Digital Cowboys Episode# 4 | Cyber Security Safeguards For Your Business

Mark Culhane: Just first establish where your assets are, what you care about, how much their worth, and then that actually guides your investment in security. You don't want to spend $100,000 protecting an asset that's only worth $200,000.

Cameron Francis: So ladies and gentleman, login to your CMS, whatever it is, make sure that the CMS version's up to date so it's the latest version of Wordpress, it's the latest version of Magento, it's the latest version of Joomla, and make sure that all of your plug-ins are updated as well.

Mark Culhane: That's a big thing that people often miss out because people automatically go in their minds to all the hackers are out there to get me, but information security is about more than that. It's about the stability of your business.

Voiceover: Digital Cowboys episode four. We discuss everything digital marketing and growth hacking for small businesses, start-ups, and entrepreneurs. If you want that competitive edge, then saddle up because Cameron Francis and Sam Roshan are about to drop some value bombs.

Cameron Francis: Hey everybody, this is Cameron Francis and this is episode four of the Digital Cowboys. Super excited today. It's Saturday. I'm in my office. It's actually a beautiful day waiting for the football to start, and I'm joined with Mark Culhane. Now, Mark is the CTO and CISO at Security Shift. Security Shift is a Melbourne-based IT company that specialize in secure Cloud services, managed IT operations, InfoSec auditing, whole bunch of nerd stuff. Mark has a track record of success at organizations and major projects, including the Department of Defense, [ARS 00:01:41] Registry, Compuware, and AssetOwl. He has fulfilled a range of roles like the Head of IT, Information Security Officer, Onsite Consultant, and Systems Administrator. He's presented on topics like information security, management systems, and attack vectors and DNS at conferences, including the Australian Internet Governance Forum. I was lucky enough to be his celebrant at his wedding and have spent some time overseas running amuck. He's probably the smartest guy I know and someone you can liken to as Sheldon from the Big Bang Theory. Ladies and gentlemen, Mark Culhane. Whoo.

Hey, Mark, how are you doing?

Mark Culhane: Hey. Good, thank you.

Cameron Francis: Get close to that microphone there, buddy.

Mark Culhane: There we go, there we go.

Cameron Francis: What's going on?

Mark Culhane: Not much. Just relaxing here in the office, in the lovely eTraffic office.

Cameron Francis: What's the biggest news that's happened to you in the last three, four months?

Mark Culhane: So it's been a busy three or four months, actually. Myself and a business partner actually founded Security Shift about four months ago so we did that through a couple of acquisitions and a couple of key clients that we have. I also, actually, had my first baby, a baby boy, yes.

Cameron Francis: What's his name?

Mark Culhane: His name's Maxwell.

Cameron Francis: Maximus Aurelius.

Mark Culhane: No, Maxwell not Maximus.

Cameron Francis: Sorry, that's Maxwell. Middle name?

Mark Culhane: Kiano.

Cameron Francis: Sorry. So his name's Maxwell Keanu.

Mark Culhane: Culhane, yeah.

Cameron Francis: Culhane. That's really nice. How come you've never told me his middle name?

Mark Culhane: Because you've never asked.

Cameron Francis: Because that exact reason. You've gotta tell me where Keanu came from. Is it the actor?

Mark Culhane: It's actually an Indonesian name. My wife's Indonesian and Kiano is an Indonesian name, which represents good luck and good fortune.

Cameron Francis: So Keanu Reeves, is he Indonesian?

Mark Culhane: No, it's a different spelling. It's Kiano, like piano with a K.

Cameron Francis: Okay. Is there any lines above any letters?

Mark Culhane: No, they don't have that-

Cameron Francis: No, they don't do that?

Mark Culhane: No.

Cameron Francis: Okay cool. I actually wanted to get you here today because you, as I was saying in the intro that you know a lot about security, right? And I think that there's a little bit of a gap for typical business owners on how to safeguard and keep their web assets safe. Yeah, first thing I wanted to go through would be what would you advise, from a security point of view, for typical businesses?

Mark Culhane: Yeah, so the place that I always start, especially small to medium businesses businesses is a risk-based approach. With IT security, it's basically a never ending bucket of money that you can spend, and there has to be a point where you say, "All right. I'm not gonna spend that money because I'm not gonna get a return on investment."

Cameron Francis: Sure.

Mark Culhane: So the place that I always start, especially for small to medium businesses, is first, establish where your assets are, what you care about, how much their worth, and then that actually guides your investment in security. You don't want to spend $100,000 protecting an asset that's only worth $200,000.

Cameron Francis: Sorry, when you say assets, we're talking purely online, right?

Mark Culhane: We're talking about any informational-based asset. That can be, for example, your website. It can be your emails and your calendar and your contacts. It can even be stuff like your brand. You might say, "If we get our website hacked, that's not actually gonna influence our revenue because we don't really get revenue from the site, but we know that a lot of our customers visit the site and if we get hacked, then that's gonna damage our brand value." And you can infer some type of financial impact from something like that.

Cameron Francis: So you would look at your assets and you basically gotta work out what's the value to you?

Mark Culhane: Exactly and it's not like a perfect science. For example, brand value, it's always difficult to pin down to a specific thing, but you can use that as a guide for, all right, I understand that this is something that we care about to an extent of, say, $100,000 a year or $10,000 a year or maybe it's something that's really not that material. Maybe it's only worth $200 to you or something.

Cameron Francis: That's really interesting. If I'm a business and I ask myself, "Okay. If my website shut down and I don't have it anymore, what impact does that have on my business?"

Mark Culhane: Exactly.

Cameron Francis: That's the question?

Mark Culhane: That's the question. That's exactly what you need to answer.

Cameron Francis: Interesting.

Mark Culhane: Because that is how you decide how much money are you gonna spend on protecting it.

Cameron Francis: Never thought of it that way. That's really interesting. Okay, so like, for example, if my website shut down, I'd reckon that it would have a very minimal impact, to be honest. I'd just build up a new one.

Mark Culhane: Exactly. Exactly. So that would mean that you would not want to spend so much money on protecting that asset, but you might say that if we're unable to communicate via phone, so if that phone system goes down, then that might be something that you want to protect more. When I'm talking about protection, it's not just oh, the hackers are out to get us.

Cameron Francis: Okay.

Mark Culhane: Information security is about confidentiality and integrity, so that's about preventing people from hacking stuff or preventing people from accessing data that should be confidential, but the other big one is availability. You can say that we want to provide information security for our phone system, and that may not be that important that it's confidential or it has integrity of its information. It may be about we need our phones to be up and available and if something happens, we need a plan for how to get them back online as soon as possible.

Yeah, so that's a big thing that people often miss out because people sort of automatically go with their minds to 'oh, the hackers are out there to get me', but information security is about more than that. It's about the stability of your business.

Cameron Francis: Very good. Very good. I can't believe we've never actually spoken about this before.

