A Relação Entre Incidentes de Segurança da Informação, Reputação de Marca e Propriedade Intelectual: Um Mapeamento Bibliográfico

Igor C. Valenciano, João V. D. Silva, Rebeca L. de Rezende, Flávia R. M. Luís, Allan G. de Oliveira, Josiel M. de Figueiredo

Instituto de Computação – Universidade Federal de Mato Grosso (UFMT)
Caixa Postal 78060-900 – Cuiabá – MT – Brasil

igor.valenciano@ufmt.br, jvdantasilva@hotmail.com, beca.rezendel@gmail.com, saneflavia@hotmail.com, allan@ic.ufmt.br, josiel@ic.ufmt.br

Abstract. *The objective of this article is to present a bibliographic review of how information security incidents can impact a brand's trust and intellectual property. The articles were selected from a bibliographic mapping applying the snowballing technique. As a result, we obtained the main impacts caused on a brand and its intellectual property, the main measures imposed by corporations after a security incident and which computational resources can act in preventing this scenario.*

Resumo. *O objetivo deste trabalho é apresentar uma revisão bibliográfica de como incidentes de segurança da informação podem impactar a reputação de uma marca e a propriedade intelectual. Os artigos foram selecionados a partir de um mapeamento bibliográfico aplicando a técnica de snowballing. Como resultado obteve-se os principais impactos causados em uma marca e em sua propriedade intelectual, as principais medidas adotadas pelas corporações após um incidente de segurança e quais recursos computacionais podem atuar na prevenção deste cenário.*

1. Introdução

A marca é um fator crítico de sucesso para as organizações, pois marcas fortes representam uma vantagem competitiva e fonte de futuros ganhos de recursos para a empresa [Oliveira e Luce 2011]. Para Neves e Correia (2016), as corporações necessitam de implementar mecanismos com capacidade de prevenção e resposta aos incidentes que coloquem em risco a segurança da informação, pois a exploração de vulnerabilidades pode afetar as infraestruturas que prestam serviços fundamentais ao público da empresa. Nesse sentido, Machado et al. (2022) afirmam que a violação de dados digitais pode comprometer gravemente a propriedade intelectual organizacional, recursos, tempo e valor de produtos das organizações.

Considerando que o crescimento constante de empresas que realizam negócios na Internet também impacta o aumento de ameaças digitais, Kamiya et al. (2021) comprovaram que anunciar uma violação de segurança está negativamente associado ao valor de mercado da empresa anunciante. Além disso, em 2023, houve um aumento significativo de 42% nos ataques de ransomware - um tipo de software malicioso que bloqueia o acesso a dados ou sistemas até que um resgate seja pago - em comparação com

o ano anterior, evidenciando o crescimento acelerado das ameaças digitais (Magar et al., 2023). Portanto, este artigo visa apresentar um mapeamento bibliográfico que relacione como incidentes de segurança da informação podem impactar na reputação de uma marca e na propriedade intelectual (PI). O trabalho é útil porque permite que as organizações possam revisar e desenvolver novos processos de gestão tecnológica para contribuir com a melhora desse cenário.

2. Metodologia

Este trabalho utilizou o método de mapeamento bibliográfico e a técnica snowballing proposta por Wohlin (2014), que se trata de um processo manual de coleta, seleção e análise de trabalhos científicos. Dessa forma, os critérios de inclusão (CI) e exclusão (CE) foram definidos e apresentados na Tabela 1.

Tabela 1. Listagem dos critérios de inclusão e de exclusão

Critérios	Definição do critério
CI	Artigos científicos que contenham princípios, métodos, estudos de caso ou estratégias que visam relacionar como incidentes de segurança podem impactar na reputação de uma marca e na propriedade intelectual.
CE1	Sites, monografias, dissertações e teses de doutorado
CE2	Artigos com o título que fogem da temática proposta
CE3	Artigos com conteúdo pago para visualização ou download
CE4	Artigos científicos que não contenham princípios, métodos, estudos de caso ou estratégias que visam relacionar como incidentes de segurança podem impactar na reputação de uma marca e da propriedade intelectual após a leitura do resumo.

A pesquisa para constituir o conjunto provisório foi realizada na plataforma Google Acadêmico utilizando as palavras chave do artigo em português e em inglês, seguindo o procedimento proposto por Wohlin (2014). Portanto, após aplicar as iterações e os critérios definidos na Tabela 1, foram selecionados 10 artigos.

