Por que falham os Security Officers?

Por **Nelson Corrêa, CISSP,** <ncorrea@cfsec.com.br>

Grupo de Restrição: Irrestrito	Emissão: 21.10.2002
Arquivo: YSP_0005	Versão: 22.10.2002

Declaração de exoneração de responsabilidade
Este documento foi publicado pela CFSEC Security Architects com o intuito de fornecer, de forma rápida, informações precisas e atualizadas. A CFSEC Security Architects tentará corrigir qualquer erro que possa estar presente neste documento, tão logo seja avisada.

Entretanto, a CFSEC Security Architects não pode garantir que as informações apresentadas no mesmo estejam corretas.

A CFSEC Security Architects alerta ainda para os seguintes aspectos:

- O material difundido comporta exclusivamente informações de caráter geral, que não pretendem referir a situação específica de um indivíduo ou de uma entidade;
- Este documento pode incluir informações que não devem necessariamente estar completas, ser exaustivas e exatas ou estarem atualizadas;
- Este documento remete para sites externos, sobre os quais a CFSEC Security Architects não tem qualquer controle e relativamente aos quais declina todas as responsabilidades;
- As informações disponíveis neste documento não são pareceres de caráter profissional ou jurídico.

Todas as informações são providas pela CFSEC somente em uma base "no estado". Em nenhum evento a CFSEC será responsável pelos possíveis danos diretos, indiretos, especiais ou de qualquer outro tipo, derivados do uso deste web site, ou de qualquer outro web site que esteja ligado a este, incluindo, sem limitação, qualquer perda de lucros, interrupção de negócios, perda de programas ou outros dados de informação relacionados ao seu sistema, incluindo o caso de que nos seja expressamente informado a possibilidade de tais danos.

Sobre o autor

Nelson Corrêa *é o CEO da* ***CFSEC Security Architects****. Atuando há mais de 22 anos na gestão de projetos e profissional de Segurança da Informação certificado pelo ISC2, Nelson Corrêa é um dos mais experientes profissionais da área em nosso país, tendo sido responsável por mais de 70 projetos em Segurança da Informação. Membro do Computer Security Institute, do Information System Security Association e do Comitê de Estudos de Normas de Segurança da ABNT, foi professor convidado no primeiro curso brasileiro de pós gradução em Internet, promovido pela COPPE/ASIT. É palestrante e articulista na área de Segurança da Informação, tendo sua opinião veiculada nos maiores meios de comunicação do Brasil.*

Prefácio

Há poucos dias, eu estava fazendo uma apresentação para alguns executivos sobre as vantagens e desvantagens de se adotar a BS7799, ou o porquê das principais empresas de classe mundial não adotarem esse modelo e alcançarem sucesso na gestão de sua Segurança da Informação.

No intervalo do workshop, um dos presentes me trouxe uma pergunta, a princípio, fora do tema que discutíamos, que foi prontamente endossada pela maioria dos presentes. Em síntese, eles me perguntaram à queima-roupa o motivo pelo qual os gestores de segurança de suas empresas não demonstram que detêm o controle da Segurança da Informação como eles, executivos, esperariam.

Que alívio! Na palestra estávamos falando de um tema tão palpitante no momento aqui no Brasil... E como todo tema “na moda”, as opiniões, às vezes, são bem antagônicas. Uma pergunta abrindo uma discussão ali no coffee break poderia derrubar minha programação de agenda e de horário.

Porém, a dúvida daqueles executivos era a mais fácil de responder entre todas que eu esperava para aquele dia. Na mesma velocidade da pergunta, devolvi uma resposta que deixou todos com a xícara de cafezinho parada no caminho entre o tórax e a boca: “Eles falham porque estão preocupados com a segurança dos computadores e afins como redes, internet, servidores, roteadores, firewalls, switches, etc.”

