



CyberEdge Sales Playbook



Bring on tomorrow



←

QUAIS SÃO AS OPORTUNIDADES DE VENDA?

QUAL O PERFIL DOS CLIENTES POTENCIAIS?

VENDER CYBEREDGE A COMPRADORES PELA PRIMEIRA VEZ?

COMO VENDER A MARCA AIG AO CLIENTE?

REBATENDO OBJEÇÕES

EXEMPLOS DE SINISTROS

RESUMO DE COBERTURAS

As ameaças cibernéticas são uma das preocupações mais importantes de risco para as empresas na era digital e esta tendência irá aumentar. Isto, juntamente com o fato de que hoje serem muito poucas as entidades que contratam uma apólice de CyberEdge, é uma grande oportunidade de crescimento para os intermediários de seguros nesta área.

1

A PREOCUPAÇÃO DO CLIENTE AUMENTA

Dentro do sector segurador são poucos os ramos que têm muitas estatísticas mostrando o crescente número de incidentes e exposições, como a responsabilidade cibernética possui. Portanto, não é de admirar que muitas empresas europeias apreciem a necessidade de contratar este seguro, da mesma forma que os gestores de risco percebem os riscos cibernéticos como uma de suas principais preocupações.

[CLICAR PARA VER A ESTATÍSTICAS >](#)

2

UM RISCO IMPORTANTE NÃO COBERTO

Além de ser uma grande preocupação para os gestores de risco, os riscos cibernéticos são, de acordo com um estudo, um dos menos contratualizados em apólices de seguros (ver gráfico). Isso mostra uma falta de cobertura significativa, pelo que os clientes mostram grande interesse em rever a sua exposição cibernética e em analisar a solução de seguro especializada.

[VER INQUÉRITO >](#)

3

UM GRANDE MERCADO

Qualquer empresa que colectar, manipular ou transmitir dados está exposta ao risco cibernético e até mesmo roubo físico. Na era dos dados digitais armazenados em rede, estes constituem uma ameaça para qualquer organização, o que significa que praticamente qualquer entidade, independentemente do seu negócio, está exposta.

Para os corretores de seguros esta área é uma oportunidade de negócio.

4

CONSCIÊNCIA DO RISCO

Apesar de haver uma consciência generalizada sobre o risco cibernético, as empresas desconhecem as reais ameaças específicas que podem enfrentar. O CyberEdge permite que os corretores de seguros tragam aos seus clientes estas exposições emergentes, enquanto se posicionam no mercado como especialistas na matéria.

[VER SÍNTESE DE COBERTURA >](#)

ACEDA AO RESUMO DE COBERTURAS

No geral, os clientes estão cientes dos riscos cibernéticos, mas ignoram os perigos específicos que enfrentam. A grande maioria das empresas até à data ainda não tem um seguro específico para protegê-los, que é uma grande oportunidade para os corretores de seguros que apostem no mesmo, bem como se posicionam como especialistas para os seus clientes, fornecendo soluções de seguro específicas a riscos cibernéticos.

SAIBA MAIS SOBRE RISCOS CYBER



6 minutos de filme online

As seções seguintes olham com mais detalhe: o mercado-alvo, os temas de vendas para compradores de cyber pela primeira vez, os pontos fortes da AIG em relação a esta linha de negócios, sugestões para a superação de obstáculos de vendas, alguns cenários de sinistros e, finalmente, um resumo da cobertura CyberEdge e serviços.

