SecureOT

Uma apostila SecureOT

Crie o caso de negócios certo para seu programa de cibersegurança industrial

Suporte de liderança premiado para iniciativas de cibersegurança de TO

A maioria dos líderes entendem a importância de proteger as operações industriais contra ameaças cibernéticas. No entanto, os líderes devem equilibrar continuamente os investimentos em cibersegurança com outras prioridades e iniciativas organizacionais.

Além de atuarem nesse equilíbrio, o conhecimento especializado de sistemas de controle industrial (ICS) e tecnologia operacional (TO) entre os líderes organizacionais pode ser limitado, juntamente com percepções sobre abordagens, ferramentas e processos modernos de cibersegurança necessários para proteger os sistemas ICS/TO.

Os líderes de TI podem ver que os recursos de TO são menos vulneráveis a ataques quando comparados aos recursos digitais de TI, incluindo redes, servidores e bancos de dados. Isso porque os recursos de TO historicamente foram isolados das redes de TI e tiveram poucas, se é que houveram, conexões externas que dariam a um adversário um caminho para o ataque. Os líderes de TI também acreditavam que o risco de um invasor ter sistemas industriais como alvo era baixo, com base na crença de que há pouco valor para os invasores em ambientes de TO, como nenhuma informação pessoalmente identificável (PII) ou números de cartão de crédito para roubar.

Hoje, no entanto, as operações da fábrica estão cada vez mais digitais e interconectadas, introduzindo silenciosamente novos riscos para as empresas. E, infelizmente, os atacantes de hoje sabem que interromper as operações da fábrica pode gerar custos astronômicos para qualquer organização. Eles aprenderam que as organizações têm uma alta disposição de pagar taxas de resgate se isso significar restaurar as operações mais cedo.

A necessidade de identificação realista de riscos

Paralelamente, a tensão geopolítica está aumentando, com os países observando ativamente infraestruturas críticas como possíveis alvos da guerra cibernética. Um ataque cibernético bem-sucedido a sistemas industriais pode ter consequências devastadoras, além do tempo de parada não programada da produção, danos ao equipamento e perdas financeiras. Esse ataque pode afetar a segurança do operador e até mesmo interromper serviços vitais, como produção e distribuição de alimentos, água, transporte, saúde e energia.

Criar um caso de negócios para cibersegurança industrial pode ajudar os líderes a entender os riscos e benefícios de investir em medidas de cibersegurança para ambientes de TO. Quantificar o impacto potencial envolve identificar vulnerabilidades ou a probabilidade de um ataque cibernético e entender que normalmente é mais barato investir na redução de risco com antecedência. Por fim, o caso certo de cibersegurança apoiará a jornada de uma organização para modernizar a cibersegurança de TO.

Isso não apenas ajuda os líderes a priorizarem seus investimentos de forma inteligente, mas os prepara com as informações de que precisam para justificar e promover o projeto com as principais partes interessadas, como o conselho de administração da organização.

80%

80% das empresas industriais tiveram um aumento significativo nos incidentes de segurança.[1]

5 dias

Período médio de interrupção do sistema devido a cibercriminosos na indústria de manufatura.[2]

Elementos fundamentais de um caso de negócios de cibersegurança industrial

Em sua forma mais básica, um caso de negócios é um documento simples que estabelece os custos associados a um investimento proposto juntamente com os benefícios projetados, demonstrando um retorno do investimento (ROI) associado.

Quando se trata de construir um caso de negócios de cibersegurança, quantificar custos e benefícios pode ser desafiador. Muitos dos benefícios vêm na forma de redução de risco e redução de custos. Além disso, os custos da implementação de uma nova solução podem precisar ser divididos por vários departamentos diferentes, incluindo TI, TO, segurança, operações da fábrica, recursos humanos, finanças e proteção.

Adotar uma abordagem metódica para criar um caso de negócios de cibersegurança pode ajudar a converter conceitos complexos e subjetivos em valores quantificáveis, tornando mais fácil para os líderes determinar com mais precisão riscos e custos, e a priorizar a cibersegurança dentre iniciativas concorrentes.

