
# Ransonware Reorientado

## Por que a gestão de crises está no coração da resiliência contra ransomware

accenture

# Segurança orientada pelo negócio

Para muitas organizações, ransomware é visto como um problema tecnológico ou de segurança – não uma questão a ser enfrentada pela empresa, para o negócio.

**Numa época de transformação digital intensiva, as organizações devem ajustar considerações em torno do papel da segurança após um ataque de ransomware. Estratégias de recuperação existentes que estejam voltadas para planos tradicionais de continuidade do negócio não são mais suficientes. Ao compreender – e se preparar para – as implicações de ransomware na companhia inteira, as empresas líderes podem se recuperar mais rapidamente após a ocorrência de um ataque. Em suma, uma resposta moderna a um ataque de ransomware e uma extorsão deverá ser tratada como um risco de negócio que exige priorização de uma gestão de crises efetiva.**

## Principais desafios

1. Planos tradicionais de reação a crises precisam evoluir – ransomware é um risco para os negócios, não apenas um problema de segurança.

2. Planos existentes de comunicação de crises carecem de transparência e agilidade para se adaptar às novas complexidades cibernéticas.

3. Ransomware não tem limites – impacta a empresa, o amplo ecossistema e os vários *stakeholders*.

# Ransomware como um problema de negócios

# A evolução do ransomware

Em nossa pesquisa O estágio da resiliência cibernética 2021, verificamos não apenas que os ataques estão aumentando, mas também que 20% dos custos associados a todos os incidentes eram atribuídos a prejuízos na reputação da marca. A recomendação? Chegar ao equilíbrio certo entre os esforços de segurança e o alinhamento com a estratégia da empresa.

Imediatamente após um ataque de ransomware, é vital compreender as prioridades da companhia. No entanto, é comum a indefinição quanto a quem detém a autoridade para a tomada de decisão ou responsabilidade geral, o que pode atrasar os esforços de reação e recuperação.

Definir a linha de frente de uma estrutura de gestão de crises envolve a identificação de limites de tomada de decisão alinhados à estratégia da empresa, à tolerância a riscos da organização, à estratégia de comunicação cibernética e à clara responsabilidade tanto pelas decisões técnicas quanto empresariais durante um evento de crise. Além disso, é essencial revisar regularmente esse critério de tomada de decisão e ajustá-lo periodicamente a fim de mantê-lo alinhado com o ritmo de mudança organizacional.

Da definição da estratégia de comunicação à implementação de uma abordagem equilibrada de combate a ameaças e sua eliminação – ou à discussão de pagar ou não um resgate –, documentar e seguir um roteiro de decisão durante crises pode ajudar organizações a se preparar melhor, acelerar as respostas e, em última instância, amenizar as pressões das demandas extorsivas.

### Respostas prioritárias

- O que precisa ser consertado primeiro?
- Quais são os sistemas ou dados mais importantes a restaurar?
- Do que dependem as receitas da companhia?
- Que dependências anteriores existem entre pessoas, processos e componentes tecnológicos?

# Vamos dar uma olhada em três desafios-chave que destacam a necessidade de um alinhamento maior entre segurança e a empresa, antes, durante e depois de um evento de crise cibernética:

1

**Planos tradicionais de resposta a incidentes cibernéticos precisam evoluir – ransomware é um risco para a companhia, não somente um problema de segurança.**

A resposta a crises na empresa é atividade exercida em equipe e requer uma função de gestão de crises focada nos negócios para lidar com eventos destrutivos modernos.

2

**Comunicações de crise carecem de transparência e agilidade para se adaptar às novas complexidades cibernéticas.**

Uma estrutura de tomada de decisão pré-definida, associada a um maior entendimento do setor, suas regulamentações e seus clientes, pode dar apoio a comunicações de crise mais robustas.

