JGL FORENSIC SERVICES

You Don’t Know What You Don’t Know

Introduction

- *"There are known knowns. These are things we know that we know. There are known unknowns. That is to say, there are things that we know we don't know. But there are also unknown unknowns. These are the things we don't know we don't know."* - Former US Secretary of Defence, Donald Rumsfeld
- There are indeed "unknown unknowns" - those things that we simply don't know we don't know
- **The uncomfortable truth:** As human beings, we simply don't know as much as we think we do
- Studies have shown that when we're asked to explain how everyday things work - things that most of us feel certain we understand - we are simply unable to do so
- "**Illusion of explanatory depth**" - a cognitive barrier that tricks us into thinking we fully understand something we actually don't

Introduction, Continue…

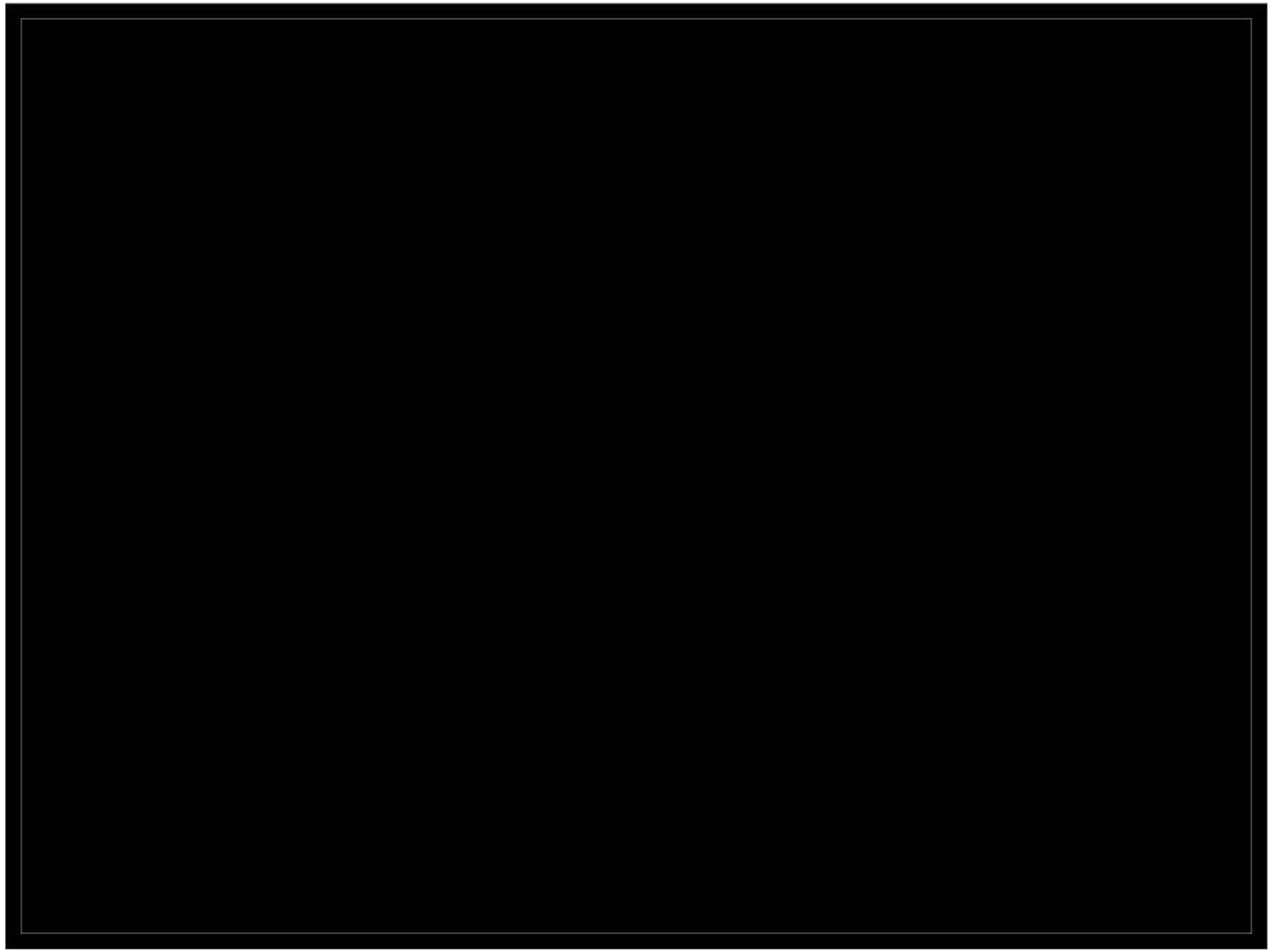
- As businesspeople we love to use the latest buzzwords and jargon to make us sound like subject matter experts
- "We are going to *Streamlining business practices*" is regularly used in meetings … with eager-to-please nods from executives
- After the meeting executives were overheard asking each other exactly what it meant
- The financial crash of 2007/8 is a classic case in point. The profound misunderstanding of complex financial products directly contributed to the devastating market collapse
- The huge knowledge gaps displayed by companies like AIG about the riskiness of the products they were insuring was to prove catastrophic