Mark Culhane: Yeah, well, it's not exactly the most entertaining of topics.

Cameron Francis: But it's important though, right?

Mark Culhane: Exactly.

Cameron Francis: Okay so, let's go with our website security. I've calculated that if it was to go down, then the cost, to me, is going to be X, so what would you invest into?

Mark Culhane: Exactly. So that's where you generally need some expertise. Like, it would be, for most small businesses that don't have an experienced IT department or Information Security Specialist, then once you've decided that, you want to figure out what the best value for money protections are. To use, I guess, a well-trodden term, you want to go for the low hanging fruit. You want to do the stuff that costs the least and provides the highest level of protection.

Cameron Francis: Example.

Mark Culhane: So for example, having a redundant web server. For example, having SSL encryption on your site.

Cameron Francis: Okay. Step one. What should someone do?

Mark Culhane: It's hard to say, specifically for a person ... You really need to have an understanding of the business and of what they're doing. Like I said, you want to start with the risk-based approach, then you want to start going into those steps, one, two, and three. For example, most business's email and website, generally import online assets, and the reason why we start there is because online assets are open to attack by everyone. It's not like your mailbox downstairs where someone actually has to physically come and access it. Anyone from all over the world can hit your emails and can hit your online applications. Just doing some basic security on those things is generally recommended.

Cameron Francis: Let's put it from a practical point of view. Okay, so I want to secure my web, hosting and my emails. Where do I go? What do I do? What do I look for?

Mark Culhane: So, generally, you'll engage someone or a company to say, "Can you have a look at what we've currently got?" And then they'll do a basic check, a basic scan. They might login and-

Cameron Francis: What are they gonna scan? What are they gonna check? So what are the questions? Yeah, you know what I mean? What are they gonna be asking?

Mark Culhane: The big thing, generally, is patching. If you're running an old version of a web server or an old version of Wordpress or old version of Wordpress plugins and stuff like that, they're generally vulnerable to automated attacks. So when you're looking at someone that's trying to attack you, there's different layers. And the vast, vast, vast majority of attacks are guys, not like really organized guys, they're guys that are just doing online scans across huge ranges of the Internet, not looking for you in particular, they're just looking for a Wordpress site or-

Cameron Francis: That hasn't been updated.

Mark Culhane: Yeah, exactly. That is just the most basic level of security is saying that I don't want to be the most vulnerable person on the Internet because you're gonna be the first one to be attacked.

Cameron Francis: So, ladies and gentlemen, login to your CMS, whatever it is, make sure that the CMS version is up to date so it's the latest version of Wordpress, it's the latest version of Magento, it's the latest version of Joomla, and make sure that all of your plugins are updated as well. Before we actually had someone managing our server itself, we had a couple of accounts that actually got hacked. When we actually did the analysis and how they got hacked, it was through these bloody plugins.

Mark Culhane: Yeah and it's not something to be embarrassed or ashamed about. I've worked at really advanced IT companies that do really serious and technical IT operations, but stuff like your websites and your blogs, they're not in the forefront of your mind, depending on what you do. It is really easy to not patch them if you don't have it automated. And having things automated is also difficult because, for example, if you're a Wordpress user, sometimes updating Wordpress breaks your site.

Cameron Francis: It always breaks your site, all right, especially if you have a lot ... Try not to have too many plugins. Every time it's updated, something always breaks. It's just the way it is and when you do that, you've gotta spend and pay money to actually get the website back to what it actually is.

Mark Culhane: Exactly.

Cameron Francis: One of the things that we do is we take a backup of the site, update the CMS version, update all the plugins, then we just check the site to see what needs to be changed.

Mark Culhane: Yeah exactly. Again, with information security, a lot of people focus on these technical wizardry and all of the cool black magic stuff, but a lot of the best value comes from just having some simple processes, like what you said. The simple processes are every week or every month we do patching. When we do patching, we take a backup, we deploy it, we do this test. This test covers those things. And just doing that basic process stuff, it's boring and it's not sexy, but that's the sort of thing that really doesn't cost a lot of money. It costs a little bit of time, but that provides a massive increase in your protection. That means that you're no longer the primary target for those guys doing random scanning around the Internet.

Cameron Francis: Now that we do that, knock on wood and you know, all of that stuff, we haven't been attacked and really that's it. You just check it. Just update it. That's it.

Mark Culhane: Exactly and that's the point where it comes to, again, a risk-based approach. I would argue if you're doing that, yes, you're gonna be much more protected, but if, for example, China or Russia or an intelligence agency comes along and tries to attack you or really advanced attacker targets you specifically, you're still gonna get-

Cameron Francis: Don't skip it. Why would China attack Billy Bob's Plumber.

Mark Culhane: Exactly. So why would they bother spending the money on protecting against an advanced system threat when they're not gonna be a target for it. I think that's a big problem in the security industry is that it's not really a differentiation between a small to medium enterprise that doesn't need to worry about those threats, and then a big enterprise that's got thousands of people that does

Cameron Francis: Okay. There needs to be some kind of tiering and I guess this is something that ... Right now, we're probably gonna be touching tier one, if that's what you want to call it, whatever's the entry level. Update your CMS. And I know that everyone has a host or they all have a web development company, don't rely on them. You should not be relying on a company that has no say in your business. That's your responsibility, as the business owner.

Mark Culhane: The other thing to be aware of is that in general, the large-scale generic hosting companies, that offer fantastic prices, if they're getting, let's say, $50, $100, or $200 a month-

Cameron Francis: You're kidding yourself, mate. It's $9 a month.

Mark Culhane: Yeah, exactly.

Cameron Francis: You know what I mean?

Mark Culhane: How are they going to make money if they have to have a system admin look at your site.The system admin, even for an hour, is gonna cost them, what, $400 in ongoing costs and all that sort of stuff. $400 an hour for a $9 a month client. It just doesn't make sense.

Cameron Francis: What would you recommend for hosting for small to medium?

Mark Culhane: So, again, it depends how important the asset is to you. If it is your primary source of income, then the hosting provider, yes and no, it does matter, but the fact that what you need is someone either internal to your organization or external just providing that high level of expertise, making sure that they actually apply those processes, and being able to understand ... So, for example, if you do a scan of the website and the server and there's vulnerabilities that come up, most people are not going to be able to say, "I know what this vulnerability means. I know that this cipher is insecure because of x, y, z." It's not realistic for a small to medium business to have people like that. In general, it's a good idea to get a company like, for example, Security Shift does that.

We'll do cursory scans of the sites and then we'll just make sure that there's nothing glaring. It's not gonna provide you with 100% protection. It's just gonna get you off that bottom rung of vulnerability.

Cameron Francis: And again, it's got to do with risk, right? If you don't have a level two, three, four, five risk, then why pay for that protection?

Mark Culhane: Exactly. Exactly.

