Transcript of webinar on cyber security for small business

Welcome to the Digital Masterclass Series, part of Glen Eira City Council's business support program. Today's topic: cyber security for small business.

Today's agenda will include: why you should bother with cyber security; the 2021 cyber security threat landscape; types of cyber security threats affecting small business; how you can develop resilience; and the question of outsourcing.

So why should you bother with cyber security? If you use the internet, then you are at risk of a potential cyber security breach. Cyber security should be a priority, no matter the size of your business. It is one of those things that is only thought about when something goes wrong, which is a very ineffective way of managing this particular problem. Prevention is the best way to manage it and there are very simple (and free) ways that you can manage your cyber security. In Australia, changes to the data breach laws from 2016 mean that you're now legally required to report a data breach, and this can lead to reputation damage.

The 2021 cyber threat landscape is an important one for small businesses to consider. That's because, although hackers have historically focused their energies on large businesses that earn a lot of money (or have a lot of sensitive information), you no longer have to have hacker-level technical skills to commit a cyber crime. What's happening now is that hacking software is now available to be bought and downloaded on the dark web. This means that anybody who has access to the dark web, and has the money to buy it, can obtain hacking software and basically just click go. Because of this democratisation, small businesses have become a much more common target for hacking. They're now at risk, where they historically haven't been of much of interest to hackers.

Having anti-virus software is no longer enough, as the range of cyber threats out there far outstrip the capabilities of automated software. You really need some kind of human thought behind your cyber security, in order to have a robust policy working there.

Here are some of the key types of cyber security threats that affect small business. Note: although a hacker (or a group of hackers) is unlikely to target a small business (unless there is a political motive), automated cyber attacks — which, as explained before, don't require a lot of technical knowledge or effort — remain and ever-growing threat. Some of the most common types include:

- **Data theft.** This can happen in a multitude of different ways. At a very simple level, it could just be a disgruntled employee that emails lists of your clients' personal information to themselves. You could have a hacker using software to access your data and take it; and then you can have it as a result of hackers targeting larger businesses that have your details. Adobe, Twitter, LinkedIn, Facebook, Canva, Dropbox, Uber and Zoom have all suffered cyber security attacks over the past decade, where hackers have stolen user data like emails, passwords, credit card information, birthdates, full names and contact information. The data is usually then sold on the dark web, or occasionally even published publicly online.
  Identity theft is the next one. It's closely linked to data theft, as once someone buys stolen data, they can then use your information to do whatever they like. Instances of identity theft don't always have to be linked with data theft, though an increasingly common type of identity theft online happens on social media. This is where copycats accounts are created to impersonate a business for financial gain. Social media platforms like Facebook have been very slow to respond to this type of identity theft, meaning that, once it has happened, if

you don’t have an officially recognised business account, Facebook may refuse to take down the copycat account. It is a relatively easy thing to do.

- **Malware is the next.** This is a blanket term for malicious and intrusive software like viruses, worms, adware etc. This is the category that can almost entirely be managed through having up-to-date anti-virus software, but this is the only one on the list that you have in front of you (so, one out of six that can be managed in this way). As mentioned before, you need to involve some human thought and engineering into your cyber security policies, if you want to have a robust one.
- **Phishing.** These are emails that try to trick you into clicking a dangerous link, sharing personal information, or providing financial information. Common phishing scams come in the guise of emails from well-known local energy or telecommunications providers, as well as banks or even the ATO.
- **Ransomware.** That’s where your data is hijacked and you’re locked out of your system. Access to your system is returned once you pay a ransom. It can be anywhere from a few hundred dollars to a couple of thousand dollars.
- **A watering hole attack.** This is a relatively new term and concept. This is where a fake version of a real website where you’re known to go is set up. It’s used to steal your personal information or infect your system.
- **The last one on that list is: a denial of service attack.** This is where a network of computers is used to overwhelm your system. This is now used to increasingly target individuals and businesses as a result of social media activity, and it’s become a common form of internet trolling. For example, if a business posts something (perhaps a little bit politically motivated), and a group of people take a dislike to it, they can commit what they call a denial of service attack on your business, by getting a whole lot of people on the internet together to create that attack.

Developing resilience: cyber criminals who target small businesses do so because they assume it’s going to be an easy payday. As mentioned, in 2021, most cyber criminals are not sophisticated hackers. They’re not going to put a huge amount of effort into accessing your system, they’re going to look for big holes and obvious vulnerabilities, and try and exploit those. Understanding what they tend to target, and then putting simple preventative measures in place, makes it much harder for an attack to be effective – and ultimately means that they probably won’t attack your business in the first place.

So, the best way to manage this, and be a aware of what they attack and target, is with education. Education and awareness are the most important tools when it comes to cyber security management. Educating yourself, your team and even your customers about cyber security is really important. That might mean learning to identify the signs of a phishing email, including cyber security education and protocols as part of staff onboarding, or putting up reminders around the office about cyber security safety.

Through your customers it might mean sending them emails, or reminders, that you would never contact them via email to ask for personal information, financial information, that kind of thing. This is to make sure that they don’t respond to phishing attacks, for example, on a systemic level.

Some of the things that you could do:

- Put in place access limitations to your system, meaning that only a few people can access sensitive information.

- Establish a password policy: this can include a whole lot of different things, like two-factor authentication or creating a regular password schedule for everybody in the office to change their passwords.
- Finally, backing up your data on a regular basis. This ensures that, if the worst happens, you have a relatively recent backup that you can go to.

Now: the question of outsourcing. Cyber security needs vary from business to business. What we've gone through today is a very broad overview of the landscape, and some very simple things that small businesses can do to create resilience and discourage people from trying to breach their cyber security. However, as a rule of thumb, if you store sensitive client information on your CRM (customer relationship management) application, that is internet-accessible, then you need to explore advanced security options. This is because, if your client's data is breached, then you potentially could suffer some serious reputational damage, and ultimately business losses.

Outsourcing could include a few different things. Usually it would include outsourcing your security to an IT specialist. This can include anything from having your data put on an IT company's server to protect it; to having them perform a review of your security; providing antivirus software; or even providing help desk support.

Another option is to invest in cyber insurance, which is now available for some small businesses.

That concludes today's webinar. If you don't already subscribe, you can receive the fortnightly e-news by emailing cityfuture@gleneira.vic.gov.au and asking for a link. If you'd like any more information on any of our programs, please don't hesitate to email us at cityfuture@gleneira.vic.gov.au. Thank you.