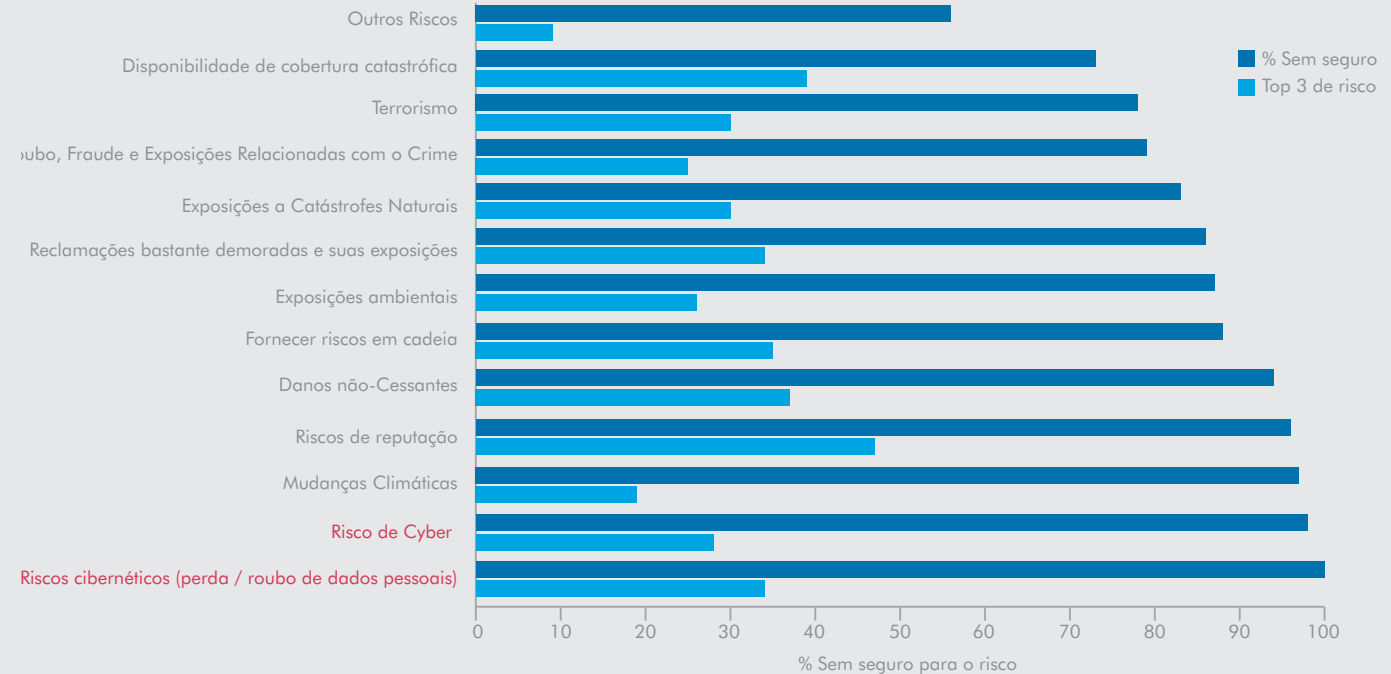
ESTATÍSTICAS

Não há falta de estatísticas sobre riscos cibernéticos.

- Em 2011, existiram 855 violações de dados que corromperam mais de 174 milhões de registos.
- A cada minuto, 232 computadores são infectados por malware.
- RSA Anti-Fraud Command Centre fechou mais de 550.000 ataques de phishing.
- Novos ataques sofisticados estão sendo constantemente desenvolvidos por autores que vão de sindicatos do crime, a hackers independentes, a funcionários, a hacktivistas, etc.
- O custo médio de uma violação de segurança da rede é superior a 5 milhões dólares
- O custo médio por registo envolvido numa violação da segurança da rede é 197 dólares.
- O preço Europeu sobre a criminalidade cibernética ao consumidor é de 16 biliões de dólares.

INQUÉRITO

MAIORES PREOCUPAÇÕES DE RISCO – INQUÉRITO A CLIENTES SEM SEGURO



101 gestores de risco foram convidados a identificar os seus 3 principais preocupações de exposição a risco e indicar se eles compraram o seguro para o risco. AIRMIC junho 2012.

QUAIS SÃO AS OPORTUNIDADES DE VENDA?

QUAL O PERFIL DOS CLIENTES POTENCIAIS?

VENDER CYBEREDGE A COMPRADORES PELA PRIMEIRA VEZ?

COMO VENDER A MARCA AIG AO CLIENTE?

REBATENDO OBJEÇÕES

EXEMPLOS DE SINOTROS

RESUMO DE COBERTURAS

O mercado para o Cyberedge tem um grande potencial porque qualquer empresa que archive, manipule, ou transmita dados está em risco de um ataque cyber ou de um roubo físico.

EMPRESAS COM OPERAÇÕES NOS EUA

Empresas europeias com operações nos Estados Unidos ou dados nos EUA têm obrigações onerosas após infrações de segurança de dados. Devem seguir as 46 legislações estaduais americanas de manutenção de padrões de segurança, com alguns estados a obrigarem a notificação aos afectados. A lei vai além das exigências estatuais e existe legislação específica da indústria que terá que ser cumprida. Adicionalmente, a SEC exige que as empresas norte-americanas cotadas em bolsa divulguem as suas exposições operacionais e financeiras depois de um ataque cibernético ou um evento Cyber.

UNIVERSIDADES

Universidades e faculdades acumulam grandes quantidades de informação confidencial (números de cartão de crédito dos candidatos, transcrições académicas, dados de pesquisa e registos de saúde). Muita informação de funcionários e alunos é armazenado em dispositivos móveis, que podem ser perdidos ou colocados num estado sem vigilância. Acesso remoto, média social e software de gestão de transacções académicas contribuem para o aumento do risco, enquanto a universidade pode não ter níveis de segurança adequados.

RETAILHISTAS

Os retalhistas são donos de muita informação de clientes, incluindo números de cartão de crédito e débito e as vendas on-line estão em ascensão através de uma base global de clientes. Isto traz obrigações de conformidade com a legislação de cada país e ao Payment Card Industry Data Security Standards (PCI DSS), expondo a empresa a possíveis multas e penalidades. Os sites dos retalhistas são vulneráveis aos ataques por hackers, que prejudiquem as receitas de vendas on-line. Enquanto isso, o aumento de clonagem de cartões de crédito pode afectar qualquer retalhista com sistemas de pontos de venda

HOTEIS, TURISMO E LAZER

Estes sectores são susceptíveis a muitos riscos, incluindo: segurança e privacidade associado a uma base de consumidores globais a transaccionarem reservas on-line, ataques de proibição de serviço e pontos de vendas de clonagem de cartões de crédito. Infrações mediáticas das principais cadeias de hotéis que incluem o corte do funcionamento dos sistemas de pagamento e informações de cartão de crédito que são perdidos. Organizações de franchise também devem garantir que os franchisados mantêm os padrões de segurança de dados prescritos para proteger a marca de qualquer dano à reputação associada a uma segurança de dados ou infração de privacidade.

EMPRESAS DE TELECOMUNICAÇÕES

As empresas de telecomunicações são responsáveis pela segurança de grandes volumes de dados pessoais transmitidos. Existe uma directiva da UE e de muitos países em relação a empresas de telecomunicações, exigindo que tais empresas notifiquem os clientes de quaisquer infrações de dados, ou seja, aumentando os custos e as probabilidades de multas, penalidades, danos à reputação e reclamações de terceiros. As transacções de cartão de crédito significam que as empresas devem cumprir com o PCI DSS. Além disso, enfrentam vírus sofisticados que ameaçam infra-estruturas bem como a interrupção operacional e a facturação das empresas.

