

Caiu o sinal? Uma análise da gestão de crise envolvendo ataques *hackers* no caso da Record TV¹

Fernanda Shelda de Andrade MELO²

Universidade Federal de Minas Gerais, Belo Horizonte, MG

Resumo

Em outubro de 2022, um ciberataque atingiu a Record TV. Além do bloqueio de materiais da empresa e danos ao acervo da programação midiática, uma segunda invasão expôs arquivos de funcionários da organização, juntamente de documentos internos. Todo esse contexto, permeado de dúvidas dos telespectadores e de cobranças da imprensa, pauta lógicas de uma crise com possíveis afetações à reputação da organização. Nesse sentido, o presente resumo expandido procura analisar o ciberataque ao considerar as escolhas discursivas e as reverberações do caso, verificando posicionamentos adotados e as disputas de sentido durante o desenrolar da crise.

Palavras-chave

Ciberataques; cobertura midiática; comunicação organizacional; disputas de sentido; gestão de crise.

Introdução

Em outubro de 2022, telespectadores que assistiam à Record TV, mais especificamente o programa Fala Brasil, puderam perceber em tempo real instabilidades que afetaram a rede televisiva durante um ataque *hacker*. Esse impacto não foi percebido somente na exibição do jornal, como também nos dias seguintes da programação da emissora que teve seu acervo afetado e documentos bloqueados de seu sistema, ação comum nos crimes cibernéticos que inserem *ransomwares*. Como a tradução literal da palavra indica, *ransomware* é uma estratégia de cibercrime que criptografa e/ou sequestra arquivos, com objetivo de conseguir um *resgate* – na

¹ Trabalho apresentado ao Grupo de Pesquisa Discurso, Identidade e Relações de Poder, atividade integrante do XX Congresso Brasileiro Científico de Comunicação Organizacional e Relações Públicas.

² Doutoranda e Mestre no Programa de Pós-Graduação em Comunicação Social da Universidade Federal de Minas Gerais (UFMG). E-mail: fernandashelda@ufmg.br.

maioria das vezes financeiro (Beaman *et al.*, 2021). Essa crise, que em um primeiro momento parece evocar lógicas de uma crise operacional, pois interrompe a prestação de serviços e o funcionamento da empresa (Benoit, 2015), perdurou por dois dias.

A surpresa, especialmente para a própria organização, é que cinco dias depois do restabelecimento dos sistemas um novo ataque volta a ocorrer (15/10/2022), retirando do ar plataformas ligadas à TV, como a assinatura PlayPlus. Pela segunda vez no mesmo mês, uma nova crise se instaura na empresa – e, dessa vez, com um grupo *hacker* assumindo a autoria do evento e divulgando arquivos internos da organização – como documentos pessoais de jornalistas da emissora, bem como planilha de pagamentos de anunciantes. Nesse momento, acreditamos que a crise também possui fortes indícios de uma paracrise (Benoit, 2015), ao afetar diretamente a imagem da empresa, projetando um ambiente inseguro na repetição do caso.

Na organização, um momento delicado e de vulnerabilidade, incluindo a perda de materiais importantes de entretenimento e também jornalísticos. Para os consumidores, insatisfação com os serviços e a falta de acesso ao material pago, como no caso do canal por assinatura. Na imprensa, cobrança por esclarecimentos e críticas à falta de informações. Em suma, uma crise organizacional pode envolver diversos atores em disputa com seus discursos que podem criar e reproduzir sentidos. No contexto permeado pelas lógicas digitais, incluindo questões como dados, privacidade e o universo dos crimes cibernéticos, imaginários específicos também podem rondar decisões tomadas no caso. Falar ou não falar, além de colocar em xeque sua relação com os consumidores e com as regulações jurídicas envolvendo incidentes cibernéticos são elementos tensionados e que podem exhibir descobertas nos estudos organizacionais, como os discursos distintos que permeiam um cenário de risco em um mundo cada vez mais dependente de sistemas digitais vulneráveis.

