Current Cybersecurity and Insurance Issues with Jock Wols

Ben: Hey, while we wait, I thought I would just make myself available here. We've got another five minutes before we get started. Just make myself so if there are questions, I can go ahead and answer those. Thank you very much. I can get those answered. We can talk about anything. I can do a song, sing, and then that would force all of you to go elsewhere right there. But next step, we've got Jock Wols and it's going to be wonderful.

Ben: So, let's see here. Talitha asked a great question here. Can you update us on the DBA director? I did speak about this at the last update. Kirstin Reader, who is on here, she left us. It was very lame excuse, something about having nine kids, homeschooling, having a business, and then doing this job full time. I thought it was weak, but that's just Kirstin in all seriousness.

Ben: I love Kirstin. Love you. Yeah. We are, I don't want to say, directorless right now. Kelly and I are handling those duties for the foreseeable future. We will be hiring another executive director at some point. I don't know when that will be. We're going to let the opportunity come for us and not look for that. I think that we'll know. ZBA and BKX is my focus right now, like 80% of it. So excited about it and getting it to the next level, because we know that this is very, very needed, but great question there, Talitha.

Ben: You vote for a song. Yes. Yeah. Let's maybe since I don't drink at BKX, and you're not going to get a song out of me there. Anyway, I love seeing over here in the chat, everybody kind of just working back and forth and helping each other and exchanging emails. This is what this is all about, right? Having that community of people that you can connect with, people that have been there, done that, gotten the T-shirt. People that can help you, and you can help others. Right? This is going both ways right there.

Ben: David asked, "I was unable to find the directory on DBA, where people were looking for work, bookkeepers who don't want a business." So yeah, let me go right back over that, David, and I'll record and document this. So, if you go to the dashboard, everything starts with the dashboard. You go down here to the DBA roster and you click on that and you say, hey, only show members who are looking for work, and click Search Members. That is where you're going to find that. Now we just released this. I don't know how many people are on there. I see some people have already added. David, you already added your photo. Boom. I love it. I love it right there. I mean, just look at this. This is wonderful. I love how this looks and I love what you guys are doing, but that's exactly where you find it right there.

Ben: Okay? Again, we'll be refining this since this is something brand new. If you notice a bug in there... I won't say if. When you notice a bug in there, let me know what that is by sending us an email because a lot of this stuff, I go by the mantra that if you didn't have any problems when you launched, then you waited too long to launch. We temper that. Right? We want to do the best product that we can, but we get an iteration going and then we improve upon it, then we improve upon it. But that's where you find those there.

Ben: So, looking for work is the people looking to get hired? Yes, Randy. That's exactly right. Yep. Yep. That's exactly right. See how many bottles of water I can go through here today. Okay. We got about a minute and I'm going to go ahead and unmute. There we go.

Jock: There we go.

Ben: There we go. I got Jock. By the way, Jock is known as insurance nerd.

Jock: Thought I'd messed it up a little.

Ben: You should definitely get insurancenerd.com. Right? That should definitely be a part of your domain.

Jock: I think it's expensive for me right now, but eventually. I think that's a holy grail there.

Ben: Yeah, that's right.

Jock: Let me see. Let's see. Video. Do you want me to do the video or just...?

Ben: If you can. If you can do video, that would be great.

Jock: I'd be happy to. I'll probably share my screen too for the presentation.

Ben: Yeah. Yeah. I'm going to do the official introduction.

Jock: Wonderful.

Ben: I'm going to get up here we're going to fan flames here in just a second, and I'm not going to share my screen because I don't want to be doing all that. Right?

Jock: Sorry, Ben just wants... It says I cannot share my video because the host has stopped it.

Ben: Okay.

Jock: Which I do get a lot but...

Ben: Yep. I'll come back to that here in just a second and allow you to... In just a second, I'll make you the host. But one thing I want to do, so we are back. Okay? Hopefully everybody can hear me. You can hear me fine, Jock, right?

Jock: Yeah, absolutely.

Ben: Okay, great. I would love to introduce. So, Jock, I was introduced as I've been introduced to most people by the lovely Gabrielle Fontaine who will be joining us next. She is a great connector, a great person and just love her to death. But Jock, I was introduced to Jock by Gabrielle. He's the CEO and founder of RiskDesk, which is an insurance broker and technology company based out of Lexington, Kentucky. Go Wildcats, right?

Jock: That's right.

Ben: He partners with Nationwide. Okay? And so, he established the PT Pro Platform, which you can see, PTProcover.com to serve small all businesses' insurance needs. He has more than 15 years of experience helping professionals manage their risk by delivering market leading errors and emissions and professional liability and cyber liability insurance. Before he established RiskDesk in 2017, Jock managed the professional liability portfolio at XL Catlin and was based in London, New York and Lexington, three cities that always go together.

