Presentación del CISO ante la DS

FING

1

Pautas para hablar ante la DS

Dé un resumen de las buenas y malas noticias al inicio

Sea claro y conciso tanto en su presentación oral como en los materiales entregados

Sea transparente y honesto. No asegure cosas infundadas

Si no sabe algo, reconózcalo y prometa volver con una respuesta.

Evite hablar en “techie” y evite las siglas y los acrónimos.

Use analogías para ayudar a la comprensión de temas técnicos.

Articule claramente el riesgo (probabilidad e impacto), las mitigaciones y los planes de seguridad.

Identifique claramente aquellas cosas que requiera acción o consideración de la DS

No sorprenda a su CEO – informe al CEO por adelantado

2

Preparese

¿Tiene en claro lo que la DS superior quiere escuchar y cuál es el punto clave de éxito?

¿Cuál es el gran objetivo de su presentación?

¿Cuál es la conclusión que desea que tengan los miembros de la DS?

Al preparar las métricas, debe responder preguntas clave:

- ¿Estamos mejorando o empeorando? Tendencias
- ¿Estamos en buena o mala forma en comparación con nuestros objetivos y / o puntos de referencia de la industria?

Describa las inquietudes, riesgos y mitigaciones de auditorías regulatorias o de TI

Menos, es más: ¿qué debería dejar fuera?

Conozca que está pasando con la ciberseguridad

Practique con el CEO u otro ejecutivo y pregúntales por posibles preguntas de la DS

Si es posible, conozca a los miembros de la DS en eventos sociales o cena antes de la reunión de la junta

3

Consejos para una presentación exitosa:

- **Practica:** Ensaya la presentación varias veces para asegurarte de que fluye de manera natural.
- **Sé conciso:** Evita la información redundante y céntrate en los puntos clave.
- **Sé claro:** Utiliza un lenguaje sencillo y evita la jerga técnica.
- **Sé entusiasta:** Transmite tu pasión por la seguridad y convence a los directores de la importancia de la inversión.

4

La utilización del miedo para concientizar

5

Concientización y miedo

Infundir miedo puede ser efectivo hasta cierto punto (llamar la atención), pero es importante equilibrarlo para no generar una reacción contraproducente, como parálisis o decisiones apresuradas.

El objetivo es crear conciencia (crear sentido de urgencia) y motivar a la acción, no paralizar o generar pánico. La idea es que la junta directiva vea la inversión en ciberseguridad como una necesidad estratégica y no solo como una respuesta a una amenaza.

Veamos tácticas recomendadas:

6

1. Casos reales y relevantes: Presentar ejemplos de ciberataques que sean relevantes para la industria de la empresa. Mostrar cómo esos ataques afectaron a otras empresas similares en términos de pérdidas económicas, daño a la reputación y problemas legales.

2. Datos y estadísticas: Utilizar estadísticas y estudios que demuestren la probabilidad y el impacto potencial de los ciberataques. Cifras concretas pueden ser más persuasivas que casos anecdóticos.

3. Impacto directo: Enfocarse en cómo un ataque cibernético podría impactar directamente a la empresa. Identificar activos críticos y los posibles daños específicos, como interrupciones operativas, pérdida de datos sensibles o daños a la infraestructura.

7

4. Narrativa equilibrada: Combinar los aspectos negativos con un enfoque proactivo. Mostrar cómo una inversión en ciberseguridad no solo mitiga riesgos, sino que también puede mejorar la confianza del cliente, la conformidad regulatoria y la eficiencia operativa. (Integración con los objetivos del negocio).

5. Plan de acción claro: Proporcionar un plan claro de inversión en seguridad, incluyendo costos, beneficios y un cronograma de implementación.

6. Enfoque en la resiliencia: En lugar de solo enfocarse en la prevención, habla sobre la importancia de la resiliencia operativa. Explica cómo la ciberseguridad puede ayudar a la empresa a recuperarse rápidamente y minimizar el impacto de un ataque.

8

Desventajas del Uso del Miedo

1. Desgaste: El miedo constante puede llevar a la fatiga y a la desensibilización, haciendo que la dirección deje de tomar en serio las advertencias de seguridad.

2. Reacción en lugar de proactividad: Un enfoque basado en el miedo puede fomentar reacciones impulsivas y parches a corto plazo, en lugar de una estrategia de seguridad proactiva y bien planificada.

