HOW TO PROTECT YOUR BUSINESS AGAINST A CYBER ATTACK

LIVE CHAT: QUESTIONS AND ANSWERS

INTRODUCTION

Any business that holds information is exposed to a cyber attack. The reality of doing business in 2015 is that data breaches can and will happen – whether initiated within the organisation or from outside.

Recent examples of cybersecurity breaches include Cryptolocker, a piece of "ransomware" that encrypts your data until you pay the hacker group money, and hacks in which prominent corporations are targeted and intellectual property released – Sony, Ashley Madison and David Jones to name a few.

This interactive infographic shows recent data hacks.

Although it is impossible to completely secure a business against these threats, there are ways to reduce the likelihood and impact of such attacks.

Top 6 Tips to Protect your Business against a Cyber Attack

1. Set-up auto-updates to implement security patches for your operating systems and applications
2. Set up your anti-virus software to update hourly
3. Ensure your anti-virus software addresses viruses, Trojans, spyware, key-logging software and warns against suspect web pages
4. Have a process in place to regularly review and replace old computers and systems
5. Ensure your employees are vigilant about potential phishing emails
6. Diminish the impact of a cyber attack with cyber liability insurance

The expert panellists who addressed members' questions and considered some straightforward approaches you can put to use in your business were:

- Dr Micheal Axelsen FCPA, Postdoctoral Research Fellow (Business Information Systems) at the University of Queensland
- Drew Fenton CPA, Director, Fenton Green and Co.

RESOURCES

- IT Checklist for Small Business
- CPA Australia's IT Management resources
- http://intheblack.com/articles/2015/06/01/improve-your-data-security-and-keep-the-hackers-out
- http://www.insurancebusinessonline.com.au/news/average-cyber-payout-for-2014-runs-into-the-millions-194639.aspx
- https://www.cpaaustralia.com.au/professional-resources/public-practice/toolkit/insurance/cyber-liability-insurance

QUESTIONS AND ANSWERS

Does anti virus software over protect by replicating what is also offered by windows?

So, no, Windows doesn't really do very much in the anti-virus space. You will need to really buy a bit of software to make sure that you are covered for anti-virus issues.

The Six Top Tips are a good guide, though shouldn't the very first tip be reduced permissions on the workstation - servers for users to limit what can and can't be installed?

Yes you're probably right, not much point having security patches if the permissions are pretty open.

Often we leave the workstations fairly open so we can install software ourselves at the laptop or on the workstation - so everything that user does is trusted, which includes the virus. Giving the user default administration rights is a bit of a problem – you should review those.

Do you know if cyber insurance is available through Fenton Green?

Yes Fenton Green and co offers CPA Australia members cyber liability insurance cover.

Does the payment of ransomware make you more of a target going forward?

Well that's an interesting question - I suspect it does. I had a student in my MBA class recently who was hit in the March and then again in the June. About that time he took my advice to review their systems properly. But yes paying the ransom did seem to make him more of a target.

What would be CPA's preferred anti virus software to protect accountants and their clients' sensitive information?

CPA Australia does not provide recommendations on anti-virus software. There are free to really expensive options available. You need to review your needs and make sure you get what you are after. Keep in mind anti virus on the workstation is the last line of defence, not the first. You want viruses filtered out of your emails and from getting on to your server in the first place. Unfortunately, network computing is really hard.

Does the Microsoft email offering via the cloud provide higher virus protection than hosting your email locally?

Yes it does because they filter the emails at the email server end - so you shouldn't be getting the viruses in the email in the first place.

I would think that a reputable "cloud provider" would provide better (including being more cost effective) security for a SME from cyber attacks than they could themselves. Do you agree?

I agree - network provision is pretty expensive for even a large corporate to do. When you look at the cost of going cloud, you start to think it's a good idea.

Are any of the free anti virus programs any good?

How long is a piece of string? I think they are worth what you pay for them. Most issues these days are coming in via email of course. So that's a reasonable place to be as far as viruses and trojan horses go. Whether it's up for corporate work? Not sure. Certainly free is better than nothing. But you usually have to pay to capture the email-type viruses well. Again though these are pretty much the last line of defence - it's better to not get the virus anywhere near your workstation in the first place.

Is CPA Australia aware of any practices that have had their systems compromised and client details accessed?

No, we are not aware of any practices that have had their systems compromised.

Is it dangerous to use products such as Dropbox and Logmein as these require some sort of access to our computers?

So it will depend on who puts files into your dropbox. Email is probably the bigger question and vector of issues coming in. If a lot of people have access to dropbox then yes, and then of course if your files are copied elsewhere that's a problem.

For those companies hit by Cryptolocker, are they usually able to easily recover through backups, or do they find their backups also affected?