Introduction, Continue…

- The Legal Practice store and have access to massive amounts of personal and sensitive client data. The rapid expansion of regulation of data and privacy via the POPI Act adds yet another layer of compliance exposure
- Legal Practitioners must furthermore adhere to Attorney-Client privilege which means any information a client shares with their attorney is to remain confidential. Essentially, the Legal Practitioner has access to trade secrets, intellectual property, etc.
- Let's take a look at the compliance issues and regulatory challenges faced by these Legal Practitioners

Business Email Compromise (BEC)

- BEC, also known as email account compromise (EAC) is, according to the FBI, one of the most financially damaging online crimes, as it exploits the fact that we rely on email to conduct our personal and professional business
- In 2016 already, BEC attacks led to an average of US$140 0000 in losses for companies globally
- How it works: The criminal sends an email that appears to come from a known source, making it a legitimate request
- According to the 2021 Business Email Compromise Report, the most common types of BEC attacks are spoofing (71 %), spear phishing (69 %) and malware (24 %)
- The intention of BEC is usually credential theft (57 %), malicious payloads (22 %) and payment fraud (20 %) – 2021 BEC Report



The Invisible Gorilla Experiment

- This experiment devised by Christopher Chabris and Daniel Simons, highlights two important facts:
  - We miss a LOT of what goes on around us
  - We have absolutely no idea we are missing so much
- If someone gives you everything you expect, it's natural to only see what you expect to see versus what's actually in front of you (We call this cognitive bias)
- It's only once someone alerts you to the possibility of a gorilla that you start looking for one. Why? Because you know he's coming

Fraudsters are smart. Scary smart!

- They know your well-established, systems and same-as-they've-always-been requirements as well as you do
- Cybercriminals are becoming ever more sophisticated in their methods. Where our biggest worry was once a forged signature on a cheque … remember cheques? ... fraud is becoming as multi-channel as the rest of our digital lives
- It moves, stealthy and insidious, between call centres, web and mobile. New schemes, such as synthetic identities (where criminals combine real and fake information to create a totally new identity), are becoming more common, smarter, and much harder to detect

The numbers…

- Here are just some of the frightening statistics:
  - By 2023, $48 billion will be lost annually to synthetic identity fraud (at around $15 000 loss per incident)
  - 61% of big banks' fraud losses come from identity fraud, 20% of which is synthetic identity fraud
- One of the biggest ironies is that our biggest weapons in our arsenal against online fraud are also the greatest source of the entire system's vulnerability

Legal Risks – POPI Act

- **POPI Act**
- Since 1 July 2021 South Africa has a new Protection of Personal Information Act (POPI Act) that changed the data, privacy and record-keeping requirements for organisations

Legal Risks – POPI Act, Continue…

- **The basic principles of the POPI Act include:**
  - Personal information may only be processed in a lawful and fair manner **AND** with the consent of the person to whom the data belongs
  - Personal information may only be processed for explicit, specific defined and legitimate reasons
  - Personal info may not be processed for a secondary purpose, unless the processing is compatible with the original purpose
  - The person whose info you are collecting, must be aware that you are collecting the info and for what purpose it would be used
  - Personal info must be kept secure against the risk of loss, interference, modification, unlawful access, unauthorised destruction and disclosure
  - Data subjects may request whether their personal info is held, as well as the correction and/or deletion of any personal info held

Legal Risks – POPI Act, Continue…

- **Steps companies should take to comply with POPI**
  - Appoint an information officer
  - Raise awareness of POPI among employees
  - Draft a privacy policy
  - **Report data breaches**
  - **Only share personal information when lawfully allowed to**

Legal Risks - Confidentiality

- **Confidentiality of client information**
- The duty of confidentiality prevents legal practitioners from, even informally, discussing information related to clients' cases. They must keep private all information related to the representation of the client, even if the information did not come from the client himself
- Legal practitioners must ensure that confidentiality is respected, protected and upheld at all times

Cyber attacks

- Cyber attacks are malicious and deliberate attempts by an perpetrator to breach the information system of an individual or organisation. Usually, the perpetrator seeks some type of benefit from disrupting the victim's network
- **Most common cyberattacks:**
  - Malware, incl. spyware, ransomware, viruses and worms
  - Phishing
  - Man-in-the-middle attack (Eavesdropping attacks where attackers insert themselves into a two-party transaction to filter and steal data, etc.
  - DNS Tunnelling

IT Regulation

- When internet-based technologies are used by legal practitioners, due diligence should be exercised before utilising a third-party service provider for the purpose of storing and processing confidential information off-site
- There should also be a written agreement that concludes that the service provider is required to establish and maintain measures that ensure the security of any personal information stored by the service provider, and also the protection and integrity of any confidential or privileged client info

How to reduce data breach and cyber security risk

- Develop a plan to prevent data breach
- A breach prevention plan must consider, at least:
  - The data types the company uses
  - Where and how the data is stored
  - Whether or not there is an obligation to notify the authority, if a breach occurs
- This plan should be highly adaptable to help mitigate constantly evolving threats.