3. Ambiente negativo: Puede crear un ambiente de trabajo negativo, afectando la moral y la motivación del equipo de TI y de la organización en general.

9

Presentaciones ante los niveles directivos

Algunas recomendaciones

Fuente Gartner

10

Para evitar que su junta se "aburra", recuerde el acrónimo

BOARD (**B**rief, **O**pen, **A**ccurate, **R**elevant, **D**iplomatic)

Breve (Brief). Asegúrese de que su presentación esté muy centrada. La presentación promedio es de unos 15 minutos.

Abierto (Open). El propósito principal de una sesión de la junta es la transparencia, por lo que la junta comprenda lo que sucede dentro de la organización para proteger a los accionistas, dueños, contribuyentes, etc.

Exacto (Accurate). Está bien decir “no sé” a la junta siempre que no refleje una falta de preparación. La necesidad de precisión, especialmente en empresas que cotizan en bolsa, es primordial.

Pertinente (Relevant). Hable sobre cuestiones de tecnología a través de una lente que sea relevante para los intereses, la experiencia y el conocimiento de la junta.

Diplomático (Diplomatic). Muchos de los desafíos tecnológicos fueron creados por múltiples tomadores de decisiones en la empresa. La capacidad de poder comunicarse estratégica y diplomáticamente es fundamental.

11

Cada interacción con la junta es una oportunidad para ser despedido. Pero sin riesgo, no hay recompensa.

Si solicita aprobación, una regla importante es saber cuándo salir y marcharse.

Haga la solicitud primero, al inicio de la presentación y no al final, y no haga que el argumento de venta sea más grande que la solicitud. Incluya solo suficiente información relevante.

Si el caso de negocio es enorme, corre el riesgo de verse a la defensiva, y eso puede dar más munición a la junta para decir que no.

También debe determinar si está dando una presentación o teniendo una discusión.

Si la junta hace preguntas, no apresure la presentación. Tenga la discusión.

Finalmente, no venda después del cierre. Si han dicho que está bien, no continúe con la presentación.

12

Una regla importante para las aprobaciones es que es más importante ser interesante que completo.

Los CIO/CISO pueden crear un enfoque en sus presentaciones al decidir tres cosas como parte de sus prepara vos para la sesión de la junta:

Sentir: ¿Cómo quiere que se sienta la junta como resultado de la presentación? ¿Emocionado, preocupado o cómodo? Las emociones impulsan más decisiones que los datos, así que tome una posición y cuente la historia.

Recordar: Es más importante ser interesante que completo, así que decida de antemano cuál será la parte más interesante y memorable de su mensaje.

Hacer: Sea claro sobre las acciones que desea que tome la junta o el equipo ejecutivo como resultado de su interacción con ellos. ¿Quiere que la junta le proporcione dinero o aprobación de la dirección? Si recibió lo que estaba pidiendo, su presentación fue un éxito.

13

Recomendaciones

- Minimizar el miedo, la incertidumbre y la duda.
- Equilibrar las necesidades para proteger a la organización con las necesidades para operar el negocio.
- Citar todo en un contexto empresarial que sea relevante para las decisiones a nivel de la junta, evitando al mismo tiempo cuestiones que son relevantes solo para el personal de TI y la toma de decisiones de TI.
- Terminar con una "solicitud" de la junta para involucrar a los miembros de la junta en el proceso.

14

Se deben abordar tres áreas fundamentales en la presentación de la junta:

1. La amenaza, los activos afectados, las consecuencias.

2. La preparación de la organización (incluida la operación básica del programa de riesgos tecnológicos y de ciberseguridad).

3. La relevancia y criticidad de la seguridad para el funcionamiento del negocio. Los miembros de la junta no tendrán mucho contexto más allá de lo que han leído en los periódicos sobre incidentes de seguridad, por lo que debe crearlo para ellos.

15

Diapositiva 1: Reconocimiento de los titulares.

Diapositiva 2: Centrarse en las amenazas específicas de la industria y la organización.

Diapositiva 3: Abordar directamente el hecho de que no existe la protección perfecta; El objetivo es crear un programa sostenible que equilibre la necesidad de proteger contra la necesidad de ejecutar el negocio.

Diapositiva 4: Presentación del concepto de madurez y la relación entre madurez y postura de riesgo.

Diapositiva 5: Estado actual del programa de ciberseguridad en comparación con un punto de referencia mundial. Identificar brechas y oportunidades de mejora.

