



Tackling the Human Aspect of Cyber Security:

THE PSYCHOLOGY OF A LAW FIRM

Oz Alashe MBE
Tom Cross

www.cybsafe.com




TABLE *of* CONTENTS

The threat to the legal sector

The psychology of a cyber-attack victim

The psychology of a law firm

- ⊙ Partners
 - ⊙ Associates
 - ⊙ Trainee solicitors
 - ⊙ Support services
 - ⊙ Remote workers
- 

Training the brain to tackle cyber risk



The threat to the legal sector

In the aftermath of headline-grabbing cyber attacks, managing partners in law firms around the world have been posing the same question to their firm's IT leaders: **"Could this happen to us?"**

"Yes" is likely the honest answer. As the legal industry has become increasingly digitised, it becomes even more susceptible to the threat of a debilitating data breach.

Law practices are a potential goldmine for cyber criminals, with confidential client records offering rich pickings. The kind of information that circulates daily in firms – banking records, company accounting reports, address details, and insurance records – can be extremely valuable to cyber criminals. Identity theft, IP theft and bank fraud, just some of the hacker's potential gains.

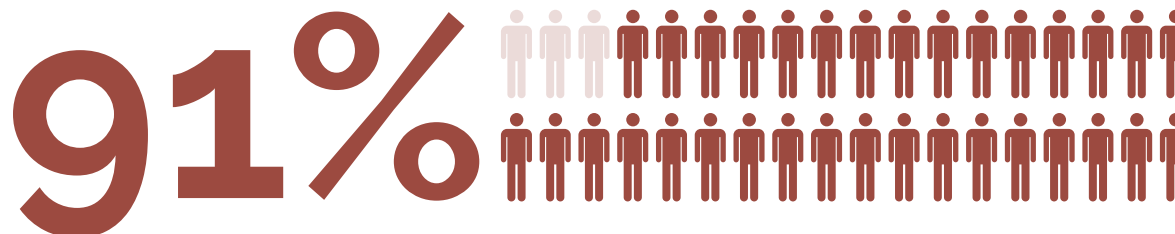
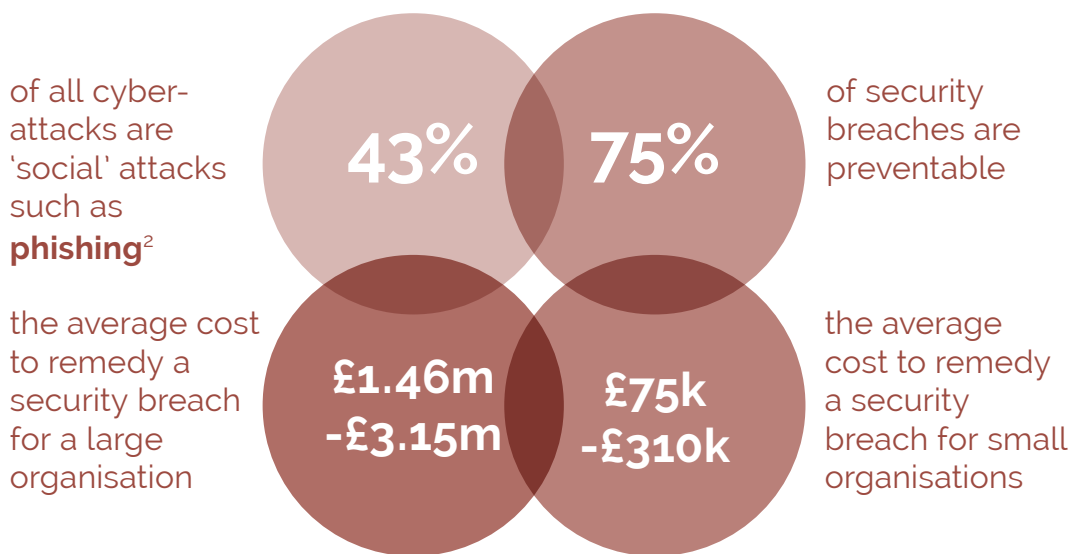
As the Law Society has stated: *"In today's interconnected world, cyber-attacks are a threat to all businesses - and law firms are particularly attractive sources of information for criminals. Commercial data, IP information and sensitive client data may all be targeted."*

Peter Wright, Chair of the Law Society's Technology and Law Reference Group, and managing director of DigitalLawUK adds: *"Cybercriminals have realised that even the biggest law firms do not have the same cyber security capabilities and resources as big multinational banks, and as such are increasingly turning their attention to professional practices to gain information on high-net-worth individuals such as solicitors, accountants and insurers."*



But what can law firms do to reduce the chances of a successful data breach?

