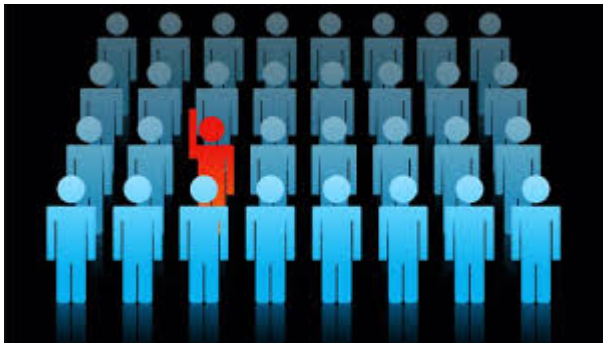
Insider threat: Risks

Una vez que ya conocemos en que consisten las **amenazas internas** y su situación actual en las organizaciones, destinaré este tercer post a hablar acerca de los **riesgos** que llevan asociadas estas amenazas internas.



http://blog.ss8.com/controlling-insider-threats-through-visibility-analytics-and-intelligence/

Primero, me parece importante destacar como el riesgo de las amenazas internas es un concepto muy **difícil de precisar**, debido principalmente al impacto que tienen los distintos factores (los privilegios, autorizaciones o puesto de la persona). Es necesario, por lo tanto, **catalogar** este tipo de amenazas, tanto las conscientes como las accidentales. Es decir, si el insider threat de forma pasiva proviene del CEO de la compañía, podríamos encontrar un sinfín de riesgos asociados ya que tiene acceso prácticamente a toda la empresa y a información muy crítica.

En cambio, si la amenaza interna es por ejemplo algún miembro del servicio de mensajería, mantenimiento o limpieza, es posible que tengan mucho menos privilegios y por ende un menor acceso a los datos. Esto no quita a que también hay que tenerles muy en cuenta ya que debido a su perfil pasan más desapercibidos permitiéndoles entrar prácticamente sin que nadie sea consciente de ello.

Realizada está pequeña explicación, ahora me centraré en las **“High impact breaches”** o, dicho de otro modo, las grandes brechas de seguridad a las que estamos expuestos debido a las amenazas internas. [1]

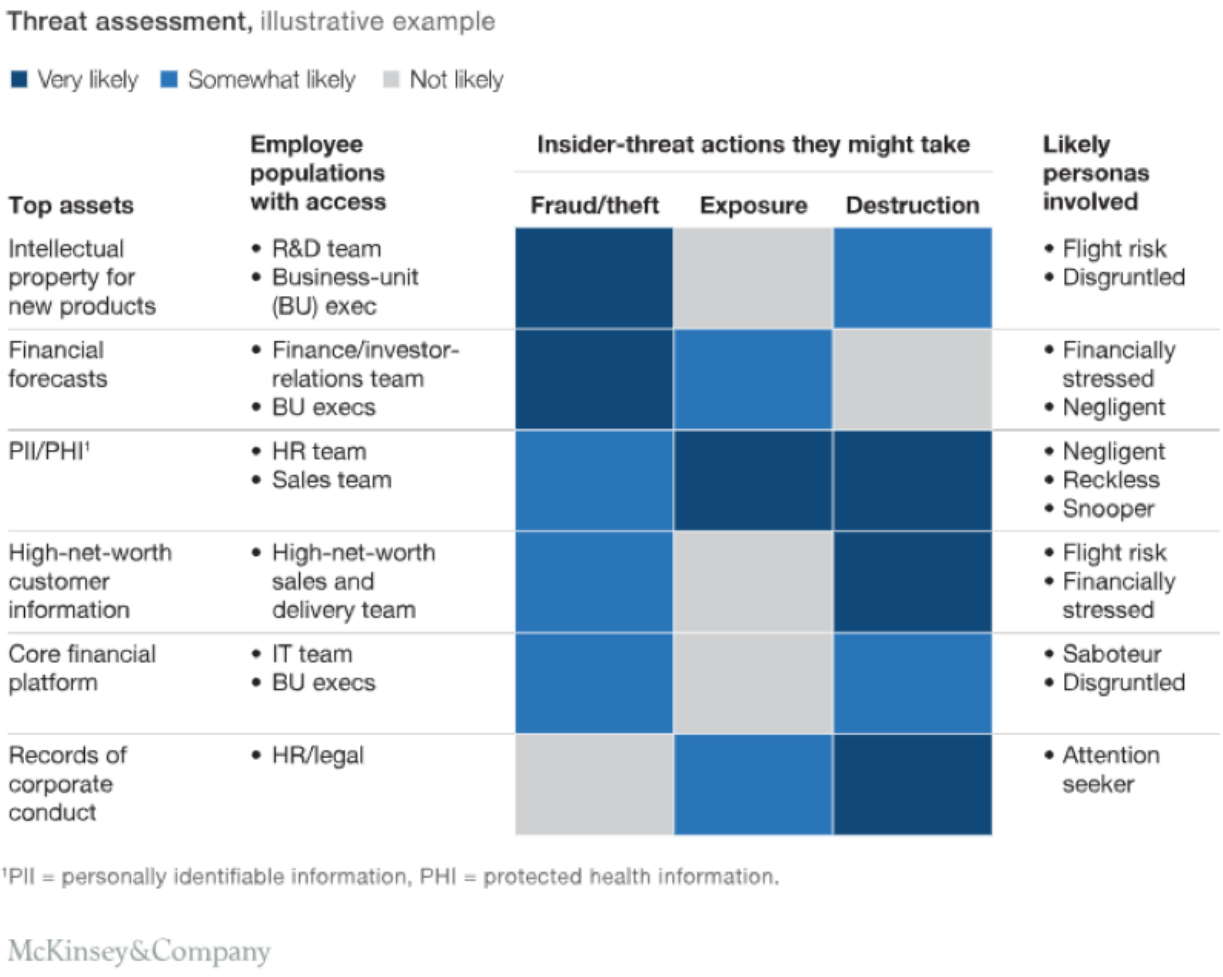
El primero puede ser el más evidente o esperado y es el **robo de información personal** que pueda identificar a una persona. Este afectaría en mayor medida a los insider threat que no son conscientes de que lo son. Si a estas personas se les roba esta información para suplantar su identidad, podría tener una gran repercusión para la organización y también para su reputación. Quiero comentar también que en este punto hay que tener mucho cuidado ya que según el **RGPD** estos datos deben seguir unas estrictas directrices de privacidad y conservación. Imaginemos que en vez de a un empleado de la empresa se la roban los datos personales a clientes de la empresa. En ese

