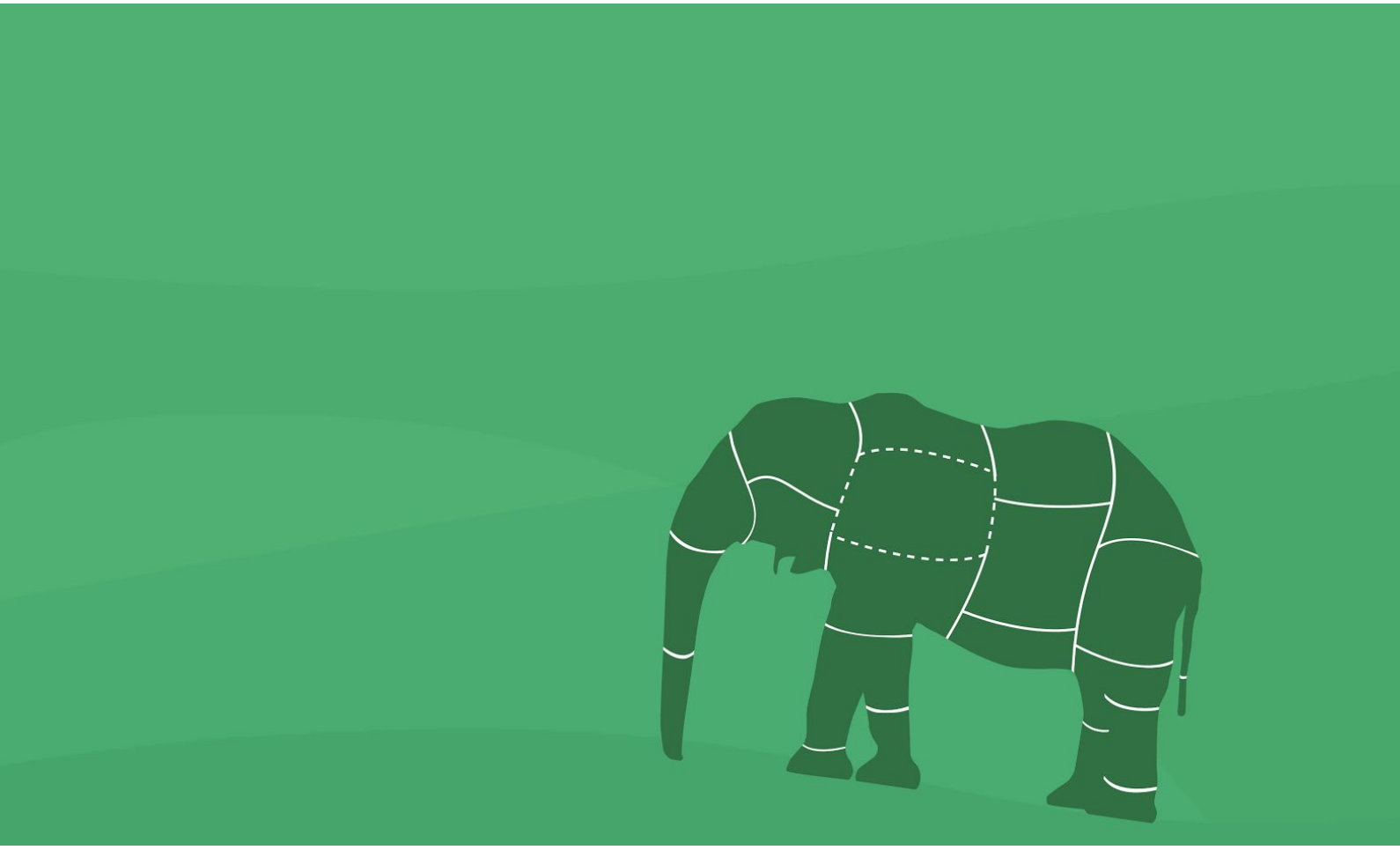
DMARC

INDUSTRY REPORT



Addressing Cyber Risks Identified in the SRA Risk Outlook Report 2016/17

Preserving email integrity and firm reputation

Introduction

Cyber crimes are again making front page news as a new strain of ransomware[1] hit some of the world's largest companies.[2] The profusion of strains of ransomware (Petya, WannaCry, Jaff)[3] compound the cyber crime problem, a problem which is already presented in the most Byzantine and convoluted way. The cyber problem due to its size and complexity seems unwieldy and unmanageable. This paper posits that this is partly due to the way cyber crimes have been classified using multiple names for the same underlying technique.

