Why Implementing a Cyber-Security Culture is Essential for The Future Of Law Firms

Attributable to Dr Jamie Graves, CEO, ZoneFox

Cybersecurity attacks are so commonplace that incidents regularly make front page news. They don't discriminate either; cybercriminals target any sized company from every sector. Most alarmingly, these acts of crime are growing rapidly. Today, the Breach Level Index, which keeps count of lost or stolen data records, shows its breach counting as sitting at just over six billion records.

Law firms are a particular favourite for such cyber-criminals. PWC's 25th Annual Law Firms Survey found that 73% of respondents suffered a security incident in 2016. Concerningly, these included all types of attacks from insider threats to phishing of login credentials and ransomware.

Law practices are tantalising targets for cyber-crooks as, by definition, they keep large amounts of extremely sensitive data for long periods. This makes them a sitting duck if their security systems aren't up to scratch.

Do Legal Professionals Lag Behind When Adopting Cybersecurity Measures?

Traditionally law firms have been slow in adopting technology, but with cybersecurity becoming such a high-profile issue, this is changing.

Two major reasons for an increase in investment is the high level of cybersecurity incidents against law firms and the need to adhere with strict compliance regulations. Both these factors, along with risk management, were the top three issues to be identified in the International Legal Technology Association's (ILTA) 2016 Tech Survey.

The Challenges of Cybersecurity for Legal Professionals

As mentioned, the challenges for law firms in mitigating security issues tend to revolve around their data given the sensitive nature of client information they hold.

The thing is, given the complexity of different cyber-attacks and the determination of cyber-criminals to get hold of the highly valuable data in their possession, a variety of different methods will be used to get hold of it.

In order to understand how the most robust measures can be put in place to prevent these attacks, it's important to learn how cyber-crooks operate and where the problem areas are. The below outlines this in more detail:

Problem Area 1: Insider Threats

The pillaging of Mossack Fonesca's database in 2016 bought this type of threat to mainstream prominence. 11 million documents exposing various offshore deals, were leaked by an employee, mainly showcasing alleged tax evasion by high profile individuals. The leaked papers were encrypted by the whistleblower and sent to reporters at a German newspaper.

Known as the 'Panama Papers', the case showed the ease with which sensitive data can be leaked and the chaos it can bring. It was an example of how difficult it can be to stop an insider who wants to release information either for revenge or financial gain. At a time when big money is paid for such sensitive data on the dark web, there is also a larger motive at stake for someone within a law firm to carry out such an attack.

In finance terms, there are also big repercussions for firms. The 2017 Insider Threat Report found that 53% of companies paid remediation costs of around $100,000 after an internal breach. Reputation damage is harder to quantify (just look at the fallout Mossack Fonesca faced) and its very likely that once a law firm is breached, it's a steep curve to climb to win back client trust.

Problem Area 2: Keeping Up with Compliance

Modern day compliance is a minefield. In a survey by RedCentric of over 150 decision makers within law firms in the UK, one of the greatest challenges identified was adhering to regulatory compliance.

Data protection regulation exists in most developed countries. For example, the UK's Data Protection Act (DPA) is a law that regulates how companies use personal data. Law firms must comply with the DPA and are subject to imprisonment and fines of up to £500,000 (around $630,000).

In the USA, data protection laws are somewhat mosaic in nature and applied on a state-by-state basis, but each dictates stringent rules around data security and privacy with associated punishment for non-compliance.

In Europe, the General Data Protection Regulation (GDPR) will come into force next year and covers the security, privacy and control of personal data. Notably, and worryingly, PWC's Law Firm Survey found just 13% of practices were prepared for GDPR.

Problem Area 3: Data Breach and The Value of Information

The 2016 American Bar Association Survey of 90,000 found that 25% of both small (10-49 lawyers) and large (500+ lawyers) law firms experienced security incidents. These incidents can have massive repercussions.

In March last year, two large New York based law firms experienced data breaches. Both firms specialised in patent and intellectual property law, pointing to hackers using the breached data for insider trading on the stock market. In the same month, 48 US law firms were specifically targeted by Russian cyber criminals looking for M&A activity to use for insider trading.