2.1. Questões de pesquisa

Com o objetivo de colaborar com esta discussão acerca da relação entre incidentes de segurança da informação e reputação da marca e propriedade intelectual, foram levantadas três questões de pesquisa (QPs) que nortearam o estudo:

- **QP1:** Qual é o impacto na reputação de uma marca e da propriedade intelectual após um incidente de segurança?
- **QP2:** Quais são as principais medidas tomadas após um incidente de segurança para minimizar os impactos negativos na marca e propriedade intelectual?
- **QP3:** Que recursos computacionais podem atuar na prevenção de incidentes de segurança e consequentemente na proteção da propriedade intelectual?

Para responder todas as questões de pesquisa, os 10 artigos selecionados foram analisados e as respostas foram agrupadas qualitativamente, agrupando quando possível, visando responder às questões.

3. Resultados

3.1. Impacto na reputação de uma marca e da propriedade intelectual

É fundamental destacar que a maioria dos artigos selecionados aponta para a perda de confiança dos clientes como uma consequência significativa das violações de segurança, resultando em impactos financeiros adversos para as empresas, como ilustrado na Figura 1. Esses resultados, como visto por Makridis (2021), podem ser avaliados através da psicologia do consumidor e do marketing, indicando que a publicidade negativa pode, às vezes, ter efeitos positivos. Por exemplo, uma empresa menor com uma violação de dados pode se beneficiar de uma atenção midiática adicional, enquanto uma empresa maior pode experimentar um declínio na reputação devido à sua visibilidade, pois a empresa deveria apresentar maior domínio de práticas relacionadas à proteção de dados.

Além disso, isso sugere que o mercado atual pode estar deficiente em disciplina e incentivos para investimentos em cibersegurança [Makridis 2021]. Medidas como uma comunicação transparente, respostas rápidas e eficazes, e uma reavaliação constante das políticas de segurança são cruciais para mitigar os danos à reputação e proteger a propriedade intelectual das empresas.

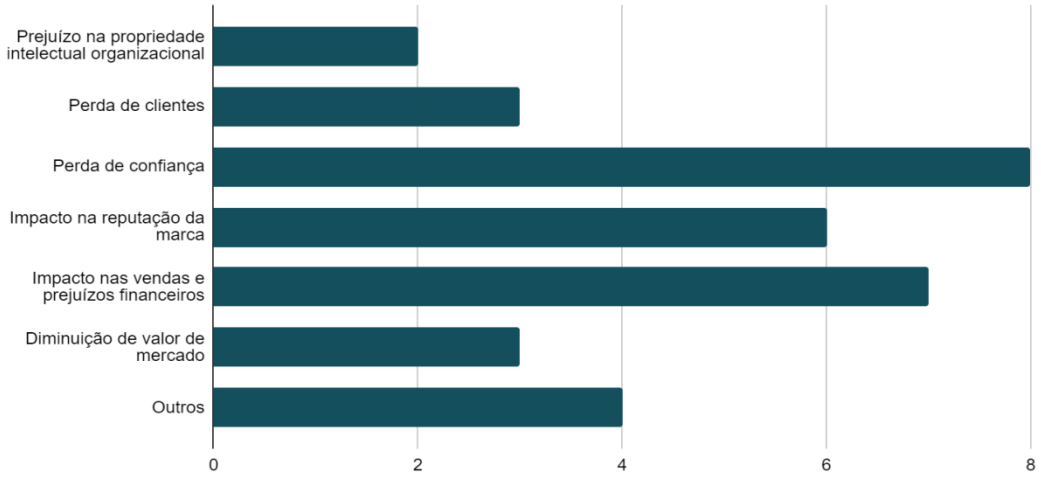

Figura 1. Impactos na reputação de uma marca e da propriedade intelectual, onde no eixo y são apresentados os fatores em si e no eixo x é apresentada a quantificação.

3.2. Principais medidas a serem tomadas após um incidente de segurança

Vale pontuar que nem todos os artigos selecionados abordaram as medidas que foram tomadas após um incidente de segurança visando minimizar os impactos negativos na marca e na propriedade intelectual. O estudo de caso realizado por Plachikinova e Maurer (2018) foi baseado na empresa Target que sofreu um ataque cibernético em 2013, afetando fortemente as operações da corporação. A medida inicial tomada pelo presidente da empresa foi a notificação das instituições financeiras acerca do incidente de segurança, visando diminuir os impactos do vazamento de dados de seus clientes.

