ARTHURANDERSEN

r

Computer Security and Forensic Society Seminar

*e*Fraud

William Gee

Partner, Technology Risk Consulting

Arthur Andersen & Co.

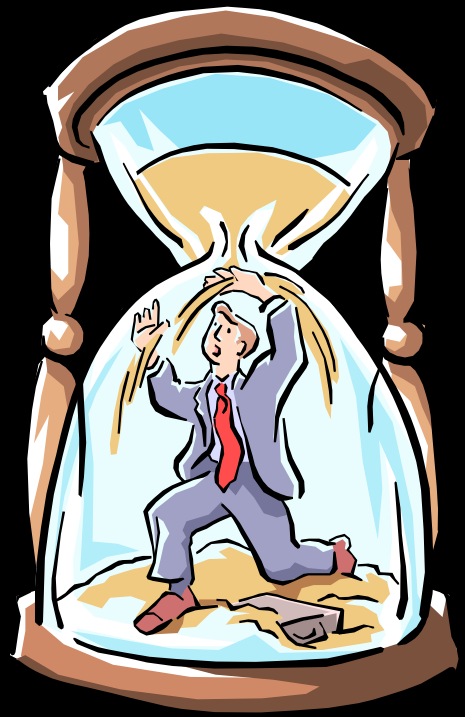
Fraud Triangle

The Internet Challenge

‘Every year, another several million people discover computer technology. Unfortunately, some of them are criminals. Computer intruders leave only electronic fingerprints. Thieves steal industrial secrets without leaving their homes.’

(Rosenblatt - High Technology Crime 1996)

“Internet Time”



Economic Conditions

Business Casual ?!

‘... many are surprised to learn that our prisons today are filled with doctors, lawyers, bankers, accountants, and other professional people who began their careers with the best of intentions. Good schools, hard work, and long hours were their trademark, and success was the payoff. But some thing happened along the way ...’

Barry Minkow, 1995

Fraud Triangle

Statistics

- 62% of organizations had a computer security breach within the last year
- 19% experienced sabotage of data or networks
- 55% had incidents of unauthorized access by insiders
- 97% reported abuse of Internet privileges by their employees
- 26% said they had experienced theft of proprietary information

1999 Computer Crime and Security Survey, Computer Security Institute in conjunction with the FBI International Computer Crime Squad

‘ ... computer crime will be the single greatest crime generator we face in the future ...”