Cameron Francis: Very good. Okay, so that's from the website point of view. What about ... actually, no, let's stay on that. Do you think that a business owner should be backing up their own website and if also they'd be paying someone, that should be a service that they should be getting?

Mark Culhane: Again, it depends on the expertise of the person. It depends whether they have an IT department.

Cameron Francis: They don't and they don't have expertise. Let's go null and null for both.

Mark Culhane: Then, yes. You need to figure out how to get a backup of your site because there's just an unending list of people that lose their sites, whether it's through malicious activities, whether it's through the hosting company having a mess-up, whether it's through them accidentally deleting their website. There's so many ways that you can lose assets online and you just need to have backups.

Cameron Francis: How often, would you say, do it?

Mark Culhane: Well, the key is to automate it. You shouldn't have to do it. You should be able to get it in a place where I know that my site and my assets are getting backed up every day and not only are they getting backed up, I know that they can be restored easily and I know how they're restored. There's no point in taking backups if you don't know how to restore them, right? It is a little bit more complicated than just, "I'm just gonna make sure that these files are all kept on this disk." It has to be also, if we do lose our site, how do we get it back up online? How long does it take? Is that acceptable for us? How much lost data do we have? If we lose all of the audience from the day, is that okay or not? There's a lot of finer grain detail when you start looking into it, but at a minimum, yes, you need to have the backup.

Cameron Francis: I'm just gonna login to our CMS now. We actually have a plugin on our site that does automatically backup the site and we set the frequency. So I want it backed up every week at this time and then I want that backup to be stored, that version, for the next three months, and then they start to-

Mark Culhane: Rotate it.

Cameron Francis: Yeah, over ... what is the word?

Mark Culhane: Overwriting.

Cameron Francis: Yeah, overwriting it. That's enough for me because I mean, shit, if you are not monitoring after three months that your website, there's a mistake on there, then it doesn't mean a lot to you.

Mark Culhane: Yes, exactly. Exactly.

Cameron Francis: Okay cool. So let's jump to emails.

Mark Culhane: Yeah, so email is one of the really, really interesting protocol that got created at the very beginnings of the Internet.

Cameron Francis: Can I tell you my issue with emails?

Mark Culhane: Yeah.

Cameron Francis: We started off ... I forget where we started. We've got Google Apps, right? And I've got a Mac. So I logged in my emails through the Mac Mail, the issue is being able to get back my emails, my archives. That's a problem. I just can't. So what I do now ... I've gone back to Gmail. Gmail has an absolutely disgusting search bar for previous ... It is terrible. I couldn't do that. I need to have my emails stored, you know? Just for my own security. So what I've done now is every single email, whether it's through inbox, sent, junk, trash, whatever it is, every single one of them's archived. It's just in my ... I've got 34,200 emails in-

Mark Culhane: That's quite a lot of emails.

Cameron Francis: But it's all there. I know that if I need something that's been sent or if someone sent something to me that's in my junk folder, it's in that bad boy right there. At some point, I'm gonna run out of space. I'll let Future Cameron worry that.

Mark Culhane: That's Future Cameron's problem.

Cameron Francis: But what do you reckon about emails? What should one do?

Mark Culhane: So definitely, in terms of storing and backing up, if you've got a requirement like that, in general the Cloud service providers like Office 365 and Gmail, they've come a long way and they're pretty good services now.

Cameron Francis: Okay.

Mark Culhane: But the interesting stuff about email is how trust-based it is and how much people believe it more than they should. For example, right now I could write a little script and send you an email from accounts@etraffic.com.au. So you're gonna receive the email to your inbox and you're gonna see that it's from accounts@etraffic.com.au. I'm gonna say, "Hey Cameron, I need you to transfer a thousand bucks to this account because we've got a lot or something." It's amazing how many people assume that when an email comes into their inbox, if it says it's from accounts@etraffic.com.au, that it's from you guys.

Cameron Francis: You just clicked this here. What I've done here is I've, this is an email from BuzzSumo. You click there and it actually has the email. Are you saying in that it'll have accounts?

Mark Culhane: Yeah, you can completely spoof an email. Email is completely insecure.

Cameron Francis: I don't believe you. Are you kidding me?

Mark Culhane: I've got a script right here. I can do it for you.

Cameron Francis: Will it take long?

Mark Culhane: I'll figure it out

Cameron Francis: If you can multitask, I'd be ... so what, ladies and gentlemen, he's gonna do, he's gonna send me an email from ... This is kinda scary now. You get this from the government, saying you've gotta pay tax, or the bank, log in, and then it would be a firewall or something that you go to a different site, you put in your details-

Mark Culhane: Yeah or even just like, so the big thing that's happening, amazingly regularly, at the moment, is corporations are losing money because people are spoofing emails from the CEO and they're sending it to accounts and saying, "Ah I'm in Japan or I'm in the Philippines or whatever, I need you to wire this money immediately." If it's a large organization and people never talk to the CEO and they know his name and they know that's his email account, they're just wiring the money and it's amazing how often it's happening.

Cameron Francis: Yeah, but see. For me, like I would be a victim of this, right? My safeguard, when you get those emails from the commonwealth Bank or you get those emails from government, when you do click there and you see it's from like aandz-bank-commonwealth.com, you know what I mean? It's not the actual ... This is where I always look. If you can actually get it so it appears the email is accounts@etraffic.com.au, that's really scary.

Mark Culhane: There are a bunch of controls that you can actually do to prevent that from being able to be done, but it's very rare, well it's not very rare, but it's very rare for a small to medium business to implement those controls because-

Cameron Francis: When you're saying controls, is this like a common sense, one, two, three step kind of pattern? So like if I see an email from accounts, the first thing I'm gonna do is I'm gonna give a call to Carla , ask her, "Did you send this?"

Mark Culhane: So that's an excellent one and that comes back to the not sexy process stuff. That is a control that would ... if you had a policy at your organization that said, "No one can transfer money to anyone without phone verification," that would stop the problem.

Cameron Francis: Okay, so everyone, implement that today and I'm not joking. That's gonna be done. The fact that ... I want you to prove it. I want you to send. Again, Mark's gonna be sending me an email saying, "Hey can you transfer some money from accounts," but that's now a protocol. If money needs to be transferred, there needs to be phone verification and is that enough of a safeguard?

Mark Culhane: Yeah, so when you say enough of a safeguard, like there's a bunch of other intricacies to it that could mess that up, but that's gonna cover so much of it that, for something that's free and you can implement right away, yeah.

Cameron Francis: I mean, it's a phone call. No one's that busy. It's a phone call, or even a text, like "Relax. Not an email." Can you spoof a text?

Mark Culhane: Yes, of course you can spoof a text.

Cameron Francis: How do you spoof texts?

Mark Culhane: These protocols are not implemented to have authentication of senders.

Cameron Francis: Okay, no texting for verification of money transfers. Wow. You're opening my eyes here, Mr. Culhane. That's excellent. All right, so we're looking at ... Okay, keep going through email protocol because this is fascinating.

