SecureOT

Un cuaderno de trabajo de SecureOT

Prepare el caso empresarial adecuado para su programa de ciberseguridad industrial

Gánese el apoyo de la dirección para iniciativas de ciberseguridad de OT

La mayoría de los líderes entienden la importancia de proteger las operaciones industriales de las ciberamenazas. Sin embargo, los líderes tienen que equilibrar continuamente las inversiones en ciberseguridad con otras prioridades e iniciativas organizacionales.

Por otra parte, es posible que los líderes de la organización no cuenten con conocimientos especializados de los sistemas de control industrial (ICS) y la tecnología operacional (OT), ni con la perspectiva de los enfoques, herramientas y procesos de ciberseguridad modernos necesarios para proteger los sistemas de ICS/OT.

Los líderes de IT podrían ver que los recursos de OT son menos vulnerables a los ataques en comparación con los recursos de IT digitales, incluidas redes, servidores y bases de datos. Esto se debe a que los recursos de OT han estado históricamente aislados de las redes de IT y han tenido pocas o ningunas conexiones externas que proporcionarían a un adversario una vía de ataque. Los líderes de IT también creían que el riesgo de actores de amenazas enfocados en sistemas industriales era bajo, arraigado en la creencia de que para los actores de amenazas los ambientes de OT tenían poco valor; por ejemplo, no había información personal identificable (PII) o números de tarjetas de crédito que robar.

Sin embargo, hoy en día las operaciones de la planta son cada vez más digitales e interconectadas, lo que introduce silenciosamente nuevos riesgos para las empresas. Desafortunadamente, los actores de amenazas actuales saben que interrumpir las operaciones de la planta puede ser extremadamente costoso para cualquier organización. Han aprendido que las organizaciones están dispuestas a pagar un rescate si eso les permite reanudar sus operaciones más rápidamente.

La necesidad de una identificación realista de los riesgos

En paralelo, el calor geopolítico está aumentando, y los estados nación están considerando activamente la infraestructura crítica como posible objetivo de la guerra cibernética. Un ciberataque exitoso a sistemas industriales puede tener consecuencias devastadoras, más allá del tiempo improductivo de la producción, los daños a los equipos y las pérdidas financieras. Este tipo de ataque puede afectar la seguridad del operador e incluso interrumpir los servicios necesarios para la supervivencia, como alimentos, agua, transporte, cuidado de la salud y energía.

La creación de un caso empresarial para la ciberseguridad industrial puede ayudar a los líderes a comprender los riesgos y beneficios de invertir en medidas de ciberseguridad para los ambientes de OT. Cuantificar el posible impacto involucra identificar vulnerabilidades o la probabilidad de un ciberataque, y comprender que normalmente es menos costoso invertir en la reducción de riesgos con antelación. En última instancia, el caso empresarial adecuado en torno a la ciberseguridad respaldará el viaje de una organización hacia la modernización de la ciberseguridad de OT.

Esto no solo ayuda a los líderes a priorizar sus inversiones de manera inteligente, sino que les proporciona la información que necesitan para justificar y promover el proyecto entre las partes interesadas clave como, por ejemplo, la junta directiva de la organización.

80%

de las empresas industriales han experimentado un aumento significativo de los incidentes de seguridad.[1]

5 días

Período promedio de interrupción del sistema debido a ciberataques en la industria de fabricación.[2]

Bloques modulares de un caso empresarial de ciberseguridad industrial

En su forma más básica, un caso empresarial es un documento simple que establece los costos asociados con una inversión propuesta junto con los beneficios proyectados, y demuestra el retorno de la inversión (ROI) asociado.

Cuando se trata de crear un caso empresarial de ciberseguridad, cuantificar los costos y los beneficios puede ser un desafío. Muchos de los beneficios se obtienen en forma de reducción de riesgos y evitación de costos. Además, es posible que los costos de implementar una nueva solución tengan que distribuirse entre varios departamentos diferentes, incluidos IT, OT, seguridad, operaciones de planta, recursos humanos, finanzas y seguridad.

Adoptar un enfoque metódico para presentar el caso empresarial de ciberseguridad puede ayudar a traducir conceptos complejos y subjetivos en valores cuantificables, lo que facilita a los líderes determinar con mayor exactitud los riesgos y los costos, y priorizar la ciberseguridad entre las iniciativas conflictivas.

