Podcast 10 – Tips for Managing Technology

Hi, it's Annette Welsford. I've got a very challenging but fascinating chat today with Tom Freer who's the managing director of Wyntec. You can see the details of Wyntec at their website wyntec.net.au.

Our guest
Tom Freer of Wyntec

Interview with Tom Freer

Annette: From what I understand, Tom, you specialize in providing IT support to companies that have between 20 to 100 computer users. Is that right?

Tom: Correct. Yes. We work with privately owned organizations with those you said, 20 to 100 computer users, and we essentially deliver stress-free IT.

Annette: Oh, that sounds good. Definitely. Gosh, there's guarantee to bring a bit of stress into your day than a computer that doesn't work when you want it to. It has never to do with us, the users. It always has to do with the piece of equipment, of course.

Tom: We try to blame these tools, don't we?

Annette: That's right. I know that not all of our listeners today are going to have a minimum of 20 users. But I'm sure that some of the information, the help that you're going to give us is applicable no matter what size your business is. Is that correct?

Tom: Yeah, definitely. I think what we found over the years is that regardless of the size, whether you've got two computers or 100 computers, your challenges are very similar and the concepts around technology are very similar, as well.

Common Problems Businesses have with Technology

Annette: What are some of the common problems that you see with people trying to use technology in their business?

Tom: The top three common problems we see talking with organizations and owners is that they don't fully understand technology and the capability of it. Everyone has got their head around about they need technology but it's not having that full understanding of what it can do, what it can't do, and then how to make it work within the business. That leads to frustration.

Annette: Yup. Big time.

Tom: Another big component is once you've got these systems in place is the downtime element of this. A big problem for organizations is minimizing that downtime and making sure their systems are available so staff and team members can access the information and systems they need to.

Annette: When you say "downtime" you mean when you're trying to use your tablet or your computer or your phone or something to get the document that you need and you just can't get it. It's crashing or whatever.

Tom: You can't get it, yeah. The crashing or you get the system not available or whatever it is, that's downtime. So your PC might be working…

Annette: Blue screen or something.

Tom: Yeah. So your PC might be actually on but you can't get to the information you need. That's where we look at that downtime element.

Annette: That's when your blood pressure rises.

Tom: Yeah. And you want to throw that thing out the window.

Annette: Yeah.

Tom: Then the third problem we see is around the perception and sometimes the reality that IT is high cost and typically high cost when you least expect it. That's a big problem that organizations deal with.

Annette: They're the problems that you see, what about mistakes people make?

Common Technology Mistakes Businesses Make

Tom: I think some of the big ones are around really underestimating the time and the financial commitment around IT.

Annette: Really?

Tom: Yeah. And that's not saying that it needs to be expensive in an ongoing massive cost. But it's really looking at how much time you're spending, whether it's you as the owner or your team is spending time to troubleshoot their own systems, their own issues. That's a time and it has a direct financial impact to your business, that underestimating what that is.

Another big one is and it leads on from that is trying to do it all themselves and not asking for help. Google is a great example where you can get on there and you can ask anything you want. But unless you know what you're looking for or you specifically know what you're asking, that'll lead you down a rabbit hole and you waste hours trying to fix a problem.

Annette: Which should take somebody else an hour to fix.

Tom: Yup. Another big thing is not really having a good strategy in place with IT and aligning that with your business strategy. When I'm talking about that, it's not about having pages and pages of documentation that we will do this and this is how it's going to manage it. It's about looking at where you want to take your business and then how technology can support that and enhance it.

Annette: For example, if a typical plumbing business is out on the road or even a builder. Let's say a builder has got four jobs running. He has got contractors and subbies and people on four different sites, and they need access to all sorts of information.

Tom: They'll need access to things like, potentially, the quotes that were provided and the plans, all those type of things.

What Equipment do Tradies Need to Manage Jobs?

Annette: E-mails, schedules, lots of stuff. What sort of infrastructure – and when I say "infrastructure" I mean equipment and software – are they going to need to manage jobs effectively out in the field?

Tom: The big thing for field stuff in that instance is having reliable communications. You're going to need a good, solid mobile Internet solution. That's typically your 4G, which most mobile phones have now or you can get dedicated to all these mobile devices.

Annette: Your 4G only works in the city, doesn't it?