Mark Culhane: So email stuff, as you mentioned, the phone call is a great process, way to protect against that. There are other automated ways. So automated ways are always a little bit better because that means that you don't have to do anything. There's stuff like SPF records, which set a policy framework, so that's like a DNS entry where you specify which servers can send emails on behalf of your domain, but again, if you're going down to a small to medium business and you go, "Can you just implement a SPF record on your DNS." They're gonna-

Cameron Francis: I don't even know what you just said. They're gonna look at you like the way I'm looking at you. Whole bunch of letters there, man.

Mark Culhane: Yeah, so there comes a point where it's worth it for an organization to not just say, "All right. We'll be aware of this and we'll make the phone call." Where it becomes worth it to say, "We're gonna get a little bit of help and get someone in that can do that extra level of automation and that extra level of assurance."

Cameron Francis: I think what it would come down to, again, guys, is when you're talking initially about the threat, like what is the risk for your business, right? The bigger the business is, the bigger the risk are. The more money you can transfer, the more levels there are to the CEO, to the person, to the accounts team. I mean, from my point of view, and for businesses of similar sizes, then that phone verification, I mean, really just implement it, right?

Mark Culhane: Yeah, yeah. Let me touch on the topic of how much large organizations spend on security. If you look at the Australian Big Four banks and the US banks, they spend literally billions of dollars on information security. It's insane how much they're spending.

Cameron Francis: Do you have any data on it?

Mark Culhane: I'm looking it up. According to Gartner Worldwide Spending on information has reached 75.4 billion in 2015. They're spending a lot of money on it.

Cameron Francis: Wow, so that's why you chose this industry, huh? Not bad. It's not bad. And the digital marketing industry comes in. Well played, sir. So you know how we're talking about storing and saving emails, I want some data around that and some steps around that, and other things that someone running a small to medium business, up to 100 employees, from one employee, what are some of the things [crosstalk 00:26:30] just the basic email.

Mark Culhane: So basic email, of course, storing and backing up the emails.

Cameron Francis: See, you know how I'm telling you I've archived 35,000? I'm not doing that with every one, right? I really should be, especially if they're sending emails through to clients, then I really should be.

Mark Culhane: One of the great things about the big Cloud service providers like your Office365s and your Gmail is you're basically getting unlimited, well not unlimited storage, but more storage than you could ever need at a price that is insanely good.It's actually really simple to set up basic email routing that will mean that every email that comes in and out of your organization will be stored in an archive account where it's something that you can go and look at and you can go and review and restore if required.

That is, of course, meaning that you're still trusting that Google and Microsoft are not going to lose your data. Honestly, for a small to medium business, I think that's pretty reasonable. Microsoft and Google have not, to my knowledge, had any major data loss of clients in the past five years. I think for most organizations, it's completely reasonable just to depend on your Cloud services provider to provide that level of assurance.

If you want to take that extra step, then there's plenty of tools available to go in and pull those emails down to somewhere offline. When I say offline, the key point of that is one of the biggest risks of how you're gonna lose emails is through accidental or bad user deletion. For example, if you accidentally delete your emails or if you've got someone in your organization who's got access to all those emails, all those email accounts, who accidentally or maliciously deletes them. Having an offline backup means that you can only send data to it. You can't go in and delete data from it. So there's a lot of services provide that.

Cameron Francis: Any recommend ... We'll put it in the show notes. What do you recommend?

Mark Culhane: Best recommendation for small to medium businesses is Amazon's Glacier Service. So basically what that is is you can send unlimited data to the Glacier Service, which is like a bunch of tapes and hard disks and you just send data to it and it's almost free to send data to it, it's like a matter of cents, and then the only time you really pay for it is when you go, "All right. We've had a major problem. I need to go and retrieve that data." You have to go through a series of validations.

Cameron Francis: I'm gonna look it up. How do you spell it?

Mark Culhane: It's Glacier, as in like the melting glaciers.

Cameron Francis: If I type in Glacier-

Mark Culhane: AWS Glacier.

Cameron Francis: AWS, all right. I'm gonna put this in the show notes and most likely gonna purchase it, but yeah, sorry, continue.

Mark Culhane: Okay. We were talking about ... I think we've covered backing up emails.

Cameron Francis: But is there anything else that someone should look for because this is actually, from my point of view and security and all of that stuff, if someone in my organization sends an email, I'm liable for the contents in that email, right? It's important that I need to have ... But then there's also confidentiality. I can't just look up my employee's emails.

Mark Culhane: Well, yeah. It depends on your information security policies and your employee agreements. So, in general, most corporations will have a part in their employee agreement that allow them, for a specific reason, to go and look at any email that's been sent or received to it.

Cameron Francis: For a reason. It's like how a policeman can frisk someone if they feel that they're suspicious.

Mark Culhane: Yes, except that this is generally contract and lawyer terms for, basically, whenever we want. It's pretty general, but the law strictly says-

Cameron Francis: Etraffickers, I'm not checking your emails, don't worry.

Okay, Glacier, checking emails, backing them all up, is there anything else that someone should ... Okay, what about the disclaimer in the email?

Mark Culhane: Yeah, that is just-

Cameron Francis: Codwalloped?

Mark Culhane: A bunch of bullshit.

Cameron Francis: I knew it. I don't have it in mine. What does that mean?

Mark Culhane: Yeah it's completely unenforceable. What it means, if you don't have it in your email, is that if someone reads your email and is trying to be really formal and thinks that important then maybe they'll be like, "Oh, well you're not a professional," but really there's no legal value to having those.

Cameron Francis: All it does, it takes up real estate. From a marketing standpoint, use that space to show accreditations and more links.

Mark Culhane: I can't believe it's lasted so long actually. You know, we've got it in our emails.

Cameron Francis: Do you really? That's so funny. See, I don't have it out of laziness, but I love that I can justify it. Yeah, so, okay cool. So we've covered website, covered backups.

Mark Culhane: Well there's more in email, there's more in email.

Cameron Francis: Okay, tell us.

Mark Culhane: So some of the biggest attack factors for small to medium businesses, via email, is not just what we call the spoofing of emails. So the spoofing of email means that I send you an email-

Cameron Francis: I'm still waiting for that spoof, just FYI.

Mark Culhane: Well, I'm talking to you.

Cameron Francis: Sure, sure. Multitask.

Mark Culhane: So, there's that spoofing of email, but there's also malicious URLs within emails. So, the reality of the Internet is that if I can get you to click on a link, there's a good chance that I can compromise your computer or compromise information from you. So that means if I send you an email and I don't even bother spoofing it, so, say, for example, I pretend it's from Westpac and I put a link. I make the email exactly the same as Westpac's email and instead of it being from Westpac, I put something that looks very much similar to Westpac. I might send an email from marketing@westpac.com.000 blah blah blah, and you can't see the rest of it. It's generally very difficult to pick that up.