caso podríamos estar sujetos a una gran **sanción** y a la correspondiente **mala reputación** que llevan asociados estos incidentes.

A su vez, es muy relevante mencionar que ahora las organizaciones deben **comunicar estas brechas** de seguridad en un **plazo máximo de 72h**. Esta legislación un claro ejercicio de transparencia pero que puede tener graves consecuencias para la imagen de las organizaciones.

El siguiente riesgo del que voy a hablar es el **sabotaje industrial**. Este en concreto posee una gran criticidad ya que podría causar estragos en la organización incluso a no poder recuperarse de ello.

El tercero que comentaré puede estar relacionado con el primero, en este caso será el **robo de información confidencial y propiedad industrial**. Para según qué tipos de organizaciones como puede ser las dedicas a sacar patentes, el robo de alguna de estas antes de ser aprobada podría suponer una gran pérdida para la empresa. También podrían darse casos de que se haga pública información confidencial. Este último escenario encajaría más en gobiernos y podría tener gran impacto en la geopolítica. Recordemos que en la actualidad los datos son considerados el activo más importante en las organizaciones como se puede apreciar en el siguiente gráfico elaborado por a consultoría McKinsey&co además de los distintos tipos de riesgos que corre cada activo fundamental.[2]



https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk#0

El cuarto es la **denegación de servicios**. En la actualidad gran parte de sus negocios tienen un volumen considerable negocio sustentado en internet, pero esto es un mal menor si comparamos lo que podría ocurrir si se realiza este ataque contra infraestructuras críticas como puede ser una central nuclear, una presa o a los satélites de un país. En definitiva, un riesgo muy a tener en cuenta.

El quinto que quiero mencionar es la **infección de software malicioso de forma extendida**. Como bien sabemos, hoy en día la mayoría de grandes y medianas empresas están informatizadas casi por completo y un malware que afecte a todos estos sistemas puede suponer un parón en el negocio con sus respectivas pérdidas y consecuencias. Pero esto es solo un escenario de la infinidad que se podrían dar. Por ejemplo, podríamos tener siempre a alguien dentro de los sistemas que pueda ver todo sin nosotros conocer que está ahí. O en un caso más extremo, ¿Qué pasaría si una persona consigue instalar y ejecutar correctamente un malware dentro de uno de los mayores bancos del mundo teniendo acceso a las cuentas de sus clientes?

El último de los riesgos que voy a comentar consiste en que los **sistemas de registros financieros se vean comprometidos**. Esto es particularmente crítico para grandes empresas que tengan que auditar de forma frecuente sus cuentas ya que si estos sistemas se ven comprometidos o inutilizados podrían causar que la auditoría no se lleve a cabo o que se haga de una forma incorrecta. Las consecuencias de que esto sucediese pueden ser grandísimas y tener un gran impacto en el mercado. Dentro de este riesgo, podemos destacar el papel fundamental que juegan los auditores TI asegurando la integridad de los sistemas y datos para la posterior auditoría financiera.

Como hemos podido observar, estos riesgos asociados tienen un gran impacto para las organizaciones de ahí el concepto que he mencionado al principio “high impact breaches”. Por lo tanto, podemos ver porque **las organizaciones están tan preocupadas** por tener un correcto plan de gestión de las amenazas internas y cada vez están más concienciadas de ello.

En el próximo post trataré de explicar y analizar las principales medidas que toman actualmente las empresas para conseguir prevenir o mitigar este tipo de riesgos. [3]

Referencias:

[1] “Types of insider threats” – Security intelligence

https://securityintelligence.com/these-5-types-of-insider-threats-could-lead-to-costly-data-breaches/

[Consultado el 22/11/18]

[2] “Human element of cyberrisk”- Mckinsey&Co

https://www.mckinsey.com/business-functions/risk/our-insights/insider-threat-the-human-element-of-cyberrisk#0

[Consultado el 22/11/18]

[3] “Managing insider threats” – EY

https://www.ey.com/Publication/vwLUAssets/EY-managing-insider-threat-a-holistic-approach-to-dealing-with-risk-from-within/$FILE/EY-managing-insider-threat.pdf

[Consultado el 22/11/18]