Usually these people run off and wait until everything's encrypted - which means your backups are encrypted too or they are so old you don't want to go back to them.

We have been told that our wireless modem incorporates a firewall and so a further firewall in our internet security program is not needed. Is that likely to be true?

No it doesn't sound likely to be true to me. Define "not needed" - you'd certainly still need anti virus.

With cloud servers how do we ensure that the country where the data is stored meets our data privacy laws etc. here in Australia?

You should check with your cloud provider to ensure that you are not in breach of Australian privacy legislation.

Who is liable if client data is compromised when using a third party online portal to host clients documents? Us or the 3rd party portal host?

I am not a lawyer but the service provider writes the contracts and you don't - so usually the balance is toward the service provider. It'll be expensive to enforce if any lawyers are involved, in my experience. It'll depend on the facts of the situation though.

My email service is provided by Optus and they filter out a great deal of spam before it gets to my computer. Is this filtering likely to be protection from viruses as well?

Yes I'd say it is protecting you from some viruses but certainly not all. You want two layers - one at the firewall/cloud service provider and one at the workstation. That way if one doesn't get it the other should do so. But you're never 100% safe.

Why are cyber insurance policies generally not taken up in Australia? Is it because we don't have mandatory reporting of breaches?

This is a new product range in Australia. It will take time for people to become aware of the product and of the risks that they need to transfer.

One of the tips is to replace old computers is this because they potentially have old anti virus software or is there a security issue with old hardware?

No, anti virus needs to be set to auto update so it's not really a problem with the 'old computer' - in fact if it's older then maybe the virus won't work on it. However, if it is an old operating system then you might find a problem that the anti virus software itself is no longer being updated. So that would be a REAL problem. I would always aim to keep up to date at least with the anti virus and then potentially upgrade the computer as needed. Honestly though I don't buy into this whole idea of buying new computers ‘all’ the time. I mean I like new shiny toys but sometimes it gets a bit silly :). I'm all for eking out the last of the useful life of the PC.

I work from home. What settings on my router/modem should I modify?

I'm afraid I really don't know. Google is your friend - search for the manual. Generally you want to be sure that it is only as open as it needs to be. If it's a consumer device then the defaults are probably fairly good - the more important thing is to make sure you change it from the default password. 'Admin' and 'password' will get you into an awful lot of WIFI routers as you drive around in your white van in the suburbs - not that I've tried or anything!

I work from home, and use Kaspersky Total Security on my PC. I leave the router on overnight - is there any risk to having the router on for long periods?

Not much extra really I wouldn't think. In fact physically they're designed to stay on for long periods - getting hot and getting cold is a problem for a lot of computing technology. However, make sure you need a physical connection to the router to actually make a change to your settings (i.e. not log in over WIFI) and change the default passwords. Though my wife is always turning our router off because she hates seeing 'all the electricity those blinking lights use' (blinking is not a euphemism). Unless it's a real problem for you with really sensitive data - just keep an eye on it. For most of us, that's not the easiest way to get your data. It's easier to ring up pretending to be your IT guy and get your data that way.

Would you recommend using a computer as a software based firewall in conjunction to the modem firmware firewall? E.g. Internet >Modem> Firewall machine> DCHP and email server > Client machines and servers? Would the cost be worth it?

Honestly - I think it's overkill if you have a reasonably good service provider. They should already be filtering your internet access, and better than you ever can I suspect. I'd think about it but really if it's filtered at the internet level and then at your router and then at your workstation - that's a pretty reasonable setup. If you have non-clean internet then yes I'd think about it but otherwise for most small businesses that's an overhead activity that's going to cost you greatly in terms of distraction. If it's your bag as a tech-head then perhaps so but otherwise it might be 'busy work' that doesn't earn you any money.

Does setting up a Logmein to my office PC with secure password make my PC anymore vulnerable to hacking?

By definition it must do as it's another avenue you have to protect. So long as you are happy that LogMeIn is a professional product the increase in vulnerability is probably not huge. I'd be more worried about having lots of these types of remote access (e.g. Skype, Windows remote desktops) is the problem and trying to keep up with them all can be painful. Hilary Clinton's email server had a bunch of remote desktop connection software on it that meant more people can access that machine - so if Hilary can't get it right then what hope do we all have trying to do that. Yes, more vulnerable, but probably not a great deal more vulnerable.

Can you please explain what malware is? We use Kaspersky PURE which seems to stop viruses but only warns about Malware and then we have to use Malwarebytes anti-malware.

According to my Google, Kaspersky Pure R2 can actually do a rollback if it finds Malware. I'm wondering if it's configured correctly, or if you don't have the proactive defence enabled? For support go to http://support.kaspersky.com/4950 All of these things are extra headaches so I'm wondering if it's possible to try and stick with the one bit of software?