UTILITÁRIOS

Muitos postos de energia, barragens e condutas têm reduzido custos, por via de controlo remoto e sistemas de monitorização, mas isso aumentou as exposições cyber - às vezes agravada por más práticas de segurança. A exposição ao cyber extorsão é amplificada por ataques a redes nacionais de infra-estrutura. No estudo de Vulnerabilidade KMPG, as empresas deste sector são mais vulneráveis a serem afectadas por problemas da versão do seu software de servidor. Enquanto isso, empresas de serviços públicos colectam grandes quantidades de informações pessoais através de transacções de cartão de crédito e estão sujeitos a conformidade do PCI DSS.

INSTITUIÇÕES FINANCEIRAS

As instituições financeiras são um dos sectores mais visados por hackers e, historicamente, a maioria dos registos de infracção vieram do sector financeiro. Instituições financeiras mantêm uma quantidade significativa de dados pessoais, incluindo: nomes completos, números de telefone, endereços, informações de cartão de crédito, históricos de avaliações de crédito. A funcionalidade Online banking abriu a indústria para novas ameaças de invasão. Hacktivismo também levou a um aumento de "Denial of Service Attacks" contra processadores de pagamentos e outros serviços financeiros.

QUAIS SÃO AS OPORTUNIDADES DE VENDA?

QUAL O PERFIL DOS CLIENTES POTENCIAIS?

VENDER CYBEREDGE A COMPRADORES PELA PRIMEIRA VEZ?

COMO VENDER A MARCA AIG AO CLIENTE?

REBATENDO OBJEÇÕES

EXEMPLOS DE SINOTROS

RESUMO DE COBERTURAS

Clientes que são “compradores pela primeira vez”, que normalmente ainda não tomaram uma decisão para adquirirem um seguro cyber, precisam de entender a extensão das suas potenciais exposições e a protecção oferecida pelo seguro. Aqui seguem algumas sugestões para pontos de discussão:

INFORMA-SE SOBRE OS PERIGOS



Curta metragem de 50 segundos.

TÓPICO

COMENTÁRIO

SERÁ QUE COMPREENDEM OS RISCOS CIBERNETICOS?

Muitas empresas estão preocupadas com a exposição Cyber, mas será que têm uma visão clara de quais são os riscos, para que se possam proteger?

As empresas enfrentam riscos de hackers, hactivists, malware, funcionários negligentes e desonestos, fraca qualidade dos controlos internos informáticos. CybeEdge oferece uma protecção transparente e estruturada: assistência especializada quando as coisas correm mal, a protecção contra as consequências financeiras e também a protecção à reputação.

[VEJA O RESUMO DA COBERTURA>](#)

TÊM NOÇÃO DOS POTENCIAS CUSTOS?

Uma infracção cyber ou vazamento de dados pode dar origem a uma vasta lista de ramificações

As consequências financeiras podem ser severas: os custos de notificação, especialistas para controlar os danos, custos de crédito e monitorização de identidades, os custos de investigação, responsabilidade civil a terceiros, reputação e perda de lucros.



Curta metragem de 10 segundos

RESPOSTA RÁPIDA É ESSENCIAL

Será que a empresa entende a importância de uma resposta rápida e eficaz para a sua reputação?

A resposta da empresa nas primeiras 24-48 horas é essencial. Deve estar alinhado com os seus advogados relações publicas forenses para controlar o impacto da sua reputação perante os seus clientes, fornecedores, funcionários, investidores, reguladores e do público em geral.

PMEs: SUJEITOS A UM ATAQUE

As PME's são sensíveis ao facto da sua exposição ser muito maior dos que as empresas de maior dimensão?

As pequenas empresas podem ter uma segurança menos robusta e as iniciativas a respostas nem serem coordenadas (talvez visto como um custo excessivo) Muitas vezes são alvos oportunistas e os criminosos podem usá-los como uma porta de entrada para ataquem empresas de maior dimensão.

PME: VULNERAVEIS A DANOS

PMEs têm em consideração a sua vulnerabilidade a danos maiores após um ataque?

As pequenas empresas podem não ter acesso aos peritos legais e forenses de relações públicas após uma falha de segurança: perda de receita, a incapacidade para cobrir as despesas operacionais e danos à reputação podem ser devastadoras.

GRANDES EMPRESAS: ALVO MAIOR

As grandes empresas têm mais dados para perder e entendidas como alvos mais proveitosos.

Grandes empresas com mais dados significam que as quebras podem levar a mais registos a serem roubados e mais custos para gerir essa perda. Também são mais susceptíveis a acções colectivas por parte de accionistas e terceiros.

GRANDES EMPRESAS: MAIS DIFÍCIL DE MONITORIZAR

Pode ser mais difícil para as grandes empresas monitorizarem os milhares de funcionários que têm.

Monitorizar as actividades de funcionários (desonestos ou negligentes), roubo ou perda de hardware consequentemente a perda de informações confidenciais é muito mais difícil em grandes organizações complexas e infracções de dados podem demorar muito mais tempo de resolver.

GRANDES EMPRESAS: QUESTÕES TRANSFRONTEIRAS

Empresas com operações internacionais enfrentam desafios adicionais após uma infracção.

Partilha de informação transfronteira, mesmo dentro da mesma organização, pode resultar em custos elevados de mitigação depois de uma infracção. Custos forenses transfronteiriços e peritos legais terão que estar alinhados para apresentaram a melhor solução possível para o cliente.