Tom: It will fall back to 3G so you still get good coverage and reasonable speed in most instances. That's typically not too much of an issue but it's about making sure you get the right one. We find Telstra have the best coverage, hands down. Whether it's in the city or out in the rural areas, they can provide that consistent service, and that's what's needed.

The other element that your tradies are going to need is to leverage cloud technology.

Annette: What?

Tom: Yeah. Not the fluffy stuff in the sky. What they're going to need to do is make sure that whatever data they need is accessible. All those things we talked about being parts of the list, the quotes and the designs, what they're working on.

Annette: So all the files that they need?

Tom: All the files that they need. They need to make sure that they're accessible over the Internet. That's where the cloud that comes into it that it's essentially an area in the Internet that you can securely access and get access to that documents. Not only while you're out on the road, but your staff in the office who are maintaining that are looking at the same copy.

Annette: So you haven't got multiple copies of the one file floating around. You update one and all of a sudden they've got a different version.

Tom: Yeah. You want to make sure that you're working off a single point of truth. The last thing you want is to be out talking to a customer and you pull off a list of material that's out of date or someone has updated it. It's about making sure that that information is accessible.

Annette: Definitely. And accessible from your phone or your tablet.

Tom: Yeah. There are a number of factors that come into it, but typically you'll have an iPad or a tablet or something that you can work with while you're out on the field. Something that's a little bit robust. But we want it to create functionality. You don't want to be doubling up everywhere. You don't want to have one device that you use out in the field and then come back and you got to get familiar with another device when you're in the office. Trying to keep it consistent is very beneficial.

Back in the office, you're going to want some good, stable computers that are fast and reliable that your staff can be using and be efficient on. Again, they'll need solid Internet links in their office.

Software Tom Recommends for Business Management

Annette: What about the software? Typical business owners try to cut back on doing invoicing at night and on weekends and stuff like that if they don't have the support staff to do it for them. Are there applications? What could they be using to improve their bookkeeping and their invoicing and to get paid out when they're out there?

Tom: Yeah, definitely. I think the big key to that is making sure that it's done quickly. You don't want to be waiting to the weekend doing your invoices and trying to remember what you did on Monday.

Annette: No.

Tom: Whatever system you look at it needs to be online. A great tool that we see used extensively is Xero. It is an online accounting system essentially that allows you to create your invoices, create quotes, send out e-mails, send out your statements, all those type of things to your customers. All in one spot, all available online over the Internet, and accessible wherever you got your computer.

Annette: Sounds good. I guess there are some apps that help you actually take money, too. Isn't it? Like PayPal has got one.

Tom: Yes. The key part to all is looking for applications that will integrate. Xero is really good for that because it allows a lot of different tools to plug into it. What I mean by that is if you've got Xero – that's where you're doing all your finances – you don't want another application that's taking money that you then have to manually start entering data back into Xero.

Annette: Yeah. That's a double, isn't it?

Tom: You're now doubling up on work. What you want to do is find tools that will natively plug into the systems. There are heaps of them. PayPal is a great example. They have all the hardware and everything you need that will plug into your phones to take payments, sync it to Xero, and it's all reconciled.

Annette: That'll save on your bookkeeping cost, too. Wouldn't it?

Tom: It saves on your bookkeeping cost, it saves on your time trying to manage and enter. Particularly if you're sole trader, the last thing you want to be doing is up to midnight reconciling everything. The more you can automate that, the better. Xero is great. It has links into just about every bank in Australia so it will automatically import all your transactions every day.

Annette: Cool. That sounds good. What are your recommendations or do you know much about on-the-job tracking, calendars, scheduling and stuff like that?

Tom: Definitely calendaring and scheduling would come down to what e-mail platform you want to use, whether it be a Gmail or an Office 365. Both of those can also be used to leverage centralizing your documents that we touched on before. You need to look at a good, solid platform around e-mail and collaboration tools.

Then you will look at how you're managing your jobs. Now, I haven't got any specific recommendations but the key is – particularly if you're using Xero, there are a number of add-in tools that are available that will do job tracking for you and job locking. You can create all your jobs in the system which could be issued out to your team of doing these three jobs today. They can then track all their time in it, which feeds back into Xero that creates your invoices and all that stuff.