When 75 percent of data breaches can be attributed to a human component, the first thing to consider is the **people in the firm itself**.¹ Different people are susceptible to different forms of cyber attacks, and analysing this victimology can be vital in helping IT leaders in law firms reduce their cyber risk profile. By identifying the most prevalent risk factors, the psychological basis for these risks and the profile of the roles most affected by these – from partner to trainee solicitor and business support– we can determine the best methods for IT teams to mitigate these risks in the legal sector.



of people "don't know much about protecting themselves online"

1 http://www.apogeeinsgroup.com/images/Marketing_Materials/lawyer_data_breach.pdf
 2 <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>



Cyber Security and the Legal Industry

The primary method for IT attacks against the legal sector is **phishing emails (33%)**³

In security awareness training exercises conducted by Verizon, just over 10% of employees in the legal industry **were successfully phished**, compared to 8.5% in financial services and 7% from the utilities sector.⁴

The legal industry is **one of the most targeted sectors in cyber espionage**, behind only manufacturing and the public sector.

3 <http://www.bluelogic.co.uk/cyber-attacks-cost-uk-legal-sector-%C2%A320-million>

4 <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/>

The psychology of a cyber-attack victim⁵

Certain demographics as well as certain psychological factors contribute to an individual's risk factor. Here are some of the most important psychological drivers in cyber security:

Trust and authority

People are significantly more likely to comply with requests from authority and trusted figures. Hackers have higher success rates in scams where the perpetrator misrepresents themselves as someone from a trusted organisation or brand the victim is familiar with. For example, in phishing emails, cyber criminals will often use logos and mimic email addresses of companies that people have confidence in such as their bank or a retailer.

5 https://www.researchgate.net/publication/272246573_Scam_Compliance_and_the_Psychology_of_Persuasion

https://www.researchgate.net/publication/262276193_Improving_Compliance_with_Password_Guidelines_How_User_Perceptions_of_Passwords_and_Security_Threats_Affect_Compliance_with_Guidelines

Stanley Milgram experiment

An experiment by Stanley Milgram, a Yale psychologist studied the limits of compliance based on two participants: a “**teacher**” and a “**learner**”. The “teacher” was told by the ‘doctor’ in charge to administer an electric shock every time the “learner”, an actor, made a mistake during the test, increasing the level of shock each time.

The result of the experiment demonstrated the extent of human compliance to authority. Under the impression that the shocks were real, at the behest of the ‘doctor’ to continue with the shocks, and despite the desperate pleas and cries of pain from the “learner”, 65% of subjects continued to the final severe shock level.

The Milgram experiment illustrates just **how compliant people can be when presented with even the mere illusion of authority**. The test goes a long way toward explaining why phishing scams from trusted sources such as banks have a high success rate; very simply, people are more likely to comply with an authority figure in the belief that the person in authority has more knowledge than they do.

Restraint bias, affect bias, and the illusion of control

Known as ‘restraint bias’, individuals usually overestimate their ability to control impulsive behaviour. This lack of self-control increases the likelihood of being conned as individuals have a harder time regulating their emotional responses. Low self-control has also been shown to be a strong factor influencing rational choice in individuals, making the prospective victims more compliant.⁶