O primeiro que resolveu trazer a xícara à posição inicial, sem beber o café, com muita surpresa me fez a segunda pergunta: “E não é com isso que eles precisam e deveriam se preocupar?” Respondi, quase sem respirar, para não dar tempo de novas surpresas: “Não, eles precisariam se preocupar é com o negócio de suas empresas!”. Bem, minha preocupação com a agenda e o horário foi para o espaço, e estendemos o cafezinho mais que devíamos. Para não sair do foco da programação daquele dia, prometi detalhar um pouco mais o assunto. Coisa que pretendo tentar neste Yellow Security Paper.

Antes de continuarmos, é fundamental interpretar a surpresa dos meus companheiros daquele dia, como uma confissão da divisão da culpa. Eles, por terem expectativas erradas, acabam induzindo ao outro lado da corda, o Security Officer, ao erro na condução da Segurança da Informação nas organizações.

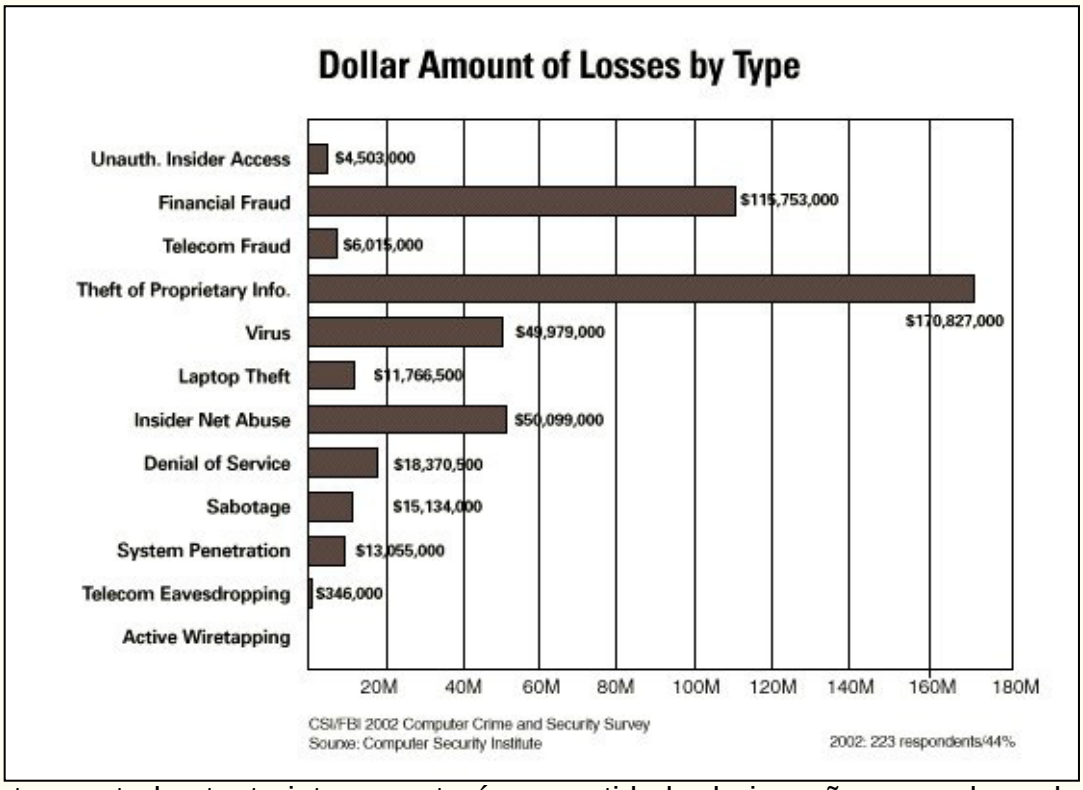
Poderia citar minha experiência, que vem do resultado de alguns anos de projetos de segurança. Mas é interessante mostrar alguns números, recolhidos de pesquisas realizadas este ano por CSI/FBI, KPMG, PriceWaterhouseCoopers, Ernst & Young, além de dezenas de outras disponíveis na Internet. Posso lhes garantir que minha experiência no Brasil, torna alguns desses números (internacionais) até “razoáveis”.