Nesta perspectiva, o apagão cibernético global desencadeado por um erro na atualização de um sistema operacional da empresa americana CrowdStrike que ocorreu em 19 de julho de 2024, reforça a necessidade das corporações definirem planos de respostas a incidentes robustos e frequentemente atualizados, visto que prejudicou operações de diversas áreas no mundo todo com prejuízos financeiros estimados entre US$ 4 e US$ 6 bilhões [George 2024]. Para De Souza et al. (2024), este evento - considerado um dos maiores acontecimentos de interrupção de serviços digitais da história recente - evidenciou que empresas que não conseguiram restabelecer rapidamente seus serviços, enfrentaram críticas e possíveis ações legais por parte dos consumidores que se sentiram prejudicados. Ainda, os demais estudos apontaram que ter uma comunicação transparente, avaliação e resposta rápida, monitoramento contínuo, reavaliação das políticas de risco, conscientização organizacional e compensação aos clientes são fatores que ajudam a reduzir o impacto negativo de um incidente.

3.3. Atuação dos recursos computacionais na prevenção de incidentes

A utilização de recursos computacionais é essencial para a prevenção de incidentes de segurança da informação, atuando de forma estratégica para mitigar riscos e proteger a propriedade intelectual. Segundo Ahmad et al. (2021), a prevenção de incidentes não se limita a controles tecnológicos tradicionais, como criptografia e firewalls, mas requer uma análise mais abrangente que inclua a estratégia organizacional.

Além dos controles tradicionais, como criptografia e firewalls, ferramentas de automação como SOAR (Security Orchestration, Automation, and Response) têm mostrado uma eficácia significativa na redução do tempo de resposta a incidentes de segurança. Segundo Kinyua e Awuah (2021), o SOAR permite que empresas automatizem processos de resposta a incidentes, desde a detecção até a mitigação de ameaças, resultando em uma redução significativa no tempo de resposta. Ahmad et al. (2021) também apontam que o uso de ferramentas automatizadas pode acelerar a resposta a incidentes, melhorando a eficiência da mitigação. Essas ferramentas permitem que as organizações lidem com incidentes de forma mais rápida e eficiente, minimizando o impacto sobre a propriedade intelectual e reduzindo as consequências financeiras e de reputação associadas a violações de segurança (Almeida e Santos, 2020).

Figura 2. Nuvem de palavras que representam quais recursos computacionais podem auxiliar na prevenção de incidentes de segurança.

Conforme ilustrado na Figura 2, a expressão "investimento em segurança da informação" destaca-se no centro da nuvem de palavras, sublinhando a importância de alinhar o investimento em tecnologias de proteção a estratégias organizacionais robustas.

Nesse contexto, Ahmad et al. (2021) enfatizam que o investimento em segurança da informação também deve incluir avaliações detalhadas de ameaças, considerando não apenas os recursos tecnológicos, mas também as motivações de possíveis concorrentes, com foco na proteção da propriedade intelectual. Essa abordagem facilita a identificação dos atores mais críticos, permitindo um monitoramento contínuo e a aplicação de medidas preventivas mais eficazes, como o controle rigoroso das interações com potenciais ameaças e a rápida resposta a atividades suspeitas.

4. Considerações finais

Este artigo discutiu a relação de como incidentes de segurança da informação podem impactar na reputação de uma marca e na sua propriedade intelectual a partir de um mapeamento bibliográfico. Os resultados evidenciaram que além dos prejuízos financeiros, a confiança dos clientes é o principal impacto causado por incidentes envolvendo principalmente a segurança dos dados dos usuários. O estudo também revelou a necessidade de definir estratégias emergenciais para aplicar uma resposta rápida e eficaz após ocorrer um incidente de segurança dentro de uma organização, visando diminuir o impacto negativo deste acontecimento em uma marca ou propriedade intelectual.

Por fim, o levantamento de quais recursos computacionais podem auxiliar na prevenção dessas ocorrências é útil para que as empresas revisem suas políticas de segurança da informação e destinem recursos financeiros e humanos suficientes a fim de garantir a proteção dos dados de seus clientes e a consolidação de sua marca. Além disso, o estudo possui uma relevante contribuição, visto que poucos trabalhos demonstram o relacionamento entre propriedade intelectual e incidentes de segurança da informação. Como continuidade da pesquisa, espera-se expandir a coleta de dados e a realização de um estudo de caso envolvendo um incidente de segurança em uma corporação brasileira.

