Como todos los años para esta época aparece el reporte anual llamado CSI[1]/FBI[2] Computer Crime and Security Survey. En su décima edición, este reporte del 2005 es considerado por muchos la encuesta más "antigua" y tal vez completa al respecto.

Luego de haberla analizado y comparado con su versión del 2004 surgen conclusiones que están relativamente entrelazadas y que trataremos de resumir a continuación.

Adicionales que se mantienen: En el 2005 se mantienen puntos que se incorporaron por primera vez en el 2004:

- La forma en la cual las empresas evalúan la performance de sus inversiones en seguridad informática.
- El porcentaje del presupuesto de IT destinado a seguridad informática.
- Las necesidades de entrenamiento en seguridad dentro de las organizaciones.
- El nivel de gastos organizacionales destinados a inversiones en seguridad.
- El impacto del outsourcing en las actividades de seguridad informática.
- El rol del acta Sarbanes-Oxley[3] del 2002 sobre actividades de seguridad.
- El uso de auditorias externas y seguros externos.

Conclusiones más importantes:

- Pese a que el ataque de virus sigue siendo el principal punto, crecieron los problemas por el uso no autorizado de sistemas de computación y por el robo de información propietaria. En realidad además de crecer en porcentaje, lo que creció es el monto de las pérdidas en estos dos puntos (entre los dos suman 62 Mu$s que adicionados a los casi 43 Mu$s producto de los virus nos dan 105 Millones sobre un total general de 130!!!. En el 2004 estaban decreciendo!.
- Se decrementa respecto a los años anteriores el costo de los ataques por virus y denegación del servicio (DoS, denial of service), creciendo el robo de información propietaria.
- Los seguros "cibernéticos" continúan bajos.
- Se incrementaron notablemente los incidentes sobre los Web sites pero los números a la fecha no representan nada.
- El porcentaje de organizaciones que reportó intrusiones en sus computadoras y lo denunció, sigue declinando como producto de la publicidad negativa.
- Aumento un 5% (87%) las empresas que realizan auditorias de seguridad.
- En el 2004, la mayoría de las empresas no habían realizaron outsourcing de las actividades relacionadas con la seguridad informática y esto continúa en la actualidad.
- La aparición del Sarbanes-Oxley Act empieza a hacerse notar
- Cada vez más se piensa que el entrenamiento en seguridad es importante y no creen que se esté invirtiendo lo suficiente en el área, haciendo mucho hincapié en la administración de los riesgos y en las políticas y complementándolas con la tecnología.

Comentarios sobre las conclusiones: estas conclusiones son los resultados de las evaluaciones del CSI/FBI, desde nuestro punto de vista requieren algunas apreciaciones que detallamos a continuación:

- En el 2004 hicimos una serie de críticas sobre lo incluido en la novena edición y creemos que ahora en la décima se aprecian y profundizan más, dándonos la razón en nuestra comparativa de los diez años de estadísticas.

[1] CSI: Computer Security Institute, del cual somos miembros.
[2] FBI: Federal Bureau of Investigation (en este caso de la ciudad de San Francisco – EE.UU.).
[3] Si no tiene claro este punto solicite información a info@kwell.net

