benchtv
a benchmark production

Précis Paper

Emerging Issues in Business Law: Cybersecurity, Data and Crime

A discussion of the importance of cybersecurity for businesses in the modern world, including law firms, covering how to detect vulnerabilities, implementing proper systems and the consequences of not doing so, as well as the legislation concerning notifiable data breaches.

Discussion Includes

- **Cyberattacks in the business world today**
- **What should lawyers be on the alert for?**
- **The cybercrime industry**
- **IT and cybersecurity**
- **How to identify a data breach**
- **Human error, social engineering and email spoofing**
- **Pretexting**
- **Cybersecurity legislation**
- **Cyber-insurance: is it worth it?**
- **Penetration testing**
- **Data breach response plans**
- **The commercial value of information**
- **Anatomy of a cyberattack**
- **Recommended processes for in depth defence**

Précis Paper

Emerging Issues in Business Law: Cybersecurity, Data and Crime

1. **In this edition of BenchTV, Dr. Allison Stanfield (Principal Lawyer & Founder, SG Legal Services) and Damian Seaton (Managing Director, Cyber Audit Team) discuss the importance of cybersecurity for businesses in the modern world, including law firms. They cover how to detect vulnerabilities, implement proper systems, and the consequences of not doing so, as well as the legislation concerning notifiable data breaches.**

Cyberattacks in the business world today

2. **There have been numerous high profile cyberattacks on businesses recently, such as the recent incident where Cathay Pacific Airways was hacked, resulting in the loss of 9.4 million customers' data. There have also been a number of trust account breaches in which 'cyber-thieves' have been able to make solicitors transfer funds into their account. These attacks are becoming ever more sophisticated.**

What should lawyers be on the alert for?

3. **Lawyers are one of the largest targets for cybercrime. Notifiable Data Breach legislation has been in effect since the 22nd of February 2018, and following three quarterly reviews recent statistics released from the Office of the Australian Information Commissioner reveal that legal fraternities rank #3, with the medical and financial sectors at #1 and #2 respectively. Globally, the legal sector ranks at #1 and #2 equally with the financial sector.**

4. **There are a number of different motives for these attacks. It could be that the attackers, known as threat actors, are looking for information. They could be attempting to commit fraud or extortion. They could be looking to exploit ransomware. The landscape is so broad and fluid, that it is difficult for any business to stay on top of it, especially as new methods and tactics are being developed all the time.**

The Cybercrime Industry

5. **Cybercrime is estimated to be a 3 trillion dollar industry, and is expected to grow by 8 to 12**
   trillion by 2022.

6. In Australia, less than 2% of businesses are not connected to the internet in some way. What's more, the internet has become a part of our lives in a myriad of ways, and it's difficult to have an understanding of all the threats this poses. The legislation at present is not keeping up
7. It is not only large firms which are at risk of being targeted. Small to medium firms also have clients who have sensitive information, or wealth which could be stolen.

8. Cybersecurity is not an IT issue, it's a business issue. Maintaining cybersecurity is as essential a part of our lives as electricity or petrol, and it cannot be simply outsourced to people who are assumed to know more about it.

9. In fact, IT workers are very rarely trained in cybersecurity. A rudimentary knowledge of firewalls, anti-malware or antivirus protection isn't enough in today's threat landscape.

10. Threat actors are highly resourced, highly skilled and keeping up to date with technology and new opportunities, what's more, the cybercrime community vastly outnumbers the cybersecurity industry. There is a large network of people who can share their skills in exchange for a portion of the value of the data breach

11. Every breach is preventable. The first thing to ask is 'What is it we don't know?' This involves undertaking some kind of assessment.

12. There are many different legislative frameworks, such as the ISO/IEC 27001:2005, the Australian Signals Directorate 35 scorecard, and the National Institute of Standards and Technology

13. Cloud providers are generally safe. However there is a general misconception that storing your information in a cloud provider's solution is safe. However, it is your device or your server which is vulnerable in this scheme. Where those devices to be breached, the information in the cloud could be accessed by a threat actor

14. It is for such reasons that an in depth risk assessment is required. What's more, software and hardware cannot prevent human error. This goes beyond just having things like having a basic firewall or antivirus.