Ben: He graduated from Washington and Lee with a BS in 2004, obtained his MBA from New York University. In 2013, you can find out more of Jock or contact him at jock.wols@myriskdesk.com. This is also listed inside of your member benefits. Remember, it's a great value. But without further ado, I'm going to make Jock the presenter here and we're going to have a lot of fun. Let me just do this real quick. Take it away, Jock Wols.

Jock: Okay. Thanks for the introduction, Ben. Let me see. Okay. Hello everyone. Let me see if I can share my screen. So just bear with me for a second. All right. Can you see that, Ben? I apologize for that light in the background.

Ben: No. Yep. We can absolutely see it.

Jock: All right. Well, welcome. Thanks for the introduction, Ben. Welcome to the cyber presentation intended to cover cyber risk and insurance today. It's nice to see a lot of familiar faces and names. Hello to you Gabrielle, and I think I saw Randy and a couple others, Andre, Denise. Good to see everyone. With some of you I've probably spoken fairly recently, so some of the content may be a little redundant and repetitive, but the purpose today is to just reiterate that content and give you some insights into the cyber insurance market.

Jock: Just a short disclaimer, nothing in this presentation constitutes legal advice, coverage, interpretation, or insurance purchasing advice. Advice can only come after the establishment of a relationship; none is established by this presentation. Potential cyber liability to claims are fact and situation specific discussions to be had with your broker and/or attorney. We do not know your facts or personal situation.

Jock: The agenda today, just a rough outline, I'll cover the state of the cyber insurance market. I think that'll provide a lot of context to most of you. It's really important at the moment. The impact that the cyber insurance market has on the application process. I talk about coverage being critical constantly. So, we'll touch on that and give you a little background to how coverage has evolved over time, what the pitfalls are. Touch on some risk management items and then some potential trends.

Jock: Just a few housekeeping items, I'd like this to be interactive. And so, if you have any questions, I've got this Q and A box up here. There's also in the chat function. I'll check it out. So, feel free to interrupt me if I miss something or if something's not clear, that's completely fine. I've left quite a bit of time for some Q and A. So just fire away those questions.

Jock: Let's see. All right, the cyber insurance market. It's going through a massive change right now. It's solely driven by claims activity or adverse loss ratios that insurers are incurring. Just to put it into context, 2020 was the first unprofitable year for the cyber insurance market as a whole and 2021 at the halfway stage was worse than the whole of 2020. So, it's a difficult period. It's unpredictable, things are changing pretty rapidly. It's disruptive and there's really no end in sight for the insurance market.

Jock: So really what that means is that insurers are looking at their portfolios, they're re-underwriting their portfolios, and it has ripple effect for policy holders in a couple different ways. Most difficult thing to kind of stomach is the increase in premium. Premiums increases are ranging between 50 and 250%. It's not five or 10%. They're just skyrocketing. Coverage restrictions are being evaluated by insurers. They're looking at where the problematic coverage parts that we are providing insurance for. What's going on with those? Do we need to apply restrictions?

Jock: They're looking at heightened cybersecurity requirements. They're mandating certain best practices be implemented, and that can have two effects. One, it can make you eligible or ineligible for a quote, and it can also impact the premium. There're some other impacts that don't necessarily impact the small business segment as much. The first one is being your insurers are managing their severity exposure. Meaning how much limit do they offer to a particular policy holder? So, they're really cutting that down. In the past, you could get a... Some of my clients who have a 10 million or 20 million program, it's almost impossible to get an insurance commit $10 million in insurance coverage. So, you have to split it up over the multiple insurers, and the programs have to be structured.

Jock: Again, for small business, not such a big deal because those limit requirements aren't there, but it just shows you, it provides you some insight of what insurers are doing in terms of managing their capital. And then the other piece is the turnaround time. The demand has skyrocketed over the last 24 months. So, insurers are being inundated with applications. I'm marketing for my middle market clients where I know there's unpredictability, or there's going to be changes, marketing it to a number of different insurers.

Jock: It just has a big impact on what you can expect from the insurers. And then lastly, and it's something that we've been impacted by is some insurers have exited the market due to unsustainable losses. Our preferred insurance provider, HDI, they withdrew from the market effective January 1st. They lost their reinsurance partner. They claimed their losses were unsustainable. So, that basically means, okay, what do we do? My role is to find a replacement carrier and tap into my network of insurers that can serve the segments who we work with.

Jock: Yeah, so it's disruptive. It's bit of the Wild West out there right now. Like I said, over the short term, the cyber threats themselves aren't... I just don't see them receding. I don't see the insurance market changing any time soon. How that impacts you from an insurance perspective or an application perspective, there's a couple different things to consider. Regardless whether you're an existing cyber insurance buyer or a new buyer, the key word of advice that I can provide to you is just give yourself time, engage in the insurance application process early, give yourself time to evaluate the application. The application will have changed, most likely have changed. There's new questions and they'll look. You need to answer those questions, think about those questions and how they apply to your own business.

