CYBER PRECEDENT

Strengthening the legal profession's defence against online threats

CHECKLIST:

CYBER SECURITY: WHAT TO DO IF YOU ARE CYBER-ATTACKED

It is now more likely than not that at some stage your business will have a cyber security incident. So, regardless of size, a practice should have an understanding of how to respond and recover from a cyber-attack.

This is the case even if it is just to understand what your cyber security expert is talking about when they are called to assist you. Below is a basic action list that should be considered by your cyber security response team, which should include an IT expert.

1. IDENTIFY THE THREAT

It is important to understand the extent of the attack, the nature and origin of the attack, and what, if any, strategies can be employed to limit the severity and consequences of the attack.

a. Determine what has/is happening.

i. Are files visible yet un-openable? Have file names become unrecognizable or strange symbols appearing in software? Most likely this is ransomware like Crypto-wall.

ii. Are strange emails coming in and going out of your inbox, credential errors occurring when accessing resources? Most likely an attack on your mail system and infrastructure has taken place whether from internally or externally.

iii. Have online resources becoming unavailable or is performance heavily degraded? Most likely an attack on the network (DoS, DDoS, network breach) or an attack on the infrastructure itself.

b. Determine if the problem is spreading and how is it spreading.

i. Can you identify any part of your system (such as emails or shared network drive) that is functioning abnormally?

ii. Are you able to identify an account, computer or group of computers that are inflicting the damage?

c. Determine if you are targeted directly.

i. Is this happening to anyone else (like all Yahoo mail services) or just your services?

Law Council OF AUSTRALIA

2. NEUTRALISE THE ATTACK

Limit the effects of the cyber-attack by quarantining the attack as much as possible while working to neutralise it.

a. Protect you and your client's data.

i. Disconnect affected devices from the network and change passwords.

ii. Contact hosting providers to request immediate remedial actions (, change passwords, freeze access to portals, stop all network traffic to and from affected resources, shut down drives).

b. Limit access to all data.

i. Segregate infrastructure by disabling all non-critical accounts and access.

ii. If necessary shut down all systems.

c. Find and remove threat.

i. Eliminate the source of the threat. (Since this can take many forms it is not practicable to list them all but it is a job that is best left to IT experts.)

ii. Be careful that, where possible, potential evidence that might help identify the attackers is not removed.

3. REVIEW YOUR SYSTEM

An audit of your computer system, including connected devises, is required. This will assist in determining how the system will be re-established and what steps need to be taken to reduce further risks.

a. Check all data to determine if it is affected.

i. Are you able to recover affected data and by what means and at what expense?

ii. Determine data recovery options such backups, snapshots or rollbacks.

iii. Isolate bad data to review at clean-up.

b. Prioritise data recovery methods.

i. Decide what data needs to recovered or rebuilt and what data is unrecoverable.

ii. Consider if any infrastructure needs be reconfigured.

iii. Consider if it is more economical to deal with third parties; such as paying a ransom.

4. RESTORE AND RECTIFY YOUR INFRASTRUCTURE

Ensuring that you have safe and secure infrastructure is essential in recovering from an cyber-attack as previous vulnerabilities should be eliminated. It is often better to replace infected machines or wipe them and start fresh to ensure eradication of threats and vulnerabilities.

a. Maintain isolation of your system.

b. Recreate and rebuild platform.

i. Determine if the infrastructure is to be rebuilt by restoring or if it needs to be rebuilt from scratch (reinstall all operating systems and programs).

ii. If restoring, do so from a point-in-time before the attack

c. Review entire system

i. Look for and patch all vulnerabilities, especially those that were the current liability.

ii. Undertake all system repairs and update all system software.

5. RECOVER YOUR DATA

Putting your data back onto the system needs to be done carefully so as to avoid any reinfection.

a. Ensure that you know what data is accurate and what data is unreliable.

i. Only restore data that has been checked and given the all-clear by a cyber-expert.

ii. Keep any suspect data quarantined until it can be properly assessed and given the all-clear.

b. Restored data should only be made accessible to critical personnel who are able to approve functionality.

6. TEST AND ALLOW OPERATIONS TO RESUME

Before the system is brought fully back on-line and reconnected to the network, thorough testing of the system should be undertaken to ensure that all systems are functioning properly and that the cyber threat has been neutralised.

a Test each component initially as it is restored and check internally and externally your network to ensure no issues.

b. Document any oddities for re-evaluation.

c. Only when convinced that all is well reconnected to the network and resume operations.

7. GOING FORWARD

Report, reflect and learn from the experience. Just as cyber-criminals are constantly learning from each attack, so should you.

a. Draft a post-incident report. Include:

i. What happened and when.

ii. What was affected

iii. What is the current state of your technology platform.

iv. Actions that were taken to rectify the situation and the results.

v. How you have improved and how you are going to prevent this in the future (if possible).

b. Implement changes based on the experience and the lessons learned during the incident.

c. Disclose to any relevant parties what happened;

i. Before making announcements consider obtaining advice from experts: lawyers, IT consultants, insurers, crisis management and public relations consultants.

ii. Report incident to proper authorities, agencies and regulatory bodies.

iii. Notify clients if appropriate.

iv. Make public announcement if appropriate.

v. Undertake a review of your cyber security response plan and update it where appropriate.