Um caso de negócios de cibersegurança pode conter as seguintes seções:

Seções de caso de negócios	Conteúdo da seção	Consulte a página
Declaração e análise do problema	Situação atual, análise de risco. Pode incluir uma avaliação de risco formal de terceiros.	5
Solução proposta	Visão geral das soluções propostas; por que é o melhor conjunto de soluções para a organização.	7
Resultados organizacionais	Estimativas quantificadas de valor da redução do risco de um ataque cibernético bem-sucedido, incluindo critérios de gestão de mudanças, análise de impacto nos negócios ou requisitos de gestão de risco do fornecedor.	8
Detalhamento de custos	Revisão dos custos de solução propostos entre as categorias de pessoas, processos e tecnologia.	11
Retorno do investimento/ valor	Valor da redução do risco de cibersegurança em comparação com os custos da solução proposta.	13

Agora vamos examinar cada uma dessas seções em detalhes, juntamente com o conteúdo de exemplo.

Declaração e análise do problema

Um caso de negócios começa com uma visão geral do problema que um projeto proposto deve resolver. A declaração do problema normalmente inclui um resumo do estado atual, uma análise das causas e uma visão geral dos objetivos de negócios que o projeto deve resolver.

Quando se trata de cibersegurança industrial, não faltam desafios para as equipes de TO enfrentarem, de cibercriminosos e agentes de ameaça estatais a hacktivistas e membros internos. Os motivadores comuns para investimentos em cibersegurança incluem:

- **Aumento do crime cibernético, especialmente ransomware**. Embora muitos líderes possam ver o crime cibernético como um problema principalmente de TI, ele representa uma ameaça cada vez mais significativa aos ambientes de TO, levando a acesso não autorizado, tempo de parada não programada e ao potencial de interrupção em larga escala.

- **Os cibercriminosos** podem visar sistemas industriais para extorquir dinheiro, roubar propriedade intelectual ou, na maioria das vezes, interromper as operações. A tendência de interrupções em larga escala e impulsionadas por nações é parcialmente fomentada pela transformação digital, especialmente pela conectividade mais ampla e profunda entre ambientes de TI e TO. À medida que os sistemas industriais se tornam mais complexos, interconectados e interdependentes, não é mais viável proteger o ambiente de TO apenas com sua separação física. O aumento da conectividade com sistemas de TI, nuvem, fornecedores terceirizados e redes 5G abre um conjunto de riscos totalmente novo para redes de TO.

- **Aumento das exigências**. As organizações industriais enfrentam regulamentações pesadas de várias fontes, que variam de acordo com o país, a região e o setor.
  As multas podem ser pesadas para as organizações fora da conformidade. Por exemplo, um ano depois que uma empresa de energia líder foi atingida por um ataque de ransomware amplamente divulgado, o Departamento de Transporte dos EUA recomendou uma multa de quase US$ 1 milhão, além dos custos já altos que a empresa pagou devido aos dias de parada não programada e aos esforços de recuperação.

87%

Os ataques de ransomware contra sistemas industriais aumentaram 87% em 2022.[3]

29%

das organizações industriais relataram ter sofrido um ataque de ransomware nos últimos 2 anos.[4]

89%

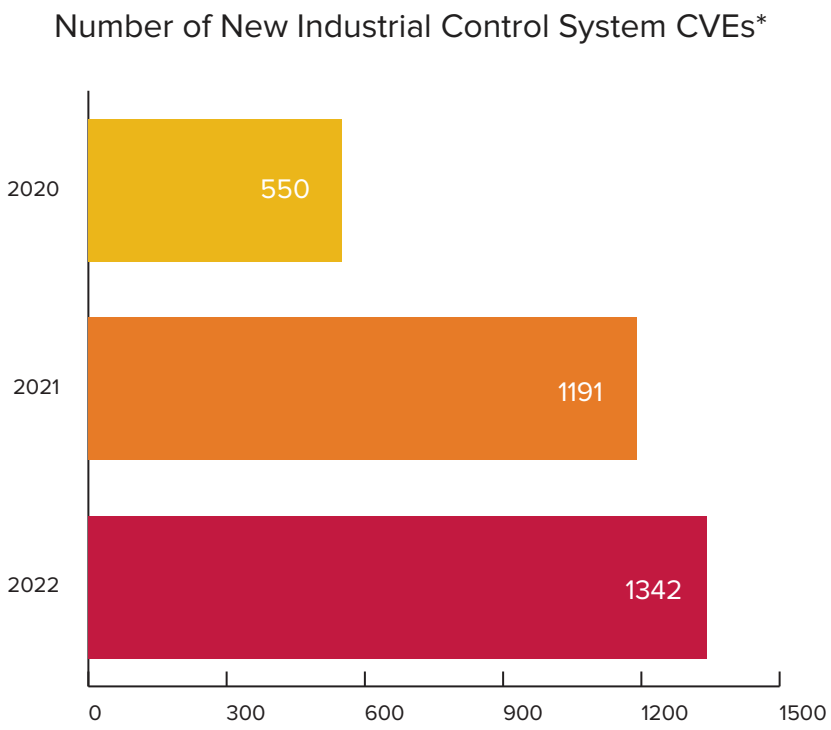
das organizações industriais tiveram suas cadeias de fornecimento interrompidas devido a ataquescibernéticos.[5]