Cameron Francis: We've all received them. You just go to your junk folder now and you'll see them.

Mark Culhane: And that's another fantastic part about the Cloud services, the Office365 and the Gmail-

Cameron Francis: Their spam folders are really good.

Mark Culhane: They have actually really impressive. I'm really impressed.

Cameron Francis: A lot of that would be to do with the volume of emails.

Mark Culhane: Exactly. They've got that massive volume and they can do like heuristics and detection and figure out who's sending all this stuff and block it. Yeah, that's a big pro for using one of those big suppliers, but still, if you get targeted by someone, they're only gonna pick up the mass spammers who are sending those emails to millions of people. If I decide to be a little bit less lazy and I start sending those emails, instead of doing it to a million people, I go to the yellow pages and do it to 10,000 people, then my emails are gonna get through.

Cameron Francis: Yeah, okay.

Mark Culhane: Yeah and so there's a number of ways that you can be malicious with the emails and some of them might be pretending to be a bank-based email and getting you a link to your bank interface and you click on the link and it looks exactly the same as Commonwealth Bank's login page, and it's got SSL and it looks perfect, but yeah, to the untrained eye it looks perfect.

Cameron Francis: But the URL would be different?

Mark Culhane: Yeah, but there's so many little techniques to make those URLs look exactly the same. You really have to be looking to be able to pick that up and even myself, as someone that works in Information Security, I don't trust myself to pick that sort of stuff up, so I put controls in place that check that.

Cameron Francis: Is there firewalls that you would put in place or Lehmann's terms?

Mark Culhane: No, so firewalls are more of a network traffic control. If you had a firewall, that would stop all emails coming in, which is no good, but a lot of firewalls do have an extra module in them that basically checks the URLs that are coming into your mailbox and checks them for malicious content and that sort of stuff.

Cameron Francis: So what protocols would you put in place?

Mark Culhane: You can use services like Proofpoint. What Proofpoint does is when an email comes to you, you first send it to Proofpoint and they have millions and millions of emails coming through them and they've got a bunch of technology in place, that before they forward the email onto your actual account for your reading, they just double check the content and all of the links in it for anything malicious.

Cameron Francis: Why wouldn't you recommend this to me previously? This is very important stuff.

Mark Culhane: It's because there's a list of thousands of those things and-

Cameron Francis: But we're only giving the ... This is one that you recommend?

Mark Culhane: Yeah, so it goes through the basics, but yeah, that's the reason why it's a hundred billion dollar industry, right, is because there's just-

Cameron Francis: There's everything.

Mark Culhane: That's the reason why I talk about the risk-based approach because if you go, all right, I want to be safe from attackers, there's just too much. Where do you start? There's just too much stuff to do. Yeah, Proofpoint's a great one. They've got an essential product that's free.

Cameron Francis: What is it? What's it called? I'm on the site now.

Mark Culhane: Yeah it's called Proofpoint Essentials.

Cameron Francis: Great site.

Mark Culhane: Yeah.

Cameron Francis: Could do with some SEO, but yeah, great site.

Mark Culhane: Yeah. That's a good one. There's a bunch of alternatives to Proofpoint, of course. I'm not associated with Proofpoint. I'm not getting money from them. So I probably shouldn't recommend it.

Cameron Francis: No, no. If that's the one you recommend, then that's one that we'll look at. Okay, so this is going to help when clicking links from email browsers.

Mark Culhane: Yes, so that's one thing it helps with. Basically, that's just, every time an email comes to you, it's first going through a washing machine. Proofpoint is a washing machine and it's gonna ... There's a bunch of things. You can either have it warn you if there's bad content and still send it to you or you can have a block or whatever, but basically, again, as we talked about with the websites, it's getting you off that bottom level of vulnerability so you're no longer the easiest target on the Internet.

Cameron Francis: We were talking about email spoofing earlier before where-

Mark Culhane: Yeah, so I guess one of the most misunderstood aspects of email is that I can send email, myself, from anyone. I can send email as accounts@etraffic.com.au to cam@etraffic.com.au and assuming you don't have any other controls in place, like sender policy framework, etc., etc. then the email's gonna come through to you and most people, when they see that the from address is someone they know or part of their organization, assume that it is from their organization.

Cameron Francis: This is the scary thing, right? I have received it. I didn't believe him. It didn't go to my inbox because of the spam. Mark's just sent me an email. First of all, it says etraffic.com. There's no etraffic.com.

Mark Culhane: Okay, sorry.

Cameron Francis: eTraffic.com.au , but you could've changed that, right?

Mark Culhane: Yes.

Cameron Francis: Yep. So there's that aspect, and then on the email, and I've just taken a photo and I'll add it into the show notes. It basically says, "Test spoof. cam@etraffic.com.au. Reply to accounts@etraffic.com.au." So if I reply to this, will this go to you?

Mark Culhane: No that would go to accounts@etraffic.com.au.

Cameron Francis: But the point is, in the text, because in the body of the email it just says, "Send me money."

Mark Culhane: Yeah, so if I really wanted to try it, then I would put an email like, "Hi, Cam. We need to pay this invoice blah blah blah blah, please transfer or go to this website."

Cameron Francis: Do another one because this is actually both interesting, alarming, and scary at the same time, the fact that you've just done this, right? In some ways, I'm in the digital text space and I didn't think that this was possible. Later on, I want you to send an email from David, saying "Dude, I need you to send me some money." And then put our bank details to see if that actually works.

Mark Culhane: It definitely will. The good part about what you guys have got is someone who has put in an SPF record in your DNS ... So what that does is ... Well, the way how the SPF record is configured means that if the email comes from a server that's not listed in something you created, so you can say, only Google servers can send email on behalf of etraffic.com.au. You've got that in place, but you've got it in place in what's called a soft block, which means that it will still go through, but it will get tagged as junk or something like that.

Cameron Francis: And that's where it went straight through to ... So if Claro , our IT guy, didn't actually have that in place, with the SPF-

Mark Culhane: Then it would go straight to your inbox.

Cameron Francis: Interesting. So, honestly, every business person, get this fixed. This is incredible. How do people get this fixed, man?

Mark Culhane: It's really simple. Anyone who's technical is listening to me saying, "You're an idiot. That's so simple to fix." And it is. It is simple, but the reason why I'm talking about it is because if you're not someone that knows about DNS and DNS records [crosstalk 00:40:23]

Cameron Francis: Hands up. Many people.

Mark Culhane: Most business owners won't know about that and it doesn't mean that they're stupid. It means that they're concentrating on something else.

Cameron Francis: Exactly.

Mark Culhane: Yeah, there's a very simple way to fix it and it's called an SPF record. The place where it gets a little bit complicated is what that does is it says, "Only these servers can send email from eTraffic," but if, for example, you use something like-

Cameron Francis: Why did it still get sent through?

