



5 Fraude Informática e Abuso

Sistemas de Informação Contabilísticos
ISCA-UA, João Batista, 2010



5 Fraude Informática e Abuso

Bibliografia:

1. O conteúdo destes slides é directamente baseado e adaptado de:
Romney, M., e Steinbart, P. "Accounting Information Systems". Pearson Education / Prentice-Hall, U.S.A., 2006 (10ª ed.), Cap. 5 – Computer Fraud and Abuse, pp. 142-187



Índice

- Introdução
- Fraude: introdução
- Quem comete fraude e porquê
- Fraude informática
- Fraude informática e técnicas de abuso
- Prevenção e detecção de fraude informática e abuso



Introdução

- Os SI estão a tornar-se cada vez mais complexos
- A sociedade torna-se cada vez mais dependente dos SI
- Os riscos sobre os SI aumentam
- “67% of companies have had a security breach in the last year, with almost 60% reporting financial losses” (144)



Introdução

- 4 tipos de ameaças
 - Desastres naturais e políticos
 - Erros de sw e funcionamento deficiente de equipamentos
 - Acções não intencionais
 - Acções intencionais (*computer crimes*)



Introdução

- Ameaças: Desastres naturais e políticos
 - Imprevisíveis
 - Podem ser altamente destrutivos
 - Incêndios, inundações, terremotos, guerras, ataques terroristas
 - “The Defense Science Board predicts that attacks on ISs by foreign countries, espionage agents, and terrorists will soon be widespread” (144)
 - Alunos: ex.s?



Introdução

- Ameaças: Erros de sw e funcionamento deficiente de equipamentos
 - Hw, sw, sistemas operativos, erros de transmissão, falhas de energia...
 - "A federal study estimated the yearly economic losses due to sw bugs at almost \$60 billion a year" (145)
 - Alunos: ex.s?



Introdução

- Ameaças: Acções não intencionais
 - Acidentes, omissões, erros de lógica, dados mal introduzidos...
 - "... the greatest risk to information system and the greater dollar losses. The Information Systems Security Association estimates that 65% of security problems are caused by human errors" (145)
 - Alunos: ex.s?



Introdução

- Ameaças: Acções intencionais (*computer crimes*)
 - Fraudes, sabotagens, corrupção, alteração de dados, adulteração de reports financeiros ...
 - “In a recent 3-year period, the number of instances where information system networks were compromised rose 700%” (146)
 - Alunos: ex.s?



Fraude : introdução

- Fraude
 - “Fraud is any and all means a person uses to gain an unfair advantage over another person. Legally, for an act to be considered fraudulent there must be
 - 1 A *false statement, representation, or disclosure*
 - 2 A *material fact*, which is something that induces a person to act
 - 3 An *intent to deceive*
 - 4 A *justifiable reliance*; that is, the person relies on the misrepresentation to take an action
 - 5 An *injury or loss* suffered by the victim” (146)



Fraude : introdução

- Quem comete fraude
 - Interno
 - Externo
 - “An estimated 75 to 90% of all computer crimes are perpetrated by insiders with the requisite access, knowledge, skills, and resources” (147)
 - *White-collar criminals*



Fraude : introdução

- Duas formas de fraude...
- A. Apropriação de bens
 - Roubo, desfalque, uso indevido de bens
 - Alunos: ex.s?



Fraude : introdução

- A. Apropriação de bens
 - Características das fraudes cometidas por empregados
 - É necessária a confiança da pessoa ou entidade a defraudar
 - São usados meios “soft”, engenhosos, para cometer fraude e para apagar rastros
 - Os processos fraudulentos tendem a continuar no tempo
 - Os autores da fraude tendem a tornar-se extravagantes e pouco preocupados em arrecadar ou investir
 - Muitas vezes os autores das fraudes tornam-se gananciosos e praticam os actos cada vez com maior frequência e dimensão



Fraude : introdução

- A. Apropriação de bens
 - Características das fraudes cometidas por empregados
 - Com o passar do tempo
 - os autores podem tornar-se demasiado confiantes e menos cautelosos
 - a magnitude das fraudes pode aumentar conduzindo mais facilmente à sua detecção
 - Os factores mais significativos que contribuem para as fraudes com empregados são a ausência de controlos internos e/ou a falha na exigência da existência de controlos internos