How to reduce data breach and cyber security risk

- Make practitioners aware of security risks
- Companies should make efforts to increase awareness throughout the organisation about, at least the following:
  - Security threats
  - Cybersecurity prevention techniques

How to reduce data breach and cyber security risk

- Train practitioners on a regular basis
- End-user is the weakest link in this chain, which leads to employee negligence being one of the main factors that may lead to a data breach.
- It is therefore important to have regular security awareness training to remind employees of evolving security threats. This will help staff to be on alert for data breach attempts and learn techniques to protect information when communicating

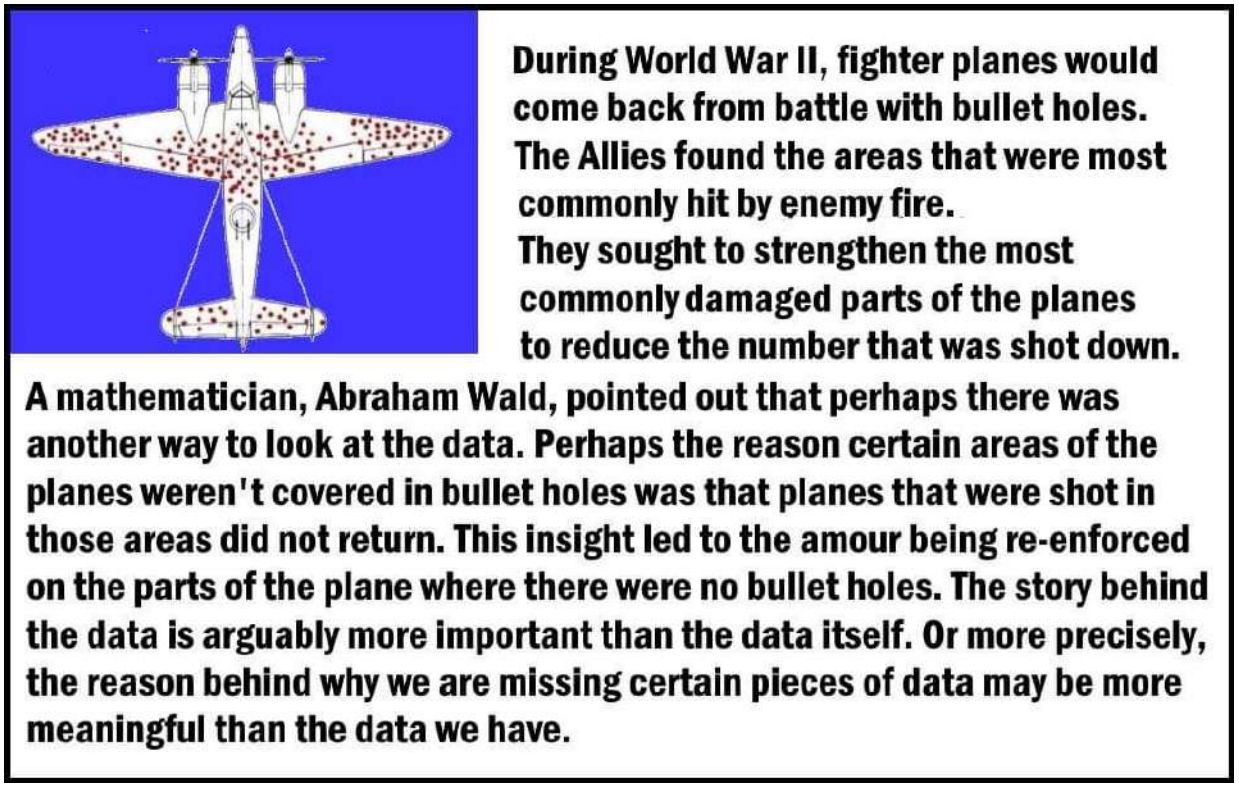
How to reduce data breach and cyber security risk

- Keep personal and business hardware separate
- The use of the same laptop or cell phone for business and personal use, significantly increase exposure, as rigorous security measures are not typically implemented on a personal device.
- Secure mechanisms must be identified to allow employees to have info on their personal devices, without creating a door to violate the security of the company and to produce a data breach.

How to reduce data breach and cyber security risk

- Have security measures in place
- Technology can be used to prevent security breaches. Examples includes:
  - Data encryption
  - Secured email domains
  - Phishing incident response tools
  - Keeping software and applications updated
  - Using VPN connections.

More systems? Better AI?



Thank you for your time

Sun Tzu, the Ancient Chinese military general, wrote in his book, *The Art of War*,

"To secure ourselves against defeat lies in our own hands, but the opportunity of defeating the enemy is provided by the enemy himself."