Un caso empresarial de ciberseguridad puede contener las siguientes secciones:

Secciones de casos empresariales	Contenido de la sección	Vea la página
Definición y análisis del problema	Situación actual, análisis de riesgos. Podría incluir una evaluación formal de riesgos de terceros.	5
Solución propuesta	Descripción general de las soluciones propuestas; por qué es el mejor conjunto de soluciones para la organización.	7
Resultados organizacionales	Estimaciones cuantificadas del valor de la reducción del riesgo de un ciberataque exitoso, incluidos los criterios de gestión de cambios, el análisis del impacto empresarial o los requisitos de gestión de riesgos de proveedores.	8
Desglose de costos	Revisión de los costos de la solución propuesta en las categorías de personas, procesos y tecnología.	11
Retorno de la inversión/valor	Valor de reducir el riesgo de ciberseguridad en comparación con los costos de la solución propuesta.	13

Examinemos ahora cada una de estas secciones en detalle, junto con el contenido de ejemplo.

Definición y análisis del problema

Un caso empresarial comienza con una descripción general del problema que se espera que un proyecto propuesto resuelva. La definición del problema normalmente incluye un resumen del estado actual, un análisis de las causas raíz y una descripción general de los objetivos empresariales que el proyecto debería lograr.

En lo que respecta a la ciberseguridad industrial, los equipos de trabajo de OT deberán enfrentar una gran cantidad de desafíos, desde ciberdelincuentes y actores de amenazas de estados nación, hasta hacktivistas y actores internos. Los impulsores comunes de las inversiones en ciberseguridad incluyen:

- **Aumento del cibercrimen, especialmente ransomware**. Si bien muchos líderes pueden considerar el cibercrimen principalmente como un problema de IT, el cibercrimen representa una amenaza cada vez más importante para los ambientes de OT, lo que conduce a acceso no autorizado, tiempo improductivo y la posibilidad de interrupciones a gran escala.
- **Los ciberdelincuentes** podrían atacar sistemas industriales para pedir dinero como rescate, robar propiedad intelectual o, con mayor frecuencia, interrumpir las operaciones. La tendencia hacia interrupciones a gran escala impulsadas por estados nación está impulsada en parte por la transformación digital, especialmente una conectividad más amplia y profunda entre los ambientes de IT y OT. A medida que los sistemas industriales se vuelven más complejos, interconectados e interdependientes, ya no es factible proteger el ambiente de OT con un simple aislamiento físico. El aumento de la conectividad con los sistemas de IT, la nube, los proveedores externos y las redes 5G abre un conjunto completamente nuevo de riesgos para las redes de OT.
- **Aumento de las regulaciones**. Las organizaciones industriales se enfrentan a estrictas regulaciones de diversas fuentes, que varían según el país, la región y la industria. Las multas pueden ser severas para las organizaciones que no cumplan con las normas. Por ejemplo, un año después de que una importante empresa del sector de energía sufriera un ataque de ransomware de gran transcendencia, el Departamento de Transporte de EE. UU. recomendó una multa de casi un millón de dólares, además de los costos ya altos que la empresa tuvo que enfrentar por los días de tiempo improductivo y los esfuerzos de recuperación.

87%

Los ataques de ransomware contra sistemas industriales aumentaron un 87 por ciento en 2022.[3]

El 29%

de las organizaciones industriales afirmaron haber experimentado un ataque de ransomware en los últimos 2 años.[4]

