Turning Operational Crisis into Opportunity: Crisis Management Tips

Effective navigation can transform crises into game-changing opportunities. VirtualDOO's Lloyd Thompson shares his best crisis management tips.

James Schramko and Lloyd Thompson

James: James Schramko here. Welcome back to my podcast. This is episode 1013. Today, we're talking about crisis, operational crisis. And maybe it's happened in your business. I've brought along my special guest, friend, partner, Lloyd Thompson from VirtualDOO.com. Hello, Lloyd.

Lloyd: Hi, James. Thanks for having me.

James: You're a funny chap, aren't you? You've decided to gravitate towards the operational part of the business, which, of course, can be a bit messy from time to time. So we're going to talk about crisis. I guess not all businesses are running along smoothly at all times. Is that true?

Lloyd: That's true. I mean, unexpected things happen. And it's really how people deal with these things that makes a difference. Some people will remain permanently in the emergency department. And some people have a process for dealing with crisis.

James: So given that it's going to happen from time to time, in most businesses, it would be good to have a crisis management plan in place, or to have some tools in our toolkit that can help us. And I've seen this, of course. I used to run Mercedes-Benz dealerships, doing tens of millions of dollars a year. One was doing about $50 million, one was doing around $100 million, with its combined repair shop. And boy, were there some crises.

If you have people, or you have customers, or you have landlords, or you have stock, or the market changes, or there's a pandemic, there's a very good chance you're going to have a crisis. So let's talk about how we can turn that crisis into opportunity. We've seen that saying about, you know, a lot of wealth is made in the downtime. Some people seem particularly good at operating around this changing situation, or recognizing that this is a growth opportunity. So I imagine there's some mental side to this as well.

How would you define a crisis?

Lloyd: Yeah, let's maybe start by talking about what a crisis is.

James: Okay.

Lloyd: You mentioned a few things there. And I would say there's an overlap between what someone would call a crisis, and if you know tech people, they might refer to as a major incident, and there's a lot of overlap there.

James: I've heard another one that starts with cluster and the second word starts with F.

Lloyd: Like, a well-known brand, French Connection. [laughs]

James: Exactly.

Lloyd: Yeah, one of those, that's another way to define it. I like it. It could be something like a natural disaster, flooding, or storms, or power outages.

James: Loss of internet.

Lloyd: For those folks who have remote teams, I'd say, you know, things in the Philippines in particular, and I've got a great team in the Philippines, they're more seem to be more prone to bad weather and flooding and power outages. So it's good to be able to plan for that.

James: I've got just a note on that, too. A lot of them can get Starlink now.

Lloyd: Yeah. Right.

James: So that's been a game changer of recent times, compared to five years ago, or 10 years ago, when I was starting out there, there are more options for people.

Lloyd: Yeah, and I mean, that's certainly one of the ways that you could plan to resolve such things. So yes, Starlink. It could be about financial failure, a surprising cash flow incident like we saw in the US recently with SVB bank, you know, what would the impact be on your business?

James: I had a very close experience with the Signature Bank one as well. Like, you just never know, you can have these things pop out of the blue. But then what you do when it happens is an interesting one.

The topic of security

What about security breaches, hacks, data privacy, all that stuff?

Lloyd: Security is huge. And that's definitely right up there. In fact, only yesterday, I heard a stat from a friend of mine who works at Amazon, and he said, Australia is hacked 24 more times than any other country. So you want to have a plan for that.

James: I thought we were the lucky country.

Lloyd: [laughs] Lucky if you've not been hacked so far by the sounds of things. So that cybersecurity is definitely something you want to be thinking about.

James: I know you came from working with banks, Lloyd. Is that something you help people with as well, this highly technical stuff?

Lloyd: Yeah, certainly for small to medium businesses. They're not really thinking about this very often. But there are some basic things you can do. And I can help them with that for sure. So just simple things like, what are you doing to back up? And how would you actually restore from a backup? And how would you manage your passwords? So yeah, that's an area that we will look into for sure.

James: Two-factor authentication across the board, etc. I hope that's on your checklist.

Does it impact your reputation?