O objetivo deste trabalho foi delimitado em analisar o ciberataque envolvendo a empresa midiática Record TV, considerando suas escolhas discursivas e as reverberações do caso enquadrado como uma crise organizacional. A metodologia contém caráter exploratório, verificando os posicionamentos adotados pela organização. De antemão, podemos verificar que a Record não realizou publicações ou emitiu avisos para os consumidores em outubro de 2022, contendo uma divulgação interna sobre o acontecimento apenas no mês seguinte. Dessa forma, nosso recorte metodológico se baseou, especialmente, na cobertura da imprensa, com a revelação

do caso e a exposição de materiais que teriam sido compartilhados apenas com funcionários, em uma função semelhante à lógica de *watchdog*³.

Podemos afirmar, então, que o *corpus* analisado faz parte de uma estratégia muito mais interna da empresa, enquanto seu posicionamento público foi silencioso. Considerando a limitação espacial e temporal da produção de um resumo expandido, separamos as próximas discussões em uma breve seção teórica, apresentando bases fundamentais na construção deste estudo. Em seguida, exibimos os principais resultados e as discussões em destaque pelos achados empíricos. Reforçamos que um dos principais destaques está na utilização do silêncio como ponto-chave.

Base teórica

Acreditamos que seja fundamental pontuar alguns aspectos que cercam esse cenário. Em primeiro lugar, definir ciberataques é uma tarefa complexa e usualmente parte de elementos técnicos da área de computação. Por isso, delimitamos esse entendimento breve enquanto a invasão de um sistema que pode ocorrer em grupos organizados ou individualmente com objetivos distintos – podem ser tanto financeiros, como com o foco de atingir a credibilidade das vítimas. A estratégia aplicada também pode variar: bloqueio ou roubo dos dados, espionagem e outras medidas podem ser aplicadas a depender do propósito (Quader; Janeja, 2021).

Isso também significa que o ataque ocorrido na Record, o *ransomware*, não é o único tipo nem categoria usada pelos *hackers*. Porém, são crescentes no Brasil: um relatório da Kaspersky⁴ enfatizou o aumento dessa tática no país, com um crescimento de 69% de ocorrências em 2025 quando comparada com o ano anterior. Além disso, pontuamos que apesar de alguns esforços acadêmicos sugerirem o abandono da palavra *hacker* ou mudanças na sua classificação, nós permanecemos enfatizando o termo pela percepção de que ele ainda é socialmente usado no imaginário popular mesmo que, geralmente, em uma ideia de vilania (Melo, 2025).

Percorremos, também, pela ideia de crise organizacional. Entendemos que uma crise pode alcançar as organizações a partir da quebra de expectativas em relação aos riscos prévios que foram mal gerenciados: Sellnow e Seeger (2013) exemplificam o caso da indústria alimentícia.

³ Ideia da imprensa enquanto “cão vigilante” que monitora os acontecimentos de interesse público.

⁴ Kaspersky: novo estudo mostra aumento das vítimas de ransomware no Brasil. Kaspersky, 2025. <https://www.kaspersky.com.br/about/press-releases/kaspersky-novo-estudo-mostra-aumento-das-vitimas-de-ransomware-no-brasil>. Acesso em 26 dez. 2025.

Esse setor deve fornecer comida segura, mas uma contaminação que afete consumidores pode resultar na ruptura daquilo que é socialmente aceito e esperado, causando desordem. Dessa forma, “uma crise pode ser definida como um evento específico, inesperado e não rotineiro, ou uma série de eventos, que gera altos níveis de incerteza e uma ameaça significativa, percebida nos objetivos de alta prioridade” (Sellnow; Seeger, 2013, p. 7). Mencionamos na introdução deste trabalho a indicação das tipologias de crise organizacional – envolvendo a lógica de Benoit (2015) para operacionalização e paracrise. Em ambas as situações, as empresas precisarão trabalhar com ações discursivas durante o desenrolar do acontecimento, tanto na ideia de evitar efeitos negativos à reputação, como para contenção de maiores danos.

