THE THREAT OF FRAUD

Craig Wooldridge
Counter Fraud Fundamentals Certification Manager

The ‘2019 financial cost of fraud report’ by Crowe UK and Portsmouth University found that the average organisation in the UK can expect losses owing to fraud to account for 3-6%, although in some cases it is as high as 10%.

The most frequent types of cyber incidents against insurers are:

- Phishing Emails-the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information,
- Malware Infections- any software intentionally designed to cause damage to a computer, server, client, or computer network.
- Data exfiltration's- a form of a security breach that occurs when an individual's or company's data is copied, transferred, or retrieved from a computer or server without authorisation,
- DDoS (Distributed Denial of Service) the intentional paralysing of a computer network by flooding it with data sent simultaneously from many individual computers

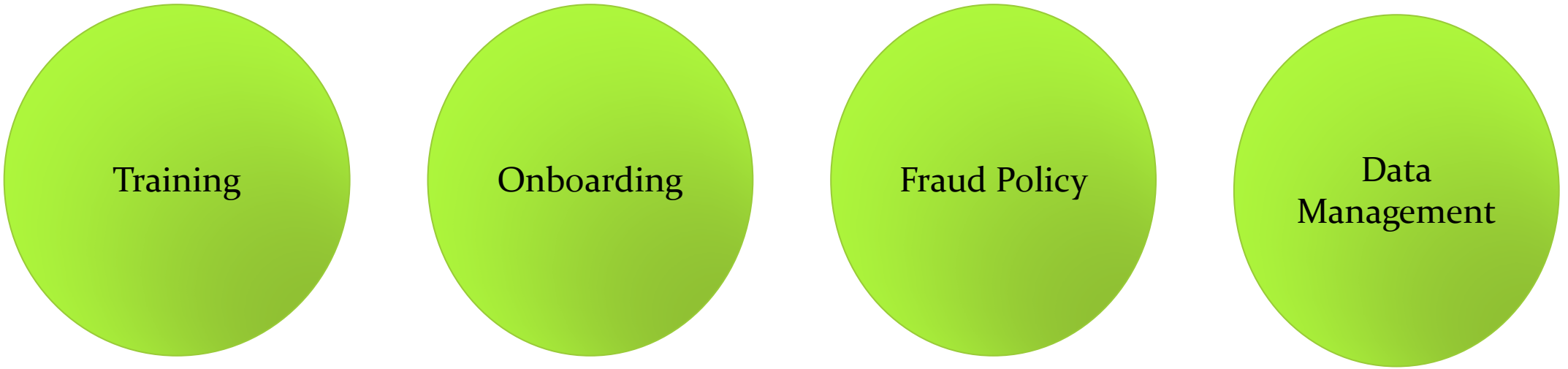
Ransomware Attack- malicious software that threatens to publish or blocks access to data or a computer system, usually by encrypting it, until the victim pays a ransom fee to the attacker.

- More than 80% of UK organisations experienced a successful attack in 2020/2021
- The average cost of ransomware attacks in the UK was around £600,000
- The second most targeted country is the UK, with 14.6 million ransomware attack attempts.
- Across the world ransomware attacks are up 151% in the first half of 2021
- The first half of 2021 has already reached 304.7 million ransomware attack attempts across the world, making it the worst ever recorded year (and we're only just halfway through it !!

Insider threat is a malicious threat to an organisation that comes from people within the organisation, such as employees, former employees, contractors or business associates, who have inside information concerning the organisation's security practices, data and computer systems. The threat may involve fraud, the theft of confidential or commercially valuable information, the theft of intellectual property, or the sabotage of computer systems.

- 500 business owners, saw 34% of them stating that their defrauding had involved collusion between employees and fraudsters
- 21% said their own employees had been behind the fraud perpetrated.

