INTERNATIONAL SEVEN JOURNAL
OF MULTIDISCIPLINARY
ISSN: 2764-9547

Navegando pelos desafios da segurança cibernética: Implicações legais e estratégias organizacionais

10.56238/isevmjv2n1-012
Recebimento dos originais: 01/12/2023
Aceitação para publicação: 02/07/2023

Jammylly Fonseca Silva

RESUMO

A crescente frequência e sofisticação de incidentes de segurança cibernética, como violações de dados, ataques de ransomware e violações de sistema, destacam desafios legais e organizacionais significativos. Apesar do aumento dos investimentos em segurança cibernética, esses incidentes continuam a evoluir, apresentando questões complexas para empresas e reguladores. As estruturas legais tradicionais, focadas principalmente em danos financeiros, não abordam danos não financeiros, como impactos emocionais e psicológicos nos consumidores. Estudos de Teichmann e Wittmann (2022) e Kilovaty (2021) revelam lacunas nas leis atuais de segurança cibernética, enfatizando a necessidade de incorporar danos psicológicos e aprimorar os padrões de responsabilidade corporativa. A pesquisa de Frank, Grenier e Pyzoha (2021) demonstra o aumento dos riscos de litígio para os conselhos de administração após incidentes de segurança cibernética. Suas descobertas sugerem que ataques cibernéticos anteriores aumentam a probabilidade de serem responsabilizados, embora a implementação de estruturas como as diretrizes de gerenciamento de risco do Instituto Americano de Contadores Públicos Certificados (AICPA) possa mitigar esses riscos. Além disso, Eijkelenboom e Nieuwesteeg (2020) analisam a divulgação de informações de segurança cibernética nos relatórios anuais holandeses, encontrando falta de transparência, apesar dos requisitos legais. Seu estudo ressalta a necessidade de uma melhor autorregulação ou possíveis mandatos legais para melhorar os relatórios de segurança cibernética. Falowo et al. (2022) examinam o impacto da interconexão digital nos riscos de segurança cibernética, observando que os ataques de malware e phishing são predominantes. Sua pesquisa destaca a importância da preparação organizacional e da adesão a estruturas como as diretrizes do Instituto Nacional de Padrões e Tecnologia (NIST) para uma resposta eficaz a incidentes. Sen (2018) identifica desafios técnicos, econômicos, legais e comportamentais contínuos que dificultam a segurança cibernética eficaz, defendendo novas estratégias para superar essas barreiras. No geral, aumentar a resiliência da segurança cibernética requer uma abordagem abrangente, integrando estruturas legais aprimoradas, transparência organizacional e gerenciamento proativo de riscos.

Palavras-chave: Incidentes de segurança cibernética, Responsabilidade legal, Danos psicológicos, Marcos regulatórios, Resposta a incidentes.

1 INTRODUÇÃO

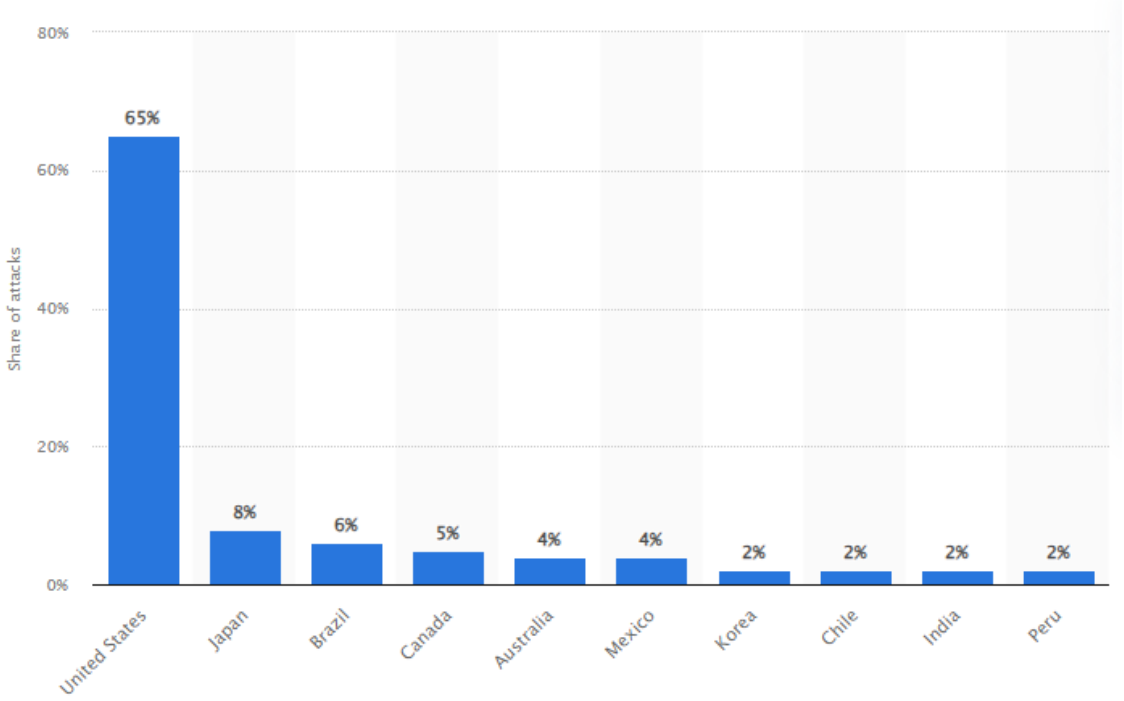
Incidentes de segurança cibernética, incluindo violações de dados, ataques de ransomware e violações de sistemas ciberfísicos, estão se tornando mais frequentes e sofisticados, levantando preocupações significativas sobre suas repercussões legais. À medida que as ameaças digitais evoluem continuamente, as responsabilidades legais das organizações envolvidas em tais incidentes tornaram-se críticas e complexas. As leis de proteção de dados, como o Regulamento

