First response checklist for law firms subjected to a cyber incident

An active cyberattack is an emergency for a law firm. The first hours and days after a large scale incident can feel overwhelming. The clear lesson from past events is that the decisions made in the first few hours can be crucial to minimising disruption, financial losses and reputational damage. Like any other overwhelming situation, it is better to briefly pause to plan, triage the first steps then work from there.

Cyberattacks vary widely in form and sophistication. The appropriate technical response will depend upon what kind of intrusion the law firm has suffered. Unfortunately, one kind of attack can also be used to launch others and sometimes one kind of attack can be disguised as another.

The starting presumption should be that all data is at risk and all systems are compromised until proven otherwise, including the backup system (whether in the cloud or otherwise).

This template checklist is a generalised response. It is not a substitute for professional advice targeted to your specific situation. Action items are marked with a checkbox (☐), information items a bullet point (•).

In summary, your response should consider the following

1. Stop the spread, prevent outgoing communication and file sharing;
2. Get help;
3. Protect trust funds;
4. Identify the attack and neutralise it;
5. Find out (to the best of your knowledge) what client data may have been accessed;
6. Let clients know, protect them and help them protect themselves;
7. Report to police, consider insurance cover;
8. Triage all other work;
9. Update clients as required, prioritise what needs to be done to protect them; and
10. Investigate fully, recover data and rebuild operational systems.

This list is in sequence, but you will need to undertake as much as you can in parallel.

Stop the spread & prevent outgoing communication

- ☐ Disconnect infected machines from the rest of the network, activate “airplane mode” or turn off wireless. If possible, leave the isolated machine running by connecting to a separate power point to enable IT to review.
- ☐ Immediately disconnect any back up system. Make sure the wireless is still off.
- ☐ Communicate with all staff to inform them and request that they do not turn on computers or other network devices until they receive further notice.
- ☐ Communicate any abnormal activity to a nominated staff member. Abnormal activity examples should be provided and might include unexpected messages (email or ‘pop ups’ on screen), unusual pc delay, unexpected programs running, uncontrolled key strokes or mouse movements – your PC security provider may be able to provide a list to your staff.
- ☐ Urgently seek qualified assistance (see “get help” below). Ask for telephone advice and follow that guidance. You may need an IT professional to urgently attend the office.
- ☐ If considered appropriate to allow limited access, ask staff to minimise the files they access and emails and files they open or send (even from personal accounts).

While you are waiting for professional assistance:

- Reset all passwords: online banking, PEXA, webmail, website, cloud storage, social media. Use a known clean device to do this. “Keylogger” malware can capture and secretly transmit the new passwords to the attackers if you use a compromised device.
- Write down the new passwords carefully in a notebook and keep them in a safe and secure place (not on the network). Don’t allow web browsers to cache new passwords until you know the system is clean.
- Undertake regular checks for unusual activity on your firm bank accounts. (See “Protect trust funds” below.).

Get help

- Ask available staff to assist.
- Contact your usual IT support, internet service provider (‘ISP’), bank and cloud storage provider/s. See what help they can offer, but don’t assume it will be free.
- For discussion with the bank see “Protect trust funds” below.
- Ask your ISP to check outbound email traffic, bearing in mind that malicious outgoing mail may be automatically deleted from your “sent” folder.
- Call your insurers. If you have cyber risk insurance, activate it. Lexon or your other insurers (such as an office policy with business record reconstruction cover) may be able to offer further advice or support – see Lexon’s HelpNow program. Lexon can also provide risk guidance on client communications following an attack.
- Consider hiring a cyberattack response consultant.
- Report any attempted fraud to the police.
- Determine who will co-ordinate the response and give others authority to speak with them if required.