Diapositiva 6: Más detalles sobre las brechas y las oportunidades de mejora.

Diapositiva 7: Un vínculo entre los resultados comerciales y la dependencia de la tecnología mediante un diagrama de la cadena de valor.

Diapositiva 8: Una lista de iniciativas y resultados comerciales a nivel de la junta para enfatizar la importancia de administrar el riesgo tecnológico de manera adecuada.

Diapositiva 9: Explicar los próximos pasos y recomendaciones para la junta sobre este tema.

16

Diapositiva 1: Empiece

La diapositiva 1 está diseñada para llamar la atención. Debe ser breve y simplemente identificar los temas que cubrirá en las siguientes diapositivas. No se necesitan detalles, pero debe indicar que la presentación incluirá información sobre la ejecución del negocio, la estrategia, los desarrollos externos y la posición de riesgo. Es de alto nivel y prepara el escenario para el tablero.

Diapositivas 2 a 6: Desempeño y contribución a la ejecución empresarial

Puede resultar difícil para los CISO demostrar cómo la seguridad contribuye al rendimiento empresarial. Sin embargo, cuando se presenta a la junta, es clave vincular (implícita o explícitamente) la seguridad y el riesgo con los elementos comerciales que los miembros de la junta valoran.

Cualquier versión de estas diapositivas que tenga sentido para su empresa le permitirá resaltar las métricas y cómo el equipo de seguridad está contribuyendo al resultado positivo. Sin embargo, también debe estar preparado para explicar las posibles áreas problemáticas y sus implicaciones. Traiga documentación más detallada sobre cómo se produjo cada métrica para cualquier miembro de la junta que lo solicite.

Estas diapositivas deben analizar cómo los eventos externos afectarán la seguridad, una evaluación de la posición de riesgo existente (esto puede cambiar según las adquisiciones y otros eventos) y toda la estrategia de seguridad.

Diapositiva 7: La llamada a la acción

Finalmente, concluya la presentación con una diapositiva de cierre para reiterar los puntos principales y los elementos de acción. La clave es cerrar con fuerza, dejando a la junta confiada en su plan y habilidades. Resuma los puntos que ha planteado y sea claro sobre todo lo que haya solicitado. Este es un buen momento para responder preguntas y agradecer a la junta por su tiempo.

17

CISO Y EL BOARD

18

Más allá de las pasiones y preocupaciones individuales, los directivos generalmente se preocupan por tres cosas:

- Ingresos: afectación en los ingresos operativos o no operativos
- Costo: evitación de costos futuros
- Riesgo: financiero, de mercado, cumplimiento normativo y seguridad, innovación, marca y reputación

19

Según Gartner
Estas son las preguntas más frecuentes que un directorio le preguntará al CISO

20

Ejemplo de preguntas del directorio

¿Estamos 100 % seguros? ¿Está Ud. seguro de eso?

¿Qué tan mal está ahí afuera? ¿Qué pasa con la empresa X? ¿Cómo nos comparamos con los demás?

¿Sabemos cuáles son nuestros riesgos? ¿Que lo mantiene despierto en la noche?

¿Estamos asignando los recursos de manera adecuada? ¿Estamos gastando lo suficiente/por qué estamos gastando tanto?

¿Cómo sucedió esto? ¡Pensé que tenían esto bajo control!

¿Por qué estamos recibiendo más ataques de phishing? ¿Qué estamos haciendo con todos estos ataques de phishing?

21

¿Estamos 100 % seguros? ¿Está Ud. seguro de eso?

Respuesta posible: “Teniendo en cuenta la naturaleza en constante evolución del panorama de amenazas, es imposible eliminar todas las fuentes de riesgo de información. Mi rol es trabajar con otras áreas del negocio para implementar controles para administrar los riesgos que pueden impedirnos mejorar nuestra imagen de marca y eficiencia operativa este año. En seguridad, no existe la "protección perfecta". A medida que nuestro negocio crece, tenemos que reevaluar continuamente cuánto riesgo es apropiado. Nuestro objetivo es construir un programa sostenible que equilibre la necesidad de proteger con las necesidades de administrar nuestro negocio”.

“Tenemos en cartera proyectos que implementaremos en los próximos 24 meses que nos ayudarán a lograr precisamente eso…”

22

¿Qué tan mal está ahí afuera? ¿Qué pasa con la empresa X? ¿Cómo nos comparamos con los demás?