89%

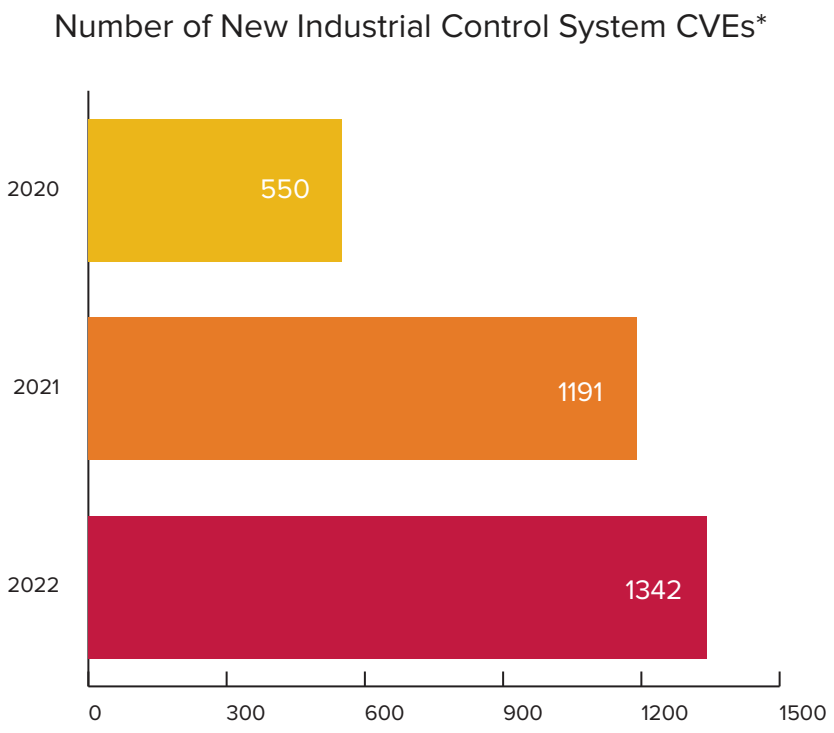
de las organizaciones industriales han sufrido una interrupción en sus cadenas de suministro debido a ciberataques.[5]

Definición y análisis del problema *continuación*

Regulación	Industria afectada
Protección de infraestructura crítica de la North American Electric Reliability Corporation (NERC CIP)	Servicios públicos de energía eléctrica en Norteamérica
Directiva de seguridad de la información de redes 2 (NIS2)	Operadores europeos de servicios esenciales
Ley de reporte de incidentes de ciberseguridad en infraestructura crítica (CIRCIA)	Proveedores del sector de infraestructura crítica de EE. UU.
Suplemento del Reglamento Federal de Adquisiciones de Defensa (DFARS)	Contratistas de defensa de EE. UU.
Ley de Portabilidad y Responsabilidad de Seguros Médicos (HIPAA)	Fabricantes de dispositivos médicos y otras organizaciones que tratan con información relacionada con el cuidado de la salud
Título 21 del Código de Reglamentos Federales (21 CFR Parte 11)	Industrias reguladas por la Administración de Alimentos y Medicamentos (FDA) de EE. UU.
H.R. 2868: Regulación de normas contra el terrorismo de en instalaciones químicas (CFATS)	Instalaciones de productos químicos
Tratado Internacional de las Naciones Unidas	Este tratado, actualmente en desarrollo, se centra en la protección de datos y la resiliencia cibernética
Marco de ciberseguridad del NIST	Un marco global para la ciberseguridad organizacional
Certificación del modelo de madurez de ciberseguridad (CMMC)	Un requisito de ciberseguridad del Departamento de Defensa de EE. UU.
MITRE ATT&CK	Base para el desarrollo de modelos y metodologías de amenazas en el sector privado, en el gobierno y en la comunidad de productos y servicios de ciberseguridad
Intercambio Confiable de Evaluaciones de Seguridad de la Información (TISAX)	Un mecanismo de evaluación e intercambio para la seguridad de la información en la industria automotriz

Ejemplos de reglamentos de ciberseguridad por industria

Definición y análisis del problema *continuación*



Este gráfico muestra el crecimiento de vulnerabilidades y exposiciones comunes (CVE).[7]

- **Aumento vertiginoso de las vulnerabilidades.** Los investigadores y proveedores de seguridad siguen divulgando nuevas vulnerabilidades de ICS a un ritmo cada vez mayor cada año. El número de actores de amenazas radicados en EE. UU. y dedicados al ataque de organizaciones industriales ha crecido en un 35% durante el año pasado, lo cual ocasionó un aumento de las transgresiones en un 87% con respecto al mismo período.[6] Estas vulnerabilidades plantean un desafío para los protectores, no solo por su volumen sino también por la complejidad que supone corregirlas. Si bien las vulnerabilidades en los ambientes de IT a menudo pueden corregirse relativamente rápido, en los ambientes de OT existen desafíos importantes, entre ellos, garantías que exigen largos procedimientos de pruebas de aceptación y plazos de mantenimiento limitados.

Ejemplo de definición del problema

En este cuaderno de trabajo encontrará breves ejemplos que muestran cómo se pueden poner en práctica las pautas en una organización industrial del mundo real.