Fraude : introdução

- B. Relato financeiro fraudulento
 - "... conduta intencional ou descuidada, por acto ou por omissão, que resulta em relato financeiro materialmente enganoso" (148)
 - Ex.s: Enron, WorldCom, etc: nestes casos, as declarações financeiras foram falseadas, conduzindo a prejuízos graves ou até a falências



Fraude : introdução

- B. Relato financeiro fraudulento
 - 4 acções para reduzir a possibilidade de relato financeiro fraudulento (148)
 - “1. Estabelecer um ambiente interno que contribua para a integridade do processo de relato financeiro
 - 2. Identificar e entender os factores que conduzem ao relato financeiro fraudulento na empresa
 - 3. Avaliar os riscos de que ocorra na empresa
 - 4. Desenhar e implementar controlos internos para assegurar uma confiança razoável na prevenção do relato financeiro fraudulento”



Fraude : introdução

- O número de casos de apropriação de bens é bastante maior do que os de relato fraudulento
- A valor das apropriações indevidas é geralmente pequeno comparado com report fraudulento
- As apropriações, porque geralmente pequenas, podem ser materialmente menos relevantes, pelo que os auditores externos estão geralmente mais preocupados com os riscos associados ao report financeiro fraudulento.



Fraude : introdução

- SAS No 99 (2002): *Consideration of Fraud in a Financial Statement Audit*. Requer-se que o auditor (149):
 - Entenda o que é uma fraude
 - Discuta os riscos de declarações materialmente fraudulentas
 - Obtenha informação
 - Identifique, avalie, e responda aos riscos
 - Avalie os resultados dos testes de auditoria
 - Documente e comunique o que descobriu
 - Incorpore a perspectiva tecnológica



Quem comete fraude e porquê

- Consideram-se 3 tipos de perfil (149)
 - Criminosos de colarinho branco (*white-collar criminals*)
 - Criminosos violentos
 - Público em geral
- Descobriu-se...
 - Diferenças significativas entre os criminosos de colarinho branco e os de crimes violentos
 - Poucas diferenças entre os criminosos de colarinho branco e o público em geral
 - não são essencialmente diferentes em termos de educação, idade, religião, estado civil, nº de anos em emprego, perfil psicológico



Quem comete fraude e porquê

- Computer fraude
 - Os criminosos tendem a ser mais novos e a possuir conhecimentos técnicos e informáticos
 - A motivação pode não ser especialmente criminosa
 - Curiosidade, desafio, forma de aprendizagem
 - Podem encarar estas actividades como “um jogo”, e não como um comportamento desonesto
 - Alguns actuam como “revolucionários” ou anarquistas



Quem comete fraude e porquê

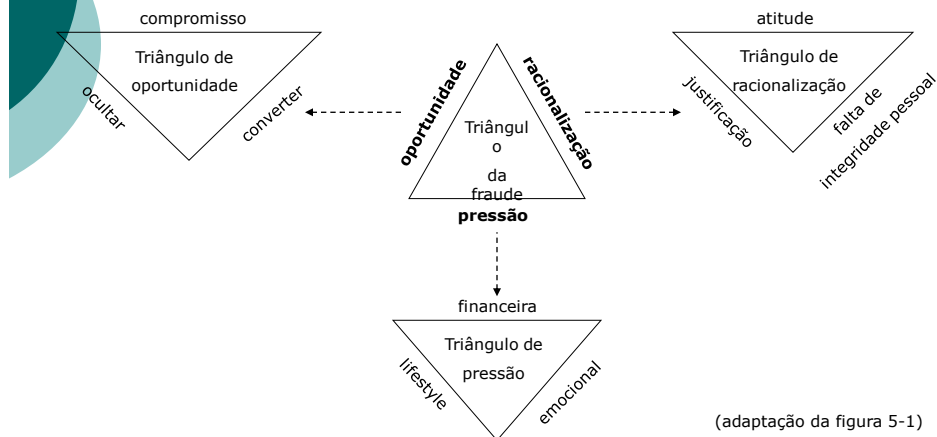
- Computer fraude
 - É crescente o número dos que procuram obter ganhos financeiros
 - Alguns vendem dados a spammers, a crime organizado, a outros hackers, ou a espionagem
 - Alguns casos são empregados insatisfeitos que procuram algum tipo de vingança
 - Outros usam posições de confiança



Quem comete fraude e porquê

- São necessárias 3 condições para que a fraude ocorra, que formam o “triângulo da fraude” (Cressey)
 - Pressão
 - Oportunidade
 - Racionalização
- ...ver figura no slide seguinte...