6 Carter, 2001; Nagin & Paternoster, 1993

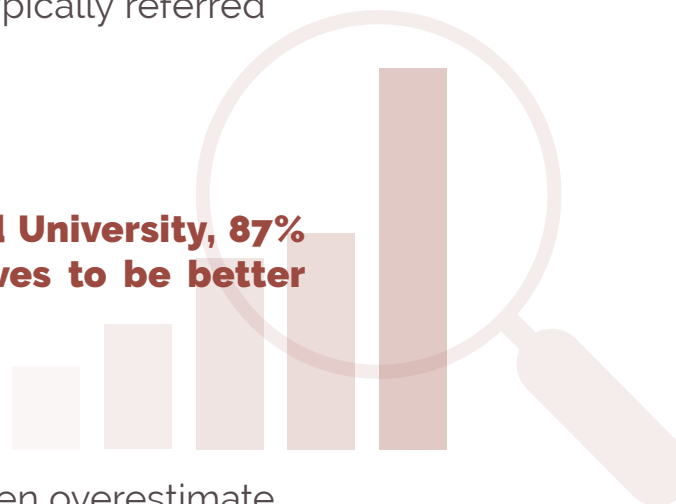
Related to the illusion of control is the capacity to be swayed by emotions: 'affect bias'. Affect bias explains the tendency for decisions to be affected by a person's mood. Excitement, curiosity, and anger, can all act as agents to change human behaviour, and can influence someone to disclose information, or click a link or wire money to a new account.

Tim Hill, technology policy adviser at the Law Society:
"We would all like to dismiss scams as something that only happen to other people, people who are not as technically capable as us. Yet basic weaknesses, such as opening the wrong link or file, are what cyber-criminals prey on."

Illusions of superiority

People are normally overly optimistic when evaluating their own ability on intellectual tasks. An individual's lack of ability at a particular task deprives them of the skills needed to recognise that lack of ability- typically referred to as the 'Dunning-Kruger effect'.

In a psychological study at Stanford University, 87% of MBA students reported themselves to be better than the median.



In other words, prospective victims will often overestimate their ability to detect cyber threats- people think that they are better at detecting threats than they actually are. This is also known as the '*optimism bias*'.

The psychology of a law firm:

⦿ Partners

Partners tend to be the most experienced and elder members of the firm. Often more trusting of communications from traditional institutions like banks and government bodies, partners are more likely to fall victim to social engineering attacks such as spear phishing.

For cyber criminals, the potential rewards from targeting a partner compared to junior members of the firm make it worth the time invested in researching and crafting these highly targeted spear phishing emails.

Commonly under most pressure and juggling various time-critical tasks, those in the highest ranks of the business world often suffer from “attentional bias”. That’s to say, due to the intensity and volume of work, these individuals have a tendency to miss fully visible objects or events simply because they were unexpected and their focus committed elsewhere.

In addition, people who have been working in the same environment for many years (typical of partners in a law firm) may experience ‘normalcy bias’, or ‘normality bias’. An individual might assume that because they have never personally experienced a disaster, they never will. In cyber security terms, this typically results in situations where people fail to adequately prepare for, or even consider, the possibility of being victim of a data breach.

What can IT do?

- Partners are more likely to be concerned with the reputational damage to the firm and lost business. Highlight any examples of lost revenue from similar companies to emphasise the importance of cyber security.
- The cyber awareness programme should prioritise a few key and non-negotiable aspects of cyber security – e.g. password management or spotting a phishing email to get the buy in of time-poor partners.
- Tackle the normality bias through penetration testing. This demonstrates just how easy it can be for the firm to be hacked.

£1 million:  **the average cost of lost business following a data breach⁷**

⦿ Associates

Often spending a significant proportion of their time out of the office, visiting clients, in court and at industry events, associates can fall victim to cyber attacks when on the move – it's easier to get someone to click on a malicious link on their phone.

In common with partners, associates work long hours and have access to some of the most sensitive data in the firm. They embody a dangerous combination of being both highly valuable and highly available to hackers. However, associates will likely spend more time online and on multiple devices, increasing their cyber risk factor compared to more senior partners.

Firmly established within the organisation, associates may also be particularly disposed to 'groupthink' - a way of thinking whereby group members try to minimise conflict and reach a consensus without evaluating alternative viewpoints. In the context of cyber security, associates may fail to act appropriately if they observe a data breach, or potential flaw in the company's cyber security strategy in an attempt to avoid embarrassment or anger from senior colleagues.



What can IT do?

- Use the Messenger effect by getting partners to explain how important cyber security is to the firm. Associates are more likely to raise their cyber awareness if partners are champions of cyber security - make the Stanley Milgram effect work for you.
- Give staff the confidence to alert you in the event of a data breach, or if they observe a potential security flaw. IT should make sure that cyber security is not a 'dirty topic'.
- The cyber awareness programme should focus on breach recovery, including reporting procedures, and tips on what to do in the event of a breach.