Declaração e análise do problema *continuação*

REGULAMENTAÇÃO	Indústria afetada
Proteção da infraestrutura crítica da North American Electric Reliability Corporation (NERC CIP)	Concessionárias de energia elétrica norte-americanas
Diretiva de segurança da informação de rede 2 (NIS2)	Operadores europeus de serviços essenciais
Lei de Relatório de incidentes cibernéticos para infraestrutura crítica (CIRCIA)	Fornecedores do setor de infraestrutura crítica dos EUA
Suplemento da regulamentação de aquisição federal de defesa (DFARS)	Prestadores de serviço de defesa dos EUA
Lei de Portabilidade e Responsabilidade de Seguros de Saúde (HIPAA)	Fabricantes de dispositivos médicos e outras organizações que lidam com informações de saúde
Título 21 do Código de Regulamentações Federais (21 CFR Parte 11)	Setores regulamentados pela Food and Drug Administration (FDA) dos EUA
H.R. 2868: A regulamentação de padrões antiterrorismo de instalações químicas (CFATS)	Instalações químicas
Tratado Internacional das Nações Unidas	No momento em desenvolvimento, este tratado se concentra na proteção de dados e resiliência cibernética
Estrutura de cibersegurança do NIST	Uma estrutura global para cibersegurança organizacional
Certificação do modelo de maturidade de cibersegurança (CMMC)	Requisito de cibersegurança do Departamento de Defesa dos EUA
MITRE ATT&CK	Uma base para o desenvolvimento de modelos e metodologias de ameaças no setor privado, no governo e na comunidade de produtos e serviços de cibersegurança
Trusted Information Security Assessment Exchange (TISAX)	Um mecanismo de avaliação e intercâmbio de informações para segurança da informação na indústria automotiva

Uma amostra das regulamentações de cibersegurança por setor

Declaração e análise do problema *continuação*



Este gráfico mostra o crescimento de vulnerabilidades e exposições comuns (CVEs).[7]

- **Vulnerabilidades crescentes.** Pesquisadores e fornecedores de segurança continuam a divulgar novas vulnerabilidades do sistema de controle industrial a uma taxa crescente a cada ano. O número de atores de ameaças baseados nos EUA dedicados a que atacar organizações industriais cresceu 35% no último ano, provocando um aumento de 87% nas violações no mesmo período.[6] Essas vulnerabilidades são desafiadoras para os defensores não apenas pelo seu volume, mas também pela complexidade envolvida na reparação delas. Embora as vulnerabilidades em ambientes de TI possam ser corrigidas com relativa rapidez, em ambientes de TO há desafios maiores, incluindo garantias que exigem procedimentos longos de teste de aceitação e janelas de manutenção limitadas.

Exemplo de declaração de problema

Ao longo desta apostila, você encontrará exemplos breves mostrando como a orientação pode ser colocada em prática para uma organização industrial do mundo real.

> “A Global Manufacturing Inc. (GMI) está vivenciando um aumento significativo nas tentativas de ataques de ransomware, colocando o ambiente de TO em alto risco de tempo de parada não programada e de perda de dados.
>
> Nos últimos 12 meses, o número de alertas de segurança relacionados a ransomwares aumentou 80%. A maioria desses ataques tem como alvo sistemas de TI, no entanto, o aumento da conectividade entre ambientes de TI e TO dentro da GMI resultou na exposição dos sistemas industriais a essas ameaças cibernéticas.
>
> Os riscos nas fábricas são especialmente altos devido a um grande número de sistemas em obsolescência com vulnerabilidades que não foram corrigidas. Em alguns casos, esses sistemas não estão mais recebendo patches de segurança de seus respectivos fornecedores. Em outros casos, a implantação de patches requer passar por um longo processo de validação regulatória e sua instalação foi adiada.”