As empresas, hoje, enfrentam uma grande variedade de ameaças cibernéticas, como:

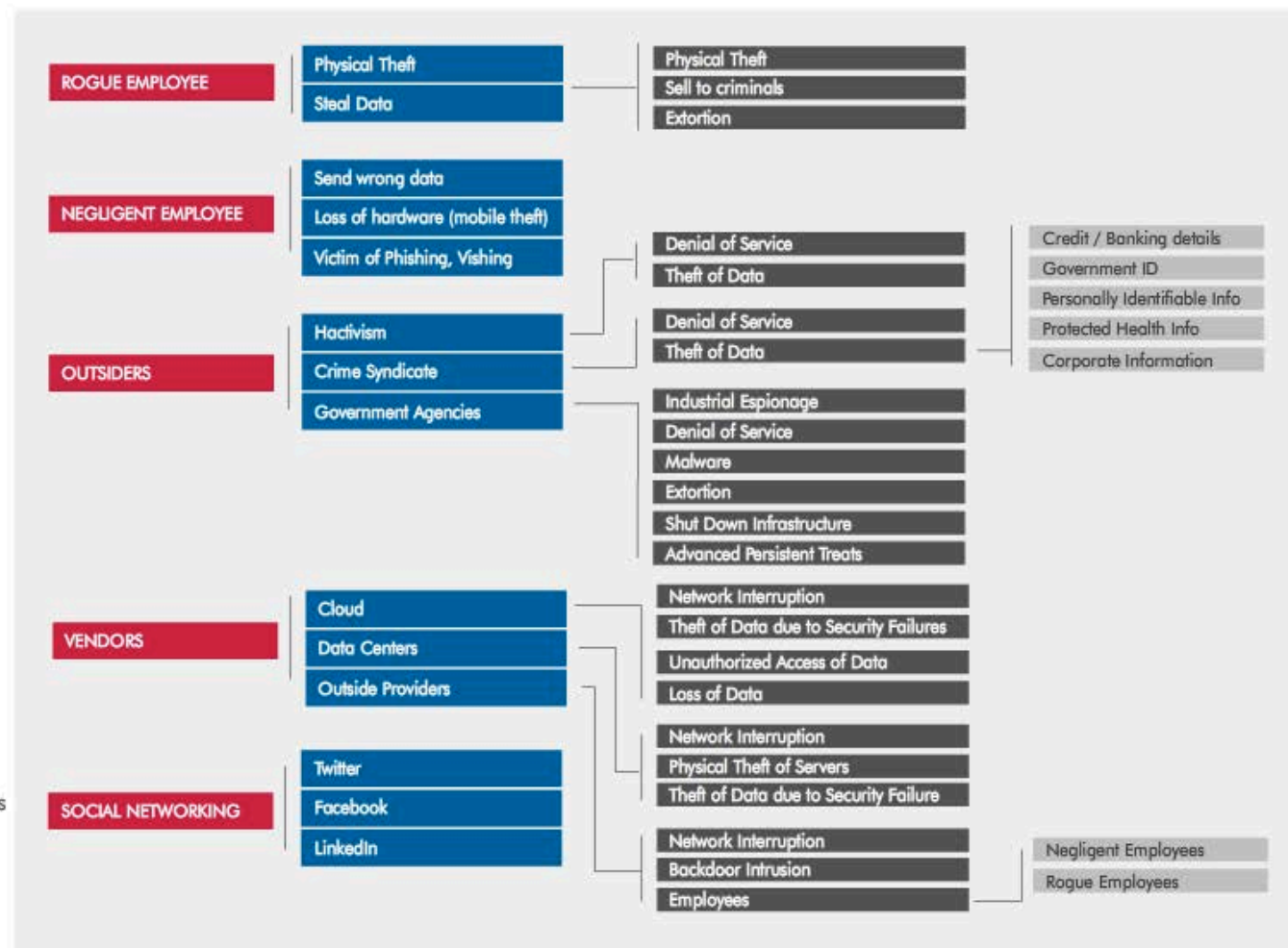
Rogue employees stealing hardware or stealing data to gain a competitive advantage or to sell on to criminal interests or for extortion.

Negligent employees sending incorrect data, losing hardware or falling victim to phishing attacks.

Company outsiders, from hackers launching denial of service attacks, to criminal syndicates stealing data, to foreign government agencies for industrial espionage.

Vendors can also expose the business. Perhaps via cloud computing permitting unauthorised access and network interruption. Or data centres and other outside providers with inadequate security.

Meanwhile social networking presents an increasing threat of backdoor intrusion into the business through employees' personal accounts.



←

QUAIS SÃO AS OPORTUNIDADES DE VENDA?

QUAL O PERFIL DOS CLIENTES POTENCIAIS?

VENDER CYBEREDGE A COMPRADORES PELA PRIMEIRA VEZ?

COMO VENDER A MARCA AIG AO CLIENTE?

REBATENDO OBJEÇÕES

EXEMPLOS DE SINISTROS

RESUMO DE COBERTURAS

Como uma das principais Seguradoras no campo dos riscos cibernéticos, construímos uma experiência rica que se reflecte na vasta amplitude da nossa cobertura e nos serviços de apoio, e nas competência e conhecimento das nossas equipas de gestão de sinistros.



Profundo conhecimento

Com mais de 10 anos de experiência na subscrição de seguros de responsabilidade cibernética a nível internacional, temos um profundo conhecimento dos riscos que as empresas enfrentam quando lidam com activos de informação. Esta experiência permite-nos assegurar a mais vasta cobertura de riscos cibernéticos que a indústria seguradora tem para oferecer.

