benchtv
a benchmark production

Précis Paper

Forensics and Data Investigation

A discussion of the forensics investigation process as it is carried out by the Forensics and Technology Services Team at Clayton Utz.

Discussion Includes

- What is Forensics and Technology Services about?
- How has the investigation of misconduct evolved and changed over the past 5-7 years?
- Is investigation all about finding wrongdoing, or can it also be used to improve workplace efficiency?
- Protection of data against misuse
- Other risks of Forensic and Technology Services' involvement in an investigation
- Protocols for collecting, preserving, and presenting data
- What developments might take place in the next five years?
- Will there come a point where the technology might be able to detect the true source of a piece of information?
- Importance of information
- The changing nature of the legal and accounting professions

Précis Paper

Video Title

1. In this edition of BenchTV, Paul Fontanot (Partner – Clayton Utz, Sydney) and Bruce Cooper (Partner – Clayton Utz, Sydney) discuss the forensics investigation process as it is carried out by the Forensics and Technology Services Team at Clayton Utz.

What is Forensics and Technology Services about?

2. Forensics is about understanding and collecting information in a certain way.

3. Nowadays, information is not only paper-based but takes many different forms.

4. On the technology front, there is the use of information via software and tools in order to extract that information in the way that Clayton Utz's Forensics and Technology Services team, headed by Paul Fontanot, would like to analyse it, and then presenting it in a way that makes sense to a client.

How has the investigation of misconduct evolved and changed over the past 5-7 years?

5. Traditionally, the investigation of misconduct has been paper-based. This is because paper is the means by which many clients and companies retain their information - for example, payroll records, invoices, purchase orders.

6. Therefore, investigations have been largely paper-based, with an extraction of their accounting information. Then, on the legal side, there has been the extraction of emails.

7. Over the years, Paul's Forensic and Technology Services team have managed to analyse financial transactions with the intent - intent being what has been expressed in an email, a text, or chat.

8. The last five years have seen an emergence of combining these two data sources to give a richer insight into the data itself.

9. Paul had a very large government client last year in connection with which there was a leak of information to the media, and there was a need for investigating who leaked this particular information. In such a case, it must be considered whether it was paper or electronic information that was leaked out. This involves an examination of: print logs; shared folders; and the printer itself to determine whether the document was actually

printed. Further, it should be determined whether the information was put into a cloud, one drive, etc, or whether it was simply emailed out.

10.   Information and investigations have evolved due to the advent of information and technology which can analyse this information. Over the past five years, it has been seen that investigators have become more adept at analysing information. As information/data sources are growing, the types of things that can be investigated are growing.

11.   Clayton Utz's Forensics and Technology Services Team has been described as having the "secret sauce". What this means is that conducting an investigation is about:
  i.   having the right people who know what to do;
  ii.   understanding the technology and the types of tools to be used - it is not enough to simply acquire a particular software, for example; different types of techniques must be applied to that software to make it work better;
  iii. the workflow/process.

12.   Clayton Utz's Forensics and Technology Services Team draws on a variety of different skill sets to apply different types of software to forensically image and extract information out of the system. This involves:
  i.   examining metadata behind the actual documents themselves;
  ii.   GPS tracking behind photographs being analysed;
  iii. tracking information of shopping logs, internet history, payroll records, Facebook and social media linkages, showing who is connected to who.

13.   This is the use of "big data", the analysis of which requires a process as well as people and technology.

Is investigation all about finding wrongdoing, or can it also be used to improve workplace efficiency?

14.   Investigation is not always about finding wrongdoing; it can also be used to enhance workplace efficiency.

15.   For example, Clayton Utz conducts the internal audits of some ASX listed companies, which involves analysing these companies' data sources for waste, error, and abuse.

16.   Innocent errors, without any intention of wrongdoing, are bound to happen, and Clayton Utz's processes and systems help clients identify whether those errors are in the system, and therefore improve their process.

17. Even though there might exist a conflict of interest, this does not necessarily mean that there is, unwittingly, abuse of it, however, there must be a segregation of duties.

18. Clayton Utz's Forensics and Technology Services team therefore has two sides: the pre-emptive side, and the post-mortem/malfeasance side. These two sides run in parallel.

19. The internal audit process has been set up under legal professional privilege. This means that if there is abuse in the system, one of Paul's fellow partners can easily be involved in any workplace investigation or commercial litigation. In doing so, they can provide any legal advice that is required for any disciplinary action, or to claim back monies that have been paid out illegally.

Protection of data against misuse

20. This is a big issue, as companies are not only collecting customer information, but also confidential information which they need to keep private.

21. The hacking of companies raises the question of what are companies doing to protect their data sources? In turn, in relation to law firms, there is the question of how the firm is protecting their clients' data.

22. Clayton Utz's Forensic and Technology Services Team contains cyber experts and ethical hackers who help provide proactive advice as to how a system could be potentially hacked, and what protections would need to be applied.

23. One option for clients is to apply cyber insurance, in which case Paul's legal partners would provide advice as to insurance cover, and draft policies surrounding due diligence and the protection required.