Cyber crime - A significant concern for law firms

While all businesses in the UK are at risk of data theft / fraud,[4] a breach within a law firm poses an exceptional risk to clients, the firm and wider society. Speaking about the impact of the legal sector generally, the Chief Executive of the Law Society, Catherine Dixon explained:

> 'The provision of expert legal services is fundamental to the success of business and commerce and underpins the very fabric of our society.'[5]

With an economic value of £25.7 billion to the UK economy and as a net exporter up 5.6% in real terms over 10 years (valued at £3.6 billion), the robust defense and protection of the UK's law firms' cyber presence is critical to law firms individually and collectively, to clients trust in the legal sector, to the economy and 'to the very fabric of our society'. The SRA's Risk Outlook report 2016/17 makes references to the increased instance of cyber crime acknowledging that it continues to be a significant concern for law firms.[6] Moreover, the Risk Outlook report stated that a 'quarter of law firms have been targeted by cyber criminals',[7] while it was also suggested that the 'true figure is likely to be higher' as a result of under-reporting or the absence of detection,

citing a report filed in 2015 by the Office of National Statistics (ONS). The contention that cyber crime is under-reported is echoed by IBM's CEO who commented that 'a significant portion of cyber crime goes undetected, particularly industrial espionage where access to confidential documents and data is difficult to spot.'[8]

There are 10,425 law firms operating across the UK, employing 370,000 in the legal services industry, 63% of those either solicitors or employed by solicitors' firms, it is likely that the vast majority are using email and maintaining sensitive client data electronically.[9] Of the 10,425 law firms, the top 100 law firms across the UK serve many of the 2,600 firms listed on the Main Market, London Stock Exchange (LSE). With the possible exception of health records, it is difficult to conceive of a greater threat to consumers than to leave law firms vulnerable.

Given the importance of the legal sector to the economy, because law firms rely upon maintaining trust, confidence and sensitive data and because British law firms attract business globally, it is imperative that UK law firms deploy robust cybersecurity measures especially in the face of easily identifiable system vulnerabilities.

Lawyers' duties

Law firms are in an unenviable position;

- they have a statutory duty to maintain client confidentiality, further to the professional principles contained in the Legal Services Act (2007),
- the SRA mandates a number of principles including an obligation on law firms to keep the affairs of their clients confidential unless disclosure is required or permitted by law,[10]
- their businesses rely on client trust being maintained,
- they are required to 'run [their] business or carry out [their] role in the business effectively and in accordance with proper governance and sound financial and risk management principles.'[11]

They must advise clients on GDPR while they themselves are vulnerable to data breaches.

- With the General Data Protection Regulation (GDPR) coming into force in May 2018, raises the maximum fine from £500,000 to £20 million or 4% of global annual turnover for certain data breaches. Meanwhile, law firms are already on express notice that they are being targeted by scammers.[12]
- they are under a duty to replace client monies, rule 7.1 of the SRA Accounts Rules 2011
- Any breach of the rules must be remedied promptly upon discovery. This includes the replacement of any money improperly withheld or withdrawn from a client account.
- Law firms may fall foul of provisions contained in the Insurance Act 2015 if they do not meet their duty of fair presentation by failing to disclose the risks vis a vis exposure to scamming instances (i.e. BEC/EAC/spear phishing/email impersonation) to the insurance company. The provisions which bite, include but are not limited to:
- s3(1) Before a contract of insurance is entered into, the insured must make to the insurer a fair presentation of the risk'
- s3(4)(a) The disclosure required is as follows...disclosure of every material circumstance which the insured knows or ought to know

- Knowledge of insured, S4(1) This section provides for what an insured knows or ought to know for the purposes of section 3(4)(a).
- s4(6) ...an insured ought to know what should reasonably have been revealed by a reasonable search of information available to the insured (whether the search is conducted by making enquiries or by any other means).