> “Global Manufacturing Inc. (GMI) está experimentando un aumento significativo en los intentos de ataques de ransomware, lo que pone al ambiente de OT en alto riesgo de tiempo improductivo no programado y pérdida de datos.
>
> Durante los últimos 12 meses, el número de alertas de seguridad relacionadas con ransomware ha aumentado en un 80%. La mayoría de estos ataques tienen como objetivos los sistemas de IT, pero el aumento de la conectividad entre los ambientes de IT y OT dentro de GMI ha traído como consecuencia la exposición de los sistemas industriales a estas ciberamenazas.
>
> Los riesgos en las plantas de fabricación son especialmente altos debido a un gran número de sistemas anticuados con vulnerabilidades sin parches. En algunos casos, estos sistemas ya no reciben parches de seguridad de sus respectivos proveedores. En otros casos, el despliegue de revisiones requiere pasar por un largo proceso de validación regulatoria y la aplicación de revisiones se ha aplazado. ”

Solución propuesta

A continuación, presentamos la solución propuesta para resolver el problema. Un sólido caso empresarial de ciberseguridad debe incluir una descripción general de las soluciones que podrían haberse considerado y un análisis de por qué la solución propuesta es la mejor para la organización. La descripción de la solución no solo debe describir la nueva tecnología o servicio que se desplegará, sino también debe proporcionar una descripción general del modelo operativo y los puntos de integración con la tecnología y los procesos existentes. Al describir la solución completa, los líderes tendrán una visión completa de cómo la nueva solución encajará con la pila de tecnología existente, lo que ayudará a generar confianza en que el despliegue se completará sin problemas.

Ejemplo de soluciones

> “El equipo de trabajo de GMI propone un proyecto para reducir el riesgo de ransomware en las plantas de fabricación, que consiste en mejorar la segmentación y filtrado de redes en todo el ambiente de OT.
>
> El control por red es la manera más eficaz de reducir el riesgo en el ambiente actual de OT de GMI. El uso de los controles de seguridad de punto final que se usan en toda la infraestructura de IT de GMI no es factible en las redes de OT, debido a la amplia gama de sistemas incorporados y sistemas operativos no compatibles.
>
> La solución propuesta consistirá en un conjunto de cortafuegos de red industrial desplegados para controlar estrechamente el tráfico de entrada/salida a la DMZ de la planta (nivel Purdue 3.5), a la LAN de operaciones de la planta (nivel Purdue 3) y a la LAN de control de la planta (nivel Purdue 2). La implementación de estrictos controles de entrada/salida en estas capas ayudará a garantizar que ningún tráfico de red no autorizado pueda cruzar los límites de las capas, protegiendo eficazmente los sistemas en riesgo. La solución propuesta también ayuda a mejorar la adherencia de GMI a las mejores prácticas en ciberseguridad industrial según lo establecido en IEC 62443.
>
> Los cortafuegos serán desplegados por el proveedor elegido durante los intervalos de mantenimiento programadas regularmente, lo que minimiza el tiempo improductivo. Después de recibir la capacitación adecuada, el equipo de ingeniería de seguridad de GMI mantendrá la solución y todas las alertas se integrarán en los flujos de trabajo existentes del centro de operaciones (SOC) de seguridad de GMI.”

Para implementaciones complejas –por ejemplo, aquellas que abarcan múltiples sitios globales o despliegan un programa completo del marco de ciberseguridad del NIST durante varios años– la solución propuesta podría ser comenzar un proyecto de fase 1 con despliegues paralelos de evaluaciones de riesgos y vulnerabilidades, detección de amenazas y procesos de respuesta a incidentes, a la vez que se planifican también las fases restantes del proyecto.

Resultados organizacionales

Este es el momento de hacer los cálculos. La base de un caso empresarial de ciberseguridad consiste en proporcionar una explicación de los beneficios que se derivan de una inversión propuesta. Los mayores beneficios de las inversiones en ciberseguridad son los que evitan los costos y los impactos asociados con una brecha de seguridad, entre ellos los siguientes:

- **Reducción del tiempo improductivo**. Una de las mayores ventajas de las inversiones en ciberseguridad para los ambientes de OT es la reducción del tiempo improductivo asociado con los incidentes de ciberseguridad. Los costos del tiempo improductivo en ambientes industriales pueden ser significativos, especialmente cuando se consideran los costos de la producción perdida, retrasos en las entregas, deterioro de productos y trabajadores inactivos.