Geral de Proteção de Dados (GDPR) na UE e a Lei de Privacidade do Consumidor da Califórnia (CCPA) nos EUA, impõem obrigações específicas às empresas em relação à proteção e notificação de dados pessoais. A não conformidade pode levar a penalidades financeiras substanciais e danos à reputação.

Além dos regulamentos de proteção de dados, as leis de responsabilidade civil também desempenham um papel crucial. As organizações podem enfrentar ações legais por negligência se não implementarem medidas de segurança adequadas para proteger as informações de seus clientes e parceiros. A responsabilidade por danos a terceiros, incluindo clientes e fornecedores, pode envolver compensação financeira por perdas devido a violações de segurança. Além disso, a legislação está evoluindo para lidar com a crescente complexidade dos crimes cibernéticos. Novas leis sobre crimes cibernéticos e ciberterrorismo estão sendo promulgadas para combater ataques graves e suas ramificações, enquanto as responsabilidades dos provedores de serviços de tecnologia e desenvolvedores de software estão sendo reavaliadas, especialmente em relação às vulnerabilidades do sistema exploradas pelos invasores.

O gerenciamento eficaz de incidentes de segurança cibernética requer uma abordagem proativa, incluindo medidas de segurança robustas, auditorias regulares e equipes de resposta a incidentes bem treinadas. Uma resposta rápida e eficaz, juntamente com o cumprimento das obrigações legais de notificação e comunicação, é crucial para mitigar as consequências legais e manter a integridade organizacional.

Figura 1: Países com a maior parcela de ataques cibernéticos evitados em todo o mundo de setembro a novembro de 2022. Fonte: Statista.



Teichmann e Wittmann (2022) investigam a crescente ameaça do crime cibernético e suas implicações para a responsabilidade corporativa. Seu estudo enfatiza que as empresas não podem confiar na sorte ou em suposições ingênuas para evitar ataques cibernéticos. Em vez disso, eles devem estar cientes dos riscos de responsabilidade associados a violações de dados e preocupações com a privacidade, que são cada vez mais regidos por regulamentações emergentes de segurança cibernética. Os autores enfatizam a importância de medidas proativas e destacam uma lacuna significativa na literatura sobre segurança de dados e regulamentos de responsabilidade.

Katkova et al. (2020) enfocam as responsabilidades legais dentro da segurança cibernética, examinando especificamente a lei ucraniana "Sobre os Princípios Fundamentais da Provisão de Segurança Cibernética na Ucrânia" de 5 de outubro de 2017. Esta lei abrange a responsabilidade por violações na segurança nacional, comunicações eletrônicas e segurança da informação envolvendo o ciberespaço. O estudo categoriza as responsabilidades legais em domínios administrativo, criminal e civil e identifica uma lacuna na regulamentação da responsabilidade robótica.

Falowo et al. (2022) investigam o aumento da interconectividade digital e a crescente dependência da internet para o gerenciamento de informações, analisando 803 incidentes significativos de segurança cibernética relatados na última década. Eles descobriram que as técnicas de malware e phishing foram responsáveis por uma grande parte desses incidentes. O

estudo enfatiza a necessidade de preparação organizacional e recomenda a adoção da estrutura de resposta a incidentes do Instituto Nacional de Padrões e Tecnologia (NIST) ou diretrizes semelhantes para uma resposta eficaz.

Frank, Grenier e Pyzoha (2021) exploram a tendência de aumento de ações judiciais contra conselhos de administração após incidentes de segurança cibernética. Sua pesquisa descobriu que os diretores são mais propensos a serem responsabilizados se uma empresa tiver sofrido um ataque cibernético anterior. No entanto, a implementação da estrutura de gerenciamento de riscos de segurança cibernética do Instituto Americano de Contadores Públicos Certificados (AICPA) pode reduzir esse risco de responsabilidade, principalmente quando a garantia externa é obtida.