Significant cyber risks

Given the innumerable types of cyber crimes that affect firms generally, it is unsurprising that the SRA Risk Outlook Report[13] referenced CEO fraud & Friday afternoon fraud. These represent a significant problem for businesses in terms of cash and data theft and the reputational damage which follows as a result when those systems are breached.
CEO fraud & Friday afternoon fraud use the same imperfection in the protocol but in a different way. Between 1 - 26 June, the SRA reported 16 email scams, a review of email scams supports the view that email scams fall broadly into two categories.

1. Sender fraud*
2. Recipient fraud

Sender fraud

With sender fraud i.e. ***email impersonation, business email compromise,*** the sender's domain has a critical vulnerability which is open to exploitation. These impersonated emails look authentic and there is no way for the receiver to distinguish an authentic email from an 'impersonated' email by inspecting even if (a) the receiver takes the time to view the emails 'original source' (b) the recipient has added the genuine sender to contacts. This scam fools not only the human recipient but also the recipient's device. Technically it is the most sophisticated of the email frauds. This email fraud appears to the recipient's device as though it is coming from the authentic sender even often times capturing the picture of the authentic sender, so if the 'sender' is already saved to contacts, it may integrate the message with the existing contact information.

It is critical to note that while this is the most technically sophisticated of the email scams, the technique does not require the scammer to be technically proficient. The imperfection in the protocol can be explained in a matter of minutes. The absence of technical complexity may help to explain why this is deployed with such frequency by cyber criminals.

Sender fraud solution

The imperfection in the protocol can be addressed, this will protect business email and prevents this type of fraud. The solution for this particular cyber crime type is the DMARC[15] standard (Domain-based Message Authentication, Reporting, and Conformance). It is 'a way to make it easier for email senders and receivers to determine whether or not a given message is legitimately from the sender, and what to do if it isn't.'[16]

OnDMARC survey

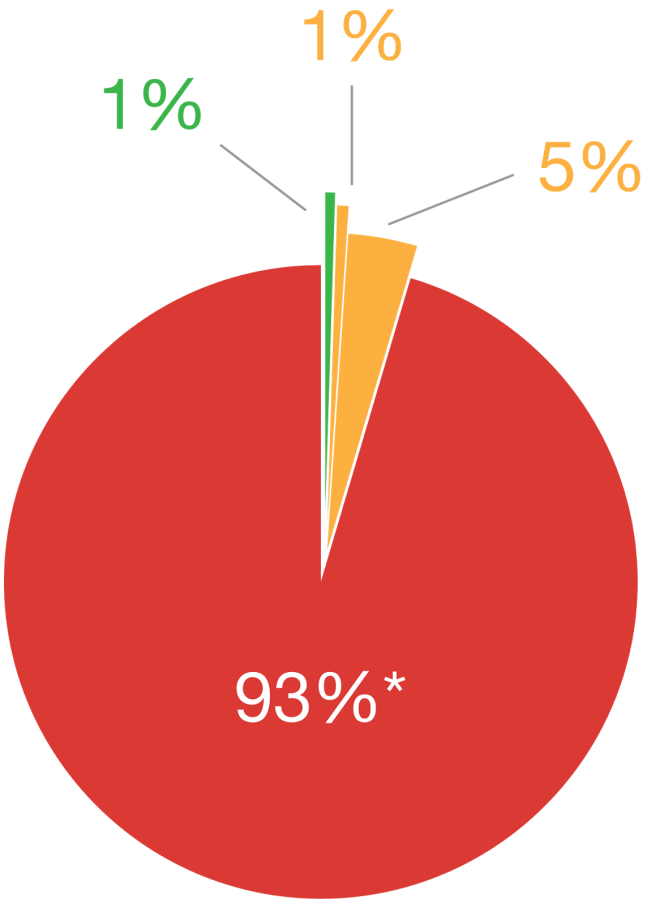
OnDMARC conducted a **unique survey**, of the top 100 law firms in the UK, only one firm had full protection in place revealing critical vulnerabilities for the remaining law firms.[17] If this vulnerability remains unresolved, it represents an open door opportunity for scammers.