- Resumimos los puntos que criticamos el año pasado y marcamos en qué estuvimos en lo correcto y en qué no:
  - No podemos evitar comparar los reportes del 2005 y 2004 con los anteriores y pese a los adicionales que detallamos precedentemente, creemos que han empeorado respecto al del 2003. Los fundamentos resumidos de nuestra apreciación son los siguientes:
    - ☑ Durante 8 años mantuvieron tablas comparativas que mal que mal permitían "ver" rápidamente la diferencia en un mismo tema o rubro a través del tiempo. En el 2004 se eliminaron la mayoría de las mismas por lo que se pierden las referencias históricas o estadísticas o se hacen más difíciles de interpretar y por sobre todo de comparar. No olvidemos que uno de los resultados más importantes de este tipo de reporte anual que lleva casi una década es permitir visualizar las tendencias.
    - ☑ Creemos luego de seguir a estos reportes durante varios años, que tal como su habitual genética delata, los encuestadores estadounidenses son sistemáticos, prolijos y muy precisos, pero que la interpretación que hacen de las estadísticas deja mucho que desear. Y esto no lo decimos luego de evaluar un solo reporte, sino comparando los reportes 2002, 2003 y 2004. Conclusión: la recolección es muy buena, lo que deducen, ya no nos cabe duda, deja mucho para opinar. Para que tengan una idea, ellos hacen un análisis demasiado fino de algunos números cuyas variaciones anuales son de 2 o 3 puntos pero no dicen nada sobre que están en bandas del 50 al 70 %.[4]
  - La interpretación de los resultados en sí mismos, desde nuestro punto de vista, es susceptible a otras formas de ver las cosas y trataremos de resaltar esas diferencias.
    - ♦ El año pasado dijimos: Reflexionan en varias oportunidades sobre que sigue cayendo y lo marcan como algo notable, la cantidad de casos de uso no autorizado de los sistemas de computación en los últimos doce meses. En 2004 están en el 53 %, en el 2003 en 55 % y estamos de acuerdo, la tendencia es que está en baja, pero lo que no se comenta es que en los últimos seis años (desde 1999) está dentro de una banda entre el 50 y el 60 % y creemos que esta lectura es más apropiada, es decir, nosotros comentaríamos: "... si bien la tendencia sigue en baja, hace 6 años que estamos entre 50 y 60 % y eso es muchísimo, entiéndase: año tras año más de la mitad de las empresas sufren estos ataques como un reloj...."
    - ☑ ¡Pero en el 2005 además de cumplirse con lo que mencionamos en el punto anterior, el valor creció al 56 %!.
    - ♦ El año pasado dijimos: Otro tema en el que diferimos un poco y dentro del mismo ítem es el relativo a la cantidad de incidentes. CSI/FBI dicen que bajan, por qué, porque en la columna de mayor a 10 incidentes en el '03 se leía 16 % y en el '04 se lee 12 %, y creció la de entre 1 y 5 incidentes del 38 al 47 %. Pero lo que no dicen es que los que NO SABEN (o no responden) en el 2003 eran el 26 % y en 2004 el 22 %. De modo tal que la lectura podría ser: "...no decreció tanto, sino que bajó la gente que no sabe...".
    - ☑ ¡Pero en el 2005 se da que bajamos respecto al 2004 de 47 a 43 % pero estamos por arriba del '03 con 38 % y de todos los años previos! Y para peor la cifra de los que no saben está muy por arriba pasando del 22 % del '04 al 28 % en este año.
    - ♦ El año pasado dijimos: Además hay algo que se mantiene en el tiempo o se incrementa: las empresas tiene cada vez menos tendencia a "informar o comentar" sobre los incidentes de seguridad fundamentalmente por temas de mala publicidad o marketing, y menos aún a denunciarlos legalmente, por lo que deducimos dos cosas: esta encuesta así como está tiene poco futuro y .... lo más importante, la seguridad informática es cada vez más un "issue" dentro de la compañía, por eso no se comenta hacia fuera....
    - ☑ ¡Y en el 2005 es igual!
  - Los resultados no aplican como tales a nuestro mercado, mejor dicho, no aplican fuera de EE.UU. por lo que requieren una adecuación para por ejemplo nuestro país o realidad. Trataremos a continuación de marcar las diferencias más notables:
    - ☑ La encuesta contempla respuestas de empresas por número de empleados, el 20 % corresponde a empresas de entre 1 y 99 empleados y el 14 % entre 100 y 499, si nos estiramos un poco llegamos al 15 % con rangos de empresas de entre 500 y 1499 empleados. El resto (hasta 9999, 49999 o más de 50000 empleados) lamentablemente no nos aplica mucho.
    - ☑ Ni que hablar respecto facturado, ya que allí las diferencias de mercado se agigantan ya que tienen en su encuesta más de un 57 % de empresas que facturan más de 100 Mu$s por año (millones de dólares estadounidenses).

[4] Es como cuando leemos, genial: la pobreza bajó el 1 %, mejoramos!, pero no dicen que estaba en el 61 % y cayó al 60%. Y pensábamos que este tipo de manejo de la información es más propio de países "bananeros".

- ☑ Se mantiene otra diferencia que apareció en el 2004, se relaciona con el tipo de trabajo de los que responden la encuesta: más del 50 % tiene cargos relacionados con la seguridad (Director, Gerente, Administrador, etc.), nos parece que en nuestro mercado son pocas las compañías que tienen a alguien "dedicado" haciendo el gerenciamiento de la seguridad.