Crimewarps, 2000

A Look at eFraud

What is Fraud

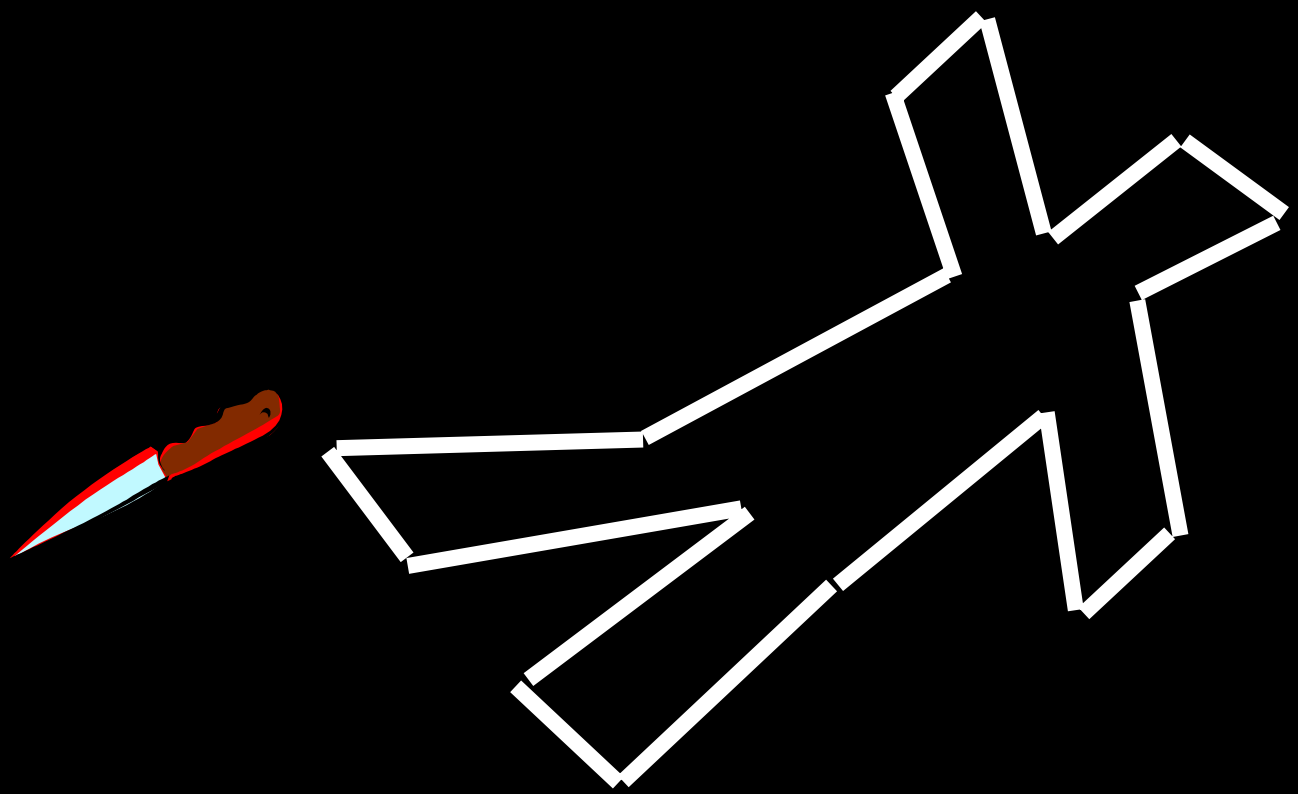
Defined in many ways, but generally involves the following factors:

- Deceit, theft, trickery, or breach of trust
- A guilty intention
- Designed to obtain some form of benefit (usually financial), or advantage at the cost of another party