Respuesta posible: "No quiero especular sobre el incidente en la Compañía XYZ hasta que haya más información disponible, pero habré de compartirlo con ustedes cuando sepa más".

“Nuestro competidor ha sufrido un ataque muy publicitado”

Respuesta posible: Tenemos una vulnerabilidad similar. Estamos trabajando para eliminarla.

23

¿Sabemos cuáles son nuestros riesgos? ¿Qué lo mantiene despierto en la noche?

Respuesta posible: Los directivos saben que aceptar el riesgo es una opción, es una decisión en respuesta al apetito y la tolerancia al riesgo de la empresa. No tenga miedo de recordarles esta realidad.

Cualquier riesgo fuera de la tolerancia requiere un remedio para traerlos dentro de la tolerancia. Esto no requiere necesariamente cambios dramáticos en cortos períodos de tiempo.

Cuidado con reaccionar de forma exagerada.

24

¿Estamos asignando los recursos de manera adecuada? ¿Estamos gastando lo suficiente/por qué estamos gastando tanto?

Respuesta posible: Esté preparado para explicar por qué los proyectos se están excediendo el presupuesto o se retrasarán. La propuesta de estrategia original debería haber incluido márgenes de error en cuanto a presupuesto y plazo. Siempre que los sobrecostos estén dentro de estos márgenes, no deberían generar controversia. Incluso si los sobrecostos están fuera de esos márgenes, puede haber razones válidas. El problema principal es que el directorio buscará la satisfacción de que el problema se manejará de manera efectiva, ya sea logrando la finalización dentro de límites razonables, posiblemente con cambio del alcance o, si es necesario, terminando los proyectos fallidos.

Muchos CIO/CISO entienden que la seguridad debe contribuir al desempeño del negocio; sin embargo, luchan por demostrar cómo hacerlo. Un método es el uso de un enfoque de cuadro de mando integral u otro tipo de tablero de KPI.

25

¿Cómo sucedió esto? ¡Pensé que tenían esto bajo control!

Respuesta posible: Un incidente es inevitable. Trátelo como una bendición disfrazada, si es posible, y como una oportunidad para mostrar sus habilidades de liderazgo. Los detalles deben mantenerse dentro del contexto del negocio. Los líderes deben ser conscientes de que, en algunos casos, los detalles del incidente pueden haber sido estrictamente controlados (por ejemplo, debido a sensibilidades particulares asociadas con el incidente). Por lo tanto, es posible que algunos o todos los miembros del directorio aún no estén al tanto del incidente.

Adoptar un enfoque fáctico, explicar lo que sabe y saber cómo investigará cualquier incógnita restante eliminará el misterio y brindará la confianza de que tiene el control del incidente.

26

¿Por qué estamos recibiendo más ataques de phishing? ¿Qué estamos haciendo con todos estos ataques de phishing?

CISO: Para luchar contra esta amenaza, la prevención es nuestra mejor defensa. La prevención comienza con la tecnología y debe incorporar los medios para identificar la reproducción de credenciales corporativas en la naturaleza.

Apoyando esta capacidad, también hemos abordado el problema de las personas y los procesos a través de una simulación y educación integrales sobre phishing para preparar a los empleados para que sean la primera línea de defensa necesaria para proteger proactivamente a la organización.

27

La ciberseguridad se ha convertido en un tema de discusión común para las juntas directivas (BoD) de todas las industrias. Esto no es sorprendente, ya que el 88% de una encuesta de Gartner consideran la ciberseguridad como un **riesgo de negocio y no un problema tecnológico**.

Como resultado de esta tendencia a los líderes de ciberseguridad se les pide cada vez más que actúen sobre una amplia gama de temas de ciberseguridad.

Éstas incluyen:

28

- Aumentar la alfabetización en ciberseguridad de la Junta Directiva y delinear su papel para abordar los riesgos de ciberseguridad de la organización.
- Describir cómo el programa de ciberseguridad está ayudando a la organización a cumplir con sus obligaciones de cumplimiento.
- Proporcionar una descripción general de las últimas tendencias, amenazas o incidentes que se destacan en los medios o se discuten en otros foros.
- Presentar la estrategia de seguridad nueva o existente de la organización para su aprobación.
- Explicar cómo las inversiones del equipo de ciberseguridad están aportando valor a la organización.