Lloyd: It is. And other things, just while we're onto the major list of sort of common crisis management items, another one is reputation. Like, if it impacts your reputation, and your reputation is now dirt, that's really going to affect your ability to trade, and thinking of a really well-known example was Volkswagen. Like Volkswagen, they cheated their emissions test, or they were found to have had some software that gamed how the emissions were being shown.

James: Were they diesels, turbo diesels?

Lloyd: They're turbo diesels. And how are they going to get out of that? So that was a crisis for their business. And of course, what we normally think about or what most businesses think about when it's a crisis, more often than not, it might be tech-related. But I just wanted to give you a complete picture of what a crisis really is. It's not just going to be something impacting your e-commerce website, or whatever, it can be all manner of things.

James: Now, it's really useful to say that. I mean, I have strong foundations in this, I love ideas of redundancy, backups. I try and hedge against negative things happening in the future. I have filters and checklists in place. But even then, you still get unexpected crises, like for example, the Signature Bank, I did have some money in that. And luckily, they sent it back, which is great.

But you know, when you wake up and see that it's collapsed, or whatever, your first thought is, oh, is that gone? But then my second thought is, well, even if that happens, it won't wipe me out, because I've got plenty of assets elsewhere, which is part of my hedging strategy, right? The other thing you mentioned is such a big thing these days, the reputation thing, and whatever, these days of social media, and people even, we're moving into an era where it's possible to do deep fakes quite convincingly.

We are definitely more exposed to that than ever before. And it's very hard to protect yourself from that. I actually recently, it's very rare, maybe once a year, I encounter a customer who might be really angry, or really upset. And usually, it's about their life in general. Something, maybe they have a bad relationship with their partner, maybe they are frustrated that they're getting older but not succeeding, maybe they get so upset that they don't implement or whatever. Sometimes they want to take out their heat on the person trying to help them.

But these days, they can threaten to make reviews, or to go out there and spread lies. But even lies can get perpetuated, and it's still no benefit. Even if it's not true, these days, I think, one way that I would hope you can protect yourself from that might be to be very, very careful who you actually select to work with you. To only choose clients who are a good fit, to be very quick to recognize when someone's not mentally well.

And they say up to a third of the population is suffering some kind of mental illness, that's pretty high stat. And when you get pressure, put on the whole population or financial pressure, like interest rate rises or inflation, people start to get angry and scared. And they seem to be very emotional, and not so logical. So I'm very interested to hear from you.

Where a director of operations comes in

Clearly, it's important to have crisis management. Where do you fit into this as the Director of Operations? You're seeing the direct impact on a business with this because you're doing the people and systems side of it, and in systems is security and so forth. But the people and systems side is going to be covering the whole business from the visionary right through to the team who are deploying the work. Well, what's your role in all of this?

Lloyd: So what you were saying about social media is really interesting, because the speed of response to a crisis is really important. In fact, briefly going back to what we were talking about security, or cybersecurity issues, I was hearing only yesterday that in Australia, if a company is hacked, a listed company, they've got 30 days to report it to the government.

There's a paper out, which is going to give them 72 hours. At the moment they can spend all the time they want getting ready. Well, how are we going to report this? What are we going to - Oh, it's not so bad. But now they're going to have 72 hours, they need to be on it and fast. So the speed to response, whether it's social media reputation, or cybersecurity is super important.

And the problem is that many businesses just don't have a plan in place, they don't know how to manage a crisis. And because they're poorly equipped, it means that quite often, this is going to fall back on the founder, who's probably already very busy if they don't have someone else in this space. And then that can mean that the crisis is elongated, they're going to lose more money, it's going to be a longer recovery period, team can be impacted. If the team are impacted for a long period of time, what does that mean to them?

You talked about emotional impact. I mean, if you're going to have a crisis and people working long hours to resolve it, because you've not been dealing with it appropriately, then that can have an impact on them, you might lose staff. And so it's not just the financial piece. But the more time you're taking people away from their day job, you are definitely getting that financial impact on the business.

So it's about how to manage a crisis. And this is where you can have a Director of Operations involved to take that away from the founder, and manage this appropriately with the team. And there are three main areas to this. And that's what I'd love to talk about today.