Solução proposta

Em seguida, apresentaremos a solução proposta para resolver o problema. Um caso de negócios de cibersegurança robusto deve incluir uma visão geral das soluções que podem ter sido consideradas e uma análise do motivo pelo qual a solução proposta é a melhor para a organização. A descrição da solução não deve apenas descrever a nova tecnologia ou serviço que será implantado, mas também fornecer uma visão geral do modelo operacional e dos pontos de integração com a tecnologia e os processos existentes. A descrição da solução completa dará à liderança uma visão total de como a nova solução se encaixará na pilha de tecnologia existente, ajudando a criar confiança em uma implantação tranquila.

Soluções de exemplo

> “A equipe de GMI está propondo um projeto para reduzir o risco de ransomware nas fábricas, melhorando a segmentação e a filtragem de rede em todo o ambiente de TO.
>
> Os controles de rede são a maneira mais eficaz de reduzir o risco no ambiente atual de TO da GMI. Os controles de segurança de endpoint que são usados em toda a infraestrutura de TI da GMI não são viáveis nas redes de TO, devido à ampla gama de sistemas incorporados e sistemas operacionais sem suporte.
>
> A solução proposta consistirá em um conjunto de firewalls de rede industrial implantados para controlar rigorosamente o tráfego de entrada/saída na zona desmilitarizada da fábrica (Nível Purdue 3.5), na LAN de Operações da Fábrica (Nível Purdue 3) e na LAN de Controle da Fábrica (Nível Purdue 2). A implementação de controles rígidos de entrada/saída nessas camadas ajudará a garantir que nenhum tráfego de rede não autorizado possa cruzar os limites da camada, protegendo efetivamente os sistemas em risco. A solução proposta também ajuda a melhorar a adesão da GMI às melhores práticas em cibersegurança industrial, conforme estabelecido na IEC 62443.
>
> Os firewalls serão implantados pelo fornecedor escolhido durante os períodos de manutenção programados regularmente, minimizando o tempo de parada não programada. Após receber o treinamento adequado, a solução será mantida pela equipe de engenharia de segurança da GMI e todos os alertas serão integrados aos fluxos de trabalho existentes do centro de operação de segurança (SOC) da GMI.”

Para implementações complexas – abrangendo vários locais globais ou implantando um programa completo de Estrutura de cibersegurança NIST ao longo de vários anos, por exemplo – a solução proposta pode ser iniciar um projeto de Fase 1 com implantações paralelas de avaliações de risco e vulnerabilidade, detecção de ameaças e processos de resposta a incidentes, ao mesmo tempo em que planeja as fases restantes do projeto.

Resultados organizacionais

Agora é hora de fazer as contas. A base de um caso de negócios de cibersegurança está em fornecer uma compreensão dos benefícios que serão obtidos com o investimento proposto. Os maiores benefícios dos investimentos em cibersegurança vêm de evitar custos e impactos associados a uma violação, incluindo:

- **Tempo de parada não programada reduzido**. Um dos maiores benefícios dos investimentos em cibersegurança para ambientes de TO é a redução do tempo de parada não programada associado a incidentes de cibersegurança. Os custos do tempo de parada não programada em ambientes industriais podem ser significativos, especialmente quando você considera os custos da perda de produção, entregas atrasadas, deterioração e trabalhadores ociosos.

  Por exemplo, em fevereiro de 2022, uma montadora global foi forçada a encerrar as operações em 14 fábricas devido a um ataque cibernético em um parceiro-chave da cadeia de fornecimento. O encerramento resultou em uma redução de aproximadamente um terço da capacidade de produção global da montadora, representando 13.000 carros por dia e centenas de milhões de dólares. Os custos reais de interrupções não planejadas variam dependendo do tamanho do negócio e do setor. As estimativas variam de US$ 8.000 ou mais por hora para uma empresa de pequeno a médio porte, até US$ 1 milhão ou mais por hora para uma grande organização industrial.[8]

  Considerando que geralmente leva vários dias ou até semanas para as equipes se recuperarem de um incidente de cibersegurança e retornarem às operações normais, é fácil ver como a prevenção de um incidente pode resultar em milhões de dólares em economia de custos.

US$ 2 milhões

Custo médio de 1 hora de parada não programada no setor automotivo.