3

**Ransomware não tem limites – impacta a empresa, o ecossistema de terceiros e os vários *stakeholders* da empresa.**

À medida que a superfície de ataque cresce, a resposta às crises precisa se ampliar para enfrentar impactos em consumidores, subsidiárias corporativas, fornecedores, terceiros, portfólio de investimentos e alvos de fusões e aquisições.

Desafio

1

# Planos tradicionais de resposta a incidentes cibernéticos precisam evoluir – ransomware é um risco para a empresa, não um problema de segurança

Estratégias de recuperação em planos tradicionais de continuidade de negócios e retomada pós-desastre não são mais suficientes para lidar com modernos ataques de ransomware.

A abordagem atual das equipes de segurança para reação a incidentes tipicamente envolve resolver os aspectos da investigação técnica de um ataque – como o hacker invadiu os sistemas? Quais sistemas foram afetados? Quais dados foram extraídos e de onde?

Mas ataques não são simplesmente um problema de segurança. A resposta a incidentes também precisa considerar processos de negócio críticos e como eles impactam as prioridades da recuperação – até onde a cadeia de valor foi afetada? Qual a quantidade de produtos que temos em estoque?

## Desafio 1

Quais os impactos nos empregados, clientes e fornecedores? Qual é nossa exposição financeira?

Fundamental para uma recuperação bem-sucedida após um ataque de ransomware é levantar e estabilizar primeiro os sistemas e operações mais críticos, depois dar atenção ao resto das atividades. Deixar de priorizar estas dependências de negócio significa ficar nas mãos dos criminosos. Por exemplo, táticas recentes de invasão incluem deletar ou danificar backups tornando-os indisponíveis – o que subverte os planos tradicionais de continuidade de negócios ou de recuperação pós-desastre.

Priorizar e estabilizar operações e sistemas vitais pode ajudar a evitar impactos posteriores adicionais de ordem financeira, reputacional, operacional e física.

As empresas devem melhorar as abordagens tradicionais de continuidade de negócios e resposta a incidentes. Com colaboração mais ampla, CISOs, COOs e outros líderes seniores podem desenvolver um plano coeso que identifique as prioridades para a empresa inteira, resolver o problema no âmbito geral e se preparar melhor para uma restauração do negócio ágil e inclusiva.

**Ao adotar um plano de comunicação robusto, os líderes podem enfrentar o ransomware pelo que ele é: uma crise que necessita ser tratada de maneira focada na empresa.**

Desafio

2

# Comunicações de crise existentes carecem de transparência para se adaptar às novas complexidades cibernéticas

Em qualquer escala, incidentes de ransomware são disruptivos e precisam de um plano de comunicação efetivo. Mas não se trata de evento com início e fim – atualizações regulares compartilhadas com *stakeholders* internos e externos são vitais para se antecipar a quaisquer desdobramentos da ocorrência.

Estas comunicações deverão muitas vezes não apenas balancear a velocidade com a precisão das informações durante um evento em rápida evolução, mas também ser apropriadas para os diferentes perfis de *stakeholders*. Entender as demandas exclusivas de um setor, sua regulamentação e as notificações e divulgações que forem aplicáveis é fundamental.

Entretanto, muitos líderes de empresa podem estar mal preparados quando o assunto é comunicação. Embora organizações possam lidar com incidentes de segurança de forma eficiente, caso os executivos não comuniquem a situação adequadamente, elas podem estar sujeitas a uma campanha pública de desinformação ou risco de erosão da confiança na empresa – ou perder credibilidade junto aos clientes.

## Desafio 2

Todo plano de comunicação tem características próprias, dependendo das obrigações informativas. E as indústrias precisam de estratégias customizadas – por exemplo, o roubo de dados de saúde envolve notificar os pacientes, assim como um banco pode ter de priorizar os rigorosos requisitos de autoridades reguladoras financeiras em todo o mundo.