  Por ejemplo, en febrero de 2022, un fabricante de automóviles global se vio obligado a interrumpir las operaciones en 14 plantas debido a un ciberataque a un socio clave de la cadena de suministro. La interrupción resultó en una reducción de aproximadamente un tercio de la capacidad de fabricación global del fabricante de automóviles, lo que representa 13,000 automóviles por día y cientos de millones de dólares. Los verdaderos costos de las interrupciones no planificadas varían según el tamaño de la empresa y la industria. Las estimaciones varían desde US$8,000 o más por hora para una empresa pequeña a mediana, hasta US$1 millón o más por hora para una organización industrial grande.[8]

  Teniendo en cuenta que a menudo los equipos de trabajo tardan varios días o incluso semanas en recuperarse de un incidente de ciberseguridad y regresar a las operaciones normales, es fácil ver cómo el prevenir un incidente puede resultar en ahorros de costos de millones de dólares.

US$ 2 millones

Costo promedio de 1 hora de tiempo improductivo no programado en el sector automotriz.

US$ 500,000

Costo promedio de 1 hora de tiempo improductivo no programado en la industria del petróleo y el gas.[9]

- **Evitación de costos de respuesta a incidentes y recuperación.** Los costos de respuesta a incidentes y recuperación tras un incidente de ciberseguridad en ambientes industriales pueden ser considerables. El primer paso en la respuesta a incidentes es investigar y analizar el incidente para determinar su causa, alcance e impacto. Esto podría involucrar la contratación de expertos externos en ciberseguridad, la realización de análisis forenses de los sistemas afectados y la revisión de registros y otros datos para identificar la fuente del ataque.

  Una vez finalizada la investigación, el siguiente paso es corregir los sistemas afectados y restaurar las operaciones normales. Esto podría involucrar la aplicación de parches a vulnerabilidades, la restauración de copias de seguridad, y la realización de pruebas y validación de los sistemas para confirmar que todos los sistemas están funcionando como deben.

  Además, en el caso de incidentes de ransomware o robo de datos, es común que los actores de amenazas exijan pagos de rescate para restaurar el acceso a datos encriptados, o para evitar la divulgación pública de información sensible. Aunque los expertos están de acuerdo, lo mejor es no pagar rescates a pandillas criminales, si bien algunas organizaciones deciden hacerlo porque podría ser el camino más rápido y eficaz en cuanto a costos para restaurar las operaciones.

- **Evitación de multas regulatorias.** Las organizaciones gubernamentales o industriales podrían imponer multas a organizaciones que no cumplan con las normas o políticas de seguridad. Estas multas se pueden aplicar por diversos motivos, entre ellos, brechas de datos, malas prácticas de seguridad y fallos de conformidad. Dependiendo de la gravedad de la brecha o infracción, las multas pueden variar entre miles y millones de dólares.

  En los últimos años se ha producido un aumento de las multas regulatorias por infracciones de ciberseguridad, ya que los gobiernos y organismos normativos buscan hacer responsables a las organizaciones de las brechas de datos y otros incidentes de seguridad. Es probable que esta tendencia continúe a medida que las amenazas de ciberseguridad evolucionan y se tornan más sofisticadas.

US$ 500,000

La mayoría de las organizaciones industriales pagaron en promedio US$500,000 o más en rescates.[10]

US$ 986,000

Sanción civil impuesta a Colonial Pipeline por el Departamento de Transporte de EE. UU. después del incidente de ransomware de 2021.

Otros resultados de las inversiones en ciberseguridad incluyen:

- **Diferenciación estratégica**. A medida que los ciberataques se tornan más frecuentes, los clientes son cada vez más conscientes de los riesgos que conlleva hacer negocios con terceros. Tener un programa de ciberseguridad sólido puede diferenciar a una organización frente a la competencia, especialmente para clientes en industrias altamente reguladas como la del cuidado de la salud, la gubernamental y la energética.

- **Factores de salud, seguridad y medioambientales**. En el sector industrial, un incidente de ciberseguridad podría causar más que interrupciones en los sistemas digitales. Ese incidente también puede tener un impacto significativo en el mundo físico como, por ejemplo, daños a la infraestructura física, daños medioambientales por derrames o contaminación de productos químicos, y amenazas a la seguridad humana.