Jock: Taking a proactive approach certainly helps. Again, in the small business segment, it is maybe a little easier in the sense that you maybe don't have that limit constraint or the turnaround time issue. With our partner, we can still generate a quote almost instantaneously or within the same business day. The biggest takeaway from giving yourself time is that if there are application questions that you respond to negatively or viewed negatively, then you want to give yourself time to look at those questions and potentially make some changes to get a positive response to those questions.

Jock: It allows you to make those implementations. Again, for small business, these questions aren't necessarily complicated or bad or unsolvable, but you just want to make sure that you have an opportunity to assess them. I think I saw someone raise their hand.

Ben: Jock, I'll moderate the questions over here for you.

Jock: Okay. Awesome. Yeah. So, Ben, if someone's got a question, just interrupt.

Ben: Yep. I got it. I gotcha. You can focus on your presentation.

Jock: Okay, good.

Ben: I'll break in if necessary.

Jock: Good stuff.

Ben: Thank you.

Jock: So, two things that we can learn from the insurance application or the renewal process inside an insurance market. One is, hey, these questions that the insurers are asking us or asking the applicant of... They're basically telling us, there's correlations with these responses in the performance of our portfolios. So, they say, if you respond negatively to not doing training or educating yourself in cybersecurity, the likelihood of you being a worse risk than the norm is higher. The likelihood of you having a claim is higher.

Jock: So, we can gain some insights in what the key areas of concern are that insurers are having, and then apply them to our own business and then allow us to make those changes. The other piece, which I've talked about its managing expectations, is the premium is going to go up on a like for like basis. If you renew the exact same program, it's most likely going to go up. So, keep that in the back of your mind and manage that, when your policy comes up for renewal in several months' time or whenever it is. So, from an insurance application perspective, give yourself time, start early, evaluate your options and take it from there.

Jock: Coverage is, like I mentioned, I talk about pretty frequently and unlike general liability or other products, cyber insurance is more complicated and it's more complicated because there's a lack of standardization with those coverage solutions. It's a newer product and the threats have continued to evolve over a period of time. And so, insurers have had to respond to those threats to make sure that the different coverage parts are up to date. Let me just take a little.

Jock: So, with that, and I've shared that with those of you who I've been on the phone with. You know, I kind of wind back to about 10 years ago where the typical type of cyber-attack or cyber security incident represented a data breach, and then that data breach or that hacking event led that business to lose information. As a result of that loss of information, it incurred expenses related to credit monitoring, notification, IT forensic expenses, business interruption costs, et cetera, et cetera. So, what businesses did from a very high-level perspective to assess the cyber risk profile, they'd say, do I operate in an industry with big target on its back? Think financial services, healthcare, the public sector, et cetera. And what's the information that I carry? Is it sensitive information? Is it social security numbers, credit card information, name, addresses, financial records, confidential information, et cetera, et cetera? How much of that do I have?

Jock: So, what's happened more recently over the last couple years, over the last three, four, five years, which has really changed the demand of cyber insurance and increased businesses, which businesses are at risk or targeted is that the threats have evolved. So, things like ransomware or social engineering fraud have become increasingly popular with cyber criminals. If you think about what ransomware does, it locks your system, locks your hardware, your software. It renders you inoperable. Basically, you get that black screen and it says, send X amount of Bitcoin to this account, and we'll send you the decryption key. It's added this operational type of risk to cyber risk where it doesn't really matter how much information you have or whether the information is sensitive, or it's almost industry agnostic in the sense that if you are handcuffed and you can't serve your clients or your customers, or you can't work with your partners, you've got a problem. You prevent it from doing business.

Jock: That's really filtered down to smaller businesses, too. And often smaller businesses are viewed as an easier target because of the lack of resource dedicated towards cybersecurity. But where it's important from an... Where the complexity resides from an insurance perspective is that insurance solutions that don't address those threats or explicitly provide coverage for ransomware or social engineering fraud, you don't have coverage for that. So, the most guilty of those solutions tend to be the bundled options. I'll pick on ourselves because we have a bundled option with Nationwide, which we just don't use. When Nationwide says, hey, here's the E&O, and we are throwing the cyber. Five years ago, we designed this product with Nationwide, most insurers were offering this type of basic cyber coverage. It basically just covers you for that data breach or that hacking event, and the expenses associated with it. No word on ransomware or cyber, no word on ransomware or wire transfer fraud, or social engineering fraud, or business interruption, et cetera, et cetera.

Jock: By the way, that solution is for free. If an insurer charges a couple dollars for it, that in itself is a red flag. So really from an assessment perspective, make sure that the insurance solution that you're looking at does cover you for ransomware, social engineering fraud, wire transfer fraud. In basic terms, bundled equals bad and standalone equals good. Again, not all standalone solutions are good. I've got issues with several of those, but that's the starting point. Really how I think about those bundled solutions is I use a homeowner's insurance as an analogy where those bundled solutions, they tend to cover you for the ground floor. They don't say they don't cover you for the basement, for the roof, for the second floor, for your garage or your back house. It's just coverage for the ground floor. It's pretty limited.

