20:53] JP: And I do think it's reasonable to expect that your senior leadership does create a culture that is security-focused, because I think if not, you're then going to have likely a culture that's prioritizing output over security, for example. And sure, maybe for some applications, it's fine just to bang something out quick. But in reality, you need to build things that are secure. You need to protect the data. I think that is seniors leadership, executive leadership intend – It should be their intention to promote security as a core component of what they do. Not as an impediment to other things, but certainly as a component.

[00:21:33] RJ: And I think that kind of Jason's statement about not being an impediment. Security, you can always do something else. You can always add another layer of security. You can always add something else in there. Security should probably be balanced against the threat that you're either expecting or observing out in the wild. You don't need to make Fort Knox for everything. Your personal blog with pictures of your pets or your kids, you don't need to have it necessarily even hosted on an SSL encrypted website. It could just be HTTP. There's a range of where I would apply different security controls, because ultimately the security should match what you're trying to defend.

[00:22:20] KP: When you're helping clients, how much of that work is proactive versus reactive?

[00:22:25] RJ: From my side, I wish it were more proactive. I'd say there's a decent split right now. What would you say, Jason, like 40/60?

[00:22:35] JP: Yeah, something like that. I mean, honestly, it might almost be half and half. But it's probably for different reasons. So I'd say we have a large group of clients that have, to your point earlier, Kyle, regulatory or compliance-driven initiatives that they're sort of working towards. And that really does help with the proactive approach.

We're also seeing some legislation now. So for example, in Connecticut, which is where we are, there's a recent bill that was passed that gave safe harbor against legal action for companies that had an incident or a breach but had adhered to a security standard. So there are some incentives that some states and some legislation puts in place to hopefully incentivize people to be more proactive. So it's not just purely compliance-driven. But certainly, we deal with a lot of incident response. And that's not to say that every company that we do incident response work for has totally ignored security. The reality is everybody is on the defensive. A motivated attacker is going to get access if they're persistent enough. But I will honestly say most of the time that we do incident response, it's because of some pretty basic things that were just overlooked or not attended to.

[00:24:01] KP: What are some of the biggest gaffes if there was a first step a company should double check they've secured? What do you see as the biggest wide open front door?

[00:24:11] JP: So certainly, we mentioned it multiple times. Basic patch management is one real significant problem that we see. And we see it all the time. There're maybe a couple of reasons for that. In some cases you definitely have applications that require your older operating systems that in the worst case might be end of life. Those are real challenges. Companies certainly can put compensating controls in, but that exists. Way more egregious are companies that simply have loose operational practices and don't routinely batch. And I think, at that point, you're really placing yourself at risk unnecessarily, because they're very addressable problems.

I think television always portrays these attacks as incredibly sophisticated and creative. When, in fact, they're kind of pedestrian and boring. And not to say passion cures all woes, but, boy, it's a step in the right direction. And we just don't see enough of that. I don't know, Russ, if you want to add anything to that.

[00:25:11] RJ: Yeah. So if you wanted to have low-hanging fruit to kind of protect the environment and shore things up, I would say review your firewalls, review your perimeter. If you're going to get in through fishing, then that's a personnel issue. And people aren't patchable. You can teach them, but you can't guarantee them. I would say go through, make sure if you have end of life systems. We see a lot of end of life windows servers hanging out in a DMZ and they get attacked. Just go through and do due diligence. See what ports are accessible to the Internet at large. See what services are running. If you have custom software sitting there that hasn't been touched in a few years, decide if it's actually necessary to be out there. If you're running Apache, Nginx, httpd, update. Make sure you're running the most up-to-date version, security patches. All of these kind of – The things we've harped on quite a bit, I would say, in this discussion, it's that patching. But for low-hanging fruit, it's that perimeter. It's make sure your external firewalls have the correct rules in place. Make sure your logging is turned on those devices. And I would say make sure your logging is turned on any device that you consider to be of importance. Because if you do get attacked, you're going to want those logs for both review and for assurance that things haven't been touched. But do your review of the firewall. Do your review of systems that are passed through that firewall. And just kind of sure-up that perimeter point. And then start working on your internals and your personnel.