James: This is the point I want to make. There's a big difference between trying to figure this out as you go with no preparation or training versus highly trained, prepared and ready for crisis so that when it arrives, you can instantly pounce on it. Now in your case, what we're talking about is two types of businesses. There's the business where they are constantly going from fire to fire to fire to fire, and the founder, the visionary, is just unloading and unleashing on everyone around them in their desperate attempt to try and resolve it.

Lloyd: Scatter-gunning the team with tasks and not working on daily operations.

James: Then of course, people start churning, they leave, they don't like this, it's not the sort of thing they desire, you could hear words like toxic, etc. We actually saw a recruitment candidate the other day, they wanted a replacement for their team member. And they said, Listen, we're a small business, we churn over two to three staff a month, we can't have sick leave or time off, we need them on 40 hours, no matter what.

And we're like, We're not replacing your candidate. That's a toxic workplace. In their mind, that was totally normal. So that's one type of business. The other type of business, they have their people and their systems dialed, they have a culture, they know exactly where everything is, exactly how everything's being done. When those emergencies arrive, they have a plan to deploy. They probably have an SOP, they have a communication style and channel. And they resolve things very quickly.

I can tell you, within minutes of my hostile client, we sent a full refund, and just ended it. Because if you don't respond quickly, you end up with chargebacks, you have six months of arguing back and forth, you get negative reviews, so it's not worth it. And then our SOP is we update our filter to never have a client like that, again. We exclude and screen from that, because so much damage can happen, you just don't want to be in a battle with someone who's got nothing to lose. Right?

Three areas to consider

So let's talk about your three things that the DOO can have in place.

Lloyd: Yeah, so the first thing is coordinating a response. So if there was no Director of Operations, or point person, this might come back to the founder, something has happened, some severe event. And it's going to need people from different parts of the team to resolve this. And so the founder might be involved.

But let's say it was an item, and I'll talk about this a bit later. Let's say it's something where there's reputational damage, and that founder has to be involved with the press or getting their face out in public. The last thing they want to be doing is getting in and then having to coordinate as well. It's just going to be too much for them.

So the first thing is having someone to bring the team in and to just manage that response and get it closed out ASAP.

The second area I want to talk about is recovery and learning. So, great. You've resolved this item. But what are you going to do to prevent this type of crisis happening again? Are you going to learn from it? Are you going to go, Hang on, what happened here? What have we learned from it? What are we going to do about it? So that's the second way, we'll talk about that.

James: That's where I will say something like, what is this teaching us? Why did this happen for us? Two things happened with my hostile client. One is we changed our offer on the page to remove the one thing that was inflammatory to this person, which for nobody else it has been. And the second thing is we adjust the application process to exclude the same set of type of client that we could ever have again. It's just a hard No for me, right, because I'm in a point where I don't want to repeat that.

I shared this information with a friend of mine, a close confidant. And we identified the one problem that we have each year is the exact same profile of person and circumstance. It's like, I get it now. This is like, three times in a row, I'm getting the pattern here. This is clear, no-go zone. So it's like, what is the lesson? Why was I sent this gift, this experience, you know?

And you almost want to thank these people for the lesson they're giving you. That's probably a healthy way to look at it, rather than to get all angry and go and get involved in a road rage incident, or go and drink a bottle of scotch or something, which is really a way a lot of visionaries handle this sort of stuff.

They just transfer, which is probably what happened to me in this case, this guy's probably had something go bad in his life and just unloaded. And that's a bad habit. It's very immature. It's acting like a schoolyard bully, like just a kid. It's a child mindset.

We have to basically become more secure, and own it, and say, Right, this happened. Like Nam Baldwin talked about in my favorite episode about NEAT, Normal, Expect it, Accept it, Tidy up. I think this comes under the tidy up. How are you going to stop this from happening in the future?

Lloyd: Yeah, we'll get to that. And then the third way is preparing for the unknown. So we've talked about, there was an incident, and how are we going to deal with it in the moment? What are we going to learn from it? The other thing is now, let's be proactive. How do we get from being reactive where we just wait until something happens, deal with it, learn from it, to actually looking at, what's out there, like what's on our radar of things that could occur? And what can we do about it? So that's the third way.