Las cifras: además de lo que se mencionó anteriormente y que se relaciona más a cómo se efectúa y quién responde a la encuesta, trataremos de reflejar los números que consideramos más significativos:

- El 48 % de las empresas gasta entre un 1 y un 5 % del presupuesto de IT en seguridad. Esto es un número muy bajo y más aún en EE.UU.. Es más, ellos mismo piensas que están por debajo de lo que deberían gastar.
- Las empresas que facturan más de 1.000 Mu$s gastan un promedio de 247 dólares por empleado en gastos e inversiones en seguridad. Las que facturan menos de 10 Mu$s gastan 643 u$s por empleado. En ambos casos hubo un crecimiento significativo respecto al año anterior (110 y 500 u$s). Notemos cómo las empresas pequeñas gastan muchísimo más en seguridad que las grandes. El mercado que más gasta en el rubro son los gobiernos estatales (antes era el federal) y en los privados: las utilities, el transporte, seguidos por telecomunicaciones, manufactura, tecnología y financieras.
- El 38 % de los encuestados emplea el ROI como métrica financiera para cuantificar los costos y beneficios de los gastos en seguridad informática, el año pasado era el 55 %. El resto emplea el NPV (Net Present Value) y el IRR (Internal Rate of Return).
- El 63 % del mercado no hizo aún ningún tipo de outsourcing de las funciones de seguridad, un 26 % hizo outsourcing de entre 1 y 20 %, 6 % entre 21 y 40 % y sólo el 4 % hizo un outsourcing de entre el 41 y el 100%. Este es un claro indicador de lo virgen que está este mercado.
- El 75 % de las empresa no tiene seguros o pólizas que los cubran de riesgos cibernéticos.
- El 56 % respondió que sus sistemas de computación fueron usados sin autorización en el último año.
- Se incrementó el número de respuestas respecto a los que no saben cuántos incidentes sufrieron durante el año (ya sea desde afuera o internos) de un 22 a un 28 %. Ahora bien la cantidad de incidentes informáticos desde el interior y desde el exterior son casi iguales. Obviamente esto no tiene en cuenta todos los incidentes de tipo "no tecnológicos" como los encuadrados en la ahora llamada "ingeniería social" o en los problemas derivados de la falta de políticas o violaciones a las mismas.
- Un 95 % reportó que sufrió más de 10 incidentes de seguridad en su web site durante los últimos doce meses. El monto en cuanto a pérdidas monetarias no es significativo, pero la cantidad es muy grande y no se registraba en el pasado.
- En cuanto a las tendencias anuales relativas a las tecnologías de seguridad empleadas tomando los últimos 6 años, podemos decir lo siguiente:
  - 97 % emplea firewalls (=)[5]
  - 96 % emplea antivirus (=).
  - 70% emplea listas de control de accesos basadas en web (=).
  - 72 % emplea sistemas de detección de intrusos.
  - 68 % emplea encripción para datos en tránsito. Esto es totalmente nuevo e importante.
  - 52 % emplea passwords de login/cuenta reusables (-).
  - 35 % emplea sistemas de "prevención" de intrusos (-10%)[6].
  - 46 % emplea archivos cifrados (encriptados) (+4%)[7].
  - 42 % emplea smart-card u otros mecanismos de one-time passwords (+7%).
  - 35 % utiliza PKI (Public Key Infrastructure) (+5%).

[5] Se mantiene aproximadamente el valor respecto al año pasado.
[6] Decreció el valor respecto al año pasado.
[7] Creció el valor respecto al año pasado.

- 15 % emplea biométrica (+4%).