[00:26:47] JP: The last thing that comes to mind for me is – And I think you're absolutely right in terms of employee education. But the reason I kind of want to bring that up a little bit is how many companies have we seen that have pretty quality technical controls in place that are subverted because somebody succumbed to a basic phishing email and then ultimately provided their credentials? And credential management is a weakness we see all the time. Either password policies that are just incredibly lax. So you have your very guessable policies or very guessable passwords, maybe no two-factor in place, or certainly not two-factor for critical applications. Managing and protecting credentials is really important.

And the other typical attack progression that we see is attacker gets access somehow, right? I'll be very general here. Is able to get even an unprivileged credential but then has access to be able to move around the network and ultimately elevate those privileges or

collect additional credentials ultimately giving them administrative access. And that really basic sort of flow is very consistent in a lot of these attacks. And being more mindful of password management practices would really improve the security for a lot of companies.

[00:28:12] KP: Great advice all around. I think adopting a lot of those as a policy would strengthen the security of an organization. They're all kind of defensive moves in that regard. I also might want to spend some of my time doing intrusion detection. Do you have any thoughts on a healthy balance of how I split my time?

[00:28:31] JP: I think my answer to that would be, for a lot of companies, just collecting the logs and you're reviewing them periodically would be a real step in the right direction. I'd say with incident response, in every single instance that we've done any, I think there might be one customer that we would say, "Hey, they had pretty quality data that we were able to review that gave us a historic perspective of what that attack looked like." In most cases, organizations aren't collecting logs and they're doing – On top of that, they're of course doing almost no review. And this being in the landscape of incredible success from the log sort of collection and review companies, right? There're a lot of companies out there that really specialize in this and I think there's interest in it. But even where they're deployed, we typically see huge gaps in the data or somebody hasn't assigned an individual who's responsible for reviewing that.

So it's certainly valuable to be able to go through and do that intrusion detecting type activity, but it needs to be staffed appropriately, and there needs to be an understanding that it's not the silver bullet. And walk before your run. So judiciously select what those logs are going to be. Understand what you're looking at so you're not constantly going down sort of rabbit holes after false positives. And sort of build it such that your analysts don't get alert fatigue, because we see that all the time as well, right? Companies, they sort of fall in two spectrums. They either don't do anything, or they buy this robust platform that overloads them with alerts and ultimately they don't pay attention to them, which is arguably almost the same thing as not doing anything. So you've got to find that sort of middle ground that makes sense for your organization, right? The same thing that Russ was talking about before, security commensurate with risk. Build it in a way that you can

actually manage it and get value from it rather than either doing nothing or building it in such a way that it just sort of makes itself almost obsolete through the noise it creates.

[00:30:42] KP: Well, let's imagine a mid-market company thinking about their security posture. Let's assume they've got some data, but not like HIPAA data. So there's nothing too compliant about it. But even if you're selling pizza, you owe it to your customers to be good stewards of their data. Let's assume they've got some IT staff, but no dedicated security professional. And they're starting to think should we add a head count for this or do we find a vendor? What are some of the key considerations in making that decision?

[00:31:15] JP: So I think certainly cost is going to be one. We've had a lot of success with what we call our virtual information security office offering. And we try to structure that a little bit differently. A lot of times that we'll see sort of that external partner being positioned as a security group or person. It's an individual assigned to a company. And with that, you sort of get whatever experience that person brings to bear, right?

So let's sort of be clear about it. If I were working for a client as their sort of external security person, if they had application security questions, frankly, I'm not really best equipped to answer that, right? That would really be best for Russ. So in our model, we sort of bring the experience of the entire team to bear to make sure that sort of any aspect of security can potentially be addressed.

So the nice thing about partnering with an organization is you do potentially get access to a lot of experience that you might not get from hiring an individual who's responsible for security, right? Because you're going to be limited to whatever their core competence might be.