Coordinating a response

So yeah, I would be quite happy to just get into the first way. So what do we do? How do we coordinate for a response? And as I was saying earlier, many small to medium businesses simply don't have a point person that they are using to deal with these events. And so that means that the founder is already very burnt out and limited when there is something that comes along.

And straight off the bat, that means that they then have to do, if they're going to do all of those three things, they need to coordinate the response, they need to make sure that they learn from the event, and they're prepared for the unknown.

So it reminds me of when I worked in corporate, I worked for this big payments company. And they had this one event that they had a payment fail, and their batch job of process overnight had failed. And the operator who was dealing with this saw this and reran the process, but didn't realize they were rerunning all the payments. And so as a result, a major supermarket got charged twice. A large number of customers were charged twice. And although they immediately spotted what had happened, although this company sort of, Okay, we've got this, will sort it, we'll immediately start refunding, the refunds only came out the next day.

There was an event where suddenly a whole number of customers for a supermarket getting charged twice. And by that point, and people have spotted that, then the CEO's getting into the press, they're wanting to interview, you know, what do you want to say about this? What's happened? What about all these people have been charged twice for their groceries? And the way this was being put out in the press is, you know, how am I going to make my mortgage payments? I mean, it was really exaggerated.

James: Well, there were a lot of people are at that checkout, hovering their credit card, wondering if it's going to clear. Like, it's a game changer for some people, that extra payment.

Lloyd: Well, so this was something that needed to have a number of different teams involved. It needed IT, it needed marketing, it needed legal, it needed the communications, all needed to be coordinated. So that was where their COO was going to be coordinating that response and making sure that that was all happening, so that that CEO can just focus on the message, and how that's going to be properly handled, and how they're going to deal with the external behavior for the company, and how that's going to be projected, rather than thinking about what's going to be coordinating internally.

So the first thing is just making sure there is someone who can bring everyone together in that war-room-like style, and just manage it until it's resolved.

James: Is that something you do?

Lloyd: It's absolutely something that we do.

James: I had a client like that. I've told this story before, but he bought an M3R from me, a very rare car. And he used to have a suitcase in the back. And I said, What do you actually do? And he said, I just get flown around the world. When someone has an emergency, I just fly in and fix it. That was it.

Lloyd: He sounds like the Wolf from Pulp Fiction, but... [laughs]

James: I hope it wasn't that kind of emergency. But it was pretty cool at the time when I was in the, you know, this was in 1995 or 1996, it was pretty cool to think about, this guy's buying literally the most rare and expensive car we had for sale. And he was very mysterious. But it just sounded cool.

And I feel like you and I do a lot of this now for businesses, we just fly in and fix things. Well you know, virtually, we zoom in and sort stuff out. And it takes a certain person. But it's good for your clients. They're lucky to have you in their corner, because you've got all the battle skills. You've seen all the scenarios unfold. I love it.

Lloyd: I've had some lessons from these things for sure. It's good to have the experience. There's a Winston Churchill quote, it ties back to what you were saying earlier, which was, never let a crisis go to waste. So in this case of that payments company I was talking about earlier, that's a great opportunity to do something there. Everyone's been working hard to get this issue resolved super quick. And now in the back of their minds, they're thinking, I hope something like that doesn't happen again.

Learning from a crisis

So this is a great opportunity to go and get buy-in from all of those different teams to work out what we can do to learn from it, and what we can do to fix it. So in this case, this is where I was involved in this was about making a case so that we could go and upgrade all of their monitoring infrastructure across the different departments so that this thing never happens again, which would be a great segue to bring us on to the second point, which is making sure there is a way to learn from these events.

So the thing is, many of these businesses struggle to handle these events in the first place. But let's just say they have resolved it effectively. Many of them still find themselves prone to deal with the event again and again. And so without a process to learn from such an event, it means that they continue to be vulnerable. And this means that if you don't have someone in place to run that particular process, then it means that, guess what, you're going to have the same folks involved in that again, that might perhaps it falls back to the founder. And, you know, much time is wasted and taking away from the daily operations.