Apoio informático especializado

Realizamos diversos processos de selecção por toda a Europa para nos certificarmos que os tomadores do nosso CyberEdge beneficiem de uma equipa de especialistas forenses e legais avançados no seu país para prestar um serviço de assistência de elevada qualidade garantida, no decurso de uma intrusão cibernética.

Inovação no produto

Temos uma equipa dedicada de subscritores, de responsabilidade na área cibernética, em campo para rever as contas dos nossos corretores e clientes. Isto significa que compreendemos quais são os receios dos nossos consumidores, e que usamos esse conhecimento para constantemente evoluir e desenvolver a cobertura das nossas apólices – é outra razão porque somos capazes de oferecer o melhor produto possível no mercado atual.

Experiência na gestão de sinistros

Desenvolvemos uma equipa de gestão de sinistros de responsabilidade cibernética avançada e a nossa estrutura globalizada permite-nos partilhar as nossas experiências de acontecimentos de segurança e privacidade à escala global. Isto significa que as nossas equipas locais são a vanguarda do conhecimento e das boas práticas com um conhecimento de todos os riscos, tendências e importância de uma resposta rápida no tratamento de assuntos relacionados com riscos cibernéticos.

Exposição internacional a riscos cibernéticos

Desenvolvemos as capacidades do nosso PassportSM, para que possamos oferecer o nosso produto CyberEdge em múltiplos países e jurisdições espalhadas pelo mundo, permitindo aos nossos clientes um acesso a peritos locais para uma eventualidade transfronteiriça relacionada com este tipo de risco.

QUAIS SÃO AS OPORTUNIDADES DE VENDA?

QUAL O PERFIL DOS CLIENTES POTENCIAIS?

VENDER CYBEREDGE A COMPRADORES PELA PRIMEIRA VEZ?

COMO VENDER A MARCA AIG AO CLIENTE?

REBATENDO OBJEÇÕES

EXEMPLOS DE SINISTROS

RESUMO DE COBERTURAS

Apesar de haver grande interesse no assunto (Exposição a Riscos Cibernéticos) entre as empresas, muitos dos obstáculos na compra devem-se a algumas incertezas das mesmas no alcance da sua exposição atual, que podem ser fortemente rebatidas em discussões do género.

NÃO PRECISAMOS – JÁ ESTAMOS SEGUROS

Não existem coberturas exaustivas para responsabilidades cibernéticas, por qualquer outra forma de seguro de responsabilidade civil. Outras apólices, tais como as de Seguro de Crime podem cobrir alguns elementos através de Atas Adicionais, mas não oferecem uma cobertura total para todos elementos de crime cibernéticos, e frequentemente estão sujeitas a taxas/comissões adicionais.

NÃO PRECISAMOS – TEMOS UMA EQUIPA DE INFORMÁTICA SÓLIDA E ROBUSTA

Nenhuma empresa está a salvo de uma ataque informático independentemente dos seus padrões de segurança, uma vez que é muito difícil monitorizar e apagar todas as ameaças internas e externas. O Software Malicioso (Malware) é frequentemente desenvolvido para retirar proveito de fragilidades de um Sistema Operativo que estão para além do controlo dos clientes e exploram o erro humano tal como deixar-se enganar por ataques de phishing e vishing.

A NOSSA INDÚSTRIA NÃO É UM ALVO DESSE GÉNERO

Criminosos cibernéticos, trabalhadores ou competidores podem muito bem estar interessados nos vossos activos digitais. Agentes criminosos frequentemente recorrem a organizações não-alvo como entradas furtivas para aceder a alvos maiores e mais apetecíveis. Se uma investigação furtiva o indiciar por causa ou meio de infiltração, estaria disposto a suportar a responsabilidade associada à transmissão de qualquer software malicioso?

O SEGURO É MUITO CARO

O valor dos prémios é muito modesto quando comparado com a dimensão potencial decorrente de um sinistro com origem em danos cibernéticos, incluindo a potencialidade agravada de lucros cessantes por dano reputacional – cifras com seis 0's não são incomuns.

NÃO PRECISAMOS – TEMOS UMA INFRAESTRUTURA ROBUSTA

PC's e materiais perdidos ou até mesmo furtados, representam um proporção significativa da violação da integridade da informação, e até com as medidas de segurança informáticas mais apertadas, se as empresas não mantêm padrões de segurança físicos apropriados, a integridade da informação continua, em grande medida, comprometida.

NÃO PRECISAMOS – NÃO ESTAMOS SUJEITOS A ESSAS PRÁTICAS REGULATÓRIAS

A Regulação apenas representa um custo isolado num incidente cibernético. As empresas têm responsabilidade para com os seus clientes de manter os seus dados seguros. A ofensa ao bom nome, no decurso de um incidente como este, pode ultrapassar qualquer custo associado ao mesmo. Ainda que sem regulação estatal, a auto-regulação nalguns sectores (como por ex.: as de cartões de crédito/débito), impõe severas penalidades aos seus associados.

NÃO PRECISAMOS – A NOSSA SEGURANÇA ESTÁ A CARGO DE PRESTADORES EXTERNOS

Muitas empresas estão a externalizar elementos de armazenamento de dados para aplicações cloud ou plataformas de entidades terceiras. Os padrões de segurança de prestadores externos devem ser frequentemente vistoriadas para certificar que mantêm os requisitos necessários – especialmente quanto à natureza da sua actividade e o volume da informação que armazenam, fazem deles um alvo apetecível. Contratos com fornecedores de segurança externos frequentemente estão limitados pela sua responsabilidade a ataques desta natureza, e por esse motivo cabe ainda às empresas suportar os seus próprios custos de defesa e de mitigação do risco.