The results are as follows:

1. DMARC fully deployed / reporting in place / full protection - 1 firm
2. DMARC partially deployed / reporting in place / partial protection - 1 firm
3. DMARC partially deployed / reporting in place / no protection - 5 firms
4. DMARC not deployed / no reporting / no protection - 88 firms

Following the survey, **a series of interviews** was conducted with a number of leading law firms, early results indicate a lack of awareness of the problem and solution, with each law firm stating that they believed a different solution was in place.

It is hard to judge an organisation's cybersecurity posture externally and harder still to normalise for comparative purposes. However, one option is to look at the adoption of fundamental cybersecurity solutions such as the DMARC standard[18] and use that as a bellwether. Fundamentally, what are the minimum steps that need to be taken by firms to protect their IT infrastructure and are those steps being taken?



Recipient fraud

Unlike sender email fraud, recipient email fraud, is not as technically sophisticated as the sender email. The fake email address can be detected by the recipient on inspection. The device will not integrate fake emails into an already existing contact. A recent example of recipient fraud was detailed recently on the SRA scam alert page.[19] Using the details of a regulated lawyer within a top tier law firm a top 100 firm (Norton Rose Fulbright LLP[20]), scammers attempted to exploit a recipient by purchasing a similar domain, sending emails from attorney@fulbrightlawchamber.com.

In instances such as these the burden is on the recipient to take care that messages are bona fide. A simple solution exists for this type of crime, as well as increasing awareness of the problem which the SRA is managing through their Scam Alert web page[21], email users need to add trustworthy business connections into their contacts at the outset. In those instances, if the email comes from anyone other than a trusted contact, the email address will look different giving the recipient a better chance of spotting a fake email address.

Cyber crime generally

Besides the email impersonation problem discussed above, the whole area of cyber crime needs attention. There is an overall lack of clarity and there is a tendency to (i) bundle the reporting of cyber crimes on the one hand and (ii) report the same exploit by a variety of names. As an instance of bundling, take for example the following headlines:

> UK fraud hits record £1.1bn as cyber crime soars[22] (reporting a 55% year on year rise).
>
> How cyber criminals targeted almost $1bn in Bangladesh Bank heist.[23]

There appears to be a tendency with reporting to agglomerate cyber crimes in a way which is not done with ordinary crimes. This conflation of cyber crimes is unhelpful as tackling 'cyber crime' is to put it colloquially, the equivalent of trying to swallow the elephant whole. But as mentioned above, the problem is further exacerbated by consigning a variety of names for the same technique.

For instance, the Federal Bureau of Investigation's (FBI) reporting unit Internet Crime Complaint Center (IC3) identified similarities in the techniques used in both Business Email Compromise (BEC) and Email Account Compromise (EAC) prompting IC3 to start treating these scams as a single crime in 2017.[24] The scam, as defined in the report, is carried out when 'a subject compromises legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfer of funds'.[25]

The BEC/EAC scam is widely reported elsewhere as 'spear phishing' defined as 'the fraudulent practice of sending emails ostensibly from a known or trusted sender in order to induce targeted individuals to reveal confidential information.' The equivalent techniques are employed in ***CEO email fraud & Friday Afternoon fraud***.[26] Therefore, while the cyber crime landscape starts to look unwieldy, it is to some degree merely unnecessarily complex. Businesses in particular without the requisite in house skills are likely to struggle with solutions to address what appears like innumerable problems.

The USA is considered 'extremely well' connected with ICT usage at 87%,[27] while recent figures compiled by the ONS, indicate an equivalently 'extremely well' connected population of the United Kingdom (UK) with 92% of the population as internet users.[28] Data from US businesses put cyber related risk as their primary operational concern.[29] In the absence of similar data from the UK, data from the US is instructive; the inference being that similarly well connected communities are likely to face the same cyber challenges.

Cyber crime constituent parts

By breaking down cyber crime into its constituent parts assists in developing cyber resilience protocols and processes, with reference to the elephant analogy, it makes sense to divide associated cyber risks into more manageable parts.

