**Errores y lecciones de la interacción con la Junta Directiva en materia de ciberseguridad por Jason Mallinder - 06.2024**

Recuerdo claramente haber entrado en la sala de juntas en los primeros días de mi mandato como CISO en un importante banco global. Quería destacar un grave riesgo cibernético para la junta: la posible pérdida de datos a través de puertos USB activos. Propuse bloquearlos.

Pero la reunión del directorio no salió como yo había planeado. Me percibieron como alguien que restringía el negocio. Uno de los comentarios que recibí fue que los datos eran muy complejos y extremadamente difíciles de interpretar por el propio banco, así que ¿cómo podría alguien externo hacer daño con ellos? Terminó siendo una reunión muy complicada.

Regresé dos meses después, esta vez equipado con mejores datos y un enfoque diferente. Por ejemplo, mostré cuántos gigabytes de datos se almacenaban en las unidades USB cada mes. Esta vez, la respuesta de la junta fue un rotundo reconocimiento: "Es necesario restringir los puertos USB".

Para muchos ejecutivos, incluso los de mayor jerarquía, una presentación ante la junta directiva es la prueba más exigente de comunicación de liderazgo. Los CISO también suelen tener dificultades. Si bien los consejos convencionales como "contar una historia" o "utilizar menos viñetas" son válidos, a menudo no abordan los desafíos únicos que presentan ciertas situaciones.

He tenido muchas experiencias personales en las que he interactuado con juntas directivas durante mi mandato como CISO y he debatido el tema con muchos colegas en los últimos años. A continuación, se presentan las lecciones y los conocimientos que he recopilado con la esperanza de ayudar a otros en caso de que tengan que hacer presentaciones ante su junta directiva.

**Por qué informar al consejo directivo es diferente y difícil**

La sala de juntas es un foro especial que requiere un tipo específico de presentación y preparación. En la mayoría de los casos, las diapositivas habrán sido revisadas por uno o dos miembros de la junta antes de la reunión y los directores probablemente habrán examinado el material de antemano. Con demasiada frecuencia, los espacios para presentaciones ante la junta se limitan a 10 o 15 minutos, pero apresurarse en la presentación de las diapositivas no logra profundizar la comprensión de la junta sobre el tema clave ni mostrar las habilidades de liderazgo del ejecutivo.

Otro desafío es que el directorio es un foro único y heterogéneo, sin comparación con otros grupos en los que participan regularmente la mayoría de los ejecutivos. A menudo está integrado por líderes empresariales, académicos, ex directores ejecutivos y directores financieros en ejercicio, que aportan experiencia de diferentes industrias y campos. Algunos miembros han formado parte de directorios durante décadas; otros pueden ser completamente nuevos.

Al presentar un informe al directorio, el objetivo no es analizar los indicadores clave de rendimiento trimestrales ni otra información que esté fácilmente disponible (los miembros del directorio pueden acceder a ella por su cuenta). En cambio, la presentación debe cubrir los desafíos más urgentes que enfrenta la organización (en un lenguaje sencillo) y describir cómo abordarlos. Recuerde que el directorio debe poder evaluar todos los riesgos de la empresa.

**Lo que me gustaría informar**

Después de haber probado diferentes enfoques a lo largo de los años, encontré la siguiente estructura más útil: centrarse en los cambios en el panorama de amenazas, el progreso en los controles y la reducción del riesgo comercial junto con las inversiones necesarias.

Riesgo e inversión: Esta era a menudo la parte más importante de mi presentación, por lo que empezaba y terminaba con ella. En esta sección, resumía el nivel de reducción de riesgos logrado a lo largo del tiempo en línea con el apetito de riesgo de la organización y el riesgo empresarial, utilizando una escala y valores indicativos en dólares para tratar de evitar una conversación financiera. Demostré la eficacia de nuestras estrategias de mitigación de riesgos y su alineación con el apetito de riesgo de la empresa. Luego, describía las inversiones futuras necesarias en controles para una reducción sostenida del riesgo, incluidas las consideraciones presupuestarias para las iniciativas de ciberseguridad y su impacto esperado en la postura general de riesgo.