Trainee solicitors

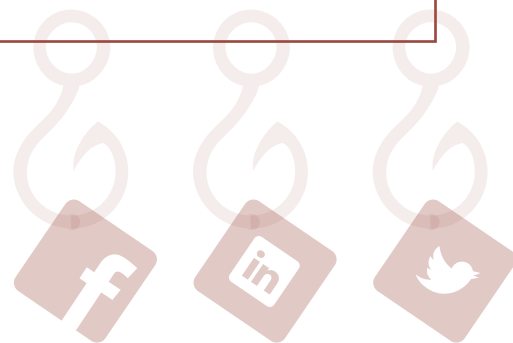
Lacking an in-depth knowledge of the ins and outs of the firm, trainee solicitors represent soft targets for hackers.

In an act of 'information cascade' – when a person observes the actions of others and engages in the same acts – trainee solicitors may adopt the poor cyber security practices of more senior peers to avoid rocking the boat.

While trainee solicitors may be more digitally savvy and more circumspect of suspicious emails, they're much more likely to expose a greater part of their lives on social media than partners. They are also more likely to reuse passwords, due to the number of online services they are signed up to, giving hackers multiple vectors to access sensitive information.

What can IT do?

- Introduce password managers such as LastPass or highlight password best practice as often as possible.
- Implement clear social media guidelines that highlight what can and can't be shared on social media.
- Gamification of cyber security can be a good way to educate trainees with engaging and educational content. This can be vital in driving behavioural change with digital native millennials.



Support services

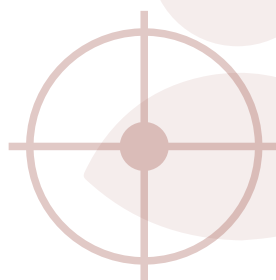
These include positions in marketing, human resources, and other roles vital to keeping the firm functioning and productive. Support staff often handle private data that could prove profitable for a cyber attacker, from bank details of suppliers, to tax information of staff.

Support staff are also more likely to work with external suppliers – the Head of Marketing will handle sensitive information with the PR agency, while the Head of HR will handle sensitive information with recruiters for example. For IT, this is an issue around securing the supply chain, ensuring that the firm's entire IT estate is as secure as possible, not just the internal systems.

What can IT do?

- IT teams should work with trusted vendors where possible, requesting cyber security audits prior to engaging suppliers and placing greater value on industry standards, such as ISO 27001.
- Introduce an awareness training programme which includes content on securing the supply chain, covering relevant legislation such as GDPR and technology commonly used by these functions, such as file transfer services.

The 2013 cyber-attack against the US retailer Target, which has already cost the company \$252 million, possibly rising to as much as \$1 billion, was the result of a data breach of the retailer's air conditioning supplier.



🕒 Remote workers

Few industries are as wedded to physical presenteeism as the legal industry. But remote working is becoming more and more common in firms around the country, with the realisation that much of the job can be done as effectively outside the office.

While this has its benefits, remote work brings with it unique cyber security threats. For example, remote workers are more likely to use unsecured public Wi-Fi connections in cafes or on trains. Without direct contact with the main office, employees can very easily fall victim to tactics such as man in the middle attacks.

The psychological theory of 'risk compensation' - the idea that people adjust their behaviour in response to the perceived level of risk - is important here. Remote workers have a greatly diminished perceived risk compared to office-based staff; they may take more information security risks as they believe the out-of-office environment - their home, a coffee shop, or a train, for example - poses less of a risk to the firm's data systems.

What can IT do?

- A fundamental trait of the human psyche is our desire to belong to a group of some shape or form- groupthink. Involve your remote workers in cyber security training in order to encourage a firm-wide culture of good cyber security practice.
- Introduce office message systems and team collaboration tools such as Slack or Yammer to foster a team ethos, which will help the remote worker feel they have a stake in the information security of the firm.
- Choose a cyber awareness programme which stresses the importance of a secure internet access when accessing sensitive documents and accounts.



Training the brain to tackle cyber risk

The emotional brain is stronger and quicker than the logical brain and this can cause people to make incorrect and rash decisions where cyber security is concerned. This is especially true in high pressure work environments. A combination of high standards and a heavy workload makes it easy for a tired brain to look for a quick fix in order to get onto the next task. Impulsive and emotional decisions are more common in this state and these can lead to a security breach.