Eijkelenboom e Nieuwesteeg (2020) examinam a divulgação de informações de segurança cibernética em relatórios anuais holandeses de uma perspectiva de direito financeiro e economia. Apesar da ausência de requisitos legais rígidos, eles descobriram que uma porcentagem significativa de empresas holandesas divulgou informações relacionadas à segurança cibernética em seus relatórios de 2018. No entanto, as divulgações detalhadas foram limitadas, comprometendo potencialmente a proteção das partes interessadas.

Kilovaty (2021) critica a lei de segurança cibernética por se concentrar apenas nos danos financeiros causados por violações de dados, negligenciando os impactos emocionais e psicológicos sobre os consumidores. O estudo defende uma nova estrutura para lidar com esses danos não financeiros, recomendando uma revisão do conceito de "informações pessoais" e a inclusão de categorias adicionais de informações protegidas.

Sen (2018) analisa a tendência crescente de incidentes de segurança cibernética, apesar do aumento dos investimentos em segurança. O estudo identifica desafios técnicos, econômicos, legais e comportamentais que impedem a segurança cibernética eficaz e destaca as limitações das iniciativas recentes de várias partes interessadas. A pesquisa ressalta a necessidade de estratégias e soluções inovadoras para superar essas barreiras persistentes e melhorar a proteção da segurança cibernética.

Em conclusão, a crescente frequência e sofisticação dos incidentes de segurança cibernética ressaltam a necessidade urgente de estratégias legais e organizacionais abrangentes para enfrentar seus desafios multifacetados. O cenário em evolução das ameaças digitais e o escopo crescente das estruturas regulatórias destacam a importância crítica de medidas robustas de segurança cibernética e gerenciamento proativo de riscos. Embora a legislação atual, como leis de proteção de dados e estatutos de responsabilidade civil, forneça uma base para lidar com danos financeiros

e negligência, ainda há uma lacuna significativa no reconhecimento e tratamento de danos não financeiros, como impactos emocionais e psicológicos.

Estudos de Teichmann e Wittmann (2022) e Kilovaty (2021) revelam a necessidade de uma perspectiva mais ampla sobre a responsabilidade corporativa e a inclusão de danos psicológicos na legislação de segurança cibernética. Da mesma forma, a pesquisa de Frank, Grenier e Pyzoha (2021) demonstra o aumento dos riscos de litígio para os conselhos corporativos, enfatizando a necessidade de adesão a estruturas como as diretrizes do AICPA para mitigar a responsabilidade. Além disso, Eijkelenboom e Nieuwesteeg (2020) e Falowo et al. (2022) destacam a importância da transparência e da preparação organizacional no gerenciamento eficaz dos riscos de segurança cibernética.

O cenário jurídico deve continuar a evoluir, abordando danos financeiros e não financeiros e incorporando avanços no gerenciamento de ameaças cibernéticas. À medida que as ameaças cibernéticas se tornam mais sofisticadas, as empresas devem não apenas cumprir os regulamentos existentes, mas também adotar medidas proativas para proteger as partes interessadas e aumentar a resiliência geral da segurança cibernética. Ao integrar essas descobertas e recomendações, organizações e formuladores de políticas podem navegar melhor pelas complexidades da segurança cibernética, melhorando a proteção e a resposta a ameaças digitais.

REFERÊNCIAS

EIJKELENBOOM, E.; NIEUWESTEEG, B. An analysis of cybersecurity in Dutch annual reports of listed companies. Computer Law & Security Review, v. 40, p. 105513, 2020. DOI: https://doi.org/10.2139/ssrn.3667418.

FALOWO, O. et al. Threat actors' tenacity to disrupt: Examination of major cybersecurity incidents. IEEE Access, v. 10, p. 134038-134051, 2022. DOI: https://doi.org/10.1109/ACCESS.2022.3231847.

FRANK, M.; GRENIER, J.; PYZOHA, J. Board liability for cyberattacks: The effects of a prior attack and implementing the AICPA's cybersecurity framework. Journal of Accounting and Public Policy, p. 106860, 2021. DOI: https://doi.org/10.1016/J.JACCPUBPOL.2021.106860.

KATKOVA, T. et al. Provision of cybersecurity in Ukraine: Issues of legal responsibility. 2020. DOI: https://doi.org/10.1007/978-3-030-37618-5_22.

KILOVATY, I. Psychological data breach harms. SSRN Electronic Journal, 2021. DOI: https://doi.org/10.2139/SSRN.3785734.

SEN, R. Challenges to cybersecurity: Current state of affairs. Communications of the Association for Information Systems, v. 43, p. 2, 2018. DOI: https://doi.org/10.17705/1CAIS.04302.

TEICHMANN, F.; WITTMANN, C. When is a law firm liable for a data breach? An exploration into the legal liability of ransomware and cybersecurity. Journal of Financial Crime, 2022. DOI: https://doi.org/10.1108/jfc-04-2022-0093.