À medida que as organizações buscam por confiança digital junto a consumidores e as pessoas se tornam mais conscientes de preocupações com a privacidade, fica ainda mais importante ser transparente e honesto sobre os fatos ocorridos e o que acontecerá a seguir – interna e externamente.

Recorrer a uma resposta tradicional de comunicação corporativa isolada do resto das atividades não será suficiente. A colaboração com profissionais de segurança, equipes jurídicas e o ecossistema da empresa ampliado garante que as equipes de comunicação tenham uma abordagem estruturada e que ajam com transparência de modo ponderado e factual.

### Perguntas-chave

- O que aconteceu?
- Quando aconteceu?
- O que sabemos?
- O que estamos fazendo a respeito?
- Quem foi impactado e como?
- O que fazer a seguir?

# Nossa rápida abordagem para comunicação de crises cibernéticas

A Accenture desenvolveu uma abordagem para resposta e recuperação após ataques de ransomware a fim de conduzir comunicados de crises cibernéticas:

**1. Selecionar e preparar**

Identifique as partes impactadas e alinhe os objetivos da reportagem, o tom, o timing, a audiência e os requisitos de notificação.

**2. Desenvolver e aprovar**

Desenvolva mensagens alinhadas à estratégia de comunicação, identifique os meios para cada grupo de *stakeholders* e obtenha as aprovações.

**3. Se posicionar e implantar**

Reforce as mensagens, treine os funcionários, estabeleça monitoramento e monte uma força tarefa de comunicação verticalmente integrada.

**4. Monitorar e avaliar**

Empregue uma abordagem rápida para avaliar e reiterar por meio de atualizações baseadas em métricas definidas, análises de sentimentos, cobertura da mídia e impactos financeiro e sobre a marca.

Desafio

3

# Ransomware não tem limites – impacta a empresa, os ecossistemas de terceiros e múltiplos *stakeholders*

Muitas vezes, a destruição causada pelo ransomware se estende além da encriptação dos dados – os sistemas caem, os clientes não podem ser contatados, e o negócio é suspenso.

De fato, como resultado do impacto sobre a infraestrutura vital das organizações em 2021, autoridades legais e governos envolveram-se ainda mais no combate aos ataques de ransomware. Por exemplo, o Office of Foreign Assets Control (OFAC), uma agência de inteligência financeira e de cumprimento de leis do Departamento do Tesouro norte-americano, lançou um novo guia em setembro de 2021 alertando companhias de que pagar ou facilitar o pagamento de resgate a uma entidade legalmente interditada sujeitará os pagadores a penalidades civis.[1] Pela primeira vez, o Departamento do Tesouro recentemente interditou uma agência russa de câmbio de moeda virtual.[2] Estas e outras ações das autoridades federais colocaram os atacantes sob pressão para encontrar novas formas de rentabilizar suas ações.

Por conta disso, os hackers evoluíram suas táticas. Em alguns casos, eles focaram menos na encriptação e destruição e mais no roubo de dados e posterior extorsão da vítima com ameaças de divulgar os

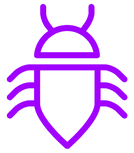
## Desafio 3

dados roubados. Esta abordagem provoca impacto rápido e dificulta a identificação dos criminosos.

Hoje em dia, você pode comprar acesso a malware e simplesmente executar um ataque ransomware ao se tornar um "associado" de programas ransomware-as-a-service (RaaS) disponíveis em fóruns criminosos. Um associado precisa apenas provar suas habilidades técnicas a grupos de ransomware para começar a distribuir ransomware e receber pagamentos. Para agravar este desafio, a transformação digital intensiva ampliou a superfície de ataque – como deixa claro o aumento de três dígitos no número de ataques observados em 2021.[3]

Apesar da intensificação da percepção, das ações governamentais e da colaboração das indústrias, ransomware não tem limites e continua sendo uma ameaça persistente. Qualquer estratégia de resposta a crises deverá considerar a variedade de *stakeholders* afetados – clientes, subsidiárias corporativas, fornecedores, terceiros confiáveis, investimentos financeiros e alvos de fusões e aquisições. Por outro lado, a estratégia de resposta também deverá abordar como responder quando qualquer um destes *stakeholders* for atacado. Por exemplo, muitas empresas adotam um serviço de folha de pagamento terceirizado. Qual a reação apropriada quando uma entidade *stakeholder* vital for impactada?