Mark Culhane: Because the way that you've got the record configured is in soft block mode. If you look at the actual DNS record, it's got a squiggle instead of a dash, and even the technical folk that are listening, a lot of them won't know the difference between the squiggle and a dash. So the squiggle and the dash means let it through, but tag it. The dash means don't let it through at all.

Cameron Francis: So would you suggest not let it through at all?

Mark Culhane: No, I actually reckon that the squiggle is fine, especially ... It's called a tilde, not a squiggle, but it's fine.

Cameron Francis: Like waltzing.

Mark Culhane: Yeah, except in ASCII mode. So, yeah, it's fine the way it is, especially if you're using an email provider like Gmail or Office365. They'll see your SPF record. They'll see that it's in soft enforcement and they'll go okay, this is junk or this is malicious. The place where it gets a little bit complicated and where some people need help is, say you didn't know that your IT guy had done this, right?

Cameron Francis: Correct because that's his job.

Mark Culhane: Exactly, and that is his job, right? But, say, for example, you wanted to do an email marketing campaign and you used a service like SendGrid or, what's the other one? MailChimp. If MailChimp and SendGrid are not listed in this record, then that means every email that you send in your marketing campaign is gonna get tagged as junk and no one's gonna read it. So that is another aspect of information security that is often sort of overlooked. What's the cost of putting in that control? Yeah, it's fantastic that you guys have got it and that email got put into junk, but I bet my bottom dollar that if you decided to do a MailChimp or a SendGrid email marketing campaign, it's unlikely that you would communicate with your IT guy and make sure that your SPF record is correct so that those emails don't go to all of your marketing targets' junk. Yeah, so that is an interesting aspect, but all in all, I'd say that you guys were successful in blocking my remedial attempt.

Cameron Francis: The fact that it came through though and I don't think that any of our clients would actually have this, we don't offer that as a service, though, right? I saw it, I didn't believe that it was possible. It did go through, went to our junk, and even then it's got my tailbone up a little bit. That's really scary.

Mark Culhane: It really is amazing.

Cameron Francis: Because that's a simple thing. You just did that in front of me.

Mark Culhane: In terms of sophistication of attacks, this is the absolute lowest, simplest ... I'm a little bit embarrassed to be talking about it because anyone that's really technical is just like, "Oh my God. That's stupid."

Cameron Francis: But that's your domain, right?

Mark Culhane: Exactly. That's why I am talking about it because we're not talking to the guys that understand this. We're talking to business owners who don't have $100,000 to pay an IT guy.

Cameron Francis: They don't need that $100,000 or IT guy, right?

Mark Culhane: No, they don't.

Cameron Francis: So what do they do to stop this?

Mark Culhane: Yeah, so there's a bunch of things that they can do. Number one is if you want to get some understanding yourself or if you do have an IT guy that's got no experience in security, get them to have a look at ... There's a lot of resources. One of the best ones that I recommend is the Australian Signals Directorate. So the Australian Signals Directorate is Australia's version of the NSA. So that's our intelligence agency that does all of the offensive hacking and all that sort of cool stuff, but what they also do is they provide Australian businesses and Australian citizens with recommendations on how to do basic security, a basic information security. So they actually publish a top 32 mitigation strategies. So that's a list of controls like SPF, what we're talking about, and patching, and all that sort of stuff. They provide recommendations on the basic things that you can do. Not every business owner's gonna be able to do that, but if they've got someone who has got the basic levels of technical ability, they're gonna be able to read that and glean from it what some basic controls are and implement them. For example, I've their top four mitigation strategies up in front of me. Number one is application whitelisting. What that means is if you've got a few staff members in your office, you want to restrict what they can install on their work stations.

Cameron Francis: North Korea, sure.

Mark Culhane: For example, if you give someone a laptop and they're working in your office, and they go home and they go, "I'm gonna stream something from, for free" or whatever. Free streaming sites are terrible because what they do is they use Flash, which is one of the most vulnerable things on the Internet, or on your computer, and they're gonna get breached, so they're gonna get a bunch of malware installed on their computer. Most of it's not that serious, but some of it is.

Cameron Francis: Can I give you an example of one? Okay, so, one of my very first jobs, actually, I was working at Corporate Choice sales company and they didn't have this in place and I downloaded [Vuze 00:46:22] and at the office, I thought, Jesus Christ, this is fast. I'm pretty sure, like, this is over a decade ago, right? So this is still dialup.

Mark Culhane: Dialup's 20 years ago, mate.

Cameron Francis: Is it? No, it wasn't. I had dialup around 15, 16 years ago. We didn't go to the rich, pretty boy school, but yeah, so I remember I was there and I thought, "Jeez, this is downloading really, really quickly." So I downloaded Vuze and I put on my TV shows. I put on my movies. At that time, they had an Internet plan where if you exceed X, you pay for every megabyte over, and their Internet bill came in, and it was a lot. From memory, it was at least $5, $6 grand, and it was 500%, 600% over. Now, because they didn't have the prevent in place-

Mark Culhane: Whitelisting, yeah. Application whitelisting.

Cameron Francis: I didn't have to pay for it, but that is a perfect example of where this comes into play and it cost them a lot of money.

Mark Culhane: Exactly. Exactly. The other aspect of application whitelisting, it's not just work sanctions, it's also the service that you have. So if you've got a web server or something like that, then you need to ensure that, if you have a basic vulnerability whereby people can do some really basic sort of exploits, you still need to have application whitelisting in place because that prevents them from escalating their privileges and from doing something really malicious on your computer. The primary thing that will happen to small to medium businesses is their server will get turned into to what's called a zombie and that becomes part of a botnet and people use them for distributed denial of service attacks.

If I send out a basic exploit that goes around to and breaches 100,000 computers just because it's got a really basic thing. I don't actually have full control of their server, but what I can get it to do is I can get it to send requests to another website. Then I say to ... One of the famous examples is a lot of the Australian online gambling companies, on Melbourne Cup Day, every single year, they get emails from these distributed denial of service guys, saying, "If you don't pay us $50 grand or if you don't pay us $20 grand or whatever, then we're going to send millions of requests to your site and no one's gonna be able to use it, so on Melbourne Cup Day, no one can place bets.

Cameron Francis: Whoa. Because that's not hard to do. Every website can only handle a certain amount of traffic. That's why you hear websites crashing. If you send any normal website millions of visitors, website goes down. They can't handle the bandwidth.

Mark Culhane: Exactly and if I'm a small to medium business, there's no way that ... The cost for preventing-

Cameron Francis: Is that a DDOS attack?

Mark Culhane: Exactly, a distributed denial of service, DDOS.

Cameron Francis: Very good. I remember because this has happened to us. It was from Russia or something like that and I randomly went to a site and it was down. I went to Claro , "Hey what's going on?" And he's like, "I'm on it." He was up really early in the morning. He said, "We're being attacked." He said, "DDOS." It was just a whole bunch of traffic. That's not even hard to do.