SOMOS DEMASIADOS PEQUENOS PARA NOS PREOCUPARMOS

Enquanto as empresas grandes continuam a melhorar os seus mecanismos de segurança, os cibercriminosos começaram a procurar alvos mais pequenos e mais fáceis. 75% dos ataques a bases de dados ocorreram em empresas com menos de 100 trabalhadores. Empresas mais pequenas poderão não ter os recursos para garantir a integridade efectiva das suas bases e prevenir perdas e danos, ou mecanismos e estratégias para atenuar esses danos depois de um ataque.

OS CUSTOS DE ATAQUES CIBERNÉTICOS NÃO MERECEM SER SEGUROS

Em 2011, o custo médio para resolver as falhas de segurança de uma rede informática superaram os \$5 milhões, ou \$197 por registo. Enquanto muitas dessas falhas rondam valores inferiores à média, ataques cibernéticos custaram às empresas milhões para serem resolvidos.

NUNCA SOFRI UM ATAQUE CIBERNÉTICO, POR ISSO NÃO PRECISO DE COBERTURA

Embora a maioria dos segurados nunca participaram um sinistro, o ambiente mudou. As empresas estão hoje mais susceptíveis a ameaças à sua segurança e privacidade do que nunca. É provável que legislação futura aumente os padrões actuais da actividade seguradora sobre esta matéria, indicando que os efeitos operacionais e financeiros de um ataque cibernético poderão ficar mais onerosos para empresas que tenham sofrido, ou contribuído de alguma forma, para uma ocorrência dessas.

QUAIS SÃO AS OPORTUNIDADES DE VENDA?

QUAL O PERFIL DOS CLIENTES POTENCIAIS?

VENDER CYBEREDGE A COMPRADORES PELA PRIMEIRA VEZ?

COMO VENDER A MARCA AIG AO CLIENTE?

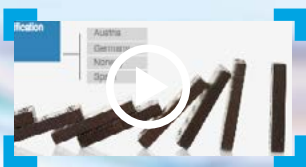
REBATENDO OBJEÇÕES

EXEMPLOS DE SINITROS

RESUMO DE COBERTURAS

Aqui estão uma série de cenários com base em factos reais que ilustram o leque de coberturas fornecidas pelo CyberEdge.

SAIBA MAIS SOBRE COMO O CYBEREDGE RESPONDE



1 minuto de filme

EXEMPLO

COBERTURA CYBEREDGE

FUNCIONÁRIO DESLEAL

- Os custos de peritos forenses para determinar quais os dados roubados e a que indivíduos.
- Os custos de notificação dos milhões de pessoas cujos dados foram roubados.
- Os custos de monitorização do crédito das pessoas afectadas de modo a certificar que não continuarão a sofrer perdas após o roubo da informação.
- Os custos de contratação de um responsável por violações legais de modo a preparar a empresa para a investigação.
- Os custos de representação e defesa da empresa na acção legal accionada contra eles.
- Os custos pelos danos imputados à empresa.

PERDIDO NOS FORNECEDORES

- Os custos de peritos forenses para determinar quais os dados roubados e a que indivíduos.
- Os custos de notificação dos indivíduos cujos dados foram roubados.
- Os custos de monitorização do crédito das pessoas afectadas de modo a certificar que não continuarão a sofrer perdas após o roubo da informação.
- Os custos de contratação de um responsável por violações legais de modo a preparar a empresa para a investigação.
- Os custos de consultoria de Relações Públicas para aconselhar e orientar a empresa nas suas comunicações externas aos media, sobre o sucedido.


HACKING - HOTEL

- Os custos de peritos forenses para determinar quais os dados roubados e a que indivíduos (cerca de meio milhão de cartões de crédito e nomes foram expostos).
- Os custos de notificação dos indivíduos cujos dados foram roubados.
- Os custos de monitorização do crédito das pessoas afectadas de modo a certificar que não continuarão a sofrer perdas após o roubo da informação.
- Os custos de contratação de um responsável por violações legais de modo a preparar a empresa para a investigação.
- Consultoria de Relações Públicas para aconselhar a empresa sobre a mitigação de danos à reputação após o incidente.

HACKING - CARD

- Os custos de peritos forenses para determinar quais os dados roubados e a que indivíduos.
- Os custos de notificação dos milhões de pessoas cujos dados foram roubados.
- Os custos de monitorização do crédito das pessoas afectadas de modo a certificar que não continuarão a sofrer perdas após o roubo da informação.
- Os custos de consultoria de Relações Públicas para mitigar de danos à reputação após o incidente.
- Os custos de contratação de um responsável por violações legais de modo a preparar a empresa para a investigação.
- Os custos de representação profissional na investigação por parte da indústria de cartões de pagamento.
- Representação legal e custos de defesa na acção legal movida contra a empresa.

MAIS EXEMPLOS >



QUAIS SÃO AS
OPORTUNIDADES DE
VENDA?

QUAL O PERFIL DOS
CLIENTES POTENCIAIS?

VENDER CYBEREDGE A
COMPRADORES PELA
PRIMEIRA VEZ?

COMO VENDER A MARCA
AIG AO CLIENTE?

REBATENDO
OBJEÇÕES

EXEMPLOS
DE SINISTROS

RESUMO DE
COBERTURAS

TEMOS MUITOS OUTROS
EXEMPLOS DE SINISTROS
CIBERNÉTICOS, INCLUINDO:

OUTLINE

SISTEMA DE UM PONTO DE VENDAS

Uma loja de um supermercado é atingido por um malware externo, desabilitando a comunicação entre as registradoras e a máquina de inventário. O supermercado ficou sem stock e teve que encerrar até que o sistema fosse corrigido e o stock reposto.