**Aumento anual de 107% nos ataques de ransomware e extorsões**



**33% de volume de invasões por ataques de ransomware e extorsões**

**Os cinco países mais afetados: 47% de ataques de ransomware impactaram organizações instaladas nos EUA, seguidos pela Itália (8%), Austrália (8%), Brasil (6%) e Alemanha (6%).**

Fonte: Accenture Cyber Investigations, Forensics & Incident Response Engagements

# De volta ao normal

Apesar da implementação de técnicas de encriptação em pontos adequados, uma empresa líder do setor de manufatura experimentou um ataque de ransomware devastador. A companhia enfrentou uma crise dramática – ficou impedida de produzir, despachar e vender qualquer um dos seus produtos. Suas cadeias de suprimento foram interrompidas. Os funcionários ficaram incapacitados de logar seus computadores. Ninguém conseguia atender ligações dos consumidores nos call centers. E arquivos essenciais, tais como detalhes necessários para concretização de uma negociação financeira no período de quatro semanas seguintes, ficaram inacessíveis. Para piorar, o CEO foi informado de que duas localizações de backup também haviam sido afetadas.

A Accenture trabalhou em conjunto com os executivos do cliente para resolver o impacto do ataque da seguinte forma:

- Gerenciando aspectos tecnológicos vitais – depurando sistemas, fornecendo garantia razoável de que o hacker não estava mais atuando e reconstruindo os sistemas na sequência certa.

- Focando no comitê executivo da companhia – estabelecendo um profunda conexão entre a equipe de cibersegurança e a estratégia de negócio da empresa.

- Executando um plano de comunicação efetivo – dirigido aos funcionários, clientes e *stakeholders* parceiros.

- Empregando um *playbook* inédito – identificando claramente as áreas de negócio onde as ações precisavam ser priorizadas.

A equipe restaurou os sistemas de negócio mais críticos – produção, distribuição e call centers de atendimento aos clientes – durante a primeira semana. As demais operações foram restabelecidas e todas as fábricas estavam de novo online em apenas quatro semanas.

# Modernização da resposta contra ransomware

**Alguns passos vitais para ajudar a gerenciar e modernizar uma resposta contra ransomware:**

Passo 1

## Ampliar a prontidão da empresa

Entenda a sua cadeia de valor ao longo de cada área da empresa e quais seriam suas prioridades no caso de um ataque. As organizações devem conhecer com confiança e consistência as muitas partes móveis que as tornam rentáveis.

Processos de negócio vitais, suas sustentações e dependências posteriores são geralmente mal entendidos ou negligenciados num típico plano de resposta a incidentes.

**Por exemplo:** produtos despachados podem depender de uma impressora de etiquetas num centro de distribuição – assim, tornar essa ação operacional, em vez de consertar alguns dos maiores sistemas ou equipamentos, pode ser o modo mais rápido de minimizar a disrupção.

Passo 2

## Comunicar abertamente com cuidado

Defina uma estratégia de comunicação que seja ágil e que leve em consideração as complexidades de um evento cibernético a partir de uma perspectiva técnica e de negócio.

As organizações devem ser cautelosas a fim de evitar compartilhar informação incorreta, e isso por vezes depende do setor. Então, é essencial verificar todos os fatos, estabelecer o tom e ser ponderado antes do processo de comunicação começar pra valer.

**Por exemplo:** Em serviços financeiros, informações de cartões de crédito roubadas estarão sujeitas a rigorosa regulamentação e exigências de conformidade antes que o público em geral tome conhecimento da violação.