- **Reducción de los costos de los seguros de ciberseguridad**. Las mejoras en las ciberdefensas hacen que las organizaciones representen menos riesgo para las aseguradoras, lo que podría reflejarse en primas más bajas, o mejores términos y condiciones.

Métricas impulsadas por resultados: La siguiente tabla resume los beneficios estimados que GMI espera ver como resultado del proyecto de segmentación de red propuesto:		**Calcule los posibles resultados de su organización a continuación:**
Número estimado de incidentes de ciberseguridad evitados:	1 incidente/año	
Costos estimados del tiempo improductivo de una planta de GMI:	US$50,000/hora	
Tiempo improductivo previsto de la planta por un incidente de ciberseguridad:	36 horas	
Ahorros calculados por tiempo improductivo debido a incidentes de ciberseguridad evitados:	US$1.8 millones/año	
Ahorros estimados por respuesta a incidentes y recuperación:	US$200,000/año	
Ahorros estimados en cargos regulatorios:	US$100,000/año	
Total estimado en beneficios anuales:	**US$2.1 millones/año**	

Desglose de costos: asigne los costos

Una vez que se han comprendido bien los beneficios de una inversión en ciberseguridad, es hora de centrar nuestra atención en los costos.

Para ayudar a los líderes a tomar decisiones fundamentadas, es importante que comprendan no solo los costos iniciales asociados con un proyecto propuesto, sino también los costos operativos continuos en los que se incurrirá con el tiempo.

Un caso empresarial de ciberseguridad típico establecerá los costos en una serie de categorías diferentes:

- **Costos tecnológicos**. Todo proyecto que introduzca nuevos controles o servicios de seguridad en el ambiente probablemente tendrá costos asociados con la compra de tecnología o servicio subyacentes. Estos costos generalmente son fáciles de obtener a través de su proveedor de tecnología y podrían incluir costos únicos, como licencias de hardware y software, así como costos anuales recurrentes, como cuotas de suscripción de SaaS.

- **Costos de despliegue**. Antes de que una organización pueda comenzar a aprovechar el valor de su inversión, la solución propuesta primero deberá instalarse y configurarse correctamente. El caso empresarial debe tener en cuenta los costos directos como, por ejemplo, cargos de consultoría y capacitación, así como los costos indirectos asociados con el despliegue, como la mano de obra necesaria para desplegar software y hardware, integrarlos en los flujos de trabajo técnicos y comerciales existentes, y cualquier tiempo improductivo programado necesario para completar el despliegue.

- **Mantenimiento de la solución**. Son pocas las soluciones que realmente funcionan sin intervención posterior. La mayoría de las soluciones requerirán mantenimiento continuo para garantizar que sigan funcionando de manera eficiente, y particularmente la ciberseguridad necesita actualizaciones continuas a medida que el panorama de amenazas evoluciona continuamente. Los proveedores normalmente cobran una cuota anual de entre un 15% y un 25% para proporcionar asistencia técnica y actualizaciones continuas. Además, el personal de asistencia técnica local deberá desplegar las revisiones de seguridad y actualizaciones de software de manera oportuna, monitorear el estado de la solución para asegurarse de que siga funcionando correctamente y ajustar las políticas según sea necesario para optimizar la protección.

- **Monitoreo de la solución**. Por último, hay costos asociados con el uso de la nueva solución de seguridad en un ambiente de producción. Muchas soluciones de seguridad generan alertas que el personal debe revisar en un centro de operaciones de seguridad (SOC). El personal del SOC debe integrar las nuevas alertas en el flujo de trabajo existente para clasificar, investigar y responder a cualquier amenaza cibernética emergente. El SOC como servicio, o los servicios SOC administrados, están disponibles y a menudo son convenientes dada la escasez de personal de ciberseguridad en todo el mundo. Si se prefiere un enfoque de SOC administrado, use este modelo de precios en su lugar para calcular los costos de mantenimiento de la solución.