Quem comete fraude e porquê



ISCA-UA, Sistemas de Informação Contabilísticos

João Batista, 2010

23

Quem comete fraude e porquê

- Pressão
 - “A pressure is a person’s incentive or motivation for committing the fraud” (150)
 - Financeira
 - Ex.s
 - Emocional
 - Ex.s
 - Estilo de vida
 - Ex.s

ISCA-UA, Sistemas de Informação Contabilísticos

João Batista, 2010

24



Quem comete fraude e porquê

- Oportunidade
 - “... opportunity is the condition or situation that allows a person or organization to do three things”:
 - Comprometimento
 - Ex.s
 - Ocultação...
 - Ex.s
 - Conversão
 - Ex.s



Quem comete fraude e porquê

- Oportunidade
 - Origem
 - Interna
 - Externa
 - “... the most prevalent opportunity for fraud results from a company’s failure to *enforce* its system of internal controls” (153) Ex.s
 - Background check dos funcionários
 - Relações com clientes



Quem comete fraude e porquê

- Rationalização
 - "...a rationalization that allows perpetrators to justify their illegal behavior" (p 154)
 - Justificação (...I only took what they owed me)
 - Ex.s
 - Atitude (... the rules do not apply to me)
 - Ex.s
 - Falta de integridade pessoal (... having what I want is more important than being honest)
 - Ex.s



Quem comete fraude e porquê

- Concluindo...
 - "Fraud occurs when people have high pressures, abundant opportunities, and the ability to rationalize away their personal integrity" (154)
 - Em geral a fraude ocorre na presença de uma combinação destes 3 elementos
 - A fraude pode ser prevenida eliminando ou minimizando um ou mais dos 3 elementos
 - "...their greatest opportunity to prevent fraud lies in reducing or minimizing the opportunity to commit fraud. This is typically done by implementing a good system of internal controls"



Fraude informática

- "... any illegal act for which knowledge of computer technology is essential for its
 - perpetration,
 - investigation, or
 - prosecution" (154)



Fraude informática

- Mais especificamente, computer fraude inclui
 - "Unauthorized theft, use, access, modification, copying, and destruction of software or data
 - Theft of money by altering computer records
 - Theft of computer time
 - Theft or destruction of computer hardware
 - Use or the conspiracy to use computer resources to commit a felony
 - Intent to illegally obtain information or tangible property through the use of computers" (154)



Fraude informática

- As fraudes informáticas têm características importantes
 - Permitem que seja roubado
 - Mais de alguma coisa
 - Em menos tempo e
 - Com menor esforço
 - Podem ser mais difíceis de detectar



Fraude informática

- Razões que tornam os sistemas informáticos mais vulneráveis, aumentando o risco de fraude
 - São acumuladas grandes quantidades de dados e informação em bases de dados
 - Muitas pessoas (funcionários, clientes, funcionários) têm acesso aos sistemas
 - Os programas apenas precisam de ser alterados num momento, e depois continuarão em funcionamento até que
 - O sistema deixa de ser usado
 - Alguém detecta a alteração



Fraude informática

- Razões que tornam os sistemas informáticos mais vulneráveis, aumentando o risco de fraude
 - Muitos sistemas são acedidos a partir de PCs, que são sistemas vulneráveis e genericamente pouco seguros
 - É difícil controlar o acesso físico aos PCs
 - Os PCs são facilmente portáteis (ou portáteis), pelo que o seu roubo é fácil
 - É difícil controlar a segregação de funções, a mesma pessoa pode ser responsável pelo desenvolvimento e operação
 - Os utilizadores dos PCs tendem a ser menos cuidadosos com a segurança