So here's a process that I've used time and time again, and it's called the PIR, or the post-incident review. And this is a common term in corporate as well, unfortunately, in corporate when people hear PIR, they think that this is going to be a place to allocate blame. And that's not what it's about.

James: Who's going to be sacked?

Lloyd: Who can we blame for this? You know, let's save face, right? It's not about that at all.

James: But it is, in corporate. Like, that actually is the way that it works. Sadly.

Lloyd: Unfortunately, there is quite often that kind of behavior. But that's not what you want. Right?

James: No, that's why I don't work in corporate. It was crazy - it was the most bent world I've ever seen in my life. It was just so disgusting. The manipulation and crime that goes on in enterprise level corporate is eye-popping, and people don't know about it. So they don't talk about it. They're just focused on when they get ripped off by a real estate agent, or you know, the things that consumers are in touch with. But at a deeper level, it's crazy, the politics that goes on.

Lloyd: Yeah, there can be a lot of Game-of-Thrones-like politics going on.

James: Well it's like, yeah, Lord of the Flies and stuff.

Lloyd: So a PIR, if it's done properly, is not about focusing and allocating blame. It's about identifying the causes. And I say causes because very rarely is there a single cause of the problem, and I'll get into that into a minute, but identifying the causes. And then here's the most important bit, is coming together with a team and working out what we're going to do to make sure this never happens again, like, what can we do about it?

So that's what a PIR is - identify the causes, and having a planning session, get the team together, get the band together, what are we going to do about it? And if I give an example that I'm sure many of us have seen before, an e-commerce website where there's a problem at the checkout. I mean, I've seen this so many times just as a visit to other people's websites. I've seen it when eBay had an outage. So this definitely happens.

And while something like that might, you know, something's gone wrong with the checkout, while that might, immediately the finger goes to the developer, okay, well, the developer develops something, and it's stuffed up the checkout might be the first thing. But when we look deeper, there's a number of things that might have gone on there.

For example, did the developer have a proper testing environment, like the production environment, but in a safe place, where they can actually test their changes?

James: Do you call that a sandbox?

Lloyd: Sandbox, or testing environment, something like that. Did they have that? Was there a particularly tight deadline put on them for some reason? Was there a planning issue? Was this poorly planned? Was the funding cut for any reason to push all of this back, so there wasn't adequate testing? Or is there a culture against speaking out? Like, did they think, oh, hang on, this deadline is just, there's no chance, we're going to have to do shimmy this change and at the last minute, cross our fingers and hope for the best and cut testing? Did people not feel safe to speak out and say, Actually, hey, if we do this, there's a huge risk that this is going to stuff up.

So there can be a number of reasons why something like that can go wrong. And it's generally not just one thing, it's a whole number of things. And so this is where you can get the team together, have a good, awesome chat about to understand all the things that have gone wrong, and then have your Director of Operations put a plan in place, all of those items with timelines to get those things done so it's resolved, so we never have these issues again.

James: So it's basically like CSI.

Lloyd: CSI?

James: Crime Scene Investigation, like you know, something simple appears to have happened, but, you know, they set up all their cones and take all their pictures and go back to the lab. And eventually, over time, the evidence will show what happened. A lot of companies are just glossing over an incident with a convenient fall guy, and then it happens again and again, right?

Lloyd: This is a great opportunity. And there's another quote, right? In the midst of every crisis lies great opportunity. It's an Albert instein one. So there's gold in there, you know, thanks. You're not feeling like it at the time. But there's a lesson in there somewhere.

James: I just think it's as simple as Yin Yang. Within every negative is contained a positive, and so forth. Like, it's there, it's hidden, it's good to look for it. That's why I said before, it's like, what is the lesson here? What is this teaching me? How am I growing from this? What will I change from this point forward?

Five ways to prepare for the unknown

Lloyd: So we've talked about how we coordinate response, we've talked about how we can learn from it. And those are two fantastic skills right there. If we've got someone who can take the heat away from the founder and manage those two things, then that's already a win. But there's another area we've not talked about, which is preparing for the unknown, like looking proactively on our radar and thinking, what can we do about it?

