CYBERSECURITY THREATS

In Australia, a majority of businesses (62%!) have reported experiencing a cyber security incident, indicating the prevalence and severity of this issue.

Such incidents, which include cyber attacks, data breaches, and other forms of cyber threats, can result in severe financial losses, reputational harm, and legal and regulatory liabilities. To manage cybersecurity risks, businesses may need to invest in specialised expertise, implement robust IT security protocols, and stay up to date with emerging threats and best practices.

Cybercrime statistics make for sobering reading, with a 75 per cent rise in ransomware attacks in the 2021-22 financial year and up to 200,000 vulnerable routers in Australian homes and small businesses.

A recent Australian Cyber Security Centre's (ACSC) annual report states medium-sized businesses with between 20 and 199 employees are the most at risk of attack, with the average cost of an attack for a business of this size being $88,407.

While the risk of cyberattack remains high, there any many preventative measures businesses can put in place to reduce the risk of attack and, should one happen, reduce its severity.

1. **Make a plan:** Your approach to cyber security should have a clearly articulated strategy that's regularly revisited. This should guide the actions taken by the business to ensure it adopts the latest cyber risk mitigation techniques. ACSC recommends adopting eight security controls to help prevent attacks. This framework is useful for directing a business's actions around cyber security. The controls include taking away unnecessary network administration privileges from employees who don't need them and putting in place multi-factor authentication for access the network. These are described in more detail below.

Above: Cybersecurity threats are rising fast

2. **Secure the business' internet connections:** Make sure all the points at which the business connects to the public internet, such as remote desktop applications, file sharing software and webmail, are secure and not vulnerable to penetration by hackers. It pays to work alongside an experienced IT professional through this step.
3. **Safeguard all devices:** All the common tools your team uses to connect back to the business such as their laptops, tablets and smart phones also need to be secured to ensure they are not a back door through which criminals can enter a business and exploit its weaknesses.
4. **Configure automatic updates for software:** The business should be fully protected for viruses and spam through the protections of a suite of leading anti-virus anti-spam (AVAS) software solutions and intrusion detection systems. Make sure any patches and updates are automatically installed so you're protected from emerging threats.
5. **Automate back ups:** Like software updates, data should be automatically and regularly backed up offsite to a system of servers not connected to the business. That way, if criminals do infiltrate the system, they cannot access back-ups through it and delete them. This means in the event of an attack, the business can be up and running in no time, having accessed the most recent back-up. These systems should also be regularly tested, well before an attack occurs.
6. **Implement multi-factor authentication:** It should be nearly impossible for criminals to get into a system if it has the right protocols in place. These can include, but are not limited to, multi-factor authentication and mandatory regular password updates. As a minimum, passwords should include a mix of lettering, numbers, symbols and cases. Passphrases are even better than passwords, as they can be harder to crack yet easier to remember.
7. **Audit third parties:** Criminals can gain access to your system through external parties such as suppliers if they can access your systems remotely. Regularly audit their cyber security protocols to identify and fix and insecurities through which hackers and scammers could access your business.
8. **Train staff quarterly:** Cyber security training should be a routine aspect of staff professional development. At least each quarter, train staff about the latest threats and run simulations to identify staff who are at risk of opening phishing emails.
9. **Respond immediately to threats:** Make sure to put protocols in place, so in the event of an attack, you can lockdown the system and stop criminals misusing it further.
10. **Put in place a cyber insurance policy:** Cyber policies can help businesses recover from an attack by paying for associated costs and helping to mitigate the effects. Your Insurance Broker can help you identify and address the cyber risks in your business.

Above: Documentation and Agreements are important parts of how you trade

LDI LAW 101

ARTICLE: BY DARI LEVY, PRINCIPAL SOLICITOR – LEVY & W

LEGAL DOCUMENTS

Having professionally drafted agreements is by far the most underrated business asset, in fact, most business owners don't even regard a brilliant contract as an asset, not believe that drafting one requires a specialist trained skill.

However if someone offered you to invest in a business asset which paid itself off over the life of your business at around 50 cents per client:

- that would protect your business and mitigate your exposure to risk;
- ensure you don't waste valuable time and stress dealing with issues
- ensure you don't have to write off your time or costs to resolve disputes
- prevent you from being liable for things you are not even the slightest bit responsible for
- deter clients from late payment, non-payment or no payment
- charge for additional time and services with ease
- retain the rights to your IP, including access to images, and being credited correctly
- were able to execute and deliver your services in a streamlined and systematic process,
- with inbuilt solutions so you didn't have to think on your feet every time something went wrong; that you were not accountable after the fact; or for other people's mistakes
- you could prevent bad reviews on-line
- being sued
- ....and that there were repercussions – a client terminating or breaching the contract leaving you out of pocket;
- that gave you the upper hand, empowered you in your business dealings providing peace of mind and confidence to take those more sophisticated jobs or higher value clients..... would you do it?

Moreover, does this sound like something you should know how to, or could put together yourself? Saving money on your business' legal work is like choosing to save on a cheap set of breaks for your car, albeit fitting them yourself. A proposal consisting of a fee schedule and scope of works is not a contract.