Fraude informática

- Razões que tornam os sistemas informáticos mais vulneráveis, aumentando o risco de fraude
 - Desafios que se colocam aos sistemas
 - Fiabilidade
 - Falhas de equipamento
 - Dependência do ambiente (energia, desastres, etc)
 - Vulnerabilidade a interferências electromagnéticas
 - Vulnerabilidade a interrupções
 - Intersecção (eavesdropping) ou desvio (misrouting) de comunicações



Fraude informática

- Razões para o rápido crescimento dos casos de fraude e dos seus impactos
 - O conceito de fraude informática não é universal
 - Ex: algumas pessoas pensam que "vasculhar" nos sistemas de terceiros não é ilegal desde que não se tenha a intenção de roubar ou danificar os dados. O facto de não haver prejuízo não legitima a acção!!
 - Muitas fraudes não são detectadas
 - Alguns estimam que as fraudes detectadas são apenas 5% a 20% do total
 - Muitas das fraudes detectadas (80%-90%) não são denunciadas
 - Evitar má publicidade
 - Evitar ser novamente "atacado"

ISCA-UA, Sistemas de Informação Contabilísticos

João Batista, 2010

35



Fraude informática

- Razões para o rápido crescimento dos casos de fraude e dos seus impactos
 - Muitas redes são pouco seguras
 - É possível obter informação detalhada, na internet, sobre como cometer fraude
 - Basta pesquisar nos motores de busca...
 - Os mecanismos legais e de investigação podem ter dificuldade em acompanhar o ritmo de crescimento e de sofisticação das fraudes
 - É difícil de determinar o custo associado às fraudes

ISCA-UA, Sistemas de Informação Contabilísticos

João Batista, 2010

36



Fraude informática

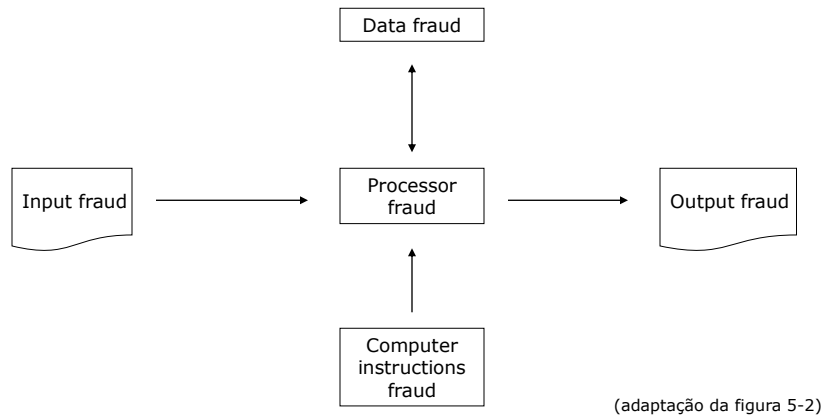
- Algumas áreas crescem de forma especialmente rápida
 - Espionagem económica
 - “at any point in time, the FBI is investigating about 800 separate incidents of economic espionage” (156)
 - Roubo de informação e de propriedade intelectual
 - “one noteworthy example was the allegation that Reuters Analytics broke into the computers of its competitor, Bloomberg, and stole lines of code that enables financial institutions to analyze historical stock market data” (156)



Fraude informática

- Classificação das fraudes informáticas
 - Input
 - Processamento
 - Instruções de computador
 - Dados
 - Output

Fraude informática



Fraude informática

○ Input

- Uma das formas mais simples e frequentes de cometer fraude é pelo input
- Não são necessários conhecimentos especiais, desde que se tenha acesso ao sistema. Pode acontecer em diversas partes do sistema
- Ex:
 - Alguém abriu uma conta num banco em NY, com um nome falso, e durante 3 dias substituiu os talões de depósito num balcão por outros com o código da sua conta. Ao fim de três dias levantou o dinheiro e nunca foi descoberto (157)
 - Mais exemplos no livro...