Jock: The biggest difference is when someone engages in or secures one of those options, they think they're covered for their entire property. They think they've got coverage for the roof or the garage or the back house. There's almost like a lack of education in the purchasing decision, which is where I come in and try to help DBA and bookkeepers.com and et cetera to make better purchasing decisions. But yeah, so from a coverage perspective, again, think, be critical about the coverage and ask your broker or your insurer, hey, is ransomware covered? Is social engineering fraud covered? Is wire transfer fraud covered? If not, then you know you've probably got a pretty limited option available.

Jock: Before I go into the different areas of concern that insurers have, you think about risk management and risk management strategy from a high-level perspective, and there's a couple different pillars to address. Six months ago, some of you would have come to me and say, "Hey, I want an insurance solution." And the insurer would've said, "Hey, what's your name and address? And here it is." Now, we're going a little backwards in the sense that the insurers are being reactive to... They're taking a reactive position to their portfolios because of the claim’s activity, but they're doing something they should have done in the beginning anyway, basically ask questions about cybersecurity.

Jock: So, if there is any kind of benefit through the changing insurance market is that these changes over a period of time will just elevate and elevate businesses' cybersecurity best practices as a whole. So, with the insurers saying, "Hey, you need to develop a general awareness. You need to be educated around cyber risk." That's not a bad thing. You need to, "Hey, here's certain best practices that you need to adopt. That's not bad thing. For your business, that's a good thing. You can use that and use those enhanced security pieces or cybersecurity and knowledge and content that then you can communicate to your clients in an elevated trust position. The insurance piece comes at the very end and insurance is saying, hey, you can't just skip the line right now. Again, not necessarily a bad thing. Bad thing is that we're paying a penalty for the lack, for the poor underwriting decisions that they've made over the last couple years.

Jock: There are several, probably four or five items that I want to kind of pick on that one, we've seen some activity on within the bookkeeping community, and then also some insights that I can share with you from the middle market and larger clients’ sector. Social engineering fraud is a big issue right now, and for those of you who don't know what that is, it's deceptive communication that triggers where the cyber-criminal tries to get, tries to trigger a certain action from their target. It's also referred to as phishing or whaling, or the most recent one is smishing is basically you get these communications via text message. And insurers, there's a big concern about it. One, the paying of claims for that. It's one of the coverage parts that is actively targeted by insurers to cap their exposure, but really what the cyber criminals are doing is they're trying to prey on human errors.

Jock: So basically, trick someone into taking that certain action. And so, they prey on emotion. There's a sense of urgency usually with this communication, and often it comes from a level of authority that then tricks that individual to bypass certain processes or certain actions that they would usually take. The most common result is either downloading or deploying a virus or malware onto a system or onto your hardware. So, think of a ransomware, or make a change or an amendment, or add bank information into a certain system, like a payroll system or wire money to a bank account that the requester is pitching.

Jock: I had a conversation with a bookkeeper a couple months ago, and she was victim of one of these incidents, and really what happened to her is she received an email from an employee at one of the clients saying, "Hey, you're processing payroll on Friday. I just got a new bank account, please update the bank account information to so and so." So, she went into the payroll system, updated the bank account information, payroll was processed, and a couple days later she received an email from the employee saying, "Hey, I didn't get my paycheck." She said, "Oh, it's gone to your new bank account." "Well, I don't have a new bank account." Okay. That's a problem. So then by the time they figured it out and tried to recover the funds. It was too late. They were long gone.

Jock: So, from a risk management perspective and this has nothing to do with intelligence or sophistication. The cyber criminals are specifically targeting emotions and trying to trick you into taking a certain action. When you kind of slow it down and say, "Well, this email came electronically, oh, I should have hovered over the email. Okay, what's the address? It said Gmail. The name is misspelled or something like that, or there's spelling errors in the body. When you slow down, of course, you're not going to just change some bank account information, but when they're taking advantage of you and you're trying to do but right by your customer, and they say, "Hey, you need to get this in as soon as possible," and maybe something's going on at home or what, you just take that action.

Jock: So, what insurers are looking at from a risk management perspective is what verification processes do you have in place? Really the highest level of verification is by phone call. Even in the absence of securing an insurance policy, I implement a verification procedure for your business. It doesn't matter if it's only you, it doesn't matter if you've got employees, it doesn't matter if you use one subcontractor or 10 subcontractors, put this stuff, think about it deliberately, put it down as part of your processes and procedures. And in the event that you do get communication electronically or by email, which says, please wire money here, or even if you don't wire money, make sure you respond to the request via phone call and say, "Hey, I've got this email from you. Just want to make sure that this is a legitimate request."