TECLAS DE GRAVAÇÃO

Mais de 200 pontos de venda em outlets (incluindo 150 filiais de uma grande cadeia de fast food) foram pirateados, permitindo a gravação de todos os dados inseridos ou o seu roubo do sistema.

TAPES DE BACK UP

Uma companhia de seguros multinacional foi punida com uma multa de milhões de libras, pelo regulador do Reino Unido, quando perdeu uma cópia de segurança com informações particulares de mais de 46 mil segurados.

OPERAÇÕES CRIMINAIS

Durante 4 anos uma operação criminosa roubou informações, propriedade de várias das maiores organizações de petróleo e gás. Tinham sido implementadas palavras-chave que filtravam correspondências e dados relevantes da indústria em matérias específicas incluindo exploração de petróleo e propostas de parcerias entre as organizações infectadas.

QUAIS SÃO AS OPORTUNIDADES DE VENDA?

QUAL O PERFIL DOS CLIENTES POTENCIAIS?

VENDER CYBEREDGE A COMPRADORES PELA PRIMEIRA VEZ?

COMO VENDER A MARCA AIG AO CLIENTE?

REBATENDO OBJEÇÕES

EXEMPLOS DE SINISTROS

RESUMO DE COBERTURAS

O CyberEdge garante um amplo leque de respostas desde violação de informação até a tentativas de extorsão.

It delivers rapid forensics - to find out exactly what data has been affected and, if at all possible, restore it.

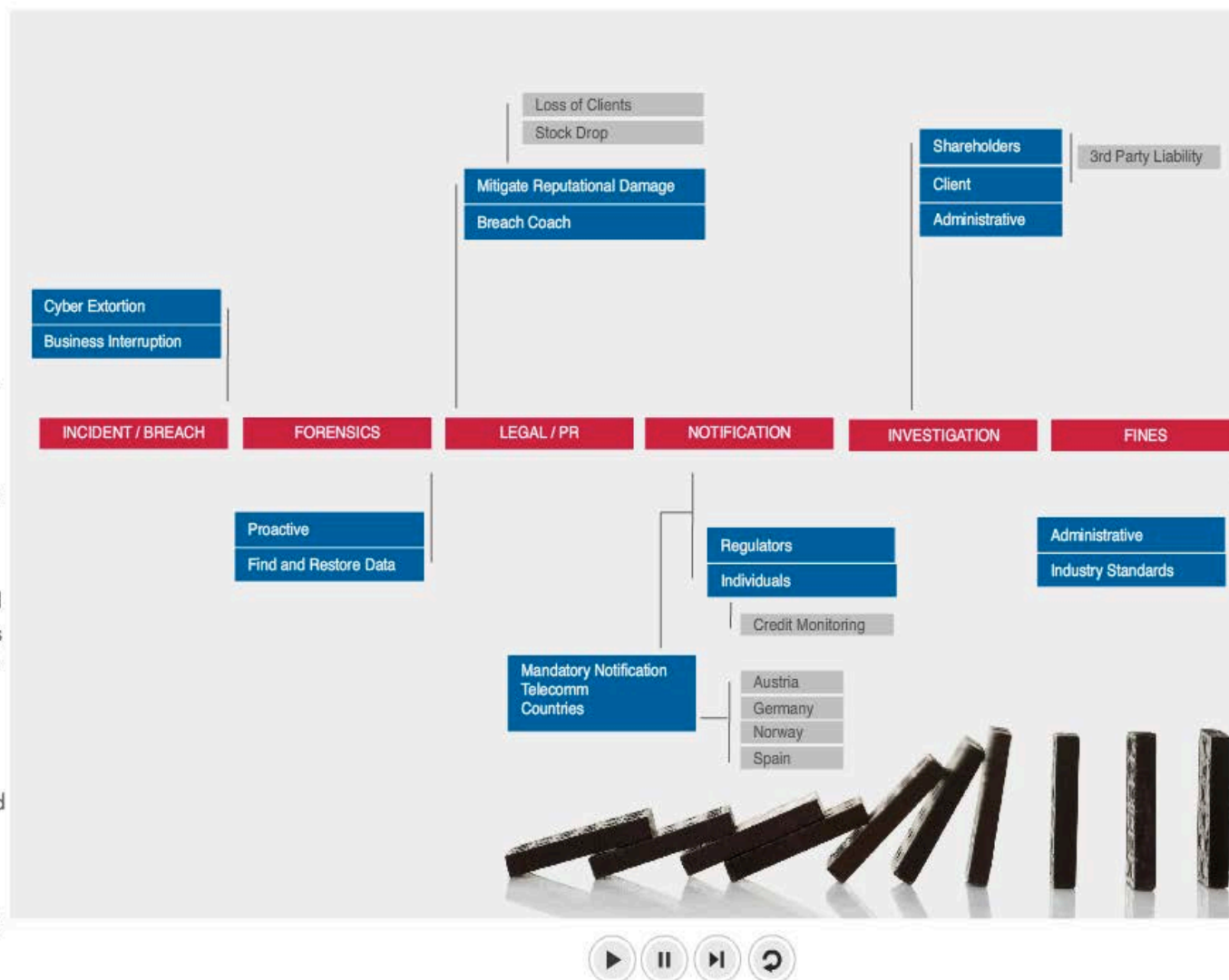
It provides expert legal and communications support, from a "breach coach" to oversee the company's response to PR expertise to contain reputational damage.