- Ahora bien, otros números a estudiar un poco tienen que ver con los tipos de ataques detectados, porque esto marca: hacia donde van los "delincuentes" y/o como "funciona" la protección, no?.
  - 7X % sufren ataques con virus, y el número ronda entre el 80 y el 95 % en los últimos 6 años, pero lo alarmante es la cifra de pérdidas debida a virus informada: 42 Mu$s, 55 Mu$s (2004) y 27 Mu$s (2003), es decir la pérdida que se había duplicado el año pasado bajó un poco pero sigue siendo alta.
  - El acceso no autorizado ronda el 3x %, y si bien bajó un poco lo que asombra son las pérdidas por 31 Mu$s.
  - 3X % sufre de DoS (Denial of Services), si bien porcentualmente venía subiendo y ahora parece que ya eso se revirtió, sigue en la banda del 30 al 40 %, pero las pérdidas cayeron a 7 Mu$s!. En el 2004 fueron 26 Mu$s y 65 Mu$s el 2003!. Este problema prácticamente ya no afecta monetariamente!.
  - Casi 10 % robo de información propietaria, lo que no se entiende es que en plata en el 2003 eran 70 Mu$s, en el 2004, 11 Mu$s y en este año 31 Mu$s?. No es fácil de comprender como cayó a la séptima parte el año pasado y en este subió por tres. Consideramos que los números del año pasado debían tener algo extraño.
  - Se mantienen los abusos internos de red.
  - El fraude financiero se manejó durante un quinquenio entre el 13 y el 14 % cayó a menos de 10 puntos, desde 10 Mu$s a 7,7 y de allí a 2,6 Mu$s.
  - Aparece el abuso de las redes inalámbricas y el web site defacement como nuevos conceptos en pérdidas (aunque los números no mueven el gran total).
  - El resto: robo de laptops, fraude telefónico, sabotaje, no afecta demasiado al total ni cambia demasiado en el tiempo. Si se nota que el IDS dio algún resultado en el último año porque las pérdidas por este motivo están por debajo del millón y eran de 2,7 Mu$s.[8]
- Por último en este campo destacamos que las pérdidas totales estuvieron en el orden de los 130 Mu$s, siendo las más bajas en la historia de la estadística: 265 M – '00, 378 M – '01, 456 M – '02, 202 M – '03, 141 – '04.[9]
- Algo que ya se comentó pero que destacamos es que se reclama por mayor inversión en entrenamiento en seguridad y dentro del mismo, los rubros más importantes son: políticas de seguridad (70%), seguridad de redes (70%), y hasta un rubro como criptografía mereció un porcentaje muy alto 51% vs. 28% del 2004.
- Respecto a lo que hacen las empresas cuando detectan una intrusión, estas dicen que en los últimos 12 meses:
  - 73 % tapó los agujeros (-18%).
  - 37 % no lo reportaron! (-11%).
  - 20 % lo denunciaron legalmente (=).
  - 12 % lo reportaron a legales internos (-4%).
- Y vean estos dos números en particular el último:
  - 43 % no dice nada por temas publicitarios o bursátiles (-8%).
  - 33 % no dice nada por miedo a la competencia!
- Finalmente empieza a aparecer el impacto de Sarbanes-Oxley Act, en 8 de los 14 sectores que responden a la encuesta, afirman que esta repercute sobre la seguridad de la información de las organizaciones.

[8] Bueno pero como dijimos en otra parte, este tipo de lectura, no es analizada por el CSI/FBI (¿?)

[9] La otra lectura es que las pérdidas de las empresa cayeron tanto como subieron la facturación los fabricantes de antivirus y productos para la seguridad. Estaría bueno hacer ese cruce de información, aunque creo que la facturación subió mucho más que la reducción de pérdidas. Que conste que cualquier tipo de asociación de eventos es culpa absoluta del lector.

Los comentarios finales: del CSI/FBI concluyen con "...los sistemas de información basados en computadoras han sido de importancia crítica para la mayoría de las organizaciones por varias décadas. Desde mitad de los años 90, Internet ha solidificado el rol central de las computadoras en el funcionamiento de las organizaciones modernas. Las preocupaciones relativas a la seguridad informática también se han movido al centro del escenario desde la aparición de Internet...". Tal como dijeron en 2004, repiten: "...en las etapas iniciales, el foco de la seguridad informática estaba centrado en los temas técnicos tales como la encripción, el control de accesos y el IDS. Más recientemente en estos años, los aspectos económicos, financieros y de administración de riesgos se han convertido en temas preocupantes para las organizaciones de hoy en día. Estos últimos son complementarios de, más que substitutos para, los aspectos técnicos de la seguridad informática....".
El párrafo anterior lo compartimos (tal como lo mencionamos el año pasado), y estamos empezando a transitar (ahora si) por la etapa inicial que ellos dicen estar superando....

"...El mayor conocimiento que tenemos acerca de las causas y consecuencias de las brechas en la seguridad informática, como así también la importancia de la seguridad informática en la forma en que se direcciona la organización, hace que sea más factible la mejora en este terreno. Los resultados de la encuesta presentados en este informe, representa la confianza que tenemos en ser adiciones valiosas a la muy necesitada base de conocimientos...."

Lo que no compartimos del todo es el cierre de la encuesta: "... por sobre todo los objetivos de la encuesta de este año son encontrar las tendencias claves relativas a la seguridad informática e identificar los importantes cambios emergentes en este terreno....". En realidad compramos a media la segunda parte de la frase y como comentamos, nos desilusionó (por segunda vez) esta edición 2005 porque no alcanza (a nuestro modesto entender) los objetivos que se plantearon.

Nota 1: por segunda vez en 10 años participaron además del CSI y del FBI, tres académicos, dos de los cuales están relacionados con altas empresas privadas de consultoría / auditoria estadounidenses.

Nota 2: todos nuestros comentarios (para aquellos que les interese) fueron enviados a R. Richardson, Director Editorial del CSI, emisor de este reporte.