US$ 500 mil

Custo médio de 1 hora de parada não programada na indústria de petróleo e gás.[9]

- **Prevenção de custos de resposta e recuperação de incidentes.** Os custos de resposta e recuperação de incidentes para um incidente de cibersegurança em ambientes industriais podem ser substanciais. A primeira etapa na resposta a incidentes é investigar e analisar o incidente para determinar sua causa, escopo e impacto. Isso pode envolver a contratação de especialistas em cibersegurança externos, a realização de análises forenses dos sistemas afetados e a revisão de registros e outros dados para identificar a origem do ataque.

  Após a conclusão da investigação, o próximo passo é corrigir os sistemas afetados e restaurar as operações normais. Isso pode envolver a correção de vulnerabilidades, restauração de backups e realização de testes e validação do sistema para confirmar que todos os sistemas estejam funcionando conforme o esperado.

  Além disso, no caso de incidentes de ransomware ou roubo de dados, é comum que atacantes exijam pagamentos de resgate para restaurar o acesso a dados criptografados ou para impedir que informações confidenciais sejam divulgadas publicamente. Embora os especialistas concordem que o melhor é não pagar o resgate a gangues criminosas, algumas organizações optam por fazê-lo porque pode ser seu caminho mais rápido e econômico para restaurar as operações.

- **Prevenção de multas regulatórias.** Organizações governamentais ou industriais podem cobrar multas sobre organizações que não atendam às normas ou políticas de segurança. Essas multas podem ser emitidas por vários motivos, incluindo violações de dados, práticas de segurança inadequadas e falhas de conformidade. Dependendo da gravidade da violação, as multas podem variar de milhares a milhões de dólares.

  Nos últimos anos, houve um aumento nas multas regulatórias por violações de cibersegurança, à medida que governos e órgãos reguladores buscam responsabilizar as organizações por violações de dados e outros incidentes de segurança. Essa tendência provavelmente continuará enquanto as ameaças à cibersegurança evoluírem e se tornarem mais sofisticadas.

US$ 500 mil

A maioria das organizações industriais pagou uma média de US$ 500 mil ou mais em resgate.[10]

US$ 986 mil

Penalidade civil imposta à Colonial Pipeline pelo Departamento de Transporte dos EUA após o incidente de ransomware de 2021.

Outros resultados de investimentos em cibersegurança incluem:

- **Diferenciação estratégica**. À medida que os ataques cibernéticos se tornam mais comuns, os clientes estão cada vez mais cientes dos riscos decorrentes de fazer negócios com terceiros. Ter um programa de cibersegurança forte pode diferenciar uma organização dos concorrentes, especialmente para clientes em setores altamente regulamentados, como saúde, governo e energia.

- **Fatores de saúde, segurança e ambientais**. No setor industrial, um incidente de cibersegurança pode causar mais do que interrupções nos sistemas digitais. Esse incidente também pode ter impactos significativos no mundo físico, incluindo danos à infraestrutura física, danos ambientais causados por contaminação ou derramamentos de produtos químicos e ameaças à segurança humana.

- **Redução nos custos de seguro de cibersegurança**. As melhorias nas defesas cibernéticas fazem com que as organizações sejam um risco menor para as seguradoras, o que pode ser refletido em prêmios menores ou em melhores termos e condições.

Métricas orientadas por resultados: A tabela abaixo resume os benefícios estimados que a GMI espera ver como resultado do projeto de segmentação de rede proposto:		**Estime abaixo os resultados potenciais da sua organização:**
Número estimado de incidentes de cibersegurança evitados:	1 incidente/ano	
Custos estimados de tempo de parada para uma fábrica GMI:	US$ 50.000/horas	
Tempo de inatividade não programada da fábrica esperado para um incidente de cibersegurança:	36 horas	
Economia calculada para o tempo de parada devido a incidentes de cibersegurança evitados:	US$ 1,8 milhão/ano	
Economia estimada pela resposta e recuperação de incidentes:	US$ 200.000/ano	
Economia estimada das taxas regulatórias:	US$ 100.000/ano	
Total de benefícios anuais estimados:	**US$ 2,1 milhões/ano**	

Detalhamento de custos: mapeie os custos

Uma vez que os benefícios de um investimento em cibersegurança sejam bem compreendidos, é hora de voltar nossa atenção para os custos.

Para ajudar os líderes a tomarem decisões informadas, é importante que eles entendam não apenas os custos iniciais associados a um projeto proposto, mas também os custos operacionais contínuos que aparecerão ao longo do tempo.