Mark Culhane: No, and amongst information security professionals or whatever, it's not a respected thing because it's something that 14 year olds can do. It doesn't require any intelligence. It just requires a willingness to break the law.

Cameron Francis: So let's just say, competitor A has a beef with competitor B, then he pays ... I mean, it's as simple as, "I'll pay this person to send thousands of ..."

Mark Culhane: 100%. There's thousands of services. They're called DDOS for hire and you can-

Cameron Francis: DDOS for hire. Don't Google that.

Mark Culhane: Yeah, I don't think we're helping the Internet.

Cameron Francis: But how do you safeguard against it?

Mark Culhane: That's one thing that I can't give a small to medium business a simple fix for.

Cameron Francis: Can I attempt? Can you just say I don't want traffic from Russia?

Mark Culhane: Yeah, you can, but so the problem is that-

Cameron Francis: Or I don't want traffic from Uzbekistan?

Mark Culhane: Yeah, so the problem is that wherever you have control up to ... So say you have control of your server or even if you're a little bit more advanced, you have control of the router in front of your server, then you can control that part and say, "Whenever traffic gets there, I want to drop it if it's from a certain area," but what happens with denial of service attacks or distributed denial of service attacks-

Cameron Francis: DDOS.

Mark Culhane: Is they throw so much traffic that the point of failure is not where your control is. The point of failure is gonna be the Internet service provider just before where you're in control, so there's really nothing you can do about it unless you pay ... Another sad thing about the information security business is now, to counteract these distributed denial of service groups, there's a bunch of companies that offer DDOS mitigation, and basically you pay them thousands of dollars a month to, when you get under attack, you route all your traffic through them, and they have huge amounts of bandwidth and they can filter that all out, but basically you pay for the privilege of being able to devote your traffic to them and then they clear it up and send it on to you. But that's getting onto-

Cameron Francis: But you know what's interesting? DDOS mitigation, Australia, searches per month, it's only 50.

Mark Culhane: No.

Cameron Francis: Yeah. Yeah. I agree. But you use it as a guide. It's no exactly 50, but the fact that it's that low, and it's that important.

Mark Culhane: Yeah, well, of course it depends ... Let's go back to the risk-based approach.

Cameron Francis: But if it happens once, right? So risk-based approach, how much will it cost your business if your website is down for a day?

Mark Culhane: Exactly.

Cameron Francis: How much would that cost you? If it happens once, okay. If it happens twice, okay. If it happens three, do something about it?

Mark Culhane: Well, yeah.

Cameron Francis: If it happens often, then someone's got a boner for you.

Mark Culhane: Even if you assess the risk. So at an organization I previously worked at, we did not actually come under a DDOS attack, but we assessed the risk of, and likelihood of, it occurring, and we decided that just the risk of it occurring was sufficient for us to pay, and we ended up paying $120 grand a year just for the mitigation of that risk. It's not realistic for every small to medium business that's gonna pay that, but when you start moving up. So say your business is making $2 million a month or $3 million a month or whatever, then it really-

Cameron Francis: You can't afford for your site to go down.

Mark Culhane: Yeah, it's like insurance.

Cameron Francis: Do you still get DDOS attacks now? Have you ever had one?

Mark Culhane: Yeah, we've had a lot of them. What? When I say we, the company-

Cameron Francis: Stop making enemies, man.

Mark Culhane: That's the thing. It really is sort of random. Because of the ease of the attack and the people that are doing it, are just doing it every day to whoever they can, and it's just extortion.

Cameron Francis: Is it malicious or is there a reason behind it?

Mark Culhane: No, it's purely malicious. It's just basic extortion. It's we're gonna attack this company because we think that they're gonna pay us.

Cameron Francis: So when you're using, is it the TAB or whatever Melbourne Cup example?

Mark Culhane: Yeah.

Cameron Francis: Do they pay?

Mark Culhane: Yeah, I believe so.

Cameron Francis: They pay for terrorists? They're funding terrorists?

Mark Culhane: Well, it's extortion. They're paying for Internet gangsters.

Cameron Francis: Wow. What would your advice be to them?

Mark Culhane: Well [crosstalk 00:54:11] My ideology is that you should never pay them.

Cameron Francis: I agree because then they'll just keep on doing it.

Mark Culhane: Exactly. It just keeps on doing it. And then, the sad part about it all is that if all of the Internet service providers actually agreed, as an industry, there's a very simple way of preventing it ever from happening again, but the fact of the matter is that there's too much politics around it all and instead of just doing the basic simple fix that could be implemented, we still all have to deal with this problem and we have to pay extortion one way or another, whether it's through paying the criminals or paying the guys that-

Cameron Francis: To fix it.

Mark Culhane: Well, the guys that charge you for the risk mitigation. Anyways.

Cameron Francis: So, no, but that's really interesting as well. Really, really fascinating topic. What would Mr. and Mrs. business owner, what should they do?

Mark Culhane: Mr. and Mrs. business owner, don't even worry about it. Until you actually have a problem with it, don't worry about it too much and don't pay unnecessarily for a DDOS mitigation service that you can't really test, you can't really ensure works, and costs thousands of dollars for something that may or may not happen. I would recommend not doing a DDOS mitigation service, but back to the topic, the reason why we're talking about that is because application whitelisting is something that prevents your server from being one of the servers that contributes to those attacks. So that's just being a good Internet citizen, is application whitelisting. Same thing goes for patching systems. Ensuring that your Wordpress, ensuring that your web server, whether it's APACHE or NGINX or whatever, ensuring that the operating system are all up to date.

Cameron Francis: So, let me piggyback a bit because I don't think that a lot of people would know that, and so what the general population would do is they would be either, so there's two. So they'd either get a BlueHost, GoDaddy, CrazyDomains, or they would pay for a company that has their own server, like us for example, and then we manage that for them. Those are the two, but they wouldn't know any of those [crosstalk 00:56:30]

Mark Culhane: Exactly. So when you say that and the business owner says, "Well, we don't have the resources to do that. I don't know how to do that." If you go with a managed service provider like a GoDaddy or a same company like that, then they basically, for better or worse, take care of your lower level patching, like your operating system and your web server and that sort of stuff.

Cameron Francis: Do you know why I don't like those? How many sites would be on one of these-

Mark Culhane: Exactly. Exactly.

Cameron Francis: And, how do you know you're not sharing a server with a porn site, a gambling site, and your website, that trickles through. That affects a lot of different things.

Mark Culhane: 100%. If you've got a business that makes money online, particularly through a website-

Cameron Francis: No, but it's not just makes money online. That’s lead generation… Mark Culhane: Exactly. Very good point. If you've got a website that's a valuable asset to your business, whether it's revenue generating or otherwise, if you say, "All right. I think this website is worth $10,000 a year or $100,000 a year or whatever." And you're paying $7 a month for hosting.