Jock: I cannot stress from a risk management perspective how critical that process and procedure is. From an insurance perspective, insurers are asking, do you have these procedures in place? Okay. Well, what does that mean? What's the ripple effect of you saying no to those? Well, if you don't have those procedures in place, firstly, they're not going to offer you the coverage. And secondly, it is a condition of the policy that you do go through that verification process to make sure that these requests are legitimate.

Jock: Social engineering fraud, a big issue. Part of it is also just developing a general awareness that these threats do exist, which I'll talk about when I come into the training piece or the education piece. It is the most prominent case, involves a mid-size company where the CFO wired money to a vendor. And basically, the communication got intercepted, and that went to trial and the litigation went to trial. It doesn't matter whether you've got a Harvard degree or you're running your own practice, it's irrelevant. It could happen to anyone. So, it makes one of the key threats that you are probably faced with from a cybersecurity perspective.

Jock: Remote access is another key driver of cyber claims and where cyber criminals try to exploit vulnerability through remote systems. It basically allows an employee or user or a subcontractor to log in remotely without adequate security. So, for a small business, you may not have a system that you subcontract to others, or you may just operate independently. So, you may not have a system that others log into, but really what's hard to think about this requirement is, hey, when you access systems, and if you do give someone access to a system, what are your security procedures around that? Think about it also from a client's or employee's perspective. There's this principle of least privilege. Basically, that applies to systems and passwords.

Jock: Basically, does someone really need access to a system? What's the least amount of access you can grant them, or your client can grant you? With some of you I've spoken to, some of you told me that, hey, your client said, hey, here's my bank account, user name and password, just go log in there. And the responses that you've given in those conversations, you're like, "Hey, I don't want that. What can I do?" There's an opportunity to coach the client and flip it around and say, "Hey, there's a security vulnerability here, if you email me your password and your email," which sort of blows my mind, that it still happens in today's age, but some of you have experienced that. Just don't do that.

Jock: You want to reduce your own cyber exposure or your cyber vulnerability, having that, and it's obviously not coming from you, you're not doing it, but having access to that exposes your client to flip it around and tell them, "Hey, don't do that." If you're logging into systems and you have access to certain systems, try to... You know, with the bank accounts, sometimes they give you read only access, which is sufficient. You want to have a limited amount of privilege and access to those tools and services or platforms that you need to do your job, enable multifactor authentication. When they say, hey, can we enable it? Don't opt out, opt in. It protects you, and it just adds another layer of protection.

Jock: Remote desktop protocol. That's a Windows feature. It allows someone to log in to control the Windows machine remotely as if they were working on it locally. Probably not a big issue or probably not a big thing here, but maybe if your client allows you to do that, think about that twice. You want to have that security component, multifactor authentication enabled with that. RDP is one of the items that insurers are looking at and very concerned about.

Jock: Let's see. So, the backup of data is the next piece. The backup data doesn't necessarily prevent a cyber-attack, but what it does do, it helps provide you with leverage or options in the event that you are the victim of a cyber-attack. For example, a ransomware attack, if you are a victim of ransomware attack and you have your data backed up, if you don't have an insurance policy in place, you can just boot it up and try to gain access to that information. If you do have an insurance policy in place, it gives you an option to negotiate with the cyber criminals and say, "Hey, I'm not going to pay $10,000 in the ransom demand, but we may pay a thousand dollars" or something like that.

Jock: So being able to access your information is critical in terms of minimizing the disruption that you would have or that you have when you have suffered a cyber security attack. You know, cybersecurity consultants are the ones who I work with. They have this 3-2-1 Backup Strategy, which basically recommends...

basically means there's three copies of the data, two different medias, and one stored off site. Again, my recommendation is not to say, hey, you need a 3-2-1 Backup Strategy. What you need to do is just think of the backup of data from a high-level perspective and think of like, okay, how can you back up your data?

Jock: Now, if you do go down that route, that's ideal, but also realize and know that you may not have the resources, or it may not be practical to do that, but as long as you think about the backup of information, the backup of data, and in the event that you can't access your systems, run the stress test. Okay, you don't have your laptop, or you can't access your files. Okay. What do you do next? Your computer crashes. It doesn't even have to be a cyber thing. How would you get that information and how would you get back up and running? So just think about it and think about what solution would work for you.

Jock: Encryption is something that insurers are asking for more frequently, and there's different types of data that can be impacted for small businesses, where we have seen the encryption question come up is for data and transit, basically communicating sensitive data and whether that communication is encrypted. So, if you are emailing your sensitive information to, and then the term sensitive information can be fairly broad, but it usually refers to PII, which stands for personal identifiable information or PHI, public health information, personal health information, and there's a couple other things, but if you are emailing sensitive information, use encryption functions that I think both Microsoft and Gmail and other email providers have. If you shared documentation or data, try to use software, Hubdoc is often referred to within the bookkeeping community.