Um caso de negócios típico de cibersegurança definirá os custos em várias categorias diferentes:

- **Custos de tecnologia**. Qualquer projeto que introduza novos controles ou serviços de segurança no ambiente provavelmente terá custos associados à compra da tecnologia ou serviço subjacente. Esses custos geralmente são fáceis de obter de seu fornecedor de tecnologia e podem incluir custos únicos, como licenças de hardware e software, bem como custos anuais recorrentes, como taxas de assinatura de SaaS.

- **Custos de implantação**. Antes que uma organização possa começar a perceber o valor de seu investimento, a solução proposta deve primeiro ser instalada e configurada adequadamente. O caso de negócios deve levar em conta os custos diretos, como taxas de consultoria e treinamento, bem como os custos de indiretos associados à implantação, como a mão de obra necessária para implantar software e hardware, integrá-los aos fluxos de trabalho técnicos e de negócios existentes e qualquer tempo de parada planejado necessário para concluir a implantação.

- **Manutenção da solução**. Poucas soluções são verdadeiramente "configurar e esquecer". A maioria das soluções exigirá manutenção contínua para garantir que continuem a operar com eficiência, e a cibersegurança em específico precisa de atualizações contínuas à medida que o cenário de ameaças evolui constantemente. Os fornecedores normalmente cobram uma taxa de suporte anual de 15% a 25% para fornecer suporte e atualizações contínuos. Além disso, será necessária uma equipe de suporte local para implantar patches de segurança e atualizações de software em tempo hábil, monitorar a integridade da solução para garantir que ela esteja funcionando corretamente e ajustar as políticas conforme necessário para otimizar a proteção.

- **Monitoração de solução**. Por fim, há custos associados ao uso real da nova solução de segurança em um ambiente de produção. Muitas soluções de segurança geram alertas que devem ser analisados pelo pessoal em um centro de operações de segurança (SOC). A equipe do SOC deve integrar os novos alertas em seu fluxo de trabalho existente para fazer a triagem, investigar e responder a quaisquer ameaças cibernéticas que surjam. SOC como serviço (SOC-as-a-Service) ou serviços de SOC gerenciados estão disponíveis e geralmente são desejáveis devido à escassez de pessoal de cibersegurança em todo o mundo. Se preferir uma abordagem de SOC gerenciada, use este modelo de preços para custos estimados de manutenção da solução.

Exemplo de custos: A tabela abaixo resume os custos previstos que a GMI espera ver como resultado do projeto de segmentação de rede proposto:		**Estime abaixo os resultados potenciais da sua organização:**
Suposições		
Custo de FTE de engenharia de TI:	US$ 150.000/ano	
Custo de pessoal FTE do SOC:	US$ 175.000/ano	
Custos únicos		
Hardware e software:	US$ 350.000	
Serviços profissionais (instalação e configuração):	US$ 50.000	
Treinamento do administrador:	US$ 15.000	
Total de custos únicos:	**US$ 415.000**	
Custos anuais recorrentes		
Suporte do fornecedor:	US$ 70.000/ano	
Manutenção de solução: 0,5 FTE de engenharia de TI	US$ 75.000/ano	
Monitoração de solução: 1 funcionário FTE do SOC	US$ 175.000/ano	
Total de custos anuais recorrentes:	**US$ 320.000/ano**	

Calcule o retorno do investimento

Munido de dados sobre os custos e benefícios da solução, é uma questão simples realizar uma análise de custo-benefício. Isso normalmente começa calculando o retorno do investimento (ROI). O ROI fornece uma métrica simples e rápida que mostra aos líderes o valor a ser obtido com um investimento em cibersegurança.

Primeiro, considere o intervalo de tempo para um cálculo de ROI*. Como os custos provavelmente incluem algumas despesas iniciais (por exemplo, custos de hardware, licenciamento de software e custos de implantação) e custos recorrentes (como assinaturas de SaaS e manutenção), geralmente é melhor realizar a análise de ROI ao longo de um período de pelo menos três anos para fornecer uma visão completa do valor a ser obtido ao longo do tempo. O retorno do investimento geralmente é mostrado como uma porcentagem e pode ser calculado usando a seguinte fórmula:

$$\text{Retorno do investimento} = \frac{\text{(BENEFÍCIOS - CUSTOS)}}{\text{(CUSTOS)}} \text{ x100}$$

Este número não deve ser visto como um retorno financeiro direto. Muito do benefício da redução de risco e da prevenção de custos antecipada são derivados das tendências e médias históricas gerais. Em vez disso, um cálculo de ROI deve ser visto como uma medida de quanto do risco pode ser reduzido para a despesa especificada e ser declarado como valor.