Apesar do aumento de investimentos, de preparação de pessoal, do aumento de profissionais certificados, os números são contundentes e mostram que a redução dos problemas não segue a mesma proporção do aumento dos esforços. Vamos olhar alguns desses números:

As perdas anuais quadruplicaram de 1997 para 2002. Com exceção de fraudes em telecomunicações, que tiveram uma redução fantástica, de 20 milhões para 300 mil dólares, todas as demais categorias subiram. Algumas com surpreendente crescimento, como abuso de acesso à Internet por pessoal interno, que cresceu de 1 milhão para 50 milhões de dólares.

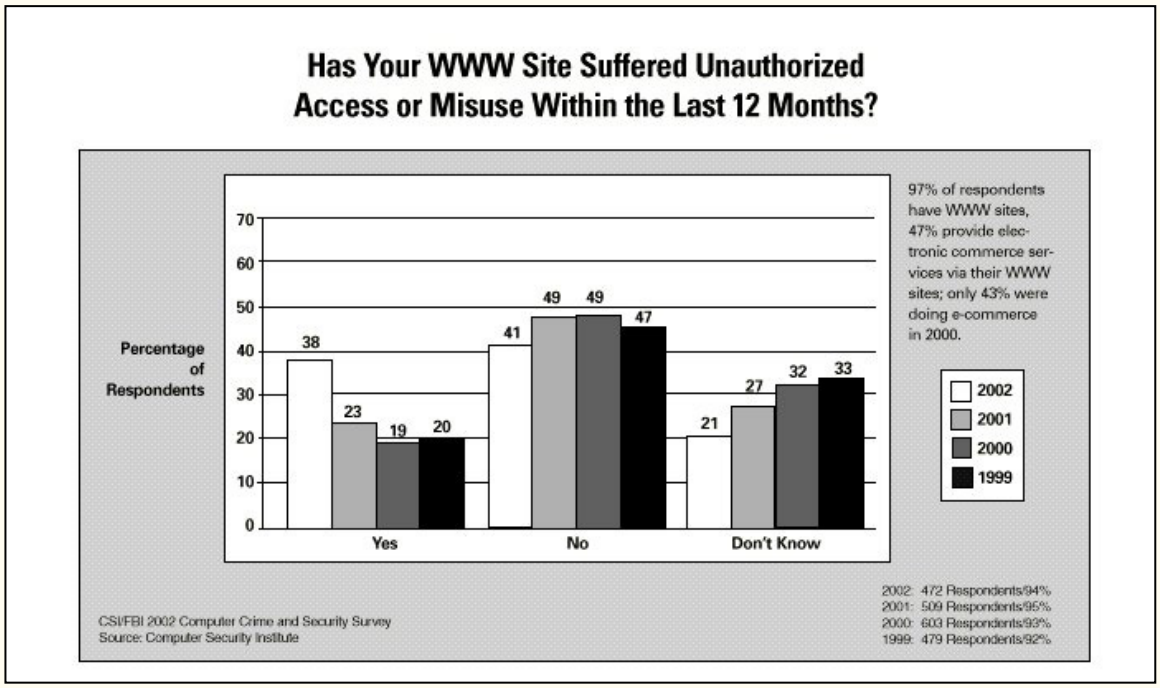
<figura The Cost of Computer Crime na última página>

Para cada de problema, as perdas financeiras são substanciais. No gráfico abaixo, o que mais chama a atenção é o prejuízo causado por contaminação por vírus e por abuso do pessoal interno, ou seja, por uma fraca gestão da segurança, que não comprometeu e nem preparou adequadamente os usuários da organização. Somadas, tais perdas chegam a 100 milhões de dólares, total muito próximo do prejuízo gerado por problemas mais sérios e bem mais difíceis de serem resolvidos, como roubo de informações críticas (120 milhões de dólares) e fraudes financeiras (115 milhões de dólares).