Annette: Oh, fantastic. You mentioned Office 365. I understand that's like Google Apps. But for those of us who are a bit technically challenged, can you just explain what you mean by that?

Tom: Yeah. Office 365 and Google Apps are very similar in what they offer. The key functions out of it are really e-mail, online file storage like cloud storage, and communication with your team so instant messaging and video conference capability.

Annette: Oh really? So if you're out on a job and you've got say an Excel spreadsheet with a list of measurements or materials or something, the office administrator has put together all the quantity surveyor or whatever, you can have a look at that on your phone or your tablet.

Tom: Yeah. You can be opening up those Excel files and you can be looking at the data that's in there. You can be adding data in there in real time that someone else is adding data in there.

Annette: Oh really? So you don't end up with two different versions?

Tom: You don't have two different versions and it automatically creates comments and who's doing what. So you can collaborate on that document as you're going. You might have your team in the office doing the proposal and you can check over it. You can open up that same document, make your notes in real time and they start seeing them, so they can quickly get it done.

Annette: That's fantastic.

Tom: And that's in Office 365, in Gmail. One of the big things, the benefits that we see moving to an Office 365 is that is a familiar platform.

Annette: Yeah, people are used to it.

Tom: They're used to using Outlook. They're used to using Word and Excel. So Office 365 really provides that benefit about not having to re-educate staff, which in any business that's a big cost is education.

Annette: You said something about messaging.

Tom: Instant messaging?

Annette: Is that like texting?

Tom: Yeah. Again, I use a scenario where you've got your admin staff in the office and you're out on the road, for example. We call it presence and status, essentially. You can change your status to say, "I'm available," or "I'm not available." You go green when you're available. So someone could send you a text message and it will ping up on your phone knowing that you're available and you can answer straight away.

What it does is it speeds up your communication because now I know when you're available and I can make that phone call or I can send you that message and I know you'll respond. Whereas, if I don't have that visibility, I'll be making the phone call, be leaving a message, you'll be calling me back, leaving a message and end up playing phone tag. How much time do you waste playing phone tag?

Annette: Yeah, true.

Tom: It's just about little efficiencies off that. They're the sort of things that you can get out of these tools.

Security and Technology

Annette: Tom, how important is security around technology for businesses?

Tom: Security is really important particularly these days viruses, malware, and attacks are really rampant at the moment and they're just continuing to evolve.

Annette: Why do people do this?

Tom: I don't know. Boredom? Some of it is driven by money particularly the likes of those the ransomware style attacks, which is where you'll get a virus infecting your machine and it locks you out from all your data and then they want you to pay money to unlock it. So it's driven by financial incentive. I'm guessing some of it is also boredom. People just think they can do it.

Annette: Oh dear. Because it's becoming more and more rampant, is it getting harder and harder?

Tom: Yeah. It is. It requires multiple levels and not only technology – this is the thing these days – some of the viruses are getting clever in that they're using very much a social engineering approach where they will use very common brands. The current ones going around are Australia Post and DHL. You think Australia Post have actually sent you a message about a parcel. You may not have even sent a parcel but it's Australia Post – why would they not send it to you? You open the e-mail and it's a virus. Even those viruses aren't getting detected by a lot of tools, as well. So you need multiple layers of website protection and reputation checks and things like that.

Annette: Oh my gosh.

Tom: It's more than just technology now. We're doing a lot of education with users continually. It's about reminding people – if you get an e-mail and you don't know who it's from, don't open it. Just delete it. If it's that important, they'll send it again or they'll phone you about it. But that's where a lot of people come unstuck. They get an e-mail, it looks legitimate, will click on the links, go to a website which then looks legitimate, enter in their details and they're done.

Annette: Is it so much not opening an e-mail or not clicking on links or attachments?

Tom: Both. It's really the things on the attachments. Some current ones are, there's a résumé one going around at the moment where you'll get an e-mail from someone random. You don't necessarily you know who it is but it will say, "Hi, I have attached my résumé for your perusal. I would love it if you've got some work opportunities." Supposing you do, "Oh okay, let me have a look at their résumé," and it's a virus.

So businesses really need to be conscious about these things and looking at not just virus protection on their machines but educating staff. They need to be looking at multiple layers of protection as well: website security, e-mail, spam, all those type of things.