Panorama de amenazas: El panorama de amenazas es amplio y muchas de ellas podrían no aplicarse a la organización. Al presentar los cambios en el panorama de amenazas internas y externas, siempre destaqué por qué esos cambios eran importantes para la organización. Mi informe incluía un análisis exhaustivo de las amenazas actuales, que abarcaba factores internos y externos. También incluí una sección sobre amenazas emergentes que podrían afectar potencialmente a la organización a mediano y largo plazo.

Controles: Siguiendo el panorama de amenazas, centré mi actualización en los avances en la implementación de controles, haciendo hincapié en lo que eso significaba en un contexto empresarial. Naturalmente, se centraron más en los controles técnicos, porque son más fáciles de medir que las personas y la cultura. Explicaría la importancia de estos controles para combatir las amenazas e ilustraría cómo contribuían a salvaguardar los activos críticos, garantizar el cumplimiento y mantener la resiliencia operativa.

**Aprendiendo de los errores del pasado: 5 consejos para elaborar informes de directorio eficaces**

A continuación se presentan mis principales errores y consejos sobre cómo prepararse y presentarse ante la junta.

**1. No eduque ni informe a la junta directiva:**  interactúe genuinamente con las personas de la junta directiva en lugar de simplemente educarlas o informarles. Estas sesiones no son solo para hacer presentaciones ante la junta directiva, sino también para que el CISO comprenda las expectativas de la junta al escucharlas directamente.

**2. Proporcione una simulación para promover el intercambio de conocimientos y la participación:** utilice ejercicios prácticos no solo para transmitir conocimientos, sino también para comprender las expectativas de la junta directiva. Como CISO, probablemente aprenderá tanto como los propios miembros de la junta directiva, por lo que puede actualizar sus manuales de gestión de incidentes en consecuencia. Una vez más, una presentación a la junta directiva es una vía de doble sentido.

**3. Comience con lo que desea que la junta aprenda:** no dé por sentado que tendrá mucho tiempo con la junta. Durante mis últimos cinco años como CISO, tuve muy pocos espacios de una hora. Lo más habitual era que tuviera 10 minutos para exponer mis ideas. La junta puede o no revisar su material de antemano, pero, independientemente de eso, es una buena idea comenzar con lo que desea que la junta aprenda de su presentación y asegurarse de alinear ese mensaje con las prioridades de la junta.

**4. Centrarse en el contexto empresarial y en muy pocos indicadores clave de rendimiento:** desde el principio, tenía métricas para todo, hasta el punto de tener más de 100 indicadores clave de rendimiento diferentes. La junta directiva me dijo que no podían ver el bosque a través de los árboles, así que los reduje a 10 indicadores clave de rendimiento. Incluso entonces, no siempre se trata de qué información estás compartiendo, sino de cómo lo haces. Por ejemplo, una vez compartí un indicador clave de rendimiento que decía que el 2% de nuestros servidores no tenían parches, lo que en realidad no tenía sentido para ellos sin el contexto empresarial. Aclaré que los sistemas de pago estaban expuestos a una vulnerabilidad crítica y que, si se veían comprometidos, podríamos perder nuestra capacidad de realizar pagos. Entonces entendieron el mensaje mucho más claro.

**5. Trabaje con un miembro de la junta antes de la reunión (si puede):** tuve la suerte de que me asignaran un miembro de la junta que me ayudó a prepararme para la reunión. Ese miembro de la junta no tenía un conocimiento profundo de la ciberseguridad, pero me ayudó a anticipar algunas de las preguntas e inquietudes que otros podrían plantear durante mi presentación. Como resultado, estaba mejor preparado y aporté mucho más valor a la empresa.

Los directorios son los máximos responsables de todos los riesgos y tienen la tarea de determinar el nivel de riesgo de ciberseguridad que sus organizaciones están dispuestas a aceptar. Al incorporar estos consejos prácticos, los CISO pueden gestionar las interacciones con los directorios de manera más eficaz, fomentando una mejor comunicación, comprensión y alineación estratégica.