Counter Fraud Controls

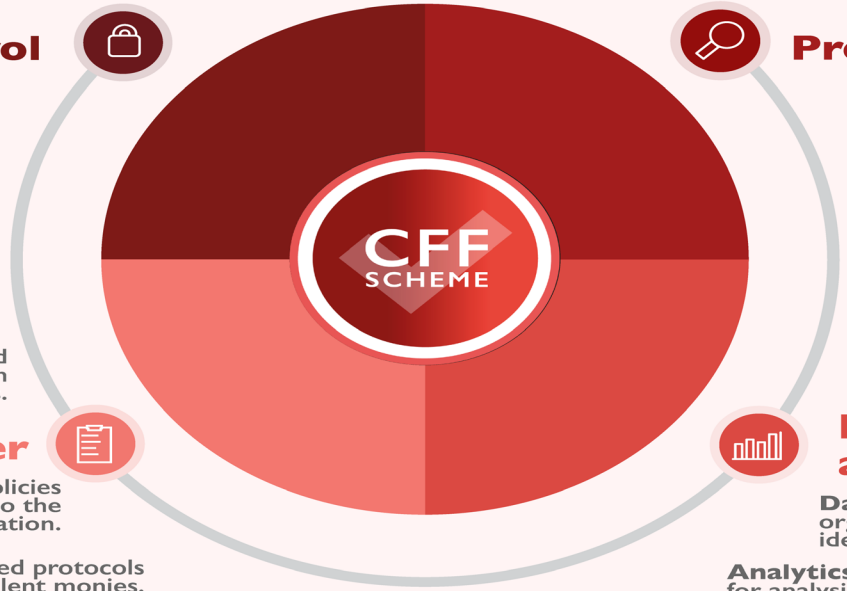


COUNTER FRAUD FUNDAMENTALS

What are the counter fraud fundamentals for managing fraud within an organisation?

The Counter Fraud Fundamentals scheme identifies the basic controls an organisation can implement to address the risk of fraud. **Below is an overview of the recommended controls.**

IASME CONSORTIUM



Oversight and Control

Good **Governance** involves documenting and regularly reviewing policies.

Quality **Assurance** in the form of audit trails of user access and activity.

Talent Management is a process to help control internal fraud.

Executive Reporting involves the collecting of counter fraud metrics.

Risk Appetite is an agreed level of fraud risk willing to be accepted by the company in order to achieve its strategic objectives.

Prevent and Detect

Onboarding describes the collection of background checks for customers, staff and suppliers at the time they are first engaged as well as with ongoing reviews.

Event Monitoring describes the need to monitor and identify potentially fraudulent activity, particularly within transactions and customer accounts.

Comms and Education relates to the communication of a company's fraud and/or financial crime policy to all relevant staff, including contractors.

Respond and Recover

Investigation relates to processes and policies needed for an organisation to adhere to the requirements for a criminal standard investigation.

Recovery includes the recommended documented protocols and procedures in place for recovering fraudulent monies.

Intervention covers the process of providing senior management with the documented evidence of completed fraud investigations and recovery outcomes.

Data Management and Analytics

Data Management describes the ways an organisation should collate data on suspected, identified and prevented fraud.

Analytics sets out the documented approach for analysing anomalous and suspicious activities.

Management Information & Operational Reporting describes the documented way for the Senior Management or Board to track progress against company's fraud strategy.

Find out more about the Counter Fraud Fundamentals scheme by visiting **www.iasme.co.uk**

IASME CONSORTIUM

CFF SCHEME COUNTER FRAUD FUNDAMENTALS

Thanks for Listening!

craig.wooldridge@iasme.co.uk

Questions answered at the end of the presentations

Counter fraud Fundamentals

- Provide a guide for which counter fraud controls should be in place.
- Reassure your customers and supply chain that you take fraud seriously.
- Attract new business with the assurance that you have taken vital steps to protect their money and information.
- Will provide customers and those within the supply chain with the assurance that the most important counter fraud measures are in place to protect their money and their information. From tyhr
- Clients/customers/supply chain/employees
- Tone from the top – Behaviors. Culture & Consequences