Ejemplo de costos: La siguiente tabla resume los costos previstos que GMI espera ver como resultado del proyecto de segmentación de red propuesto:		**Calcule los costos potenciales de su organización que aparecen a continuación:**
Suposiciones		
Costo de personal a tiempo completo de ingeniería de IT:	US$150,000/año	
Costo de personal a tiempo completo de SOC:	US$175,000/año	
Costos no recurrentes		
Hardware y software:	US$350,000	
Servicios profesionales (instalación y configuración):	US$50,000	
Capacitación del administrador:	US$15,000	
Total de costos no recurrentes:	**US$415,000**	
Costos recurrentes anuales		
Asistencia técnica del proveedor:	US$70,000/año	
Mantenimiento de soluciones: 0.5 personal a tiempo completo de ingeniería de IT	US$75,000/año	
Monitoreo de soluciones: 1 personal a tiempo completo de SOC	US$175,000/año	
Total de costos recurrentes anuales:	**US$320,000/año**	

Cálculo del retorno de la inversión

Si se tienen los datos sobre los costos y los beneficios de la solución, es fácil realizar un análisis de costo-beneficio. Para empezar, generalmente se calcula el retorno de la inversión (ROI). El ROI proporciona una métrica simple y rápida que muestra a los líderes el valor que puede obtenerse de una inversión en ciberseguridad.

En primer lugar, considere el intervalo de tiempo para un cálculo del ROI*. Dado que los costos probablemente incluirán algunos gastos iniciales (por ejemplo, costos de hardware, licencias de software y costos del despliegue) y costos recurrentes (como suscripciones y mantenimiento de SaaS), a menudo es mejor realizar un análisis de ROI durante un período de al menos tres años para proporcionar una visión completa del valor que se generará con el tiempo. El retorno de la inversión se muestra normalmente como porcentaje y se puede calcular con la siguiente fórmula:

$$\text{ROI} = \frac{(\text{BENEFICIOIS} - \text{COSTOS})}{(\text{COSTOS})} \text{x}100$$

Este número no debe considerarse un retorno en dólares. Gran parte del beneficio de la reducción de riesgos y la prevención de costos prevista se derivan de tendencias y promedios históricos generales. En cambio, un cálculo del ROI debe considerarse como una medida de cuánto riesgo puede reducirse para el gasto especificado y declararse como valor.

Ejemplo de cálculo del retorno de la inversión: La siguiente tabla resume los costos previstos que GMI espera ver como resultado del proyecto de segmentación de red propuesto:		**Calcule el retorno de la inversión esperado de su organización como se muestra a continuación:**
Estimado de evitación de costos/valor en el primer año	US$2,100,000	
Estimado de evitación de costos/valor en el segundo año	US$2,100,000	
Estimado de evitación de costos/valor en el tercer año	US$2,100,000	
Total de beneficios en los 3 años:	**US$6,300,000**	
Costos de despliegue	US$415,000	
Costos de operación en el primer año	US$320,000	
Costos de operación en el segundo año	US$320,000	
Costos de operación en el tercer año	US$320,000	
Total de costos en los 3 años:	**US$1,375,000**	
$\text{ROI} = \frac{\text{US\$6,300,000} - \text{US\$1,375,000}}{\text{US\$1,375,000}} \times 100$		
Valor de la inversión en los 3 años:	360%	

* Para simplificar nuestros cálculos, hemos ignorado los cambios en el valor del dinero con el transcurso del tiempo. Un análisis más sofisticado reflejaría el hecho de que, debido a la inflación y otros factores, un dólar en el año 1 vale más que un dólar en el año 3. Esto podría variar ligeramente el resultado general de los cálculos pero no debería afectar la conclusión más amplia.

Presentación de su caso

Completar un caso empresarial de ciberseguridad es solo el comienzo de un proceso de toma de decisiones e implementación más amplio. Armado con un problema, una solución, unos beneficios y unos costos bien documentados, ha llegado el momento de presentar el caso empresarial a los líderes, que estarán bien preparados para evaluar el caso empresarial en función de sus propias perspectivas y prioridades.

Asegúrese de invitar a su presentación a los presentadores y partes interesadas adecuados. A menudo en ciberseguridad industrial, eso significa incluir a personal clave tanto de IT como de OT. Prepárese para responder a preguntas difíciles y ensaye con antelación. En algunos casos, convendrá contar con expertos experimentados en consultoría de ciberseguridad externos a la organización para que le ayuden a responder preguntas basadas en su experiencia en implementaciones anteriores.