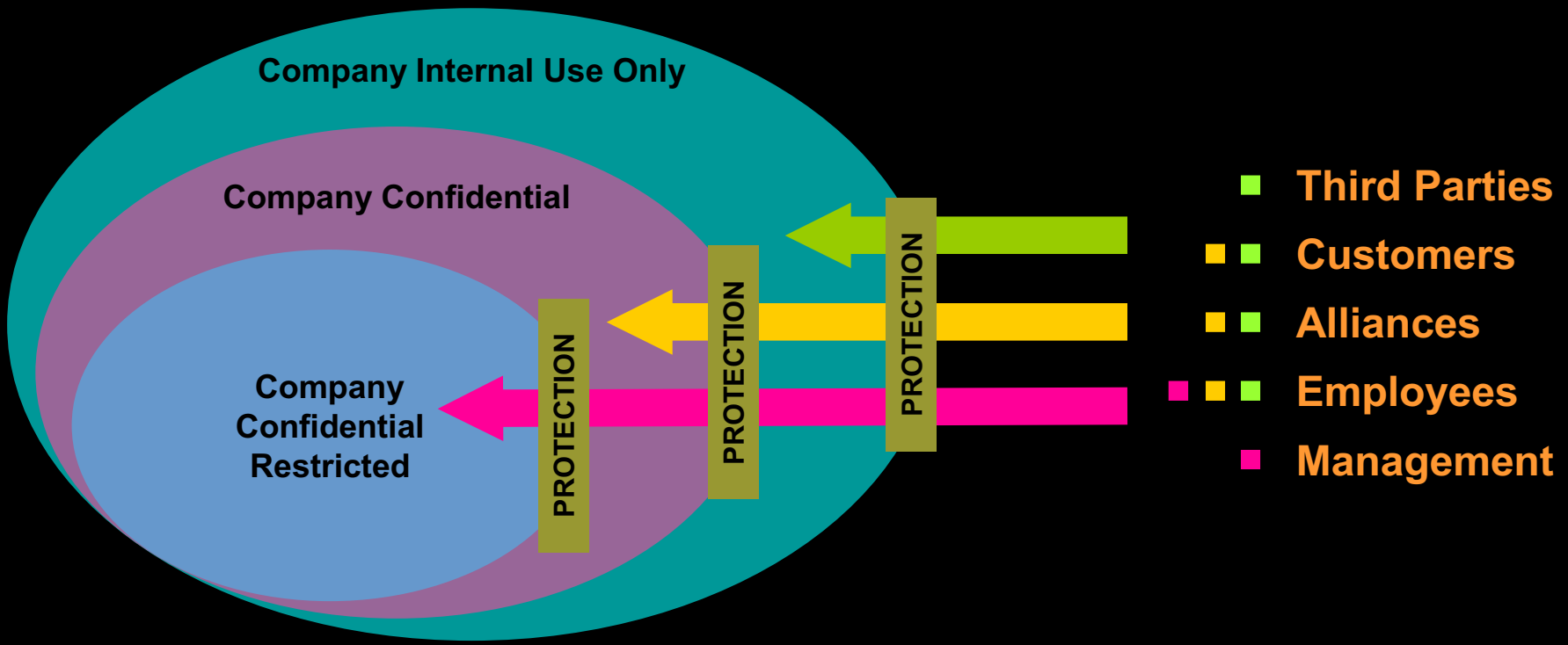
The Three Types of Fraud

- Fraud committed against a company by outsiders
- Fraud committed by management or employees for their personal benefit
- Fraud committed by management or employees for the benefit of the company

The Role of Technology



Ways to attack information



Fraud from an IT security perspective

- While IT security devices becomes ever more sophisticated, no system can be 100% secure:
  - Lack of awareness