Once organisations begin to take a modern, psychologically-minded approach to their cyber security, they'll find an actual, tangible change in online behaviour.

By accounting for this 'human factor' in cyber security - a combination of psychology and education - law firms can start to seal the cracks in their cyber defences and reduce the chances of succumbing to a data breach. Whether a firm wishes to prevent phishing, malware, password attacks or ransomware, employees can be a first line of defence.

A good cyber security strategy starts with people.

The National Cyber Security Centre found that even though 75% of respondents ran ongoing awareness programmes, only 15% exhibited the positive behaviours and heightened awareness the programme was designed to create.

It's one thing to train staff; it's quite another thing for staff to act on that training.

Through awareness raising and training we are suggesting that the rational brain can be increasingly accessed to form a more effective mindset in tackling cyber risk. Organisations need their people to have a curious and questioning brain, but one that follows cyber security processes even when under internal or external pressures—that ideal mix of the emotional and rational.

Ciaran Martin,

CEO of the National Cyber Security Centre:

"[Businesses need to] get serious about understanding the human being in all this... I think this is the most important shift in thinking over the past year or so, the wider recognition of the importance of the user... To get cyber security right, we need to connect those human factors to that Boardroom conversation."

Simon Holdsworth, Managing Partner at Thrings:

"Cyber-attacks are rising at an unprecedented rate and becoming increasingly sophisticated. As a law firm, we take the protection of our own and our clients' data extremely seriously. Managing our infrastructure in the most efficient and cost-effective way possible is vital."



The tick box approach: taking a check box approach assumes that everything will be OK if firms comply with a set of rules or training standards.

The training manual approach: overwhelming staff with technical information or giving staff unwieldy 'training manuals' is ineffective; simply reading facts doesn't mean those facts will be acted on.

The one-off training session approach: these painfully unengaging marathon sessions have little impact due to the required concentration for the training to be consumed.

The "doom and gloom" approach: simply telling individuals how damaging a cyber attack could be won't elicit changes in behaviour. It can increase the danger of 'data breach fatigue', which can be counter-productive in changing behaviour.

A behavioural approach: education needs to transform human psychology itself and fight against our instinctual human emotions – analogue instincts must be adapted for the digital age.

A bite-size approach: it's well documented within educational psychology that people digest more information in smaller, regular bites.

An adaptive, individualised approach: different people learn in different ways so incorporate a variety of video, text and images to cater for the individual.

A modern approach: embrace modern technology that enables training to be done at a time and place convenient for the individual.

A verified approach: individuals should be tested to ensure they have retained information adequately and would be able to act on that information.

To find out what your company can do to become secure, head to www.cybsafe.com

ABOUT *the* AUTHORS



Tom Cross,
*CPsychol, HCPC Psychology
& Behaviour Change Expert*

Tom looks at the behavioural science and psychology aspects of CybSafe. He is a performance psychologist and behaviour change expert and has a successful track record of using his experience to help people achieve extraordinary results in business and elite sport. Tom's professional and academic insight into human psychology and the optimisation of human performance make him an invaluable member of the CybSafe team.

Tom has a keen interest in technology, the way in which we interact with it as humans, its impact and the psychology behind its usage. As a result, Tom's interest in cyber security is largely focused around behaviour change, coaching and leadership.

Tom is a British Psychological Society (BPS) Associate Fellow, a Chartered Sports and Exercise Psychologist and a Registered Practitioner Psychologist with the Health Care Professions Council in the United Kingdom.



Oz Alashe MBE
CEO & Founder of CybSafe

Oz has been the driving force behind CybSafe - the concept, vision and platform.

A former Lieutenant Colonel in the British Army and UK Special Forces, Oz has a successful track record of developing strategy, driving innovation and leading implementation in both the public and private sectors.

His background gives him a unique insight into the socio-technical realities of cyber security and the sensitivities around changing human behaviour.

Oz was awarded an MBE for personal leadership in the most complex and sensitive of conflict environments.

CLICK HERE

if you would like to hear more about CybSafe and how it helps you address the human aspect of cyber security risk.