**Passo 3**

# Trazer CEO e *board* a bordo

Testar e validar a prevenção, detecção e resposta contra ataques e a recuperação é uma condição de vida para a maioria das organizações, mas este passo prático pode ser reforçado com o envolvimento do CEO e do *board*.

Exercícios de simulação são geralmente empreendidos pelo pessoal da segurança. Ao evoluir tais exercícios a fim de incluir simulações de nível executivo, as organizações podem não apenas testar suas defesas contra um típico ataque de ransomware, mas também introduzir o risco e a adrenalina de um verdadeiro cenário de ataque.

**Por exemplo:** Os executivos poderiam ser informados de que três linhas de negócio tiveram suas operações interrompidas devido a um ataque, e que o invasor está exigindo resgate de US$ 10 milhões. É pedido aos executivos que determinem em tempo real quais linhas de produção deverão ser restauradas, como comunicarão sua resposta e quem será responsável por tomar essas decisões.

# Você está preparado?

A evolução dos eventos de ransomware e extorsões requer um modo de pensar diferente – um que se concentre na empresa e na segurança.

Pergunte a si mesmo:

- Nossos executivos de negócio estão alinhados com as equipes da segurança para lidar com crises de ransomware?
- Temos os planos de comunicação corretos para promover uma resposta efetiva?
- Estabelecemos os fatores de decisão baseados em risco no caso de uma interrupção?
- Que ações podemos tomar e quais processos podemos implementar hoje que nos ajudarão a restaurar as atividades mais rápido?
- Qual é nosso limite financeiro caso não consigamos despachar a produção?
- Quanto da produção precisamos manter em reserva se não pudermos produzir durante três dias?

Com capacidades de gestão de crises mais ágeis, robustas e transparentes, as empresas podem enfrentar melhor eventos de ransomware e aumentar a resiliência cibernética geral.


# Autores

**Robert Boyce**
Diretor executivo,
Accenture Security
Líder de Global Incident
Response & Transformation

Robert Boyce

@therobertjboyce

**Ryan Leininger**
Gerente sênior,
Accenture Security
Líder de Global Proactive
& Readiness Services

Ryan Leininger

## Referências


1. Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments, U.S. Department of Treasury
2. Treasury Takes Robust Actions to Counter Ransomware, U.S. Department of the Treasury
3. Pesquisas, investigações forenses e compromissos de resposta a incidentes conduzidos pela Accenture entre janeiro e dezembro de 2021.


## Sobre a Accenture

A Accenture é uma empresa global de serviços profissionais, com liderança nas capacidades de digital, cloud e segurança da informação. Combinando experiência ímpar e competências especializadas em mais de 40 indústrias, oferecemos serviços de Strategy e Consulting, Interactive, Technology e Operations – impulsionados pela maior rede de centros de tecnologia avançada e operações inteligentes do mundo. Nossos 699 mil profissionais cumprem a promessa da tecnologia e da criatividade humana todos os dias, atendendo a clientes em mais de 120 países. Nós abraçamos o poder da mudança para criar valor e sucesso compartilhado com nossos clientes, pessoas, acionistas, parceiros e comunidades. Visite-nos em **www.accenture.com**

## Sobre a Accenture Security

Accenture Security é uma provedora líder de serviços de cibersegurança end-to-end, incluindo defesa cibernética avançada, soluções de segurança cibernética aplicada e operações de segurança gerenciadas. Trazemos inovação em segurança, associada a escala global e a uma capacidade de entrega mundial por meio de nossa rede de centros de tecnologia avançada e operações inteligentes. Com nossa equipe de profissionais altamente especializados, possibilitamos aos clientes inovar com segurança, construir resiliência cibernética e crescer com confiança. Siga-nos @AccentureSecure no Twitter ou visite-nos em **www.accenture.com/security**



220023