Jock: I think, Ben, correct me if I'm wrong. I think Keeper also has that kind of functionality, but you try to adopt a consistent approach that you then share with your clients in terms of the communication of information. There's certain clients and they will always respond with an email and say, hey, here's my social security number for my, and I'm just making stuff up, for my tax return or whatever, but it's like, no, don't do that. As long as it doesn't come from you, you're mitigating your risk. Or if you make that communication through one of these portals or software tools, then again, it doesn't eliminate the exposure, but it significantly reduces it.

Jock: Data at rest just refers to a data that's collected in one place. It's often a target or targeted by cyber criminals, because it doesn't move around. Within the small business community or small businesses, it hasn't... You know, insurance isn't requiring that that data at rest is encrypted. And so, if you think about your Google Drive or Dropbox, those tools offer a form of encryption. I'm sort of skeptical in the sense of like, okay, well maybe the information is encrypted, but what if someone accesses your system and then it bypasses the encryption piece? They can still extract that information. They can't break and force their way in, but if they are in your system, then what does that mean in terms of extracting that information? Data at rest is something that medium and large businesses are constantly asked by insurers. Some insurers are saying, hey, if you don't encrypt your data at rest, you're ineligible for a quote.

Jock: Again, it's not applicable to the small business segment right now, but it's something that we've noticed happening more frequently in the insurance markets. So maybe that's a potential trend that's going to come. I've spoken with some of you in terms of the data and document sharing guidelines that you share with your clients. Some clients comply, others just don't care, or they just don't get it, or part of least resistance for them. They don't want to access the tool, but adopt a consistent approach and again, communicate the value and elevate your own trust level with them in terms of your focus on cyber security.

Jock: Training and education. Believe it or not, most insurers, if you say, "Hey, I'm not committed to education or cybersecurity training," you wouldn't be eligible for quotes. That's a pretty negative signal that they view because that's indicative of the rest of your organization. They want to see, hey, you are engaged, and the training is... The thing I always laugh about the training question, it doesn't set a minimum standard or benchmark of like, you need to do X amount of training or X amount of hours per month or per year or per quarter, whatever it is. But what they want to accomplish is there's a commitment and things like sitting in on a webinar. Okay, that arguably constitutes training or education around it. So, you're developing this general awareness. And especially it circles back around to that social engineering fraud exposure, where the training is often heavily geared towards social engineering fraud.

Jock: Hey, don't click on an email. If you hover over the email address, you can see, is it a completely random email? Try to identify those tricks which say, "Hey, download this invoice." And that then lets you download or deploying a ransomware or the malware. So again, from an insurance perspective, it is a mandatory requirement. Keepers.com has got a great cost created by Gabrielle. Insurance vendors or insurance providers or insurers are starting to provide content, too. With our preferred insurer, they offer access to training and content. So yeah, it's something to certainly pay attention to and continue to educate yourself. And again, these threats are going to continue to evolve and change. You know, what was a big issue maybe 12 months ago, it's going to be supplanted by something else. So constantly being up to date with what the cyber security exposure are is important.

Jock: In terms of the trends that we can potentially see, premium, I just don't see the premium changing anytime soon in terms of the market softening. Partly, partly what's going to drive that is cyber threats or cyber risk today is very different to what it was 24 months ago. Ransomware payments are significantly higher. The volume of a tax is significantly more frequent. So, over the short term, until these risk management and cyber security best practices start to kick in, I don't really see much of a change in that, but that's just something.

Jock: Again, that's where the insurance market hopefully kind of kicks in as portfolios start to mature and certain insurers start to benefit from better portfolios. Hopefully, that'll over time will lead them to often more competitive terms. The other piece, what I've seen with insurers is they're starting to integrate into cybersecurity or other software vendors right now, and the purpose or the objective there is, hey, if you use a tool or a risk management solution or some cyber security solution, then that makes you a better or protect you and reduces your risk.

Jock: Right now, what insurers are saying is, "Hey, that's sort of like a minimum that we're looking at." They're not offering, I don't know, a premium discount on that. Over time that will hopefully change as those, if they can identify correlations with that yield to a better performing portfolio, but giving access to their policy holders to, I mean like cowbell with the training, that's the certain things that the continuing products notice are that they're building out.

Jock: When it comes to social engineering fraud, obviously the requirements is around the processes and procedures that you currently have in place within middle market and my larger clients. In some case, some insurers will say, "Hey, we've got a requirement around phishing simulations." What does that mean? It's like there's emails that get sent to the employees at the organization any vendor or partner, which says, "Hey, click here, and then they test the response to those simulated phishing attacks. And then those responses get filtered back to management, "Hey, 5% of your workforce opened this particular email. You need to drop those numbers. You need to commit and then that again kind of goes through to the education point. Right now, it doesn't seem like it's going to filter down to the small business sector, but it's something that, again, we'll just going to notice happening and occurring and increasing in frequency amongst the middle market sector.