Cameron Francis: Yeah.

Mark Culhane: Why do you think that there's service providers that provide a higher level of service at a higher price? If that shared hosting was fine, there wouldn't be a market for better services. There are downfalls to it. I'm not gonna go through them all right now, there's no point, but if you care about it, at least you're engage a company that's gonna give you the support and tell you, "All right. You need to be aware that your Wordpress is not patched. You need to be aware that you're getting DDOS. You're on your own IP address so you're not gonna get blacklisted because there's some other site going around."

Cameron Francis: Very important. Actually, you know what? From a marketing perspective, it actually affects your SEO.

Mark Culhane: Of course.

Cameron Francis: No, it does because if you've got a site on the same server as you and they're getting spammed like you wouldn't believe and they've got all of this negative stuff, that trickles through to you because-

Mark Culhane: There's so many aspects to it, as well, because most of the search engine, especially Google, for example, they're gonna say, "Is the person searching for your site in Australia? Is your server in Australia? Does it have its own IP address? What else is on that IP? It all affects everything.

Cameron Francis: We're actually doing some SEO for a customer and we're doing everything right, we're ticking all the boxes, doing a normal A to B, C to D, and their results were not what we expected. Some person recommended that we get them off, I would say X server provider, and get them onto someone else, and it had an immediate impact.

Mark Culhane: Yeah.

Cameron Francis: Immediate. And if you think of your website as a revenue generating tool, it's an asset, not for branding, not just for [crosstalk 00:59:36]

Mark Culhane: Well the other argument to that is if you're paying $9 a month for hosting, then the hosting provider does not care about your service. Well, they care about your service, they don't care about your website.

Cameron Francis: No, they don't.

Mark Culhane: They're not gonna go overboard.

Cameron Francis: But if your site goes down, do they notify you or do they try and ... That's a really important aspect, right? That's what I wanted to talk about as well. How do you know if your sites down?

Mark Culhane: Good question. It's a lot more complex than is your site down. If your site-

Cameron Francis: It's A or B.

Mark Culhane: No, it's not A or B. That's an amazingly complex question for something that's so simple. For example, one of the hardest things to pin down when you're providing ... Say you're providing a government agency or a large organization with a really hugely important application, and you've got contracts in place that say this site has to be available 99.9% of the time or 99.9999% blah blah blah. How do you establish whether the site is available or not? Does that mean that when you go to the site, if it responds in 20 seconds or 30 seconds, is that available?

Cameron Francis: Okay, I see what you mean.

Mark Culhane: If it responds with an error, is that available? If all of the pages, except for one, works, is that available? There's a lot of intricacies to it and-

Cameron Francis: But would it be to do purely with the server because everything else has got nothing to do with the actual hosting company itself?

Mark Culhane: Again, that depends on how valuable the asset is to you. At Security Shift, we manage some extremely high-value assets and, for example, government agencies say this is something that handles legal tender, we cannot allow that to go down. It doesn't matter if [crosstalk 01:01:33] That's the thing. If you've got the money to spend, then, for example, we have multiple honed routes to our site so if our ISP and three other ISPs go down-

Cameron Francis: But what was the ... Obama Health?

Mark Culhane: Yeah.

Cameron Francis: That went down. [crosstalk 01:01:53]

Mark Culhane: The Australian Census, that was a massive one. So the Australian Census was a huge disaster. They spent hundreds of millions of dollars setting up the census and telling everyone to do it, and then when everyone went to it, it was broken.

Cameron Francis: Yeah.

Mark Culhane: I guess the point that I would make there is that when you're seeking help, you need to go to someone with a good track record and who's reputable. Even the Australian Census, that was done by IBM and when they did the investigation on why all of that failed, most technical people would say it was remedial things.

Cameron Francis: Let's talk to Mr. and Mrs. business owner. Should they just be relying on the managed hosting company to just be on top of it?

Mark Culhane: If I-

Cameron Francis: Or would ... I think we use Pingdom.

Mark Culhane: Yeah, Pingdom's a good external monitor. You also want to have internal monitoring. So you wan to know if you're going to run out of disk space. You want to know if you're running out of resources on your server. There's huge amount of effort you can go to. Load balancing, Any cast/cost (?) connecting to your site. You can do so much stuff. And, again, it's that risk-based approach whereby you say, "This is how much this is worth to me. This is how much I'm willing to spend on doing it." Then, you need to find someone who is capable of saying, "All right. I understand this is how much it's worth. I understand this is how much you're willing to spend. Now I'm gonna put the most cost-effective controls in place to provide you with what you want for the money that you want to spend."

In general, you want to find someone, a company that's technically able to do that. There are a lot of companies that do it. Finding people that are capable of doing it is the hard part.

Cameron Francis: What would expect the cost to be? Don't give me the risk analysis.

Mark Culhane: You have to because for example, at Security Shift, we have clients that pay upwards of $60,000 a month for hosting versus people that pay $10 a month for hosting.

Cameron Francis: Yeah, but I think the people that spend $10 a month for hosting don't actually understand what they're paying for and they just see the dollar amount, right? I think that this is gonna help them understand if that goes down ... Hosting's not just hosting.

Mark Culhane: Yep. If people want someone like Security Shift, our business is really focused not so much on small to medium business. We do offer services for small to medium businesses, but at least we can provide ... If someone wants help and they say they need help, then you can contact us at accounts@securityshift.com and we will point you in the direction of someone that can provide you with the service that you're looking for. It might be us. It might be someone else.

Cameron Francis: This was really fun, man. I really loved it. Do you want to add some final words?

Mark Culhane: Yeah, I think we've gone through it all. Obviously, if you need some help, contact us at securityshift.com, but yeah, otherwise it's been fun.

Cameron Francis: And really, really good luck everyone. Everyone, this has really opened up my eyes on the email that Mark sent me from my accounts team, just opening my eyes up of the fact that your website can be hacked really easily, DDOS attacks, research it. Just look into it. Don't just rely on that $10 a month hosting account and thinking that you're safe because there's so much more variables to it. You've gotta think, how valuable is your online asset to your business?

Mark Culhane: Sorry. One more thing that I will say is to all the technical people that have been frustrated with me talking about the very basic exploits and vulnerabilities, strong recommendation to listen to the Risky.biz podcast, made out of Melbourne by Patrick Gray. It's one of the best podcasts I can recommend, so Risky.biz.

Cameron Francis: He's adorable. Thank you very much, Mark Culhane.

Mark Culhane: Cheers. Thank you.

Voiceover: Thanks for listening to the Digital Cowboys with Cameron Francis and Sam Roshan. Now, if you enjoyed today's episode, head on over to iTunes and give us a five star rating and please, write a review. Also, head on over to digitalcowboys.com.au, where we post the latest episodes and content pieces for all of our listeners. So saddle up and join us next time for another edition of the Digital Cowboys.