  - Management over-rides
  - ‘Emergency’ handling and response
  - Incomplete / ineffective management & control infrastructure
- Corrupt individuals that work in the IT world would exploit such limitations to their advantage

Examples of *e*Fraud

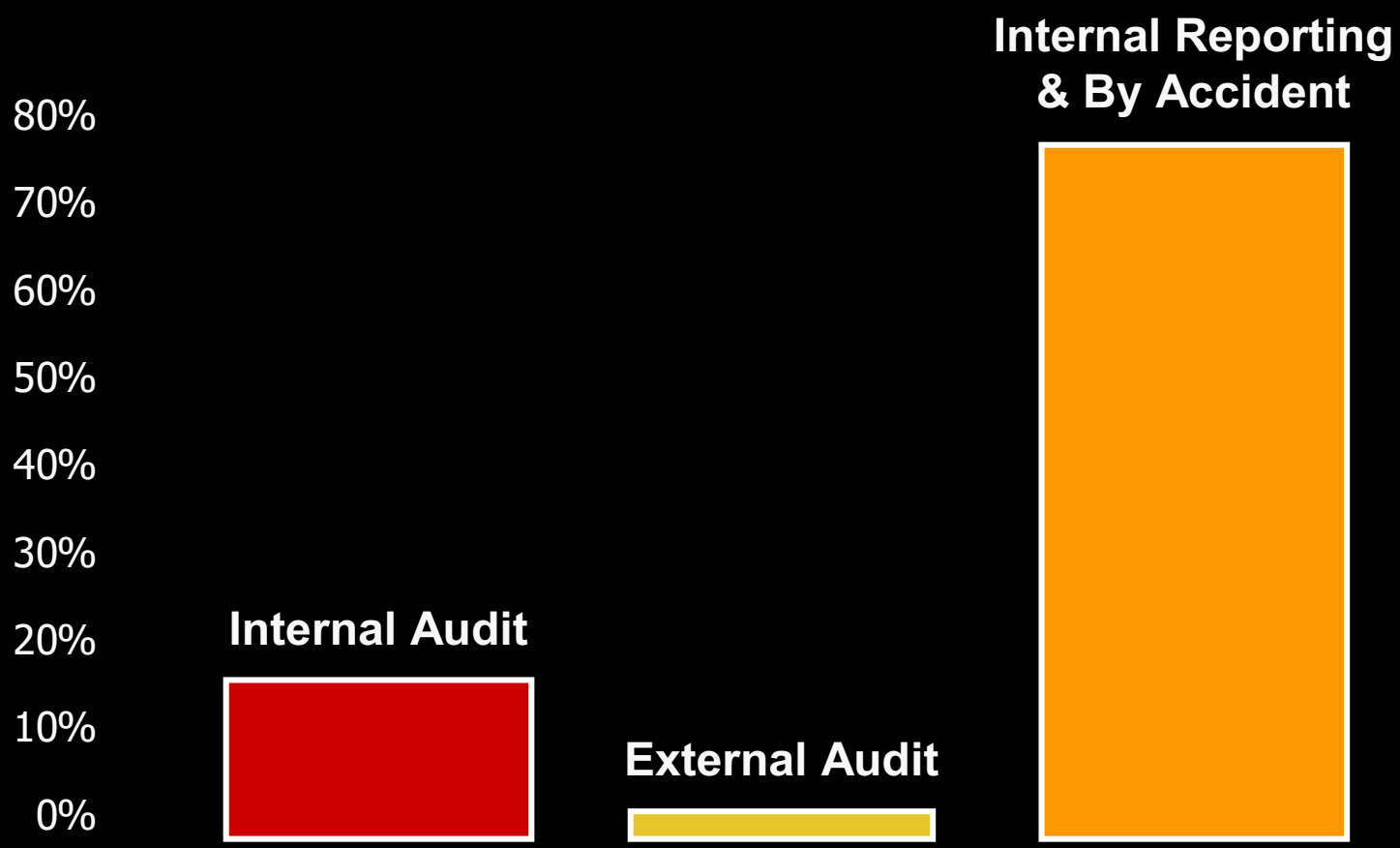
- High yield trading schemes
- False statements
- Online auctions
- Illegal investment
- Unregistered investment advice
- Information related offences
- Market manipulation