As Professor Wall's matrix of cyber crimes[30] clearly delineates, there are really only three types of cyber crime: -

Crime Types ⟶	Crime against machines/ Integrity- related	Crime using machines/ Computer-related	Crimes in the machine/ Content - related
Opportunities ↓	/ Harmful / Trespass	Acquisition/ (Theft / Deception)	Obscenity/ Violence
Cyber-Assisted Crimes - Traditional crime using computers More opportunities for traditional crime	• Phreaking • Chipping	• Frauds • Pyramid Schemes	• Trading sexual materials • Stalking • Harassment (personal)
Cyber-Enabled Crimes - Hybrid cybercrime New opportunities For traditional crime (e.g., organisation across boundaries)	• Cracking/ Hacking • Viruses • Hactivism	• Multiple large-scale frauds • 419 type fraud • Trade secret theft • ID Theft	• Online Sex trade • Camgirl sites • General • Hate speech • Organised paedophile rings (Child abuse)
Cyber-Dependent Crimes - True Cybercrime New opportunities for new types of crime (Sui Generis)	• Spams (list constuction and content) • Denial of Service • Information Warfare • Parasitic Computing	• **Intellectual Property Piracy distribution** • **Online Gambling** • **E-auction scams** • **Phishing, smishing, vishing**	• Cyber-sex • Cyber-pimping • Online Grooming • Organised • Bomb talk /Drug talk * Targeted hate speech • [Social network media crimes]

(i) crimes against machines
(ii) crimes using machines
(iii) crimes in the machine (i.e. content)

Wall by introducing an additional layer of classification into his matrix succeeds in simplifying cyber crime into more manageable segments -

(a) cyber assisted crimes, traditional crimes using computers e.g. fraud, harassment.
(b) cyber-enabled (hybrid)[31], new opportunities for traditional crime e.g. viruses, hacktivism.
(c) cyber-dependent crime - new opportunities for new types of crime e.g. phishing, denial of service.

This simplification is critical to re-thinking solutions, by refining the language around cyber crimes, it is possible to hive off the elephant into manageable chunks. Instead of lumping all the types of crime and criminal opportunities under a single nomenclature, when discussing cyber crime, it helps to be more specific. In order to achieve this we need the input of technical experts, legal practitioners and legal researchers working together to (a) better understand the underlying technique (b) then properly classify cyber crimes and (c) develop cyber solutions.

The operational risk to businesses is now so well understood that addressing cyber matters is now a board level responsibility[32] and is no longer the province of the IT department or a single entity within a firm. With the introduction of the General Data Protection Regulation (GDPR) in Europe, the penalties alone for data breaches are set to rise to eye-watering levels increasing from a maximum of £500,000 to £20 million or 4% of annual global turnover, whichever is higher.[33]

As early as 2015, cyber crime was considered 'the greatest threat to every profession, every industry, every company in the world'[34]. By 2019 the cost of cyber crime is projected to reach US$2 trillion globally.[35] The World Economic Fund (WEF) estimated the cost to the global economy of cyber crime at $445 billion a year,[36] while hacking attacks in the UK alone have cost businesses £42 billion since 2013.[37] And according to the Office of National Statistics, cyber crime is on the rise.[38]

In a study conducted by Oxford Economics, a typical FTSE 100 firm share price will decline by 1.8% on a permanent basis following a severe breach (this equates to -£120m on average) further amplified to a 15% decline in value.[39] The long term damage to the firm cannot be overstated.

When cyber crimes are reported, typically there are a myriad of ways in which firms and individuals have been defrauded. The National Crime Agency lists six common cyber threats for consumers which includes phishing, ransomware, keylogging and screenshot manager.[40]

Typically, society does not tend to report or discuss non-tech crimes in such a manner. To what degree it's unhelpful is a matter of speculation, but take the following example:

To safeguard against burglary, diligent homeowners lock their windows and shut their front doors. It's a simple practice, that is well understood and adopted. Yet, nobody would expect that taking these particular steps would protect against pickpocketing on the London Underground. They are recognised as two separate crimes even though both involve the misappropriation of property contrary to section 1 Theft Act 1968[41]. Moreover and more importantly, these crimes are conducted in a different manner. A different 'skill set' is employed by the thief or thieves in each instance to achieve their objective. Similarly cyber criminals, like the real world criminals, deploy a different tool set to achieve similar objectives and guarding against one, won't guard against another.