Outro ponto bastante interessante é a quantidade de invasões e quebras de segurança detectados em web sites. Sabemos, por experiência, que a web tem sido foco de forte investimento em tecnologias e novos projetos por parte das organizações que procuram se posicionar com relação ao comércio eletrônico e ao relacionamento eletrônico com clientes e fornecedores.

E os ataques continuam a crescer. Como consolo, se é que isso serve de algum consolo, a percepção de que se sofreram ataques também aumentou. Ou seja, já se tem coragem de falar que o web site foi atacado, ou melhor, já se consegue saber, depois do problema ocoirrido, que ele existiu. Vejamos mais uma figura da pesquisa 2002 do CSI/FBI:



A empresa norte-americana de consultoria KPMG também publicou o resultado de sua pesquisa 2002 de Segurança da Informação. Não temos resultados que mostrem tendências diferentes das outras pesquisas, ela só vem confirmar o que nós, profissionais de Segurança da Informação, percebemos na prática do dia-a-dia.

Com relação a perdas financeiras, ela mostra que no último ano, as empresas entrevistadas perderam juntas 10 milhões de dólares por conta de problemas com vírus de computador. A perda média por empresa foi de 162 mil dólares, com média de 62 dias de trabalho perdido por empresa.

Ainda nas perdas financeiras, pesquisa 2002 da KPMG mostra que falhas em sistemas críticos provocaram 80 dias perdidos e 155 mil dólares na média por empresa, com um total de 4 milhões de dólares nas empresas entrevistadas.

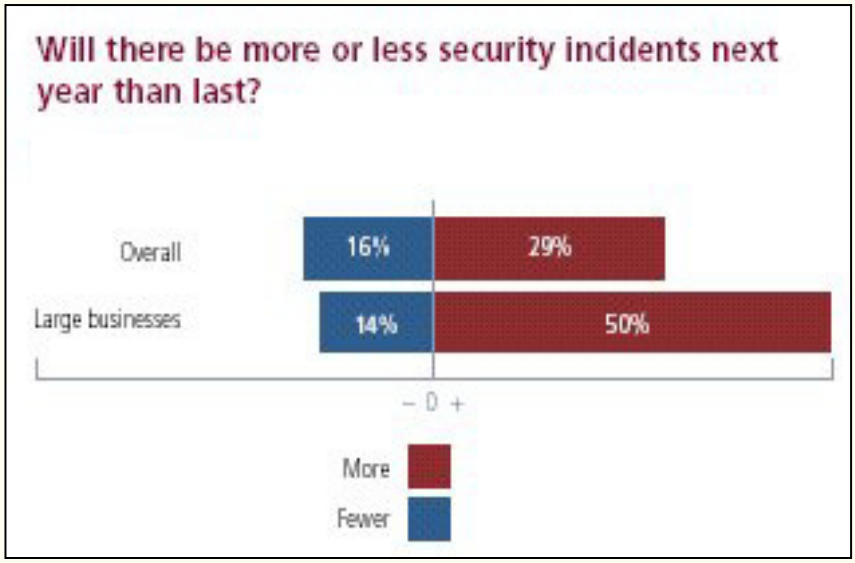
Mas o ponto mais interessante desta pesquisa é quando se pergunta aos entrevistados se eles concordam que suas empresas tomam precauções razoáveis para se protegerem de quebras de Segurança da Informação. Incríveis 96% concordaram que suas empresas tomam precauções razoáveis. E 58% concordaram enfaticamente com isso.