15. The assessment must identify the gaps which are non-compliant, and then build a road map, which takes into account the size of the business or organization, the risk appetite, and the budget.

<u>Human error, social engineering and email spoofing</u>

16. There are hackers who will monitor a company's email over an extended period of time, learning the typically speak within that company in order accurately mimic a person's

manner, in order to trick another into transferring money. This is an example of where further checks are needed, and why it is not enough to simply rely on email alone when it comes to important transactions.

17. Human error accounts for over 95% of every breach. This includes such things as lack of awareness, sloppy practices, lack of training, malicious intent, or misconfiguration of the IT systems

18. It can also involve social engineering. Simply put, social engineering is convincing someone to do something that, if they knew the ulterior motive, they wouldn't do.

19. One form of this is email spoofing. This is where a threat actor sends an email from a hacked email account, posing as a member of the business. It is referred to as business email compromised, CEO fraud, and whaling. For instance, a threat actor hacks into the account of a CEO or the managing financial controller. They can do this by, for instance, convincing a junior person in the firm to open an attachment or visit a website that has got malicious malware on it, which infects the computer system and gives the threat actor access, where they will be watching, listening and learning. Threat actors will spend time, effort and money to get as much information as they can about the company.

20. People think they can spot dodgy emails, however it is really only the most inept of spoof emails which are detectable. Spoof emails have become much more sophisticated and really cannot be prevented without the right technology in place.

21. It is a requirement to have someone in IT to assist with these measures. There are a range of measures recommended by the Australian Signals Directorate: DKIM, SPF, DNS, Quad9. They would require the IT department to have a look and see what could be done with those tools. Specialist cybersecurity experts can come in at this point to make sure that these processes are locked down properly. These measures operate like an encryptedWhat handshake involving codes, which prevent emails from outside sources from getting through.

22. There a various tactics used in social engineering. Spoof emails can create a sense of urgency, they could say something like 'I need you to do this urgently'; they can adopt a tone of confidentiality, so that the recipient believes they cannot communicate the contents of the email to anyone else. eg 'This is a merger and acquisition that nobody else knows about'. They can use fear, for instance suggest that is the instructions in the email are not carried out there will be consequences.

<u>Pretexting</u>

23. Because a sophisticated threat actor will have been monitoring a business for a long period of time, they will be able to convincingly mimic whoever's email account it is they have hacked.

24. This is a part of what's known as pretexting, where a threat actor spends months acquiring an in depth knowledge of a company or organization's workings, such as who all of the staff are, who are the clients, what is some of the lingo which is used internally. Once you've got this information,

25. This sort of cyberattack is often known as Friday Fraud, because it is indeed often done on a Friday when people are eager to head home and enjoy the weekend and are not as focused as they might normally be. What's more, Friday Fraud usually occurs after 2PM, and it gives the threat actor the whole weekend when people don't really communicate before anyone realizes what has actually happened.

<u>Data breach legislation</u>

26. There are already regimes in place in Europe dealing with notifiable data breach liability, and we can expect Australia to implement similar regimes in the next 5 years. It is important for business to start looking at these issues now so that they are prepared in the coming years for this legislation.

27. Not only can you be held liable, being found responsible for a data breach can cause irreparable damage to the reputation of your business.

28. The Notifiable Data Breaches Scheme came into effect on the 22nd of February 2018. It is essentially an amendment to the *Privacy Act 1988 (Cth)*

29. Businesses need to realise the value of their clients' information, and the damage that can be done if it is lost or stolen.

30. For instance, in cases where names. addresses, dates of birth and mobile phone numbers have been lost. Those four pieces of information are not often given much thought, but they can be very valuable to a threat actor. Damian Seaton's firm has seen cases where laptops have been stolen containing this unencrypted information, which resulted in the names being used as by Uber or Lyft drivers in the USA. Because this has been reported to police, that person's name has been placed on the Department of Homeland Security's watch list, and this has resulted in at least one high net-worth individual being barred from entering the USA.