The computer
"... the burglary tool of the future ..."

Crimewarps, 2000

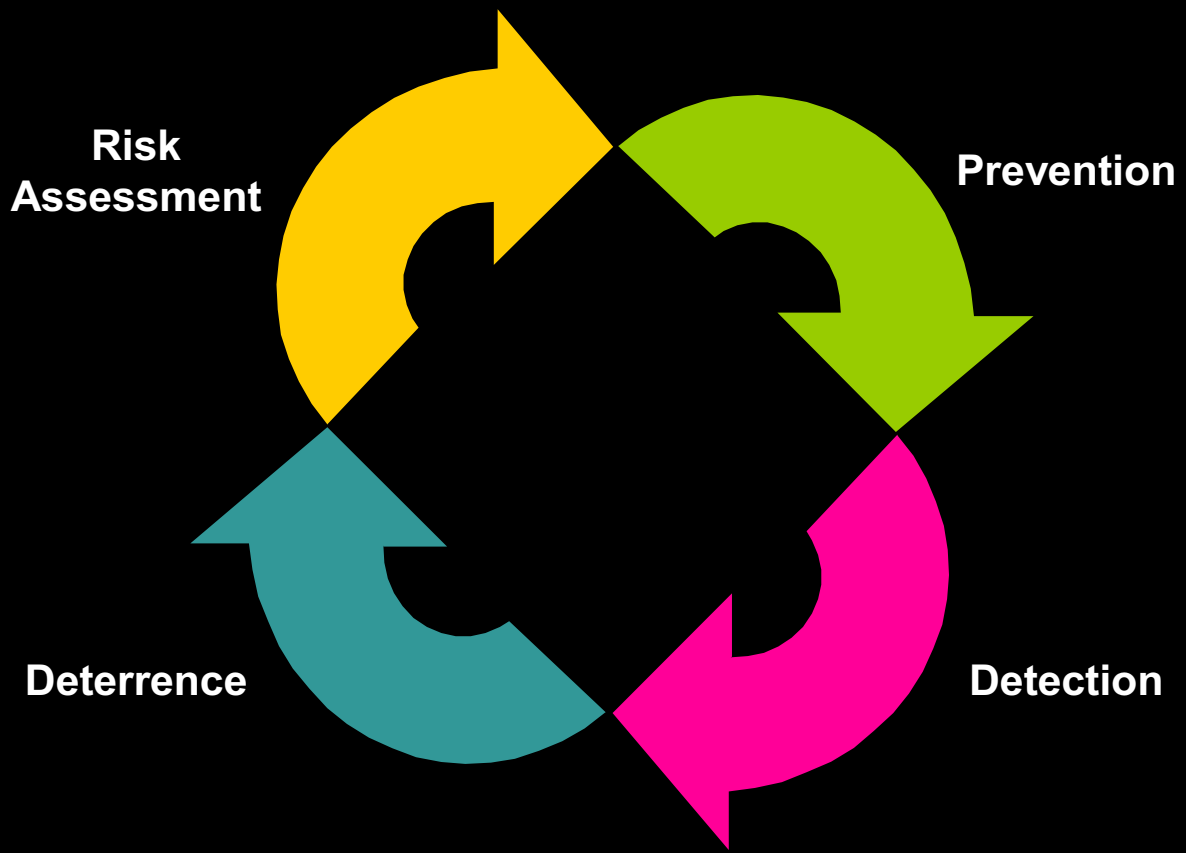
Preventing Fraud

How Frauds are Discovered



Managing & Reducing Fraud Risks

Integrated Fraud Risk Management Strategy:



IT Security Management

- Innovations in technology has advanced creative security for the confidentiality, integrity and availability of information:
  - Encryption
  - Digital Signature
  - Network monitoring
  - Intrusion detection
  - Application monitoring
  - Behavioral characteristics of users
- Advances in security means reduced opportunity for fraudsters to exploit loopholes
- Effective IT security risk management will result in fewer incidents of fraud as the fraud triangle is managed

‘ ... absolute security is an unrealistic goal. An adversary with sufficient motivation, resources and ingenuity or a natural disaster can often compromise even the most secure system ... ’

‘Economic Crime Prevention’, RCMP, June 1999

The Weak Link ...

Information Technology Security

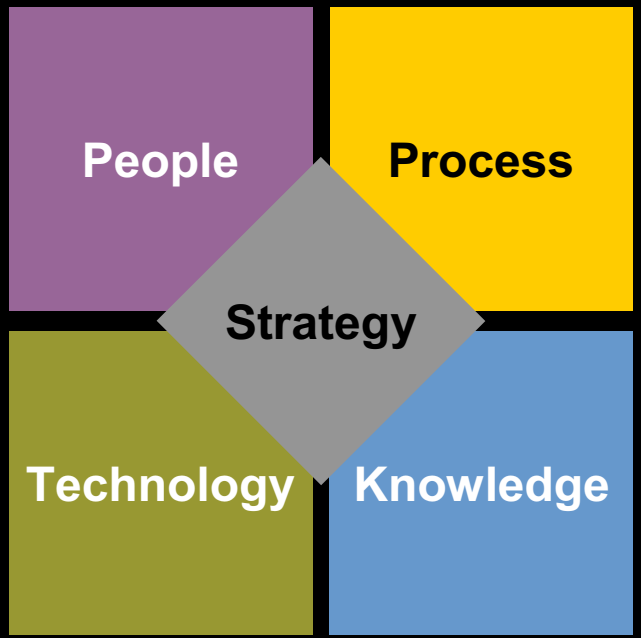
conclusions

Battling against fraud in the information age

- The threat is not entirely technology based ... so neither is the solution
- The key to prevention is understanding the threat to your industry and your consumers
- Technology (intrusion detection system, encryption, digital signatures, audit trails, etc.) do:
  - offer many creative ways to deter individuals from committing crime
  - help identify corrupted individuals and respond to unauthorized activities in real or near-real time
  - offer several methods to assist in the prosecution of cyber criminals
  - provide a wide range of tools to battle fraud

Conclusions

- Technology is *not* the only focus; good business practices still applies
- Clear strategy and management commitment is essential
- Awareness and education is important
- Nothing can be 100% secure: opportunities
- Need on-going vigilance
- Need to maintain equal focus on Technology, People, Process and Knowledge



Are you solving problems? Or creating them?

The best answers start with the right questions. Let's talk.

William.Gee@hk.arthurandersen.com