Lock the digital doors: cybercrime and your business

By Fordham

31 March 2023



It's an image beloved of screenwriters. The businessperson shutting up for the night, carefully

counting up and cleaning out the till, then double locking the doors on their way out. 'Business owners are careful,' the footage tells us. They protect what's theirs.

These days the careful locking up is just as important. It's just that the enemy is no longer a hooded thief lurking in an alley. It's an opportunistic hacker locked in a room with laptop. A sophisticated cybercrime operation. Or it's one of your staff.

Cybercrime is the threat to business today. Some Australian Cyber Security Centre (ACSC) statistics show just how threatening it can be.

- Last year there were 76,000 reported instances of cybercrime – that's up 13% on the year before. (ACSC Annual Cyber Threat Report, July 2021 to June 2022).
- That equates to a cybercrime report every 7 minutes.
- The amount of cybercrime is growing - and so is its cost. The ACSC says the average cost per cybercrime is **$39,000** for small business. It's **$88,000** for medium business and over **$62,000** for large business (who typically have more sophisticated defences).

Cybercrime has become such a big issue – for the whole economy – that Australia now has a Minister for Cyber Security. That makes Australia the first country in the G20 with a dedicated cyber security minister.

At Fordham, our extensive owner-business connections have their own tales of cyber woe. One client we spoke with had an external bookkeeper who was directed by email to pay over $100,000 a new account in payment of an invoice. It turned out a cybercriminal had "mirrored" the owner's email. Our client then had to battle with insurers and the bank in order to seek recovery of the lost funds due to the cyberattack.

Fortunately, there are a wide range of measures you can take to protect your business. In the balance of this article, we're going to look at the most important ones. (We have a companion article: Cybercrime: Protect your client, protect their privacy, protect your business that will help you understand your obligations when it comes to protecting your **clients' personal information** from cybercrime).

Your lines of defence

Backup, backup, backup

Experts say your data backup needs a **3:2:1 strategy**. You need to keep at least three copies of your data. Two should be stored at separate locations and one should be stored off-premises.

Harden your software

Security software is a vital layer of protection for any modern business. You need to get it installed across your business computers and devices.

According to Fordham Partner, Adrian Palone, security software is too often seen as set and forget. “We encourage all our clients to make sure their security software is up to date. Just as importantly, we remind them that using old versions of their business software – including their payroll software, CRMs and operating systems – means they’re missing out on the latest security updates. And that makes their business vulnerable.” A core element of making sure your software is secure is taking the time to set up a firewall and turn on your spam filters. Every little bit helps when it comes to reducing incursions into your systems.

Restrict administrator privileges

Administrator privileges on your software allow the identified administrator to enact higher order technology changes (such as installing new programs or creating new user accounts). They’re a classic backdoor entry point for hackers. You should restrict these privileges to as few people as possible. Or consider disabling them altogether.

Get cloud cover

Business security experts encourage businesses to use cloud-based systems rather than run servers on their premises. With cloud-based systems you get the benefit of having thousands of security and technology specialists building data protection into Amazon’s AWS, Microsoft’s Azure and Google’s Cloud Platform.

Verify in multiple ways

Multi-factor authentication is an increasingly common security measure used by companies like Xero and many financial institutions. It typically requires additional proof of identity (such as verifying or using a passcode sent to your personal mobile number) before you enact a financial transaction. It might add a few seconds to your daily banking for example – but it adds a crucial layer of security.

Train your people to protect your business

Whilst external cyber threats are very real, a significant proportion of cybercrime is either committed by a staff member or occurs thanks to their errors. Just as you’d train your staff to

secure your office or factory you need to train them to secure your cyber domains. Some of the key training elements include:

- Training them to use pass phrases rather than passwords – they're harder to hack
- Managing their devices. Backing up their phones and computers (using the 3:2:1 method). Updating their software and any security/anti-virus packages.
- Being careful in the use of public Wi-Fi and avoiding, wherever possible, the use of USB sticks. They're basically a key into your network.

In the same way you'd train your staff to handle customers or machinery, you should run compulsory and ongoing cybersecurity training for all your staff. This should cover everything from device security to their responsibilities around protecting customer data.

Disaffected staff are a major cyber risk. If you have to terminate or make staff redundant, or they leave for a competitor, get all their devices back in your hands and remove any and all forms of access to your systems. And do it straight away.

Insurance protection

The threat of cybercrime has made cyber insurance an increasingly popular product. Covering your business from the damage of cybercrime can protect your bottom line. And in the same way that insurance companies incentivise less smoking and safer driving they help businesses adapt better cybersecurity practices.

What next?

Today, digital technology is what business uses to get things done. So bad actors will use technology to target businesses. With difficult economic times on the horizon it's likely cybercriminals will be even busier in the next few years. We believe the measures outlined above can help protect your business. But if you'd like a more customised look at how to protect your bottom line, your customers and staff, reach out to your Fordham Partner for assistance.

This information has been prepared by Fordham Business Advisors Pty Ltd (Fordham) ABN 77 140 981 853. Fordham's liability is limited by a scheme approved under Professional Standards Legislation. It is general

information only and is not intended to provide you with advice or take into account your objectives, financial situation or needs. You should consider, with a financial adviser, whether the information is suitable for your circumstances. To the extent permitted by law, no liability is accepted for any loss or damage as a result of any reliance on this information. This information is believed to be accurate at the time of compilation and is provided in good faith. Fordham is a subsidiary of Perpetual Limited ABN 86 000 431 827.