31. People can also have financial fraud committed against them. For instance, nowadays the requirements to get a credit card are not as stringent as they used to be, and with those four pieces of information it is possible for someone to fraudulently obtain a

credit card. Following financial fraud, it can take people 15 years to get their credit rating back, and in that time they could have their mortgage called in and all of their credit cards cancelled.

32. A company is liable to suit if their data is breached. It is a fiduciary duty, and a directors and officers responsibility, to make sure that clients' data is safely encrypted. The Notifiable Data Breaches scheme came in to prevent business owners, directors and officers from offloading responsibility for this duty to their IT department.

33. Law firms are beginning to realise that the problem is much bigger than they thought and that they are highly exposed, regardless of the size of the company. It doesn't matter if your business is small or large, your liability is still the same.

<u>Cyber-insurance: is it worth it?</u>

34. Professional indemnity insurance will not cover negligence in the case of a notifiable data breach.

35. Cyber-insurance can offer good value, but it is still in its infancy and has not been tested enough. Although we can expect to see a lot of shoring up of the cyber-industry in the next 5 to 10 years, at present there is uncertainty and a lot of bad product. Cyber-insurance policies tend to contain many loopholes, and when looking at a cyber-insurance policy it is better to ask what you are not getting, rather than what you are getting. On the whole, money is better spent ensuring that your systems are protected and safe. That way, if there is a breach, you can at least show that you have taken steps to protect your data in accordance with compliance legislation.

<u>Penetration testing</u>

36. A penetration test in itself does nothing if you have never done anything before, other than highlight issues that you were already aware of. Damian Seaton uses the metaphor a newly built house consisting only of walls and a roof. Anyone could point out that it requires doors and windows, and then locks and security cameras and a surrounding wall. What's more, penetration testing looks only at the IT aspect of cybersecurity.

37. Your systems need to go through an assessment first, which would take into account an array of potential weaknesses, both in the system itself and the way that people use it. This would include such things as:

- How are you onboarding/offboarding?
- Are you police checking or background checking your staff?
- What does the staff contract/privacy statement look like?
- How are the staff trained? What education is given, and how often?
- How do you maintain knowledge?

38. Cybersecurity requirements are still embryonic. In Europe, the GDPR fine for non-compliance rose from €500,000 to €20M, as previously companies were all too willing to simply pay the fine and ignore the problem. However, a business must ask itself, regardless of legislation, what is the financial implication of damaged brand and reputation, as a result of a data breach? This is not only the effect it will have on clients. Staff will potentially leave, the CEO or managing director could be sacked. It could lead to board resignations, and lack of morale.

39. With regards to the *Corporations Act 2001 (Cth)* and the laws in Australia covering directors duties, it's not enough to simply leave the issue of cybersecurity to the IT department. The director of a company has to show that they have read the material, understood it, asked questions, and have had the company bring in the right people to address these issues, otherwise they will find themselves exposed to directors liability.

40. IT departments tend to be extremely busy, and their job consists of, for the most part, 'keeping the lights on'. A lot of people in IT do not have security training. And yet, all too often responsibility for cybersecurity is palmed off to the IT department. The Government says that companies should look to specialists in cybersecurity, and bring them into their existing infrastructure.

Data breach response plans

41. The NDBS, as well as the GDPR, says that companies should have a data breach response plan, so if there is incident, you know how to investigate it. The data breach response plan needs to be tested in order to make sure that it works.

42. Defense in depth means getting as much protection as possible, like a well-fortified castle.

43. Cybersecurity requires an understanding of the value of information. Due to this lack of awareness, information is far more accessible nowadays than hard cash.

The commercial value of information

44. Intellectual property is of enormous value to countries like China, North Korea, Iran, Pakistan and Russia. Australia holds a vast amount of IP and is a prime target.

45. Cybercrime is low risk, with only a 1% chance of the threat actor being caught. Police and intelligence agencies have only been faced with this problem for a relatively short period of time, and do not yet have all of the resources and skill sets to deal with it effectively, and staying ahead is a challenge.

46. However, everything can be prevented, once you know what the risk is. This is why it is important for businesses to think laterally about this problem.