Exemplo de cálculo de retorno do investimento: A tabela abaixo resume os custos previstos que a GMI espera ver como resultado do projeto de segmentação de rede proposto:		**Calcule abaixo o ROI esperado da sua organização:**
Prevenção de custos estimada/valor ano 1	US$ 2.100.000	
Prevenção de custos estimada/valor ano 2	US$ 2.100.000	
Prevenção de custos estimada/valor ano 3	US$ 2.100.000	
Total de benefícios de 3 anos:	**US$ 6.300.000**	
Custos de implantação	US$ 415.000	
Custos operacionais ano 1	US$ 320.000	
Custos operacionais ano 2	US$ 320.000	
Custos operacionais ano 3	US$ 320.000	
Total de custos de 3 anos:	**US$ 1.375.000**	
$\text{ROI} = \frac{\text{US\$ 6.300.000 - US\$ 1.375.000}}{\text{US\$ 1.375.000}} \text{ x 100}$		
Valor do investimento em 3 anos:	360%	

* Para simplificar, ignoramos o valor temporal do dinheiro em nossos cálculos. Uma análise mais sofisticada consideraria o fato de que, devido à inflação e outros fatores, um dólar no ano 1 vale mais do que um dólar no ano 3. Isso pode alterar o cálculo geral em alguns pontos percentuais, mas não deve afetar a conclusão geral.

Apresentando seu caso

Concluir um caso de negócios de cibersegurança é apenas o início de um processo maior de tomada de decisões e implementação. Munido de um problema, solução, benefícios e custos bem documentados, é hora de levar o caso de negócios aos líderes, que estarão bem equipados para avaliar o caso de negócios com base em suas próprias perspectivas e prioridades.

Certifique-se de convidar os apresentadores e partes interessadas certos para sua apresentação. Muitas vezes, na cibersegurança industrial, isso significa incluir cargos chave de TI e TO. Prepare-se para perguntas difíceis e ensaie com antecedência. Em alguns casos, você quer especialistas experientes em consultoria de cibersegurança de fora da organização para ajudar a responder a perguntas com base em sua experiência em implementações anteriores.

SecureOT: Protegendo aquilo de que o mundo depende

O SecureOT é um pacote abrangente de soluções de cibersegurança industrial projetado para fornecer operações resilientes para todos os níveis de maturidade de cibersegurança. Com mais de um século de experiência em automação industrial e décadas de experiência em cibersegurança específica de OT, o SecureOT ajuda as organizações a projetar, implementar, gerenciar e otimizar programas de cibersegurança que se alinham aos objetivos de negócios e às prioridades de risco. Saiba mais aqui.

Entre em contato com a Rockwell Automation para falar com um especialista em cibersegurança industrial hoje mesmo.

Notas de rodapé

[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

Fale conosco.

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

AMÉRICAS: Rockwell Automation, 1201 South Second Street, Milwaukee, WI 53204-2496 EUA, Tel: (1) 414.382.2000
EUROPA/ORIENTE MÉDIO/ÁFRICA: Rockwell Automation NV, Pegasus Park, De Kleetlaan 12a, 1831 Diegem, Bélgica, Tel: (32) 2 663 0600
ÁSIA-PACÍFICO: Rockwell Automation SEA Pte Ltd, 2 Corporation Road, #04-05, Main Lobby, Corporation Place, Singapore 618494, Tel: (65) 6510 6608
BRASIL: Rockwell Automation do Brasil Ltda., Rua Verbo Divino, 1488 – 1° andar, Chac. Sto Antonio, 04719-904, São Paulo, SP, Tel: (55 11) 5189-9500, www.rockwellautomation.com.br
PORTUGAL: Rockwell Automação, Lda., Av. Prof. Dr. Cavaco Silva, Edificio Ciência II, n.º 11 - 2ºC, Taguspark, Porto Salvo 2740-120, Tel.: (351) 214 225 500, www.rockwellautomation.com.pt

Publicação GMSN-SP022B-EN-P DEZ 2025