Continuando a pesquisa, só entre estes “enfáticos 58%” foi verificado que:

- 10% não testam suas medidas de segurança e, conseqüentemente, não sabem se elas funcionam na prática;

- 52% não usam nenhum tipo de tecnologia de detecção de intrusos (não perguntaram sobre gerenciamento de detecção de intrusos – IDM);
- 87% sofreram algum tipo de violação (quebra) de segurança no último ano, incluindo:
    - 61% vírus
    - 28% spam e-mail
    - 15% denial of service (DoS)
    - 13% perderam software
    - 12% website hacking

A Price Waterhouse Coopers também publicou uma pesquisa sobre Segurança da Informação em 2002. Para não sermos redundantes e chatos, não vejo necessidade de repetir as mesmas coisas já vistas nas outras pesquisas, mas vale a pena retirar um dado interessante desta última: a previsão que os entrevistados fazem sobre futuros incidentes, mostrada na figura abaixo:



Voltando à minha primeira afirmação do erro no tratamento da Segurança da Informação, é verdadeiro que o primeiro errado é o executivo que espera do seu gestor da Segurança da Informação uma atuação operacional, em cima de tecnologias.

Por conta disso, o Security Officer é contratado para estar sempre subordinado ao responsável pela área de informática (CIO). E este não é o pior dos mundos! Existem mais duas situações que são bem piores. Uma seria “escalar” algum técnico de informática para ser o Security Officer. A Segurança da Informação continua com o CIO e com foco no computador. A outra seria achar que com uma auditoria de sistemas forte, os auditores

corrigirão o problema de segurança e criarão boas práticas para os sistemas e seus computadores. É certo que, se mantivéssemos os parques tecnológicos por uma década inalterados, talvez, ao final desse prazo, os auditores conseguissem criar cultura e boas práticas para a Segurança da Informação.

Pronto, o primeiro passo foi dado de forma incorreta. Todos os demais que serão dados a partir de agora pelo Gestor da Segurança da Informação continuarão na direção errada.

Só para confirmar seu direcionamento, veja se você se encaixa em alguma dessas situações:

1. Área de Segurança da Informação totalmente dissociada da segurança física e patrimonial, sem perspectivas de futuras interações no curto ou médio prazos;
2. Área de Segurança da Informação com foco operacional. Essa é uma das mais comuns, e talvez a pior das situações que podemos encontrar de direcionamento errado e conseqüente tendência ao fracasso do Security Officer. É nessa situação que a área de segurança é responsável por cuidar do cadastramento e configuração de direitos de usuários nos sistemas informatizados e monitorar firewalls e outras tecnologias de segurança da informação que existam na organização. A conseqüência imediata é uma sobrecarga de trabalho e uma equipe sempre em número inferior à quantidade de "incêndios" a serem apagados. Se isso já gera um forte e desnecessário estresse, pior é o executivo analisar superficialmente este problema e chegar à conclusão que, como a segurança está sempre precisando de mais funcionários, ter uma área de segurança "inchará" a empresa e será sempre economicamente inviável. A contratação de consultorias pontuais é o recurso normalmente "mal" utilizado.
3. Gestor de Segurança da Informação despreparado e sem apoio da alta direção pula de vendedor para vendedor, comprando produtos que o mercado reconhece de fornecedores grandes e conhecidos. Portanto, se gastou desnecessariamente, talvez ninguém nunca saiba. Se algum problema acontecer, ele lava as mãos e garante o emprego.
4. Busca para resolver os problemas de Segurança da Informação nas soluções da moda. Essa é a tábua de salvação para quem não tem certeza qual deva ser o melhor caminho. E compram-se tecnologias e políticas por existir quem as venda, não por necessidade do negócio. Aumenta-se a complexidade do ambiente; conseqüentemente aumentam-se as vulnerabilidades, ameaças e o risco. Nesse perfil,

não é difícil encontrar tecnologias superdimensionadas para o ambiente, redundância de equipamentos somente em algumas partes do ambiente, na maioria das vezes, sem nem saber se aquelas informações que trafegam por aquele ambiente precisam de alta disponibilidade. Hoje introduzem-se Políticas de Segurança copiadas de outras empresas, sem que haja a preocupação com a manutenção dessas políticas nem com sua disseminação entre os usuários.