I think a lot of mid-sized businesses can really benefit by having, in essence, external security council helping to guide those sort of internal operational practices. And I think that's been a nice that's been a nice middle ground that we've seen. Budget is of course a component of it. I do think in regulated environments having the designated CISO is really beneficial. But in most cases I would say companies really just need guidance. They need assistance with policy development. They need a sounding board as they're trying to make

institutional decisions. They need somebody with experience to be able to say, “These are the things I’ve seen work in the past. These are things I haven't seen work in the past. This is where your organization might fit with that.” So enterprise typically hires mid-market very often relies on an external partner, and I think it's finding one you trust is the most important part.

[00:33:17] KP: And when people are finding you, are they typically thinking about the future and planning? Or are you often brought in media res during an incident?

[00:33:27] JP: So there's no doubt that incident response has been a great way to find clients. And I don't mean to say that tongue-in-cheek in any way. Customer acquisition and building that trust, it takes time. During an incident, that time is reduced from potentially months to hours. And so if you're finding a partner reactively and you're lucky enough to get somebody who's got sort of good qualifications, you could potentially really short circus that initial process, right?

Looking for the right vendor, it's worth doing that proactively. It's worth interviewing a variety of companies. Fit makes a difference. Not every company has the same set of capabilities. Some might be very specific, in that they focus maybe on application security or network security. Some are going to be broader and sort of have a wide range of folks that they can bring to bear. I think you just need to figure out what are your priorities. What are you looking to address and trying to find a company that actually meets those needs?

[00:34:31] KP: Whenever I hear about a new zero day exploit, I find it kind of terrifying, because it implies that even if you've done all the patching and all of that, you're still exposed. I mean, that's intrinsically true. But how much of a threat is that really? Should I stay up at night worried about zero days?

[00:34:48] RJ: I mean, I do. But that's for totally different reasons. So, no. Ultimately, do your due diligence. If you expose something that has zero day, maybe you care a little bit more. But you'll see a lot of things like spectre and meltdown. Yeah, there were terrible attacks. There's a lot of hardware-based attacks. We don't really see them being used

because they're so specialized. Sure, they're out there, and I'm not saying that they're not things you need to ignore and you can just kind of toss aside.

Again, it goes back to that secure to the degree of what you're trying to protect. If you're the federal government, if you're a large entity and you have something super sensitive, maybe you need to be a little bit more concerned about that. But you probably have a security engineer who is up at night worrying about the zero days that are popping up. And every day I do see something pop-up in my feed and I say, "Oh no. I need to check whether Z, Y or Z customer has that." But ultimately, for day-to-day technical people, I would say do that due diligence and read about the zero days because they're interesting, especially to me. But I say, in general, towards the tech community, zero days can be informative about what people are researching currently and what kind of attacks are being used.

[00:36:21] JP: And I think it's also important, Russ, that companies look for threat intelligence information and read it regularly. So, ideally, you're never in a position where you have a zero day that impacts you. But the reality is you will. And what you don't want is for an issue like that to occur and not know about it for a month and then take another month to react to it, right? You really want to at least be current with the threat intelligence out there and then have the discussions to figure out what should your response be and what level of urgency do you need to address it. It is all about simply balancing, again, risk with the potential reality of getting attacked.

[00:37:04] RJ: Yeah, absolutely. And so if you are staying up at night, you don't have to. But you can you can certainly check your email in the morning.

[00:37:14] KP: Well, I'm not an expert in this, but when I think of a physical bank getting robbed, rarely do I think of a situation where the bank made a bunch of gaffes. It's usually some hardened criminals who came in with guns and really took advantage of a situation. On the digital side, when you hear about a major incident hitting the news, what's your response? Do you think, "Oh, that company was laxed in security? Or is this just the times and everyone's vulnerable?

[00:37:43] JP: Both.

[00:37:43] RJ: Yeah, I would echo that. I think there is a lot of organized cybercrime. There is a massive amount of nation state activity. But at the same time, there're a lot of opportunistic people who just happen to see something and they go in and grab it. It's all over the board.