Social scientists have conducted experiments in the real world which show that: "untended property becomes fair game for people out for fun or plunder, and even for people who ordinarily would not dream of doing such things and who probably consider themselves law-abiding."[42] By analogy, it is likely that opportunistic individuals are set to take advantage when the prospect of prosecution is unlikely or because jurisdictional issues add a layer of complexity to an already knotty problem.

Significant risks for business

Given that cyber crime is on the rise generally, that technological risks are considered by the World Economic Forum (WEF) to be a significant concern, with massive data fraud/theft ranked in 5th position of the most likely global risks to occur in 2017, then it follows that mitigating against technological risks, specifically the risk of massive data fraud / theft should be the highest priority for businesses in the UK.

A review of the Global Risk Report 2017, compiled by the WEF, of the technological risks data fraud/theft was returned as a top five risk global risk in terms of likelihood[43], moving up three places since 2016. In the United States (US), the top risk in 2016 was cyber attack followed by data theft (or fraud). Whereas the expression 'cyber crime' is being used to connote multiple crime types and opportunities, conversely, some crimes are being described by several different names adding a layer of complexity that is unhelpful.

With email a primary communication tool for most businesses, it is imperative that business take practical steps to robustly protect and defend email communication so that it can be trusted. Having identified data theft / fraud as the most significant issue for businesses to address, which sector in the UK is likely to suffer the most from this risk?

What works?

Assimilating what we know works in the real world into the cyber world is instructive in building robust processes to develop countermeasures to combat cyber crimes. As a starting point, it is well understood that failing to mend broken windows[44] in a community acts as a signalling effect of community disorder. Similarly, failure to maintain publicly testable protocols to protect email signals to scammers that the system is incorrectly configured and that it is not being properly maintained or monitored. By implementing practical, well supported and endorsed solutions that can be adopted simply at scale, will assist businesses in sending out the right message that there system is tougher to tamper with.

Conclusion

Cyber crimes need to be articulated with a higher degree of sophistication than is currently the case and Prof. Wall's matrix proves an instructive and elucidating starting point. Thinking about cyber crime as crime types and opportunities helps to carve up the cyber crime elephant into crime types and opportunities.

Specificity when considering the area of cyber crime needs to be embraced as does a more sophisticated classifying system based on the technique rather than victim type (e.g. business email compromise, ***CEO fraud***) or indeed the time of day an event is likely to occur (e.g. ***Friday afternoon fraud***).

The conversation about cyber crime would benefit from a multidisciplinary approach.

Just as we accept carrying a bundle of keys to lock a front door, there is concomitant trade off for deploying security measures. But as with all risk management strategies, the deployment of the protection is considerably less painful than the consequences arising from the breach.

In the same way that we don't have a single pill for all ailments, society cannot expect a single solution to resolve the challenges facing an entire community, there is no silver bullet to restrict motivated individuals from causing injury whether in the real world or in cyber space. As with our personal security, different devices need to be deployed to address specific risks. In the matter of email impersonation, a solution exists which is both ***'affordable and proportionate'***. The DMARC solution, which validates emails is the result of industry wide collaboration, is not only approved but endorsed by the National Cyber Security Council (NCSC) part of GCHQ. The adoption of this fundamental solution has not kept pace with the rising tide of cyber crime.

OnDMARC is an award winning London based Cloud Cybersecurity provider that helps organisations deploy DMARC with confidence.

Author
Dr. Rois Ni Thuama

Dr. Rois Ni Thuama LLB LLM PhD has worked with technology & new ventures since 2002 including Sakhalin Energy Investment Company (a Shell, Mitsubishi, Mitsui joint venture), Credit Suisse First Boston (now Credit Suisse), Armstrong & Cavendish, IAS Medical. She worked together with software developers and FTSE 350 clients to understand their engagement needs. As well as delivering seminars at undergraduate and post graduate levels, she works with OnDMARC to address pressing cybersecurity issues. Her academic interests include Corporate Governance, IT Governance, Cyber Crime, Cybersecurity, Law and Technology.