5. Atitudes policialescas são adotadas para coibir ações dos usuários. Sua adoção é feita de forma unilateral, sem apoios vertical e horizontal na hierarquia organizacional, e sem nenhuma preocupação em educar o usuário e, principalmente, em justificar tais atitudes nas necessidades do negócio da organização. Essas ações são conhecidas como “bumerangues”, pois voltam trazendo a revolta de todos com os “policiais” da segurança, que “só pensam em engessar os processos”. Além dessa repercussão negativa, precisa-se desfazer o que foi feito – trabalho jogado fora.

Se até aqui você não se encaixou em nenhuma dessas situações, verifique pelas perguntas abaixo se a Segurança da Informação na sua organização já deve estar falhando ou vai falhar em breve:

1. A estratégia de Segurança da Informação faz parte do seu Plano de Negócios?
2. A alta direção da organização reconhece e traz para si as decisões estratégicas relacionadas à Segurança da Informação?
3. Você mede a eficácia das medidas de segurança adotadas na sua organização?
4. Você conhece os riscos do seu negócio e gerencia-os de forma a diminui-los, assumi-los ou transferi-los dependendo de sua decisão estratégica?
5. Você sabe quanto gasta em segurança da informação e pode separar esta conta da área de Tecnologia da Informação?
6. Alguma vez, despesas ou investimentos em Segurança da Informação foram justificados em função de alguma necessidade do negócio ou teve um ROI calculado?
7. Se um evento fora do normal se abater sobre seu negócio, em partes ou no todo, você está formalmente preparado para recuperar o seu negócio dentro do tempo que ele possa continuar a sobreviver e no mesmo nível que se encontra hoje no posicionamento de mercado?
8. Novos negócios, novos projetos, novos produtos ou novos serviços contam com a participação formal da Segurança da Informação desde sua concepção?

9. Sua auditoria funciona somente na área de sistemas e contabilidade ou também audita a Segurança da Informação?
10. Você pode dizer, com certeza, quais falhas de segurança aconteceram e quanto foi gasto para recuperar o ambiente, independente da informação estar num computador ou fora?

Existem claramente dois caminhos em quase tudo que fazemos na vida. Um nos leva obrigatoriamente ao fracasso, e o outro nos dá muitas chances de atingir o sucesso. Com a Segurança da Informação isso não é diferente. Se olharmos a segurança como um problema tecnológico e operacional, ou seja, olhando para a segurança do computador, tenho certeza que o resultado será sempre o fracasso. Por outro lado, nossas chances de sucesso crescem de forma geométrica, se olharmos a Segurança da Informação, olhando para a segurança do negócio.

The Cost of Computer Crime

The following table shows the aggregate cost of computer crimes and security breaches over a 72-month period.

Note: In 2002, 80% of our survey respondents acknowledged financial losses, but only 44% of respondents could quantify the losses.