Jock: Multifactor authentication, it's also referred as two-factor authentication. There's already some suggestion that hackers are trying to crack those codes. Does that mean, "Okay, we're heading down to a triple-factor authentication?" I don't know, but that's something to keep an eye on. I don't think that's going to happen anytime soon, but these things also do change pretty quickly.

Jock: Zero trust security is security framework that requires all users to be authenticated and authorized or continuously have validated. So, I think about it, it's like multifactor authentication, but if someone wants to use a particular system or platform is, if that username has been set up or that user has been set up six months ago, are those credentials still valid? Insurers are starting to look at that and how can they apply that, or is that a requirement that they have of organizations. Again, more impactful on mid-size to larger organizations, where there are lots of different systems and lots of different parts of organization that talk to each other or interact with each other and keeping that segregated. And then I mentioned the data at rest piece and the backup of data.

Jock: From an insurance benchmarking perspective, the premiums that we offer through Cowbell, they tend to range between 300 and $1,200 from a hundred thousand to a million-dollar limit. And the average premium of the bookkeeping policy holders is roughly $533. In terms of, and sort of enjoy looking at this graphic or this graph. It shows the average revenues generated by the bookkeeping policy holders across the different limit tiers, and clearly there's a progression in terms of the average revenues. Roughly goes 25 to 40 to, I think it's 60 or 70 to 100,000. Again, with insurance, with the purchasing decisions, they're heavily influenced by, okay, well, how much does it cost? What's my budget? What's my risk tolerance level?

Jock: The nice thing about the hundred thousand with premiums increasing, the $100,000 limit option does allow us to give a very robust coverage solution at a lower premium. So, businesses that are starting out or practices that are starting out can have access to a market leading insurance solution, and then graduate towards that next limit of liability as their business grows and as they see success. I mean, that's pretty much it from my perspective. If you want to reach out to me, I've spoken to many of you, feel free to just give me a call or send me an email. Set up a meeting. Happy to discuss. If you've got an insurance policy in place, then I'll try to weigh in an objective.

Jock: If it's a good solution, I'll tell you if it's a good solution. The key objective on my end is yes, offering an insurance policy is one part of it, but also when it comes to cyber insurance, there a lot there. I think with the range of insurance solutions, it gets complicated. Even when certain kind of coverage parts are covered, you got to look at exclusions. It can be a little confusing, but again...

Jock: How are we on time, Ben? Let me see. Okay. We've got 15 minutes. Do we have any questions?

Ben: Yeah, we do. We do have some questions here. I'm going to take back being the... I'm going to reclaim host.

Jock: Go for it.

Ben: I am now reclaiming my host. Okay. Great presentation, Jock. Thank you for scaring the crap out of us. We appreciate it always.

Jock: Yeah, -

Ben: But you know, as part of being a digital bookkeeping professional, this is very, very applicable, right? It's probably as applicable if not more so than errors and omissions of insurance, and we know how important that is. So, thank you for opening our eyes. This is not the sexiest of topics that we want to talk about, but it's certainly one of those that we need to talk about. We do have some questions and I am going to ask those and just let you...

Jock: Yeah.

Ben: All right. If we currently have our insurance with you, so I know a lot of people here do, will you send us the info ahead of our renewal, or do we need to contact you for the extra time to make changes if needed?

Jock: Yeah. With this new partner, we've kind of gone through the integration process over the last, I think it's started in September and October, where we looked at a bunch of different insurance vendors. Now we're settled on one. I'm a little backed up in terms of reaching out to you. I will reach out to you. So don't worry on that. The good thing is that in terms of the actual coverage, we're pretty much set. And the responses so far with the bookkeeping community, most of those procedures, there's about eight questions that they'll ask a couple of which are pretty basic.

Jock: We haven't had any kind of pushback or resistance that would prevent them from offering a quote option. So, if you're on my list over the next couple weeks, just look out for an email from me. So yes. Yes, to Renee.

Ben: Okay. Also, I think you covered this, but do you have any suggestions on specific training for our remote team members?

Jock: Yeah, so I believe the Cowbell solution that we access provides access to employees or other users, which you can integrate. That insurance solution, I think, and I'll get back to you guys on that, but I think it does allow the policy holder to delegate access. Let me just jot that down as a takeaway, Ben, and I'll...

Ben: Okay.

Jock: I mean, in Gabrielle's course, which Gabrielle and I, as mentioned, we've had a longstanding relationship. And so, I've been involved, provided feedback on her course over the years, and I feel like that's been well received amongst the bookkeeping community and it's some very high standards. So, a very bookkeeping specific course is great. I don't know how you've kind of set it up in terms of @bookkeepers.com where the...

Ben: Yeah. It's on bookkeepers.com. It's in our courses there. Yeah, that's great. Okay. I think we answered this one. Can we get an idea of the premium? So, you saw Jock had that, it was average, or sorry, from 300 to 1,200, I believe the average was 533 on that. I can tell you that probably in a couple years' time, it'll be double or triple that. I mean, that's just one of those things. I don't, like you said, see that rate going down, but it's just a cost of doing business and something that we factor into the rates that we charge to our clients.