And so if you do this well, you can be prepared for an event before it happens, and just jump on it super fast and save yourself any financial impact. And so many businesses just don't even do this. And so, I would just summarize this into five ways, if you like, five main ways.

Determining what's a crisis

And the first way is to classify. So you want to know that what you're dealing with, is it actually a crisis, or is it not a crisis? Because if you treat everything like a crisis when it's not, your team are never going to focus on what's important - the daily operations, the founder's managing, pulling their hair out, oh, this is a crisis, when it might not be.

James: There are some people in that mode perpetually.

Lloyd: I've seen it.

James: I know. They're your perfect clients, actually.

Lloyd: We help them with rhythms and we get them out of it.

James: The more crisis they have on a perpetual basis, the more you're going to be the best hire they ever had.

Lloyd: So the first thing is, is this actually a crisis? So a crisis, yes, you want 24/7 people on it until it's resolved and gone and finished. But how do you determine it's a crisis? So factors might be a large number of users, and that amount of users impacted. How widespread it is, is it a data breach, has it got reputational damage? Those things would put it right up the top as a crisis, you know, let's jump on that, or a major incident if you like.

And so I think about, again, a payments company I've worked with, where they lost their SMS provider, you know, those payments company need to do that kind of thing for 2FA. And they only had one SMS provider. And that meant that suddenly people couldn't add their cards to digital wallets anymore. So number of users impacted, huge reputational cost if they're providing that service, quite large.

So what was an appropriate response? 24/7 get everyone on it, get the tech team on it, get marketing, get ops. And that kind of issue, definitely a critical high severity incident. And it was resolved very, very quickly. They hooked up another SMS provider very quickly. And now as the learning from that, they'd go out, and they've looked at other what we call spots or single points of failure to say, Well, where else are we exposed? What's the lesson we've learned here? Is there any other places where if we lose that, we're in trouble?

So that's an example of a critical incident. An example where it might have on the surface looks critical, but in fact is not, well, let's go back to our e-commerce. At the checkout, I worked with a company and they'd put out a special deal. But something went wrong in the checkout with that special deal. And the customers just couldn't put that special deal through.

So when you look at it, actually, there was only a handful of users that were impacted. And for those number, they would actually be able to call them up individually. So it wasn't a very high number. So reputational wise, it's actually pretty low because reputation as a result of this ended up better. They rang up everybody, made them feel super loved and offered them something special, and so forth.

So the appropriate response for that is like 48 to 72 hours, it's no longer an emergency. So that's an example where it can be classified as low. There's no data breach, the reputation is intact, it doesn't impact a high number of users. So first item was classification.

What are the risks?

The second item would be risk assessment. So this is where if you've got a project coming up, or if you want to have a session periodically with your team, you can say, Hey, folks, what do we know that's out there? You know, for example, we lost our SMS provider recently. Is there anything else like that out there we should know about?

And we can have the team come up with, whether it's financial risks, system risks, and list those out, have a brainstorming session. Now it doesn't mean that we plan for every one. Because we need to look at what's the impact this thing has, and then how likely it is? So I don't know, let's say the internet went down globally, how likely is that? Incredibly small, globally, right? What's the impact?

James: I don't know. I reckon it's increasingly going to be an issue.

Lloyd: Perhaps so.

James: In the back of my mind, I've, what's my plan if there's no internet? Because if we get to that point, I will need a plan.

Lloyd: So then perhaps in your team, you'd say, Right, okay, here's what we will do. You know, we'll go back to doing X, Y, Z. For the case with the SMS provider, that's a really good example of where they are actually going to do something about it. So this is where you come up with those risks. And then you work out whether you're going to plan and actually do something about it, or you're going to accept it.

And all the time, if the likelihood is so incredibly low, and the cost to actually put a plan in place is high, you can just accept it, you're not going to accept everything. So that's the risk assessment. So something you can do, you can do that on a project by project basis, or you can do it quarterly or so forth, to say, what's out there, what should we resolve?

How would you recover?

The third area I'd like to briefly mention is disaster recovery, and or business continuity, they overlap a lot. So this is simply like, do you have a backup in place for your systems? If something goes wrong, how would you restore it? Can you restore it? Have you rehearsed restoring from a backup? So that's something you can do.