[00:38:02] JP: And it's easy in the – I'll call it the physical space, right? So in the example you just used, I think of the Wild West, right? Somebody rides up and shoots their way in. But you can look at a building and you can say, "Well, we put a fence around that building to protect it. Hey, look over there, there's a hole in the fence." And it's really obvious. I think that the interrelationships of technology, it can be really challenging to build that mental picture of where are my vulnerabilities. Where are my gaps? And so it is easy to overlook when you have 500 servers many of which might be exposed to the Internet all potentially in varying states of sort of patch or support or maintenance to know really where your risks are. Good companies do it well. Frankly, most organizations do the best they can and overlook some things. And I think that's probably why we both reacted with a little bit of – We kind of see both sides to some degree. It is challenging to keep up with all of the sort of vulnerabilities that exist or securing every system appropriately through the firewall and with all the other sort of controls that might exist. In some ways, it's easier to deal with certain physical security things. And I think part of that is simply because you can see them. And that is really where we go a lot.

[00:39:29] RJ: And I really like the analogy there of the fence, because the zero day is kind of a good example if you use that analogy. Your fence isn't going to disappear because you look at it from a slightly different angle. So you can have software that is rock solid until some researcher finds some exploit in it. And now there's a big hole in that fence or there's a gap there. Your fence is going to rust out at the rate that it does and you're going to replace it when you need to. You're going to be well aware of these things ahead of time.

[00:39:57] JP: Right. And again, you can look at it, "Hey, for my house, I'm okay with a four-foot fence that keeps the neighbor's dog out." For a bank, you want an eight-foot fence with your razor wire and maybe you have some cameras. And it's a little easier. And it does somehow feel a little bit more straightforward to build security around a physical location.

Certainly, I don't want to make that sound trivial, because I know a lot goes into it. But there is a tangibility or physicality to it that I think is different than trying to do everything from an electronic standpoint with data moving everywhere.

[00:40:32] KP: Well, cyber security in general is a very important contemporary topic. I've been tuning into Vancord's CyberSound podcast. Can you tell listeners a little bit about the types of contents you get into there?

[00:40:44] JP: Ah, that's great. And I appreciate bringing that up. And I actually hope you found some of those episodes interesting. The intent for us really was to build a podcast that is geared more toward that mid-sized business owner. More so probably even the traditional security practitioner. I think there's a lot of great podcasts out there that focus on that's delivered by and delivered for security practitioners. And our goal really is to try and make some of these security challenges a little bit more accessible to people who don't live in breathe security every day.

So we talk about things like cyber liability insurance and why you might need it. And what some of the pros and cons might be. We'll talk about protecting a remote workforce during a transition like we've just seen. So it really is geared toward, I hope, your pragmatic solutions to some of the challenges that we kind of see organizations facing every day.

[00:41:39] KP: Anything you want to add before we sign off?

[00:41:42] JP: This was pretty comprehensive. I would want to add, I think, by simply advocating for companies to be proactive about security. And that can range from simply reviewing and making sure you're passing to your sort of more mature decisions around certain hardware products and implementations that are a little bit more specific. But if you wait until an incident and you haven't given thought to things as basic as is your data backed up? Is your data backed up and offline in some format, right? What's your capability of restoring? Things are just much more difficult. If you're not confident that you've got your data well protected at a bare minimum, I would encourage anybody listening to reach out to somebody who could help with that. Because, ultimately, the genesis or sort of the desire for this attacker is business interruption and ultimately extortion, that kind of lends itself to

you know encrypting data or stealing data. You need to protect that. So if you're not confident that you could restore in the event of attack, even if you're not confident your security is great, give somebody a call and start looking at backups. I don't know if we spent a ton of time there, and I think that's a really important topic.

[00:42:59] KP: Good advice. Absolutely. Well, Jason and Russell, thank you both so much for coming on Software Engineering Daily.

[00:43:05] JP: Yeah, it's been a pleasure, Kyle. Thank you.

[00:43:07] RJ: Thanks for having us.

[END]