References

1. FT Reporters, Cyber Attack hits global businesses and Ukraine government, Financial Times, 28 June 2017. https://www.ft.com/content/6ee9147a-5b43-11e7-b553-e2df1b0c3220?mhq5j=e2 last accessed 28 June 2017.
2. Firms that were hit recently include WPP, Rosneft, Merck, as above, see para.1.
3. For a coherent overview of the WannaCry ransomware infection, see Powar, Rahul https://medium.com/postmasters/wannacry-what-happens-next-f57aff9b394a last accessed 28 June 2017.
4. Fraud and cyber crime are now the country's most common offenses. Evans, Martin & Scott Patrick via http://www.telegraph.co.uk/news/2017/01/19/fraud-cyber-crime-now-countrys-common-offences/ last accessed 21 June 2017.
5. Croft, Jane,. Law Society points to £25.7bn contribution of legal sector 22 March 2016 via Financial Times available to download from https://www.ft.com/content/3018f37e-ef73-11e5-aff5-19b4e253664a?mhq5j=e2 Last accessed 27 June 2017.
6. P.15 Trends para. 1
7. P.15 Trends col.2 para 1.
8. Said Birch, Sofia,. 'IBM's CEO on hackers: "Cyber crime is the greatest threat to every company in the world' available via IBM's website https://ibm.co/2sYuGbY. Last accessed 21 June 2017.
9. Unable to find figures for this.
10. Outcome 4.1 SRA Code of Conduct 2011
11. SRA Handbook, Principles, Part 1, principle 8 https://www.sra.org.uk/solicitors/handbook/handbookprinciples/part2/content.page
12. See generally SRA Risk Outlook, Information Commission, Law Gazette, Solicitors Journal, press articles including The Guardian, Financial Times et cetera.
13. http://www.sra.org.uk/risk/outlook/risk-outlook-2016-2017.page see p.16. Last accessed 21 June 2017.
14. http://www.sra.org.uk/alerts/. Last accessed 26 June 2017.
15. https://www.gov.uk/government/publications/email-security-standards/domain-based-message-authentication-reporting-and-conformance-dmarc last accessed 26 June 2017.
16. https://dmarc.org/wiki/FAQ#Why_is_DMARC_important.3F last accessed 21 June 2017
17. Since the publication of the top 100 a number of firms, merged reducing the number to 95.
18. https://governmenttechnology.blog.gov.uk/2016/10/04/why-you-should-be-doing-dmarc/ Last accessed 28 June 2017.
19. http://www.sra.org.uk/consumers/news-alerts.page last accessed 26 June 2017.
20. http://www.sra.org.uk/consumers/scam-alerts/2017/Jun/norton-rose-fulbright-llp.page Last accessed 26 June 2017.
21. http://www.sra.org.uk/consumers/news-alerts.page
22. Trenor, Jill https://www.theguardian.com/uk-news/2017/jan/24/uk-fraud-record-cybercrime-kpmg 24 January 2017, last accessed 21 June 2017. Treanor writes: The value of fraud committed in the UK last year topped £1bn for the first time since 2011, prompting a warning about increasing cyber crime and the risk of more large-scale scams as the economy comes under pressure.
23. Mallet, Victor & Chilkoti, Avantika., Financial Times, 30 March 2016, available to download at https://www.ft.com/content/39ec1e84-ec45-11e5-bb79-2303682345c8 last accessed 21 June 2017.
24. Internet Crime Report 2016, FBI available to download from https://pdf.ic3.gov/2016_IC3Report.pdf, last accessed 27 June 2017. See p.9, see also p.17 for crime types by victim count, BEC/EAC had 12,005 victims but phishing/vishing/smishing and pharming had 19,465.
25. Internet Crime Report 2016, FBI available to download from https://pdf.ic3.gov/2016_IC3Report.pdf, last accessed 27 June 2017. See p.9, para 1. Curiously, the IC3 are currently reporting phishing, vishing, smishing and pharming as a single crime type. The differences in the techniques of these crimes is easily identifiable from the outset, with vishing relying on the telephone system, while criminals employing smishing techniques use SMS (text) to mobile phones. These distinctions are critical in understanding the size of BEC/EAC/phishing problem. In 2016, the victim count for phishing, vishing, smishing and pharming was 19,465 whereas BEC/EAC was recorded at 12,005. To what extent BEC/EAC represents a more significant problem is difficult to identify when phishing is reported separately.