Jock: Yeah. I mean, exactly. So, you can pass it on to your clients if possible. Like I said, the nice thing about this carrier who we're working with, they do offer us a lower limit option. So, it doesn't compromise on coverage, and it provides you with an entry level option that you can then grow with over time as your business scales up.

Ben: Yeah, absolutely. And then Wendy says, "Our premium is on a yearly basis. So, the premium, I think, amount, do you pay that all up front? Can you pay monthly? What's the deal on that?"

Jock: I think Cowbell does have a monthly option, but I believe there is a finance charge associated with that. They just finance the premium with the finance company. If that helps, then great. If you like me and you don't like paying finance companies a finance charge and you're not forced to do it upfront. I think that premium level starts at $500. The one restriction which I do have, which I know, which I bumped into recently is in Connecticut, Hawaii, and I think it was Vermont, they're waiting for approval from the insurer. So, it's just a matter of time for that. They have options, but those options are just premium wise, they're just not fit. It starts with like $2,000. It just doesn't make sense if you...

Ben: Gotcha. Yeah. A couple of just comments right here. Katie Says, "Jock has been so helpful and I really appreciate all his help this last month, as I changed E and O and a new cyber insurance plan, too." So, there is a kudo for you right there. Mindy says, "While listening to you, my best friend just told me someone hacked her email and many accounts and bought a $2,000 laptop on Amazon." Very unfortunate, but that happens all the time. Very sad. Let's see. There was a question right here. Basically, you ever hear about any of these thugs getting arrested and put in the big house for what they do?

Jock: Yeah. I mean, one of the prominent ransomware gangs, the REvil group, there were some arrests and many of these, I think 75% of the ransom payments go to gangs in Russia, but that gang closed shop. I think it was in the press maybe two, three months ago that there were some arrests that have been made. It's not going to change cybersecurity or the threat level, but I think as governments start to step in, and personally, I think cryptocurrency is a big enabler for these cyber criminals to accessing and trade highly efficiently. So, until that, I don't know if regulation needs to be put in place, but cryptocurrency basically is a haven for criminals in general. I think as cyber security and cyber threats continue to be an issue; governments will start paying attention to that a little more.

Ben: Yeah. Denise says, "Thanks for taking great care of my insurance needs. Just added cyber awesome there." Yeah. So, Jock's contact information. You can also find inside of the member benefits page. His contact information is on there, and of course he shared it here as well. So, you can reach out to him. If you have specific questions, you want to get a quote on your insurance, it's a great value. When we were looking at adding this, we were looking for not the cheapest provider, right? A discount's great, but having a valuable product or having a product that has good coverage and Jock can help you navigate those waters. He's been really invaluable in helping our members, whether or not they buy insurance through you.

Jock: It doesn't matter. Yeah. That doesn't matter. So...

Ben: Right, right. Like the guy that's over your shoulder there, he's about to come buy some insurance from you right there. Yeah.

Jock: Yeah. This guy there, so...

Ben: Yeah, yeah. Yeah, he's looking to buy some insurance.

Jock: In the office, so...

Ben: Yeah, exactly. So yeah, this has been great, Jock, and we appreciate it. Again, everybody, if you have questions on your insurance, please reach out to Jock. It is not a simple... It's kind of like answering legal questions. There is always a it depends, and it bases on the facts and circumstances of each individual situation. This is a moving target that is going at cheetah speed, not at turtle speed. It's changed, like Jock mentioned, over the last six months, radically with people getting out of this industry because it's just so vulnerable right now. So, the key takeaway here is to do everything that you can to mitigate that risk, but also to have yourself covered in case something happens.

Jock: Ben, I had an insurer of one of my who serves my law firm clients come and say, "Hey, here's a notification. We're making changes to our portfolio. And this is going to be the impact." They sent that communication on Monday. On Friday, they said, "Hey, hang on. We're going to make actually these changes." And then the following Friday, they said, "Hey, we're going to make some further change." It's just mind blowing in the sense that it's like, okay, well, you didn't know. It's like, well, actually something changed this weekend. You know, management made this decision and then the following weekend, oh, they made another. I've never really experienced anything like that in the insurance industry, but it's pretty wild right now.

Ben: Yeah. Well, Jock, thank you so much, and I appreciate everything that you do.

Jock: Thank you. Thanks for having me.

Ben: Yeah. Thanks for being here. Okay. It is 1:54 in the Eastern standard time, and next up is going to be the one, the only Gabrielle Fontaine. We are going to take a five-minute break and come back at the top of the hour, but first real quick, Gabrielle, are you there? And can you hear me?

Gabrielle: Yes, I'm here and I can hear you.

Ben: Awesome. Okay. Well, here's what we're going to do. We're going to take a five-minute break, come back, and then you're just going to drop some wonderful knowledge on everybody here, and we will be back.