Assim, outro aspecto importante nesta pesquisa é entender estratégias que muitas vezes são usadas nessa gestão, como as ideias de compensação, mortificação e afins (Coombs, 2019). Ainda enfatizamos que o ator central do resumo é uma empresa de comunicação e, como tal, enseja uma base de comunicólogos que pode exibir uma práxis da área. Afinal, quando somos nós, aqueles que analisam os aspectos comunicacionais, que estamos no centro do problema, também seguimos as padronizações teóricas da área? Essas e outras reflexões podem trazer ideias interessantes para o aprofundamento futuro do trabalho.

Análise empírica

Como mencionado na introdução deste resumo, nosso caminho metodológico procurou resgatar, especialmente, duas facetas da comunicação organizacional na perspectiva da complexidade (Baldissera, 2009). São elas as dimensões comunicada – processos oficiais da organização, ou seja, seus discursos direcionados, além da falada – quando os debates estão fora do ambiente da empresa e, neste caso, alocamos os registros na imprensa e suas reportagens sobre o caso que informam aspectos fora do controle da estratégia da organização. É importante enfatizar que, no primeiro momento da invasão em 08 de outubro de 2022, a TV Record não se pronunciou. Não houve um relato oficial sobre o incidente, mas essa decisão não passou despercebida nos veículos: a Uol⁵ enfatizou que, mesmo quase 72 horas após o ocorrido, a

⁵ Record hackeada: o que se sabe até agora sobre ataque e sequestro de dados. Tilt Uol, 2022. Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2022/10/17/ataque-hacker-record-roubo-de-dados-pode-ter-sido-um-dos-maiores-do-mundo.htm>. Acesso em 26 dez. 2025.

Record ainda não tinha emitido um posicionamento claro, enquanto o jornal O Globo⁶ e a Folha de S. Paulo⁷ apontam buscas pela assessoria da empresa sem respostas.

A decisão da organização foi de preencher os vazios da programação com arquivos que a empresa ainda possuía acesso. A situação chegou a virar piada no meio dos consumidores, com ironias sobre o excesso de exibição do seriado “Todo Mundo Odeia o Chris”. Não há afirmação nem negação de que o ciberataque ocorreu, afastando-se tanto da confirmação do acontecimento como da delegação de culpa (Benoit, 2015). Quando os sistemas são restaurados dias depois, a organização ocupa um local de silêncio, em que adapta a estratégia de não reviver o caso e deixá-lo para trás (Silva, 2018). É válido lembrar que o silêncio também é uma estratégia discursiva e, nesse caso em específico, também parte da crise operacional pela falta de acesso – o que pode incluir instabilidades no sistema interno, o que dificultaria a própria divulgação do posicionamento. Normalmente, esses relatos podem ser repassados à imprensa pelos representantes, mas no caso da Record isso seria ceder material às suas próprias concorrentes, gerando um dilema entre a ética e os interesses privados.

É aí que o segundo ataque ocorre, no dia 15 de outubro de 2022, dessa vez com o vazamento de arquivos *online* e a interrupção de plataformas de propriedade da Record. Acreditamos que a crise nesse segundo momento se instaura ainda mais no meio midiático porque ela traz uma abertura e exposição do caso fora do ambiente controlado pela empresa (Baldissera, 2009). As notícias na imprensa agora começam a enfatizar que foram dois casos em apenas uma semana, além das denúncias dos documentos vazados. Mesmo assim, a organização se manteve em silêncio, sendo as informações do caso exclusivamente fruto da imprensa externa.