24. In relation to ensuring that Clayton Utz has the right protection for its clients, the firm has had its ISO27001 certification for the third year running.

25. Further, Clayton Utz has spent time developing its protected environment, which will hold confidential and top secret information. In particular, this is information for the federal government and those companies that do not want to put their data into a cloud.

26. Clayton Utz is certified to hold this confidential, top secret information. It is vital that Clayton Utz, as a law firm, provide clients with the comfort that that it has been externally assessed for these certifications.

Other risks of Forensics and Technology Services' involvement in an investigation

27. A challenge has always been having the right information, as it is only the information at hand that can be disclosed and presented.

28. Currently, because the data sources have grown over time, their complexity and volume require further tools to enable extraction.

29. There is therefore a continual evolution to find that further information, and there will always be a risk that one has not looked in the right place, or has not extracted the right pieces of information.

30. There is a standard of proof that must be worked towards in investigations. In a disciplinary inquiry, this standard is the balance of probabilities, while in a criminal matter, the standard is beyond a reasonable doubt.

31. The same procedures are followed in each investigation in collecting the information so that an 'evidence trail' can be shown. This trail shows how the information has been collected, preserved, analysed, who had access to it, and how it is presented.

Protocols for collecting, preserving, and presenting data

32. Previously, law firms had typically outsourced much of the front-end data collection, preservation, and analysis. The information was then taken into a document repository to be analysed for legal professional privilege and confidentiality.

33. Through its Forensics and Technology Services Team, Clayton Utz has captured all of these steps under the one umbrella.

34. The data sources must firstly be identified. There are tools that may assist with this process. For example, if information containing photographs has been collected from a web server, tools may help determine the GPS co-ordinates of those photographs, and in turn, who is talking to whom.

35. Secondly, the information must be collected and preserved. Tools such as Catalyst and EnCase assist with collecting information in a forensically sound manner. They extract not only the content of the information, but also the metadata behind it.

36. Once the information has been collected, it is placed into a software called Nuix, which assists with de-duplication and indexing. De-duplication cuts out all the intermediate

interactions in a trail of email correspondence, and distills the main chain of the email. De-duplication therefore assists in identifying and mapping out a chain of evidence.

37.   The information is ultimately produced into a visualisation tool called Tableau, which maps out all of the information in a way that allows the client to make sense of it.

38.   These methods allow for a holistic picture of information to be presented to the client - taking account of the background as well as the foreground. For example, a document might look like one particular person drafted it, but the metadata might show that ten other have people edited it. This means that though these people had knowledge of the document, they were never part of the email chain.

What developments might take place in the next five years?

39.   With the advent of new technology, data scientists, and ways of thinking, the use of artificial intelligence will increase. However, in order to apply this artificial intelligence to the data sources, the right tools and data scientists are needed.

40.   Conceptual searching will also start to be seen. Conceptual searching will look at a person or document and identify themes, such as, for example, procurement in the retail space. The computer carrying out the conceptual searching will then look at, for example, the next 50,000 documents and see if it can identify the same themes.

41.   Another development will be scripting and machine learning. This applies to very large data sources, and extracts and manipulates these sources.

42.   Object detection is another development. This is where data sources are examined for matching objects. Clayton Utz's Forensics and Technology Services Team is applying continual learning to different data sources.

43.   A final development is continual monitoring. This involves continual checking, where, for example, a procurement or an authorisation needs to be done, that the payment will be paid in the right way.

Will there come a point where the technology might be able to detect the true source of a piece of information?

44.   Yes – this can be achieved through 'sentiment analysis'. This process analyses a writer's word choices and expression in a sentence to determine how the writer is feeling and what their manner of writing says about them as a person.

45.   Clayton Utz's Forensics and Technology Services Team is being engaged by many universities in this regard, asking for such analysis of the research being provided to them.

Importance of information

46.   Information is all-important. The more information that can be gathered, the more analysis can be applied to it. The insights that Clayton Utz can provide to its clients, from a legal as well as a proactive perspective, will be a key to the future in this area.

The changing nature of the legal and accounting professions

47.   There is a blurring of the professional environments in which the accounting, legal, and even information technology professions operate.

48.   As such, the future of a law firm may include technology and accounting, and likewise, an accounting firm may include law and technology.

BIOGRAPHY

Paul Fontanot

Partner, Clayton Utz, Sydney

Paul is a Chartered Accountant and licensed forensic investigator. He has worked with many multi-national clients in identifying and managing fraud and corruption risk, as well as cyber risk. His experience includes conducting fraud and regulatory investigations, designing and implementing anti-fraud and corporate compliance programs, managing IT forensic analysis, preservation and data review programs, as well as forensic accounting.

Bruce Cooper

Partner, Clayton Utz, Sydney

Bruce specialises in energy, project, and infrastructure work across a broad spectrum. Bruce's sector area experience covers the power, oil and gas, water, transport, mining, and processing industries. Bruce's practice also encompasses all aspects of banking work. With a particular emphasis on project finance and commodity finance, he has also had significant experience in restructurings and work-outs for borrowers and lending groups on large project deals.