What is a "phishing" site and what danger are they?

They are sites that look exactly - EXACTLY - like a site you might use e.g. your bank's website. You think you're in the right place (e.g. please pay your red light camera fine), log in, and you're not in Kansas any more. Of course this too means that Bad People have your username and password for your bank site. So they might be able to get into your banking service (usually not, banks are pretty on top of it with physical keys etc.). What's interesting too though is often your username and password are used everywhere else (coz who's got time to remember all those passwords) so with that they can try your credentials on other websites so that's a problem too. They're very creative these people. If only they used their power for good instead of evil :).

What's the vulnerability with Skype?

The safest computer is one in a box in the basement so as soon as you add connections you get problems with other people being able to access it (e.g. if it is unpatched for a zero day vulnerability). Skype itself is Pretty Good but there's always a vector. Someone else might have their username and password compromised and send you a phishing link (see above) and your users click on it - ouch. Again though user education can be a bigger issue.

Can cookies collected from websites cause any security issues?

They can, that's where a number of zero day exploits can come from but I have to say usually it's pretty good. More a problem if your browser isn't patched to the latest problem is my understanding, and the reality is cookies aren't usually the biggest problem. But if you go to what I will euphemistically refer to as "dodgy" sites cookies might try it on. So you are best off always evaluating websites and being sure that they are actually fairly reputable before going there (some - not all - anti virus programs will warn you of the afore-mentioned dodgy websites before you go there). That's handy.

With Ransomware, can it affect other VMs on the same server? I am pretty sure it can't but doesn't hurt to check. Maybe if it can access a shared storage area to affect the other VMS?

Thanks for the answer on the firewall. I was just thinking a headless machine and Linux setup would come in under 300 and it is saves me work in the long run.

For the moment I'm going to say no it can't, but if it's in shared storage, yes. For those that don't speak internet VM = Virtual Machine. Not too sure how permanent that arrangement will be.

Look you sound like you know what you're talking about and so yes a headless machine Linux setup wouldn't be a bad idea. But for a lot of people that would give them the cold sweats and I'd think about using a reputable ISP.

With the prevalence of threats coming in via email attachments and links - including false google drive and dropbox links, as well as most organisations imposing attachment size limits, what would you recommend as a, client friendly, way to transfer large documents and files?

It's going to depend a lot on exactly what level your client is at. Despite my recent issues with Office 2016 (long story), I think the Office 365 offering has a lot to offer and there's a good chance that OneDrive is not as vulnerable/common. That might be worth exploring. Though perhaps people need educating not to click on fake dropbox links.

CONCLUSION

OK yesterday I (Micheal) was at an IT breakfast and they identified cyber-security (KPMG) as a big problem but nobody knew what to do with it. In fact, a lot of people weren't too sure what it is. So I do think that for a lot of businesses - SMEs in particular, since they don't have the resources of the big boys - still have a lot to learn about cyber-bullying.

The biggest thing I think you need to do though is make sure that your workforce is educated about what is going on. One of my MBA students had *ahem* gone through a red light and then received an email about such a thing. Anyway everyone was ripping out the cords all over the place when he clicked on the links - he called it a 'Career Limiting Move'.

Another point that I think is really interesting is going to be cyber-bullying - perhaps your staff using the tools you have to bully your people (up here in Brisbane we had someone getting a bit too free with the CCTV, and there was that real estate agent in Tasmania who defriended someone and that was bullying). So I think this goes back to your people and user education.

The risks are here and now, and are growing. We would recommend seeking professional advice about managing and transferring risk from your service providers, such as IT providers and brokers.

FURTHER INFORMATION

For more information on cyber security go to

http://www.cpaaustralia.com.au/itmanagement

http://www.cpaaustralia.com.au/professional-resources/public-practice/toolkit/insurance/cyber-liability-insurance

For help or to suggest other topics for live online chats please email publicpractice@cpaaustralia.com.au

CONTACT

Dr. Micheal Axelsen FCPA

E: m.axelsen@business.uq.edu.au

Fenton Green - Cyber Liability Insurance

E: cpa@fentongreen.com.au

DISCLAIMER: CPA Australia Ltd has used reasonable care and skill in compiling the content of this material. However, CPA Australia Ltd makes no warranty as to the accuracy or completeness of any information in these materials. The above material is only general in nature and not intended to be specific to the reader’s circumstances. Further, as laws change frequently, all practitioners, readers, viewers and users are advised to undertake their own research or to seek professional advice before making any decisions or relying on the information provided.

BE HEARD.
BE RECOGNISED.

CPA
AUSTRALIA