Referências

OLIVEIRA, Marta Olivia Rovedder de; LUCE, Fernando Bins. O valor da marca: conceitos, abordagens e estudos no Brasil. REAd. Revista Eletrônica de Administração (Porto Alegre), v. 17, p. 502-529, 2011.

NEVES, Paulo Jorge Baptista das; CORREIA, Fernando Jorge Ribeiro. Resposta a incidentes de segurança da informação: uma abordagem DOTMLPI-I. Cyberlaw, 2016.

MACHADO, José dos Santos et al. As principais ameaças digitais e suas formas de mitigação no contexto da segurança da propriedade intelectual. Conjecturas, v. 22, n. 8, p. 147-162, 2022.

KAMIYA, Shinichi et al. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics, v. 139, n. 3, p. 719-749, 2021.

WOHLIN, Claes. Guidelines for snowballing in systematic literature studies and a replication in software engineering. In: Proceedings of the 18th international conference on evaluation and assessment in software engineering. 2014. p. 1-10.

CHOONG, Peggy et al. Protecting the brand: Evaluating the cost of security breach from a marketer's perspective. Journal of Marketing Development and Competitiveness, v. 11, n. 1, 2017.

PUTRI, Nadia Anggraini; FACHIRA, Ira. Consumer Brand-Relationship and Privacy Concerns to Repurchase Intention in Online Shopping Application. Ekonomi, Keuangan, Investasi dan Syariah (EKUITAS), v. 5, n. 1, p. 214-222, 2023.

PLACHKINOVA, Miloslova; MAURER, Chris. Security breach at target. Journal of Information Systems Education, v. 29, n. 1, p. 11-20, 2018.

LEE, MinJae; LEE, JinKyu. The impact of information security failure on customer behaviors: A study on a large-scale hacking incident on the internet. Information Systems Frontiers, v. 14, p. 375-393, 2012.

MACHADO, José dos Santos et al. Proteção da Propriedade Intelectual: Uma revisão da segurança dos dados digitais e seus desafios. Revista Conjecturas, v. 22, n. 5, 2022.

CAVUSOGLU, Huseyin; MISHRA, Birendra; RAGHUNATHAN, Srinivasan. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. International Journal of Electronic Commerce, v. 9, n. 1, p. 70-104, 2004.

KAMIYA, Shinichi et al. Risk management, firm reputation, and the impact of successful cyberattacks on target firms. Journal of Financial Economics, v. 139, n. 3, p. 719-749, 2021.

MAKRIDIS, Christos A. Do data breaches damage reputation? Evidence from 45 companies between 2002 and 2018. Journal of Cybersecurity, v. 7, n. 1, p. tyab021, 2021.

AHMAD, Atif et al. Teaching Information Security Management Using an Incident of Intellectual Property Leakage. arXiv preprint arXiv:2103.14838, 2021.

MAGAR, Bibek Thapa; POUDAL, Swachchhanda Shrawan; BOGATI, Anish. The cybersecurity rollercoaster of 2023: Ransomware and the evolving threat landscape. Logpoint Security Research, 2023.

ALMEIDA, José; SANTOS, Ricardo. Cloud Backup and High Availability Solutions. IEEE Xplore, 2020.

AHMAD, Atif et al. Security Automation Research. arXiv preprint, 2021.

KINYUA, Johnson; AWUAH, Lawrence. AI/ML in Security Orchestration, Automation and Response: Future Research Directions. Intelligent Automation & Soft Computing, 2021.

NEVES, Paulo; CORREIA, Fernando. Resposta a Incidentes de Segurança da Informação. Revista Cyberlaw, 2016.

GEORGE, A. Shaji. When Trust Fails: Examining Systemic Risk in the Digital Economy from the 2024 CrowdStrike Outage. Partners Universal Multidisciplinary Research Journal, v. 1, n. 2, p. 134-152, 2024.

DE SOUZA, Alcian Pereira et al. Apagão global online, dependência digital e o impacto aos direitos fundamentais. REVISTA DELOS, v. 17, n. 58, p. e1630-e1630, 2024.