Até que, um mês após o ocorrido (em novembro do mesmo ano), a emissora emitiu alertas para os funcionários e ex-colaboradores de que dados internos poderiam ter sido acessados, avisando que essas informações podem ser usadas de forma indevida. O arquivo também chegou à imprensa⁸ por meio dos sujeitos destinatários. As denúncias aqui apontam algo diferente: que o aviso parecia ter sido motivado por questões jurídicas, como a obrigação da Lei

⁶ Record TV retira programa do ar e muda a programação ao vivo após sofrer ataque de hacker. O Globo, 2022. <https://oglobo.globo.com/cultura/televisao/noticia/2022/10/record-tv-retira-programa-do-ar-e-muda-a-programacao-ao-vivo-apos-sofrer-ataque-de-hacker.ghtml>. Acesso em 26 dez. 2025.

⁷ Record tem suspeita de ataque hacker e paralisa programação ao vivo. Folha de S. Paulo, 2022. Disponível em: <https://f5.folha.uol.com.br/televisao/2022/10/record-tem-suspeita-de-ataque-hacker-e-paralisa-programacao-ao-vivo.shtml>. Acesso em 26 dez. 2025.

⁸ Record alerta funcionários sobre vazamento de dados após ataque hacker. Veja, 2022. Disponível em: <https://veja.abril.com.br/cultura/record-alerta-funcionarios-sobre-vazamento-de-dados-apos-ataque-hacker/>. Acesso em 26 dez. 2025.

Geral de Proteção de Dados (LGPD) em avisar possíveis danos em casos de falha de segurança digital. O comunicado inclui um resumo de ações de proteção que a empresa estaria fazendo, além de enfatizar que teria avisado a Agência Nacional de Proteção de Dados (ANPD).

Vemos alguns pontos importantes nessa esfera: em primeiro lugar, a empresa optou pelo silêncio durante todo o acontecimento, mesmo após o segundo ataque. Focou na restauração dos serviços da crise operacional e manteve o aviso interno como principal elemento comunicativo do caso. Enquanto isso, a imprensa parece ter agido em um formato mais vigilante, denunciando as situações ocorridas e ainda contando com *whistleblowers* internos – isto é, funcionários e outras pessoas ligadas à organização que vazaram informações durante o acontecimento.

Referências

BALDISSERA, R. Comunicação organizacional na perspectiva da complexidade. *Organicom*, v. 6, n. 10, 2009. Disponível em: <https://revistas.usp.br/organicom/article/view/139013>. Acesso em 26 dez. 2025.

BEAMAN, C. et al. Ransomware: Recent advances, analysis, challenges and future research directions. *Computers & Security*, v. 111, 2021. Disponível em: <https://doi.org/10.1016/j.cose.2021.102490>. Acesso em 26 dez. 2025.

BENOIT, W. *Accounts, excuses, and apologies*. New York: Suny Press, 2015.

COOMBS, W. *Ongoing Crisis Communication: Planning, managing, and responding*. California: Sage Publications, 2019.

MELO, F. Imaginários dos públicos sob a ótica dos ataques cibernéticos: caso das Lojas Renner. *Lumina*, v. 19, n. 2, 2025. Disponível em: <https://periodicos.ufjf.br/index.php/lumina/article/view/46860>. Acesso em 26 dez. 2025.

QUADER, F. JANEJA, V. Insights into Organizational Security Readiness: Lessons Learned from Cyber-Attack Case Studies. *Journal of Cybersecurity and Privacy*, v. 1, n. 4, 2021. Disponível em: <https://doi.org/10.3390/jcp1040032>. Acesso em 26 dez. 2025.

SELLNOW, T.; SEEGER, M. *Theorizing Crisis Communication*. Nova Jersey: John Wiley & Sons, 2013.

SILVA, D. Comunicação organizacional e as estratégias de invisibilidade e de redução/direcionamento da visibilidade nas mídias sociais. Tese apresentada ao Programa de Pós-Graduação em Comunicação e Informação da Universidade Federal do Rio Grande do Sul, Porto Alegre, 2018. Disponível em: <https://lume.ufrgs.br/bitstream/handle/10183/180564/001072602.pdf?sequence=1&isAllowed=y>. Acesso em 26 dez. 2025.