Protect trust funds

- Instruct your bank to freeze all online access to firm accounts.
- Confirm that you will still be able to undertake manual transactions at the local branch. Factor in the extra time it may take to perform manual transactions for time sensitive matters.
- Find out if there have been unauthorised withdrawals.
- If necessary ask the bank to cancel unexpected pending transactions and assist you to trace funds. Contact police urgently.
- Ascertain if clients have received fraudulent instructions to deposit funds elsewhere. These instructions may be quite targeted and may look quite authentic.
- Contact QLS as any trust account irregularity must be reported to QLS immediately.

Identify the attack and neutralise it

- This is a specialist IT function.
- Do not assume that you are dealing with only one form of attack or that if you pay a ransom it will all be over.

Find out what client data is affected

- At every stage, ask your IT support to identify what data has been or may have been compromised as soon as they can tell you.
- Make sure they know that you may need to start responding before final conclusions are reached.

- ☐ Start to prioritise who should be contacted and by what method. If email is compromised, or communication from your firm has been blocked by virus scanners consider fax, secure social media and telephone.

Let affected clients know – first notification

It is tempting to put off notification until you are sure data has been lost. This is not a viable solution. Cybercriminals know they need to act fast. Even if statutory mandatory reporting obligations do not apply to you, your ethical responsibility requires that you inform a client as soon as you know or reasonably suspect that they may be at risk.

Client impact can include:

- Directions to deposit money to diverted accounts.
- Fake invoices with altered payment details.
- Receiving emails from "your firm" with malware attached.
- Critical data or all files being encrypted, deleted or (sometimes even worse) altered.
- Theft of their own customer's data.
- Identity theft.
- Fraudulent credit card transactions.
- Blackmail.
- Use of their confidential information for criminal purposes.

If you can run draft disclosure communication past your insurers before sending it that is helpful. It is also a good idea to get a trusted third party to read it to check tone and content. Ensure that any email communication is being sent from a clean, secure device and location but remember that you may now be a "blocked" sender if infected mail was sent previously.

- Prepare for a high call and email volume.
- ☐ Ensure staff have a script and a list of appropriate questions. Don't promise answers you don't have, but don't be evasive.
- ☐ Have a nominated 'go to' person for staff to communicate queries or issues that arise.
- ☐ Take a log of all calls and emails to track communications.

Other work

- Distraction is always dangerous from a negligence perspective.
- Do not take on new work if you can avoid it.
- ☐ Diarise all upcoming deadlines and allocate someone to monitor these to check that critical dates are not missed. Consider immediately printing all diaries and task lists so that dates can be accessed even if the network system fails altogether.
- ☐ Talk through "to do" lists with staff so that everyone appreciates what they should be prioritising and/or postponing.
- ☐ Where appropriate, take steps to notify parties on the other side of transactions of the issues, and consider obtaining extensions with client permission. Take a moment to consider if there might any unexpected consequences of seeking an extension (e.g. affected by other contract dates, financial year implications, interest etc.).
- ☐ If the attack has meant you are unable to access client files on the system, confirm paper files are complete and up to date. If needed, consider asking other parties (firms, barristers, and banks, courts) to provide copies of correspondence and documentation.
- ☐ If your email is affected, consider sending a fax to clients, barristers, other parties and courts requesting that correspondence be faxed instead of email until further notice.

Once you have more information - update clients and establish what they need to do

- Hopefully your professional IT advisors should be able to tell you what kind of penetration has occurred.

- Issue guidance to your clients, but make it clear that they should obtain their own expert assistance.
- Issue further updates as information becomes available.
- Obtain and follow directions from relevant insurers concerning admissions of liability.

Further resources

- There are many resources available online.
- A good starting point is the Law Council of Australia “CyberPrecedent” website. It has basic materials for non-specialists and links to detailed response manuals.
- https://www.staysmartonline.gov.au/
- https://acsc.gov.au/contact.html

A serious breach maybe very stressful. Remember that LawCare counsellors are available if you are a member of the Society on 1800 177 743. Take care of yourself and your team.

Authorised, Director, QLS Ethics Centre

13 July 2017