Anatomy of a cyberattack

47. Millions of bots scour the internet. After gathering information, it gets to a human threat actor.

48. Small firms may think they are not a big enough target to be at risk, however many small businesses being targeted altogether can add up to a sizable value for a threat actor.

49. Companies working in conveyancing and real estate can use online platforms such as PEXA, which is reasonable secure. However, once it is only as secure as the people who are using it.

50. During mergers and acquisitions, there could be people attempting to infiltrate your data room for inside information, or if the data room itself is secure, accessing the computer system to listen in on surrounding conversation.

51. Law firms need to recognize that they are at risk. That they do have information and transactions that are potential sources of revenue for threat actors.

Recommended processes for in depth defence

52. Assessing means getting a specialist in who will do an in-depth assessment to really understand your business, someone who is going to work together with you and your IT provider and any other third parties who have access to your system

53. Remote desktops must be considered. People working from home are an area of particular vulnerability. Home computers also need to be assessed. Damian Seaton has found in such assessments that 99% of the time people have not changed the generic username and password on their router.

54. Children at home can also be a potential risk. Threat actors will approach children for information, for instance over online gaming platforms, and will offer money in exchange for information such as usernames and passwords. Children need to be informed of these risks.

55. Mobile phones also require a device management policy to keep them secure. What's the policy should a phone be lost? If the owner is leaving the company, is the phone being wiped, and how?

56. There is also what is called shadow IT, when information is being stored in an outside provider (eg. Dropbox, Google Drive). What sort of policies are in place to keep track of where data is being stored outside of the system?

57. People will do things in order to save time, and those are areas where vulnerabilities can arise, so looking at people's habits in depth is important.

58. There are many things to do in the process of making your organization secure, but it is about taking it in sequence, step by step.

59. In addition to a data breach response plan, you must think about having a data breach letter to hand, order to advise the affected clients should a breach occur

60. Determined hackers can be stopped with real time monitoring, which is the equivalent of a highly secured building with security guards, fences, CCTV etc. over your entire network. If someone from the outside is trying to get in, or someone on the inside is doing something that they shouldn't real time monitoring will set off alarms, which are monitored by a team of people who will then call your IT department to inform them and check to see why this is happening.

61. When you have a data incident, you have to think about whether or not it could be a notifiable data breach. Untrained IT providers may not be able to recognize this and will not deal with the problem adequately. If you do not make proper checks in these circumstances, you are non-compliant.

62. Once all of these things have been assessed, then you can begin penetration testing and staff training. This includes testing the staff on such things as social engineering. Also encourage staff to report anything suspicious that they may have noticed.

63. We need to change the culture and realize that we are all invested in the strengthening of our cybersecurity defenses

BIOGRAPHY

Dr. Allison Stanfield

Principal Lawyer & Founder – SG Legal Services, Wauchope

Allison has over 25 years' experience as a lawyer and in business. She advises business owners on all aspects of setting up, running, selling and acquiring businesses, and provides her clients with advice on corporate structure and property leasing.
In addition to her business law expertise, Allison also provides a range of technology law advice to clients.
Allison has a list of publications, speaks regularly at conferences, seminars and on webinars, and lectures in Business Law at Charles Sturt University.

Damian Seaton

Managing Director – Cyber Audit Team, Brisbane

Demonstrating 30 years' experience across Cybersecurity, Information Security, Data Protection & Privacy, Governance, Risk and Compliance, Digital Forensics, Information Communication Technology, Criminal Psychology, Law Enforcement.
Damian has worked with and advised organisations such as the British, American and Australian governments, ASIC, ATO, ACCC, CDPP, AFP, Tier 1 banks, Insurance companies, NFPs, Financial Practices, multinationals, and SMEs.
Damian is a Graduate of Queensland University of Technology and holds an Executive Masters of Business Administration, is an Executive Committee member of the Australian Information Security Association - the peak body for the Information Security and Cybersecurity profession in Australia, and is SAI Global qualified in Management Systems Auditing.

BIBLIOGRAPHY

Legislation

Privacy Amendment (Notifiable Data Breaches) Act 2017 (Cth)

Corporations Act 2001 (Cth)