Copying and pasting from other people's agreements is also not the solution. You are breaching copyright laws by copying someone else's intellectual property, or worse the IP of the lawyer who drafted it. Templates are less costly, yes, but unless it's drafted by a sophisticated lawyer, it will not be tailored to your business.

Above: Employees and Contractors have different legal rights and obligations

Regardless, how would you determine if it is a good, legally sound document that would serve your business? How do you know what terms you absolutely require to be in that agreement and how would you ascertain which provisions are not beneficial or appropriate for you and what the implications of including them are?

How do you know what to add in or take out so that you are completely covered, or so that it won't bight you on the... ? The answer is you couldn't know. The question is why you are gambling?

It is true some people have more luck in business, they cruise through with no major issues and debunk my arguments but, without wishing ill on anyone, it will only ever take one bad job, or one bad client for the tables to turn.

It is without doubt that in every Court room, every legal issue and every lawyer's job is to sort out the messes that could have largely been prevented with sound documents or good advice. In the end it's just not worth the risk, the costs and the investment in stepping up is worth its weight in gold.

This is not a sermon; it's a message directly from years working

firsthand on that factory floor.

CLIENT ENGAGEMENT AGREEMENT

This document should be your business blueprint. It defines the relationship between you and your client, sets out the terms and conditions under which you provide your services as well as covering the extent of your relationships with third parties.

The agreement should include but not limited to; the nature of the services, transparency of services, the delivery of services (including digital), and the limitations to what you will assume responsibility for, especially in relation to third party suppliers and contractors and supervision or management.

It should cover additional fees for additional services (including revisions, consultations, site visits, and anything outside of the original scope of work) procurement processes, hourly rates, commissions, trade discounts and product warranties.

The agreement should stipulate the client obligations, working hours, a communication, variations, delivery, delays, completion, disputes, termination, insurance, confidentiality, privacy, liability, consumer warranties, indemnity and the standard regulatory commercial terms.

In addition your fee structure, fees, and payment terms must be set out clearly, consistent with lead times, the work undertaken, and the invoicing system you use and any failures to meet these obligations.

It should include strong protections for your intellectual property, acquiring images of your work and authorisation for the use of IP.

DISCLAIMERS

It is important to have a legal disclaimer to protect your liability for any advice or recommendations you make during a consultation (as well as the copyright in any materials provided), prior to entering into an agreement for your services.

Your designs document should include a visible professional disclaimer and copyright notice to protect your intellectual property and liability and a short-form version for your schedules, digital documents.

For emails with clients, suppliers and anyone whom you deal with on behalf of your business, you should have an email disclaimer to protect the privacy, copyright in your professional communications.

WEBSITE LEGAL NOTICES

Whereas the client agreements are between you and the client, the website legal notices are essentially the agreement between you and the public. It is therefore important your business website has professional terms and conditions (T&Cs) which have references to commercial and consumer legislation, and the correct digital protections, which also extend to any social media platforms linked to the website. The T&Cs also include disclaimers for content:

- to protect your on-line information, or that you share via social media, as well as to ensure any references to products, third parties and testimonials are classified correctly;
- a services disclaimer;
- and a regulatory disclaimer with the relevant parts of the legislation and other regulatory and statutory provisions, such as the building and construction regulation, work health & safety, fair trading.

For intellectual property that you display on the website (such as images or designs) you should have a stringent copyright notice to protect people from copying your designs and content, and to acknowledge you are not breaching the copyright of others.

In addition, a privacy policy is now mandatory for the use of forms and contact messaging via the website, as well as other forms of data collection, including the client's personal details for the project.

EMPLOYEES

By law, employees are required to have employment contracts which meet the legislative provisions for casual, part-time or full-time workers. Notwithstanding, it is extremely important you to protect yourself against intellectual property theft, termination, confidentiality and restraint of trade, including taking clients from the business.

Above: The job is incomplete. The Designer, Contractor, Suppliers and the Client could all be involved

CONTRACTORS

Contractors are independent providers who run their own business. If you are engaging a contractor the key provisions of the agreement cover the nature of the relationship, the working arrangement, remote and in-office hours, responsibilities, deliverables, specifics regarding the project, intellectual property protection, privacy and confidentiality, insurance, tax, super, payment and invoicing.

If you contract your services out as a contractor to another designer, the most important provision is to limit your liability only to the design work provided to the designer and to meet any obligations to the client or for the finished product.

Outsourcing agreements are an agreement usually used for a specific project between a business and a service entity for the provision of a once off service in exchange for a fee such as virtual services or IT or social media.

Often the more casual the arrangement the more likely that things will go wrong, so deliverables and key terms are essential. These agreements are especially important when you provide the outsourced entity with your company intellectual property or access to confidential information.

A non-disclosure agreement should be used with anyone who you have not entered into an agreement with that you share your ideas, such as collaborations. You can also have a disclaimer on your brief or proposal when sending to clients to protect them from saving a copy of your work without engaging you.