Could you work from a different location? Now all of my teams work remotely. And so that's fine, but what if your apartment, or your house, or your office gets flooded? Could you go and work from another location? Or if a particular office where you've got people and they get COVID, what would you do about it? So you can plan around those things as well and put processes in place, your SOP.

The fourth one we've already mentioned, it deserves a category of its own, cybersecurity. Like, do you have a plan in place for cybersecurity?

Training is essential

And then finally, number five, is training. We've talked about so much today, like all of those things, coordinating response, how we learn from it, how we prepare for the unknown. People don't just have this and get going, you need to train the team how to be involved. So training for all of those things is another area where we can be proactive.

James: For sure. I mean, even all hospitals, schools, etc., they have a meeting point, hotels in the event of a fire. You know, they know the most typical risks, and they have a plan around it, and they drill on it. So I imagine in your case, Lloyd, you have a comprehensive checklist when you go into a client, and you just basically will show them all the things that they could choose from to implement?

Lloyd: Yeah, we either start our engagement with an audit or assessment, if you like, and then we can go back, play that back and say, Look, this is what we will do. Or we just get started, and we say, Look, we've already seen this, this is on our checklist, we've seen this, we've seen this, and go from there.

James: And the more businesses you work with, the more exposure you've had to the things that can go wrong. Like me, I've seen thousands of things now. So I can recognize, very straightaway, even when people tell me what they're going to do and they're not even talking about risks, I can point out there is, like I can say, Well, that's great, except if you get that domain, that could be a trademark.

It's like when Jasper came out, it was called Jarvis. And my first thought was, that's a really strange choice, because if you're going to do an AI tool, wouldn't that be a trademark infringement on the movie franchise, who has Jarvis as an artificial intelligence thing? And then they actually got a cease and desist letter, according to some Facebook post I read, this is just off my memory. So don't take my word for it. But I feel like that happened.

And I could anticipate that immediately. At the first instance someone suggested that name, I would have said, this is a risk. And they had to rebrand because of that. So yeah, the more database you've got access to, the more incidents you've been exposed to, the better your checklist gets. So you've got diagnostics. I've got diagnostics.

From continual crisis to smooth sailing

So a business could basically go from the bad fire to fire to fire to crisis business to a well-run, smooth operation. As I say on my weekly calls with my small group, if we don't have any drama, or whatever, we celebrate that lack of drama. Because drama is just, it taxes your adrenal gland, it makes you strung out, it makes you reactive, it just has a knock-on effect. You can eliminate a large degree of that by anticipating, by coordinating, by recovering well, by training on it, and bringing in a professional like Lloyd, VirtualDOO.com.

Lloyd: And we've gone from these places where they've had that chaos feeling and it felt like the emergency department to a place where they've got rhythms in place and how they resolve these things quickly, it feels nicer for everybody, it no longer feels like Whack-a-Mole anymore.

James: It used to take me about two and a half years to turn around a dealership from start, and that's if everything's broken. I mean the wrong people, bad culture, no SOPs, not getting results, failing in every possible way. Two and a half years it took me to get them to a high-performance machine. And then the next 18 months typically was enjoying that rest, and things operating hands off until my next deployment.

So I did that twice in a row before I came online. But a small business like the ones we're talking about, it can happen much faster than that. Even listening to this podcast, if there's one thing that you've thought, oh, that could be a risk, and caused you to make one action item, then this has been worth listening to.

Lloyd: Yeah. Well, that's it. The main thing is have a plan, you know, have a plan. How are you going to do it? How are you going to coordinate a response? That's probably the most important item on that list.

James: I love it. Thank you, Lloyd. It's always a pleasure to chat and share your viewpoints and wisdom. This is episode 1013. And if you need some help with your operations, Lloyd is the guy. If you just want someone to chat to as a sounding board with your online business, and you've got a good product and you're going okay, then I'd be happy to help out, too. Speak soon.


JAMESSCHRAMKO
esc
tab
caps lock
shift
fn
control
option
command
Optimize your business strategies with James's help