Fraude informática

- Processamento
 - Através de acesso não autorizado
 - Inclui roubo de tempo e de utilização de serviços
 - Os incidentes podem incluir
 - Navegação na internet
 - Utilização dos recursos organizacionais para benefício próprio
 - Uso dos sistemas da empresa para conduzir negócios alheios ou até concorrentes



Fraude informática

- Processamento
 - Ex (158)
 - Dois contabilistas sem direitos de acesso tiveram a possibilidade de entrar no sistema de Cisco que gere os pagamentos de stock options. Forjaram os forms necessários para autorizar e transferir mais de \$6.3 milhões das acções da Cisco para as suas contas pessoais. Venderam as acções e usaram parte desses fundos para levar uma vida extravagante, incluindo um automóvel de \$52,000, um anel de diamantes de \$44,000 e um relógio de \$20,000



Fraude informática

- Instruções de computador
 - Envolve “mexer” (*tampering*) no software que faz o processamento dos dados
 - Pode incluir
 - Modificação do software
 - Realização de cópias ilegais
 - Uso não autorizado
 - Pode incluir também a criação de programas ou módulos que desempenhem actividades não autorizadas



Fraude informática

- Instruções de computador
 - Tradicionalmente este era um dos tipos de fraude com menor ocorrência, porque exige competências técnicas que os users geralmente não têm
 - Actualmente é mais frequente este tipo de fraude ocorrer dado que muita da informação necessária se encontra disponível na internet (por exemplo, sobre criação de virus)



Fraude informática

- Dados
 - Inclui
 - Alterar ou danificar os dados da organização
 - Pode ter origem interna (empregados) ou externa
 - Ex: num caso foi usado um magneto para danificar os dados guardados em tapes magnéticas
 - Ex: caso de um empregado que retirou as etiquetas das tapes
 - Ex: ataques em web sites de organizações, alterando dados (vandalismo)
 - Ex: alunos?
 - Copiar, utilizar ou pesquisar ficheiros sem autorização
 - Por vezes as pessoas não têm consciência da gravidade destas actividades
 - Ex: alunos?



Fraude informática

- Dados
 - Inclui
 - Roubo de dados
 - Ex: um empregado descontente roubou os ficheiros de dados das instalações informáticas e fez o mesmo das instalações externas onde se armazenavam os backups. Pediu então um resgate para devolver os dados. Foi apanhado na troca...
 - Ex: um engenheiro tentou roubar planos de fabrico de processadores da Intel. Como os dados podiam ser lidos mas não gravados ou impressos, ele teve de fotografar cada screen
 - Os dados podem ter valor financeiro e podem ser objecto de venda a terceiros



Fraude informática

- Output
 - Inclui
 - Roubo de output
 - Como os output estão geralmente em screens ou reports impressos, o que permite...
 - Que sejam observados
 - Que as suas imagens sejam registadas
 - Que sejam copiados ilegítimamente
 - Os outputs podem ainda ser forjados ou falsificados
 - Ex: as falsificações com pagamentos de salários representam 20.000 milhões de dolares por ano nos EUA



Fraude informática e técnicas de abuso

- Têm sido desenvolvidas muitas técnicas para cometer fraude informática e abuso
- Alguns exemplos são descritos a seguir, e os restantes devem ser consultados na bibliografia (159-170)



Fraude informática e técnicas de abuso

- “Data diddling”: alteração de dados antes, durante, ou após terem sido introduzidos no sistema. A alteração pode ter em vista o apagamento, a alteração propriamente dita, ou o acrescento de dados importantes.
 - Ex: um empregado de uma correctora de Denver alterou os dados de uma transacção de 1700 acções da empresa Loren Industries considerando um valor de 2500 dolares quando o seu valor era de 25000 dolares



Fraude informática e técnicas de abuso

- Email forjado
 - Uma técnica consiste em enviar a mensagem através de um re-mailer que remove o cabeçalho da mensagem, tornando-a anónima
 - Outra técnica: spoofing: faz com que uma mensagem pareça ter uma origem que não corresponde à verdade



Fraude informática e técnicas de abuso

- Phishing
 - Envio de email pretendendo ser quem não é, e solicitar dados. O destinatário é solicitado a responder ao email ou a preencher dados num web site e a submeter esses dados. A informação recolhida é usada para roubar uma identidade ou para roubar fundos de contas bancárias
 - Ex.s ...



