Como todos los años para esta época aparece el reporte anual llamado CSI[1]/FBI[2] Computer Crime and Security Survey. En su novena edición, este reporte del 2004 es considerado por muchos la encuesta más "antigua" y tal vez completa al respecto.

Luego de haberla analizado y comparado con su versión del 2003 surgen conclusiones que están relativamente entrelazadas y que trataremos de resumir a continuación.

Adicionales del 2004: se incorporaron una serie de temas que no habían sido tenidos en cuenta anteriormente y que son importantes:

- 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:

- Decrece el uso no autorizado de sistemas de computación.
- Se incrementa respecto a los años anteriores el costo de los ataques por virus y denegación del servicio (DoS, denial of service), bajando el robo de información propietaria.
- El porcentaje de organizaciones que reportó intrusiones en sus computadoras y lo denunció, sigue declinando.
- Muchas organizaciones efectúan algún tipo de evaluación económica de sus gastos en seguridad.
- Más del 80 % de las empresas realiza auditorias de seguridad.
- La mayoría de las empresas no realizaron (aún) outsourcing de las actividades relacionadas con la seguridad informática, piensa que el entrenamiento en seguridad es importante y no creen que se esté invirtiendo lo suficiente en el área.

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:

- No podemos evitar comparar el reporte del 2004 con los anteriores y pese a los adicionales que detallamos precedentemente, creemos que ha 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,

[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

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.
  - 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 este año 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...."
  - 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 45 %. Pero lo que no dicen es que los que NO SABEN (o no responden) el año pasado eran el 26 % y ahora son el 22 %. De modo tal que la lectura podría ser: "...no decreció tanto, sino que bajó la gente que no sabe...".
  - 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....
- 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 19 % corresponde a empresas de entre 1 y 99 empleados y el 15 % entre 100 y 499, si nos estiramos un poco llegamos al 13 % 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).
  - Otra diferencia, pero que apareció este año, se relaciona con el tipo de trabajo de los que responden la encuesta: el 53 % tiene cargos directamente 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:

[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".

- El 46 % 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$s gastan un promedio de 110 dólares por empleado en gastos e inversiones en seguridad. Las que facturan menos de 10 Mu$s gastan 500 u$s por empleado. El mercado que más gasta en el rubro es el de las empresa de transporte, seguidos por el gobierno, las empresas de telecomunicaciones, las de tecnología y las financieras.
- El 55 % de los encuestados emplea el ROI como métrica financiera para cuantificar los costos y beneficios de los gastos en seguridad informática. 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 y sólo el 7 % hizo un outsourcing de entre el 41 y el 100%. Este es un claro indicador de lo virgen que está este mercado.
- El 72 % de las empresa no tiene seguros o pólizas que los cubran de riesgos cibernéticos.
- Algo absolutamente nuevo: el 89 % respondió que tuvo entre 1 y 5 incidentes es sus web sites en los últimos 12 meses.
- En cuanto a las tendencias anuales relativas a las tecnologías de seguridad empleadas tomando los últimos 6 años, podemos decir lo siguiente:
    - 99 % emplea antivirus y el valor se mantiene en el tiempo.
    - 98 % emplea firewall y viene creciendo.
    - 71% emplea listas de control de accesos basadas en web, anteriormente se media el control de accesos en general, pero si tomamos que es más o menos lo mismo, este valor cayó.
    - 68 % emplea sistemas de detección de intrusos, bajó un 5 % respecto al '03, pero la tendencia era en subida.
    - 56 % emplea passwords de login/cuenta reusables, creció y venía en bajada constante.
    - 45 % emplea sistemas de "prevención" de intrusos. Y este es un nuevo concepto prevenir en lugar de detectar (porque en la detección seguramente ya fue tarde).
    - 42 % emplea archivos cifrados (encriptados), bajo mucho este número que tenia 5 años de subida.
    - 35 % emplea smart-card u otros mecanismos de one-time passwords, no podemos comparar.
    - 30 % utiliza PKI (Public Key Infrastructure), no podemos comparar.
    - 11 % emplea biométrica, se mantiene estable.
- 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?.
    - 8X % 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: 55 Mu$s y en el 2003 fue de 27 Mu$s, es decir se duplicó la pérdida en un año!.
    - 37 % sufre de DoS (Denial of Services), si bien porcentualmente venía subiendo, sigue en la banda del 30 al 40 %, pero las pérdidas cayeron a 26 Mu$s de 65 Mu$s registradas en el 2003!
    - 10 % robo de información propietaria, sigue en picada bajando desde el 20 %, y en plata cayó de 70 Mu$s a 11!
    - 37 % sufre de abusos internos de red, baja en porcentaje pero no en plata.
    - El fraude financiero se manejó durante un quinquenio entre el 13 y el 14 % cayó 10 puntos, desde 10 Mu$s a 7,7.
    - El resto de los números: robo de laptops (jaja), 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.[5]

- Por último en este campo destacamos que las pérdidas totales estuvieron en el orden de los 141 Mu$s, siendo las más bajas en la historia de la estadística: 265 M – '00, 378 M – '01, 456 M – '02, 202 M – '03.[6]
- 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 bastante alto (28%).
- Respecto a lo que hacen las empresas cuando detectan una intrusión, estas dicen que en los últimos 12 meses:
  - 91 % tapó los agujeros.
  - 48 % no lo reportaron!.
  - 20 % lo denunciaron legalmente.
  - 16 % lo reportaron a legales internos.
- Y vean estos dos números en particular el último:
  - 51 % no dice nada por temas publicitarios o bursátiles.
  - 35 % no dice nada por miedo a la competencia!

Los comentarios finales: del CSI/FBI concluyen con "...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 este año, 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, con la consideración que en nuestro caso todavía no hemos transitado por la etapa inicial que ellos dicen estar superando....

El que no compartimos definitivamente es el de 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 anteriormente, nos desilusionó (por primera vez) esta edición 2004 porque no alcanza (a nuestro modesto entender) los objetivos que se plantearon.

Nota 1: por primera vez en los 9 años participaron además del CSI y del FBI, tres académicos, dos de los cuales están relacionados con altas empresas privadas de consultoría / auditoria estadounidenses. No dudamos de su capacidad y aporte, sólo lo mencionamos como curiosidad histórica.

Nota 2: todos nuestros comentarios (para aquellos que les interese) fueron enviados a R. Richardson, Director Editorial del CSI, emisor de este reporte. Inclusive el error de la página 15 donde dice 57 percent, debería decir 42.

[5] Bueno pero como dijimos en otra parte, este tipo de lectura, no es analizada por el CSI/FBI (¿?)
[6] 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.