Annette: Is securing the whole environment an expensive exercise?

Tom: It can be. There are ways and means to do it, to get levels of protection. It's all about how customers be risked in their organization. You're not going to be out to protect from every single element but that's where you start spending lots and lots of money. But it may be overkill in some instances, so it's about spending the money in the right spot.

Definitely any virus software, some element of spam and any virus on your e-mail, and that would be the minimum. Then depending on the size of the organization and how the networks are laid out, you want to definitely be looking at secure fire walls so people can't attack and come into your network. The final piece is really around content control and securing what people can browse to and putting in protections around that from a website perspective.

It’s like blocking particular sites and putting any advanced virus scanning. When you go to a website, it scans the site first to see if it is a known malicious site or if it has got malicious content and things like that. That’s where we start getting into more advanced technologies to be able to do that.

Annette: How would businesses protect their own websites?

Tom: That’s another big challenge. Again, it comes down to using a very reputable hosting provider, a known brand. When you are using a website and things like WordPress and Drupal and those type of technologies, the base ones, it’s making sure that they're being updated, as well. Because, inevitably, people will be looking for ways to hack in or attack those sites so the developers are then releasing patches and fixes. Then that goes for the hosting company where you want to make sure that they're updating their servers and putting the latest protections on there and things like that.

Annette: I guess passwords need to be quite difficult, too, and things like that.

Tom: Yes. There are plenty of layers. On a WordPress – it’s a great example – making sure you have got a strong password, making sure you're not using the default username which I think might be “admin.” Lots of people use admin and admin. Making sure you're changing both of those. Making sure you're putting in the latest updates. Even changing things like where the administration page lives. Rename it. Look at those sort of things, so you're not using the default settings.

Annette: What impact does the social engineering have? We haven’t even talked about phishing, have we?

Tom: That’s the social engineering aspect – phishing e-mail, phishing attacks. They're essentially where you’ll be sent an e-mail that looks legitimate to either visit a website or open attachment and you do. It might get an e-mail from your bank or a bank, “Click here to update your personal details.” You click on the link and it goes to a site that looks like your bank site. But unless you look carefully at the address, it’s dodgy site collecting information.

Annette: You should have a look at the spelling.

Tom: Yeah. It’s about being vigilant and being aware. Having lots of awareness. Users typically are so busy doing what they need to do and getting through. They’ll get an e-mail and they just click, open, and do whatever they normally do.

You do have to think about what you're doing and looking at things like the spelling, the address that the links are going to. If you do happen to land on a website and you're not quite sure, have a look. Does it have the padlock, the security certificate there? Does those things look legitimate. And it’s about slowing down. You need to be aware. Slow down and take care when doing those things.

Annette: I know that Microsoft seem to regularly release updates and patches. How important are these for security? Are there any other vendors that do updates like Microsoft do?

Tom: Yeah. Microsoft – they're the ones who say the most, they’ve got such a large install base so they're very proactive in releasing updates. Those updates are both security updates. There are flaws and vulnerabilities that are found in systems, so they're addressing those. Even additions and fixes for general operating system. But they release at least every month. Lots of other vendors do release some, as well, probably not as regularly as Microsoft but you'll see the likes of Adobe. Apple are releasing updates but they're not generally security-focused but they're still releasing updates and they should all be applied.

It's about that extra level of protection. Because what happens in those situations is that a hacker or someone looking for it to be proactive about it will find these flaws and release the flaws to Microsoft and say, "Hey, we found this. This is what would happen." Then people will go and directly exploit those vulnerabilities. So if you're not patching your systems and your workstations and your servers, you're leaving yourself open to vulnerabilities and direct attacks.

Annette: So the regular updates and security checks is part of the service that you provide?

Tom: Yes. It's making sure that workstations and servers are all updated on a regular basis, that the software running is the latest. And it's just adding that extra level of protection because that aligned with virus protection in different levels, that's where you're going to get the highest level of security. You might have the best virus protection on your machine but if a hacker is looking at a particular exploit that's not virus-related, you can still be compromised.

Annette: Of course, yeah. So there are other security issues apart from viruses.

Tom: Yes. It's attacks and hacking and things like that. You hear that in the big, public organizations where such-and-such is being attacked. There are lots in the U.S. and they're specifically targeting those organizations. But then there are others who are just doing random Internet scans looking for systems that are vulnerable.