Prevenção e detecção de fraude informática e abuso

- Existem medidas que podem ser tomadas para prevenir e detectar fraude e abuso (170-171)
 - Reduzir a possibilidade de a fraude ocorrer
 - Aumentar a dificuldade de cometer fraude
 - Aperfeiçoar os métodos de detecção
 - Reduzir as perdas por fraude



Prevenção e detecção de fraude informática e abuso

- Reduzir a possibilidade de a fraude ocorrer
 - Criar uma cultura de integridade e compromisso com valores éticos e de competência
 - Adoptar uma estrutura organizacional, uma filosofia de gestão, um estilo operacional e uma abordagem ao risco que minimize a probabilidade de a fraude ocorrer
 - Procurar o envolvimento de um comité de auditoria activo e independente
 - Atribuir autoridade e responsabilidade de objectivos do negócio a departamentos e indivíduos específicos; encorajar iniciativas que contribuam para a resolução de problemas, com vista a atingir os objectivos propostos



Prevenção e detecção de fraude informática e abuso

- Reduzir a possibilidade de a fraude ocorrer
 - Identificar os eventos que conduzam ao aumento do risco de fraude; tomar medidas para prevenir, evitar, partilhar ou aceitar o risco
 - Desenvolver uma política de segurança que oriente a concepção e a implementação de procedimentos de controlo, que seja efectivamente comunicada aos empregados
 - Implementar políticas de recursos humanos para a contratação, compensação, avaliação, orientação, promoção de empregados que dê indicações sobre os níveis pretendidos de comportamento ético e de integridade



Prevenção e detecção de fraude informática e abuso

- Reduzir a possibilidade de a fraude ocorrer
 - Supervisionar os empregados, incluindo a monitorização do seu desempenho e a correcção dos seus erros
 - Formar os empregados sobre considerações éticas, de segurança e de medidas de prevenção de fraude
 - Exigir que os empregados cumpram períodos de férias, que as suas funções sejam rotativas, e que assinem compromissos de confidencialidade
 - Implementar projectos rigorosos de desenvolvimento e de aquisição de controlos, e de controlos de gestão de mudança
 - Aumentar as penalizações por fraude promovendo a instauração de procedimentos legais



Prevenção e detecção de fraude informática e abuso

- Aumentar a dificuldade de cometer fraude
 - Desenvolver um sistema forte de controlos internos
 - Segregar as funções de contabilidade
 - Autorização
 - Registo
 - Custódia
 - Implementar um programa de segregação de funções nas funções de sistema
 - Restringir acesso físico e remoto ao sistema
 - Exigir que as transacções e actividades sejam autorizadas por supervisores. Os sistemas devem autenticar as pessoas e os seus direitos de realizar as transacções antes de estas ocorrerem



Prevenção e detecção de fraude informática e abuso

- Aumentar a dificuldade de cometer fraude
 - Utilizar documentos e registos apropriados à captura e ao processamento de transacções
 - Salvar os bens, os registos e os dados
 - Exigir verificações independentes ao desempenho, como a reconciliação de conjuntos independentes de registos, sempre que possível e apropriado
 - Implementar controlos informáticos sobre o input dos dados, o seu processamento, o seu armazenamento, a sua transmissão e o output
 - Encriptar dados armazenados e transmitidos de forma a protegê-los de acesso e uso não autorizado
 - Corrigir vulnerabilidades de software instalando os últimos updates aos sistemas operativos, de segurança, e das aplicações



Prevenção e detecção de fraude informática e abuso

- Aperfeiçoar os métodos de detecção
 - Criar um audit trail de modo que as transacções sejam individualmente identificadas entre o sistema e as demonstrações financeiras e vice versa
 - Realizar periodicamente auditorias internas e externas, bem como auditorias de segurança às redes
 - Instalar software de detecção de fraude
 - Implementar uma "fraud hotline"
 - Criar o lugar de "computer security officer", bem como contratar consultores informáticos ou especialistas forenses quando necessário
 - Monitorizar as actividades de sistema, incluindo a utilização de computadores e de redes, logs de utilização e de erros, e todas as acções maliciosas. Utilizar sistemas de detecção de intrusão para automatizar o processo de monitorização



Prevenção e detecção de fraude informática e abuso

- Reduzir as perdas por fraude
 - Manter seguros adequados
 - Desenvolver planos de contingência por fraudes, de recuperação de desastres, e de continuidade do negócio
 - Armazenar cópias de segurança de programas e de ficheiros em localizações seguras, remotas
 - Utilizar software para monitorizar a actividade do sistema e recuperar de fraudes