It's a big, bad world out there: 5 IT Security Principles Every Firm Must Know

It's time for us all to roll up our sleeves and understand that IT Security is now everyone's job, writes Damian Huon, legal technology specialist & CEO of Huon IT.

There's a lot of hype in the media around the growing risks of IT Security - and unfortunately, most of it's true.

Not a week passes that we don't see another cyber-security horror story in the news… and they're only the high-profile ones we actually hear about. Breaches happen every second around the world, to businesses both big and small. The cliché that 'no one is safe' has never rung truer.

And the costs of these breaches – both financial and to reputation - are soaring. There is simply no longer an excuse for being unprepared. A focused IT security strategy is now a bare-minimum requirement for any modern firm.

Here are five simple tips to strengthen your firm's IT security strategy:

1) MAKE IT A BUSINESS (NOT AN IT) ISSUE

IT security is a business-wide issue that deserves business-wide attention.

Far beyond the sole responsibility of your IT team, raising the profile of security amongst senior leadership across all departments is a must. Make it a top-down priority so that it filters into every facet of your firm.

LITMUS TEST - HOW HEALTHY IS MY FIRM'S APPROACH TO IT SECURITY?

The quickest way I assess a business' attitude to IT Security is via one simple question; '**Is IT Security a permanent recurring agenda item at your partner meetings?**'

If **yes**, your firm has at least acknowledged the importance of IT security as a business issue.

If **no**, you might have deficiencies in security risk awareness and responsiveness.

2) CREATE A SECURITY AWARE CULTURE

Even with the latest and greatest technology safeguards in place, the 'human factor' still leaves your firm at risk.

Cyber criminals are very creative and often quite convincing; tricking users into clicking dangerous links, unintentionally downloading malware, or accidentally releasing their password.

All staff should be educated on password and log in safety, how to recognize suspicious emails and websites (and what to do with them), and generally encouraged to exercise 'healthy paranoia' when it comes to IT security.

Then after training, go one step further – test them. There are 'fake scam' phishing emails which can be safely sent to your team to assess how they respond.

Going forward, cyber security awareness should also become a standard part of every employee induction process, too.

3) GET INDEPENDENT SECURITY AUDITS ONCE A YEAR

The world of IT security isn't static – it is ever changing, and so must be your security strategy.

To check you're still on the right path, annual security audits should become as routine as EOFY planning.

There are countless options on the market, but two core reviews every firm should undertake are:

- **Network Penetration Testing** – this looks from the outside, in. By mimicking attack patterns, any web-facing elements of your network (IP addresses, websites and infrastructure) are put to the test to identify exposures.
- **Vulnerability Assessment** – this looks internally to identify risks inside your network, including all core infrastructure, end user security, and access controls.

These audits will provide insights into any weaknesses and recommend opportunities for improvement, so that you can balance your investments versus what risks you can afford to take.

4) DO YOUR HOMEWORK ON ADAPTIVE MARKET LEADERS

While I always preach caution around bleeding-edge technology, when it comes to security, you want to select established vendors that stay ahead of the game.

IT security isn't an exact science and there's no single formula that will work for every firm. There's so many technologies on the market, the choice can be overwhelming.

And the reality is that in a few months, the threat landscape will change yet again. So it's important to select security vendors that invest heavily in research and development, and that are forward planning. Ask probing questions around the vendor's technology roadmap and frequency of updates, so that your investment will stay up to date longer in this fast paced world.

5) FINALLY, ALWAYS PREPARE FOR THE WORST

The world of cyber crime is advancing at an alarming rate and you should never become complacent. Even with state-of-the-art security defenses in place, you're still very much at risk of an attack.

Your IT department should have best practice protocols in place, including incident response management, roll back or issue isolation, clear escalation channels and appropriate reporting so that any issues are visible to senior management. This should be well rehearsed both internally and with any third parties.

DAMIAN HUON
Damian Huon is CEO of Huon IT, an IT consultancy firm specialising in strategic technologies for legal firms.