We cover notification costs – some countries have mandatory requirements, so the business must individually contact and inform anyone whose data has been affected

And we cover the costs of credit monitoring for the impacted individuals as well, to make sure they suffer no ongoing losses after the breach

We cover the costs of preparing for and professionally representing the business at any subsequent investigation into the breach. And we also cover the third party liabilities and insurable fines and penalties resulting from it.

Finally CyberEdge can also be extended to cover the business interruption caused by a security failure, with the option to extend coverage for system failure or prevention of access to Cloud services.



Aqui está um resumo das coberturas facultadas pelo CyberEdge. (Note que é apenas um resumo para orientação geral e que não substitui os termos e condições da apólice).

CUSTOS FINANCEIROS

Custos de notificação dos clientes (ou da autoridade reguladora) de que os seus dados foram roubados. Custos razoáveis de formação em roubo de identidade e de monitorização de crédito das pessoas afectadas.

Custos de defesa e danos se a empresa (ou a empresa em outsourcing) permitir a fuga de dados pessoais ou corporativos

Custos de defesa e danos caso a empresa contamine dados de terceiros com um vírus.

Custos de defesa e danos caso seja roubado á empresa um código de acesso ao sistema, por meios não electrónicos.

Custos de notificação dos clientes (ou da autoridade reguladora) de que os seus dados foram roubados. Custos razoáveis de formação em roubo de identidade e de monitorização de crédito das pessoas afectadas.

Custos de defesa e danos se a empresa (ou a empresa em outsourcing) permitir a fuga de dados pessoais ou corporativos.

Custos de defesa e danos caso a empresa contamine dados de terceiros com um vírus.

Custos de defesa e danos caso seja roubado á empresa um código de acesso ao sistema, por meios não electrónicos.

Custos de defesa e danos caso seja roubado á empresa um código de acesso ao sistema, por meios não electrónicos.

Custos de defesa e danos caso a empresa sofra um roubo de hardware que contenha dados pessoais.

Custos de defesa e danos caso um empregado da empresa desencadeie uma divulgação de dados.

Custos de aconselhamento jurídico e representação em conexão com uma investigação de protecção de dados.

CUSTOS FINANCEIROS DE LEGISLAÇÃO DE PROTEÇÃO DE DADOS

SERVIÇOS DE CONSULTADORIA

CONSULTORIA DE ESPECIALISTA EM IT DURANTE E APÓS O ATAQUE CIBERNÉTICO

Uma equipa de resposta a incidentes cibernéticos para assistir o cliente caso este julgue estar a ser alvo de um hacker.

Assistência especializada após uma violação de dados dos tomadores de seguro, para que a empresa possa recuperar os seus sistemas e firewalls e regressar ao seu negócio habitual.

Os custos de honorários incorridos para determinar que os dados electrónicos podem, ou não, ser restaurados, recolhidos ou recriados.

CONSULTORIA ESPECIALIZADA PARA PROTEGER E RECOMPOR A REPUTAÇÃO DA EMPRESA APÓS UM ATAQUE CIBER

Custos de consultoria profissional de modo a evitar ou minimizar os efeitos potencialmente adversos de um ataque cibernético significativo.

Os custos de consultoria profissional de modo a minimizar potenciais danos à reputação de qualquer indivíduo na empresa (por exemplo o Responsável de Informação).

COBERTURAS ADICIONAIS

OPÇÃO DE INTERRUPÇÃO DE REDE

Perda de lucro líquido, como resultado de uma interrupção material na rede do segurado, causada por uma falha de segurança.

OPÇÃO DE EXTORSÃO CIBERNÉTICA/ PRIVACIDADE

Pagamento de resgate (perda por extorsão) a terceiros envolvidos em terminar uma ameaça à segurança.

OPÇÃO DE RESPONSABILIDADE MULTIMEDIA

Danos e custos de defesa relacionados com a violação de propriedade intelectual de terceiros ou negligência ligada a conteúdos electrónicos.



www.aig.com

AIG EUROPE LIMITED – Sucursal em Portugal

Av. Liberdade, 131 – 3º

1250-140 Lisboa

Email: portugal-geral@aig.com



Bring on tomorrow

American International Group, Inc. (AIG) é uma organização mundial líder em seguros que presta serviços a clientes em mais de 130 países e jurisdições. As Empresas que integram o Grupo AIG servem clientes empresariais, institucionais e individuais, através de uma das mais extensas e inigualáveis redes de seguros não-vida à escala global da indústria. Para além disso, as empresas do Grupo AIG são líderes em Seguros Vida e gestão de Fundos de Pensões nos Estados Unidos. As acções da AIG estão cotadas na bolsa de Valores de Nova Iorque e de Tóquio.

AIG é a designação comercial para as actividades seguradoras Vida e Não-Vida à escala global do American International Group, Inc. Para mais informações, por favor visite o nosso sítio da internet www.aig.com. Os Produtos e serviços são subscritos e fornecidos por subsidiárias e afiliadas do American International Group, Inc. Na Europa, o nosso principal segurador é a AIG Europe Limited. Este material tem apenas e somente fins informativos. Nem todos os produtos e serviços se encontram disponíveis em todos os países e jurisdições, e a cobertura de seguro é estabelecida nos termos e condições previstos na apólice ou no contrato de seguro. Alguns produtos e serviços poderão ser fornecidos por entidades terceiras independentes. Os nossos seguros poderão ser comercializados através de entidades afiliadas ou não do Grupo AIG. Algumas coberturas de Danos e Responsabilidade Civil poderão ser providenciadas por Seguradoras de Linhas de Excesso. As Seguradoras de Linhas de Excesso não participam, em regra, nos fundos de garantia do Estado e, por conseguinte, não estão protegidas por esses mesmos fundos.