Attacks like this highlight the worrying ease with which such organisations can be targeted and how much turmoil can be created.

Solving Cybersecurity for Legal Firms

When you see the numbers associated with the costs of cybercrime you would be forgiven for believing the problem is insurmountable. However, despite the growing and very lucrative cyber-crime market, the security industry has been working hard to challenge these criminals by developing new and innovative technologies.

Despite this it's important to remember that technology only goes so far to stop such attacks and should always be combined with a human element of caution and education. Here are some tips that should be followed in order to stay a step ahead and protect your firm from potential cyber-danger.

Solution One: Training and Security Awareness

One of the fundamental steps in ensuring that cybersecurity incidents are mitigated is ensuring all employees are 'security aware'. It sounds simple but creating a security culture and providing security awareness training is included in a number of regulations, including the global cyber-security standard, ISO 27001. It's also remarkable just how many businesses simply assume their staff won't slip up in the face of a dodgy email or phone call.

Security awareness instils a sense of 'security hygiene' throughout a company and mitigates against any number of potential security issues – from phishing to browsing unsafe websites or becoming a victim of social engineering. Being aware of where you might get caught short can go a long way to preventing seemingly innocuous activities turning into a devastating breach that will cost a firm's reputation and bottom line.

Solution Two: Dealing with Insider Threats

Not all insider threats are malicious. The majority of perpetrators are innocent and quite often open a gateway to a breach by clicking on something they shouldn't. This can be prevented by some straightforward, ongoing security training.

When it comes to solving the problem of a malicious insider, it's a far more complex game, especially at a law firm that provides rich pickings for someone intent of selling on proprietary data for revenge or a big pay-cheque.

To combat it is to understand threats and insider threats often follow a complex chain of events. A combination of both expected behaviour and more unusual actions can make spotting risky activities a complex and time-consuming issue to solve.

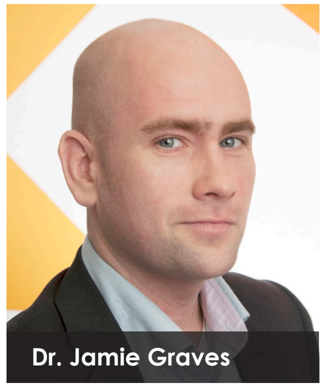
Using user and entity behaviour analytics (UEBA) technology can give firms far more insight into the network behaviour of users. Using machine learning, the technology gradually builds up a profile of 'ordinary' behaviour of the user - where and when they access data from, what files and systems they use regularly and if they download and remove information from the network.

This means that deviations from the norm such as late-night file access, the downloading of sensitive information and logging in from completely new devices can be flagged up, potentially alerting the firm to risky or anomalous behaviour before it would be possible for a human to spot it.

Getting an Absolute Discharge for Cybercrime Events

Law firms are prime targets in this new wave of organised crime with numerous methods used in order to get inside their firewalls. The resulting financial, reputational and ironically, legal damage, can often be hard to come back from – particularly for a small firm.

As cyber incidents from both sides of the fence continue to increase, law firms need to take positive action to contain the onslaught. Human beings will always push the boundaries, we can prevent those boundaries being broken using a combination of knowledge, education, training and state-of-the-art technology. If such methods aren't adopted and cyber-security isn't prioritised at board level, then it's all the more likely more attacks targeted at law firms will continue in attempts to obtain the precious data they possess. **LM**


Dr. Jamie Graves

About ZoneFox

ZoneFox is a world-class security platform that effectively combats the growing issues of insider threats to organisations across multiple sectors. Through ground-breaking and sophisticated UEBA and machine learning, the technology delivers rapid, actionable insights around user behaviour and data flow, both on and off the network.

ZoneFox strengthens security posture and enables security teams to see where business critical data is going, who is accessing it and importantly who is doing things with it that they shouldn't be – either accidentally or maliciously – quickly, easily and without impacting on endpoints or user privacy.

Based in Edinburgh, ZoneFox is headed up by Dr. Jamie Graves, a former PhD student at Edinburgh Napier university.