26. Jones, Rupert, 'I thought I'd bought my first home, but I lost £67,000 in a conveyancing scam' via The Guardian, available to download from https://www.theguardian.com/money/2017/jan/14/lost-67000-conveyancing-scam-friday-afternoon-fraud-legal-sector-email-hacker Last accessed 27 June 2017. See also https://www.lawgazette.co.uk/news/sra-warns-of-friday-afternoon-fraud-risk/5047315.article
27. Global Risk Report, 2016
28. Internet Users in the UK: 2017 report available via ONS https://www.ons.gov.uk/businessindustryandtrade/itandinternetindustry/bulletins/internetusers/2017. The report cites the following figures: 99% for recent internet usage in the 16 to 24 and 25 to 34 years age brackets, an increase in internet usage for the 65 - 74 age group rising from 52% in 2011 to 78% in 2017, while recent internet use by the economically inactive has seen a rise of 16 percentage points, rising to 86% over the same period.
29. WEF, Global Risk Report 2016. The matter was not addressed in the same way in the 2017 report, however, technological issues specifically data fraud/theft had moved up the ranks from 8th position in 2016 to 5th position in 2017, discussed elsewhere in this paper.
30. Wall, David S., The Internet as a Conduit for Criminal Activity (October 21, 2015). Information Technology and the Criminal Justice System, Pattavina, A., ed., pp. 77-98, Sage Publications, Inc., 2005 (revised 2010, 2015). Available at SSRN: https://ssrn.com/abstract=740626. See especially table 4.1 page 4.
31. Wall gives an example of 'organisation across boundaries' as a cyber-enabled or hybrid crime.
32. 10 Steps: A Board Level Responsibility, sponsored by Centre for the Protection of National Infrastructure Cabinet Office, Department for Business Innovation & Skills https://www.gov.uk/government/publications/cyber-risk-management-a-board-level-responsibility/10-steps-a-board-level-responsibility
33. http://www.eugdpr.org/key-changes.html para 3, penalties.
34. Morgan, Steve, IBM CEO on Hackers: Cyber crime is the greatest threat to every company in the world' via Forbes http://bit.ly/2rUPdhf 24 November 2015 quoting IBM's Chairman, President and CEO Ginni Rometty, last accessed 21 June 2017.
35. Cyber crime will cost businesses over $2 trillion by 2019.
36. https://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion.
37. World Economic Forum https://www.weforum.org/projects/cybercrime.
38. Rodionova, Zlata,. Cyber security report: Hacking attacks on UK businesses cost investors £42bn
39. http://www.independent.co.uk/news/business/news/cyber-hacking-attack-cost-uk-business-investors-ftse-companies-lose-120-million-a7678921.html
40. Improving crime statistics in England & Wales. Office for National Statistics, 2015
41. The Cyber Value Connection - Revealing the link between cyber vulnerability and company value, available to download https://www.cgi-group.co.uk/system/files/cybervalueconnection_full_report_final_lr.pdf last accessed 21 June 2017.
42. See generally http://www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime last accessed 21 June 2017.
43. Basic definition of theft. S1(1) A person is guilty of theft if he dishonestly appropriates property belonging to another with the intention of permanently depriving the other of it; and "thief" and "steal" shall be construed accordingly.
44. Wilson, James Q; Kelling, George L, Broken Windows: The police and neighborhood safety, The Atlantic (Mar 1982). See also the experiment conducted by Philip Zimbardo discussed in some detail by Barrow, Lauren, Rufo, Ronald and Saul Arambula, Police and Profiling in the United States, Applying Theory to Criminal Investigations Boca Raton: CRC Press 2013, p. 170.
45. Global Risk Report, 2017, p.5.
46. See Wilson, James Q; Kelling, George L, Broken Windows: The police and neighborhood safety, The Atlantic (Mar 1982). See the experiment conducted by Philip Zimbardo discussed in some detail by Barrow, Lauren, Rufo, Ronald and Saul Arambula, Police and Profiling in the United States, Applying Theory to Criminal Investigations Boca Raton: CRC Press 2013, p. 170.