Annette: I guess the security services that you provide for your clients also include internal security for users. So if somebody leaves the company you have steps and you also set up access so certain staff can only see certain elements of the company's data and all that stuff.

Tom: Yeah, very much. It's about taking a holistic approach, not just updates in viruses and things like that. It's about looking at processes and controls that are within the organization. Who has access to what data? Who has access to what folders? You don't want everyone in the organization having access to the payroll folder, or the HR folder seeing everyone's details. That's security. You don't want people who have left the organization – and we see this all too often where people have left the organization but their account is still active. So if there is any sort of remote access, they could still get in.

Another is regularly changing passwords on your machine. Not using the same password for every site – and that's common as well and that's because it's easy to remember – but if you lose that password or you've written it down on a piece of paper and stuck it to your monitor, that's not great.

Again, it's educating staff and putting in systems, controls, and processes to almost enforce some of that change, as well, so people are changing their passwords every 60 or 90 days. It would be ideal, but yeah.

Annette: Tom, thank you so much for sharing some of these fantastic tips with us because I know with a lot of the clients that I've been chatting to in the last few months, systems and getting organized and running the show a lot more efficiently is one of the biggest bug bears of all. And when you don't understand much about technology and as you say, you go to Google and you look something up, you're overwhelmed with the amount of conflicting advice and choice and whatever. That's really hard to get your head around.

If somebody is wanting to get your help with, not only helping to setup systems but providing support for when things go down and they've got the size of company that you're talking about, 20 or more, I'll put a link to your website on the show. They can contact you for a bit of a chat.

Tom: Yeah, I appreciate that. I'm more than happy to chat with them.

Annette: That's excellent. If you're smaller than that and you're not at the Wyntec size, I will also put some links into other companies that I know that do what Tom does but for the smaller two or three men band type operations.

That's fantastic, Tom. We'll finish up off there. But if you could just finish off with your one final tip for our listeners, that would be awesome.

Tom: One final tip. I think the biggest thing is ask for help. If you do nothing else then ask someone who's in that field for some help. It'll save you a lot of frustration, a lot of time, a lot of money.

Annette: We all need to save those things. That's for sure.

Tom: That's right.

Annette: Terrific. Thank you so much, Tom. That has been very interesting, a really good chat. I really appreciate your time.

Tom: No problem, Annette. Any time.

3 Key Learnings

1. Not really understanding just how much technology can really help you in your business. There's so much you can do to improve the way you run your business if you have the right programs, apps and devices to help you. The right tools improve productivity, make life easier for your team and can really improve the service that you deliver to your customer.
2. Security. Hacking, phishing, identity theft and scams are prolific. Make sure you and your team are aware of what can go wrong and what to look out for. Make sure your systems are protected with virus checkers and malware, and that your website is backed up regularly, the user and passwords are not obvious and that it has the security plugins on it.
3. Don't waste time trying to fix problems yourself. Just cause you drive your car doesn't mean you should also know how to give it a full service. Same with computers. Get them serviced and tuned regularly and when things go wrong it will cost you less money and time to get an it expert to fix it.

Resources

We've listed here details of Tom's company Wyntec if you have more than 20 users and you want stress free IT. We've also listed a couple of other companies that we are aware of that provide this type of support for businesses with less than 20 users.

Wyntec.net.au
Tradiepad.com.au
Computercures.com.au (Melbourne only)

And for help with securing your website – contact us at commonsensemarketing.com.au

Need Marketing Help?

If you want help with marketing and growing your business, that what we do. Check out our list of services at tradiesuccess.com.au/services. We've helped trade business owners of all types (plumbers, electricians, builders, concreters – you name it) all over Australia to grow and manage their business, through our mentoring and done for you marketing services.

Feedback?

If you have any comments or questions about this episode, we'd love to hear from you – simply enter them in the comments area below this episode on the website tradiesuccess.com.au

Share With More Tradies

Please share this episode with any other tradies or business owners you think would find it useful – share on Facebook or Google Plus or LinkedIn, share one of the tweetables in the show notes or even send a link by email! And make sure you never miss out on an episode, subscribe by clicking on the itunes or stitcher links.