How money was lost

	Respondents w/ Quantified Losses						Lowest Reported						Highest Reported						Average Losses						Total Annual Losses					
	'97	'98	'99	'00	'01	'02	'97	'98	'99	'00	'01	'02	'97	'98	'99	'00	'01	'02	'97	'98	'99	'00	'01	'02	'97	'98	'99	'00	'01	'02
Theft of proprietary info.	21	20	23	22	34	26	$1K	$300	$1K	$1K	$100	$1K	$10M	$25M	$25M	$25M	$50M	50M	$954,666	$1,677,000	$1,847,652	$3,032,818	$4,447,900	$6,571,000	$20,048,000	$33,545,000	$42,496,000	$66,708,000	$151,230,100	$170,827,000
Sabotage of data of networks	14	25	27	28	26	28	$150	$400	$1K	$1K	$100	$1K	$1M	$500K	$1M	$15M	$3M	10M	$164K	$86K	$163,740	$969,577	$199,350	$541,000	$4,285,850	$2,142,000	$4,421,000	$27,148,000	$5,183,100	$15,134,000
Telecom eavesdropping	8	10	10	15	16	5	$1K	$1K	$1K	$200	$1K	$5K	$100K	$200K	$300K	$500K	$500K	5M	$45,423	$56K	$76,500	$66,080	$55,375	$1,205,000	$1,181,000	$562,000	$765,000	$991,200	$886,000	$6,015,000
System penetration by outsider	22	19	28	29	42	59	$200	$500	$1K	$1K	$100	$1K	$1.5M	$500K	$500K	$5M	$10M	5M	$132,250	$86K	$103,142	$244,965	$453,967	$226,000	$2,911,700	$1,637,000	$2,885,000	$7,104,000	$19,066,600	$13,055,000
Insider abuse of Net access	55	67	81	91	98	89	$100	$500	$1K	$240	$100	$1K	$100K	$1M	$3M	$15M	$10M	10M	$18,304	$56K	$93,530	$307,524	$357,160	$536,000	$1,006,750	$3,720,000	$7,576,000	$27,984,740	$35,001,650	$50,099,000
Financial fraud	26	29	27	34	21	25	$5K	$1K	$10K	$500	$500	$1K	$2M	$2M	$20M	$21M	$40M	50M	$957,384	$388K	$1,470,592	$1,646,941	$4,420,738	$4,632,000	$24,892,000	$11,239,000	$39,706,000	$55,996,000	$92,935,500	$115,753,000
Denial of service	n/a	36	28	46	35	62	n/a	$200	$1K	$1K	$100	$1K	n/a	$1M	$1M	$5M	$2M	50M	n/a	$77K	$116,250	$108,717	$122,389	$297,000	n/a	$2,787,000	$3,255,000	$8,247,500	$4,283,600	$18,370,500
Spoofing	4	n/a	n/a	n/a	n/a	n/a	$1K	n/a	n/a	n/a	n/a	n/a	$500K	n/a	n/a	n/a	n/a	n/a	$128K	n/a	n/a	n/a	n/a	n/a	$512,000	n/a	n/a	n/a	n/a	n/a
Virus	165	143	116	162	186	178	$100	$50	$1K	$100	$100	$1K	$500K	$2M	$1M	$10M	$20M	9M	$75,746	$55K	$45,465	$180,092	$243,845	$283,000	$12,498,150	$7,874,000	$5,274,000	$29,171,700	$45,288,150	$49,979,000
Unauthorized insider access	22	18	25	20	22	15	$100	$1K	$1K	$1K	$1K	$2K	$1.2M	$50M	$1M	$20M	$5M	1.5M	$181,437	$2,809,000	$142,680	$1,124,725	$275,636	$300,000	$3,991,605	$50,565,000	$3,567,000	$22,554,500	$6,064,000	$4,503,000
Telecom fraud	35	32	29	19	18	16	$300	$500	$1K	$1K	$500	$1K	$12M	$15M	$100K	$3M	$8M	100K	$647,437	$539K	$26,655	$212,000	$502,278	$22,000	$22,660,300	$17,256,000	$773,000	$4,028,000	$9,041,000	$346,000
Active wiretapping	n/a	5	1	1	0	0	n/a	$30K	$20K	$5M	$0	$0	n/a	$100K	$20K	$5M	$0	0	n/a	$49K	$20K	$5M	$0	$0	n/a	$245,000	$20,000	$5,000,000	$0	$0
Laptop theft	165	162	150	174	143	134	$1K	$1K	$1K	$500	$1K	$1K	$1M	$500K	$1M	$1.2M	$2M	5M	$38,326	$32K	$86,920	$58,794	$61,881	$89,000	$6,132,200	$5,250,000	$13,038,000	$10,404,300	$8,849,000	$11,766,500
Total Annual Losses:																									$100,119,555	$136,822,000	$123,799,000	$265,337,990	$377,828,700	$455,848,000

CSI/FBI 2001 Computer Crime and Security Survey
Source: Computer Security Institute

Grand total of Losses reported (1997-2001): $1,459,755,245