SecureOT: Para proteger las cosas en que confía el mundo

SecureOT es una completa suite de soluciones de ciberseguridad industrial concebida para permitir operaciones resilientes en cualquier nivel de madurez de la ciberseguridad. Respaldado por más de un siglo de experiencia en automatización industrial y décadas de experiencia en ciberseguridad específica de OT, SecureOT ayuda a las organizaciones a diseñar, implementar, gestionar y optimizar programas de ciberseguridad que se alineen con los objetivos empresariales y las prioridades de riesgo.
Obtenga más información aquí.

Comuníquese con Rockwell Automation y converse con un experto en ciberseguridad industrial hoy mismo.

Notas a pie de página

[1]Omdia: https://omdia.tech.informa.com/
[2]Trendmicro: https://www.trendmicro.com/en_us/research/22/j/manufacturing-cybersecurity-trends-threats.html
[3]Dragos: https://www.dragos.com/year-in-review/
[4]Dragos: https://hub.dragos.com/hubfs/Reports/2021-Ponemon-Institute-State-of-Industrial-Cybersecurity-Report.pdf?hsLang=en
[5]Trendmicro: https://www.trendmicro.com/en_us/research/21/d/new-survey-report-released-the-state-of-industrial-cybersecurity-part-2.html
[6]Dragos: https://hub.dragos.com/rockwell-automation/ics-cybersecurity-year-in-review-executive-summary-2022
[7]Synsaber: https://14520070.fs1.hubspotusercontent-na1.net/hubfs/14520070/Collateral/SynSaber_Industrial-CVE-Retrospective_2020-2021-2022.pdf
[8]Pingdom: https://www.pingdom.com/outages/average-cost-of-downtime-per-industry/
[9]Siemens: https://www.siemens.com/global/en/products/services/digital-enterprise-services/analytics-artificial-intelligence-services/predictive-services/senseye-predictive-maintenance.html
[10]Dragos: https://hub.dragos.com/hubfs/Reports/2021-Ponemon-Institute-State-of-Industrial-Cybersecurity-Report.pdf?hsLang=en

Rockwell Automation

Conéctese con nosotros.

rockwellautomation.com — expanding **human possibility**®

AMÉRICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 USA, Tel.: (1) 414.382.2000
EUROPA/MEDIO ORIENTE/ÁFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Bélgica, Tel.: (32) 2 663 0600
ASIA-PACÍFICO: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608
ARGENTINA: Rockwell Automation S.A., Av. Leandro N. Alem 1050, Piso 5, Ciudad Autónoma de Buenos Aires, Tel.: (54) 11.5554.4040, www.rockwellautomation.com.ar
CHILE: Rockwell Automation Chile S.A., Av. Presidente Riesco 5435, Piso 15, Las Condes, Santiago, Tel.: (56) 2.290.0700, www.rockwellautomation.com.cl
COLOMBIA: Rockwell Automation S.A., Edf. North Point, Carrera 7 N 156-78 Piso 19, PBX: (57) 1.649.9600, www.rockwellautomation.com.co
ESPAÑA: Rockwell Automation S.A., C/ Josep Plà, 101-105, Barcelona, España 08019, Tel.: 34 902 309 330, www.rockwellautomation.es
MÉXICO: Rockwell Automation de S.A. de C.V., Av. Santa Fe 481, Piso 3 Col. Cruz Manca, Deleg, Cuajimalpa, Ciudad de México C.P. 05349, Tel.: 52 (55) 5246-2000, www.rockwellautomation.com.mx
PERÚ: Rockwell Automation S.A., Av. Victor Andrés Belaunde N 147, Torre 12, Of.102, San Isidro Lima, Perú, Tel.: (511) 211-4900, www.rockwellautomation.com.pe
PUERTO RICO: Rockwell Automation, Inc., Calle 1, Metro Office #6, Suite 304, Metro Office Park, Guaynabo, Puerto Rico 00968, Tel.: (1) 787.300.6200, www.rockwellautomation.com.pr
VENEZUELA: Rockwell Automation S.A., Edf. Allen-Bradley, Av. González Rincones, Zona Industrial La Trinidad, Caracas 1080, Tel.: (58) 212.949.0611, www.rockwellautomation.com.ve

Publicación GMSN-SP022B-ES-P Diciembre de 2024