Síminn? More like, you can "sí" minn personal information :(

T-401-ICYB: Lab 6

Alexander Joseph Emilsson Alfa Reynisdóttir Gísli Hrafn Halldórsson Kim Anna Hudson

Executive Summary

This dossier presents an OSINT investigation of Síminn hf., Iceland's leading telecommunications provider. Critical findings include outdated JavaScript libraries (jQuery 3.5.1) with known XSS vulnerabilities, technical infrastructure details disclosed through employee LinkedIn profiles (Cisco routers, Fortinet firewalls), and personal information about CEO María Björk Einarsdóttir readily available on Facebook. Combined with Síminn's documented history of regulatory violations—including a 2011 privacy breach, 2012 anti-competitive pricing, and a 2021 service outage—these findings demonstrate how public information creates significant attack surfaces for both technical exploitation and competitive pressure.

I. Introduction

This investigation targets Síminn hf., Iceland's primary telecommunications provider, as an academic exercise in open-source intelligence gathering. Síminn operates as a publicly traded company (kennitala: 4602070880) offering mobile, internet, television, and IT services throughout Iceland. Our objective is to demonstrate how publicly available information can be systematically collected to reveal organizational vulnerabilities. All information was obtained through legal, ethical means using only publicly accessible sources.

II. Methodology

Our investigation combined automated tools and manual research. We used DNS enumeration and WHOIS lookups to map Síminn's digital infrastructure and identify subdomains. Personnel intelligence came from observer accounts on LinkedIn, Facebook, and Instagram, allowing us to view publicly shared information without deceptive practices. Corporate data was gathered through Iceland's public business registry (Fyrirtækjaskrá), financial disclosures, and investor relations materials. Web technology analysis used BuiltWith and manual inspection. All sources were cross-verified and properly documented.

III. Open Source Intelligence

A. Corporate Profile

Síminn hf. (legal name: "Síminn (Iceland Telecom Ltd.)") operates from headquarters at Ármúli 25, 108 Reykjavík, with kennitala 4602070880[1][2]. The company provides mobile, fixed voice, internet, television, IT services, and equipment sales[3]. As of March 2024, Síminn reported total assets of ISK 40,723 million and employed 311 staff[4][5].

Subsidiaries include Síminn Pay ehf., Radíómiðun ehf., Billboard ehf., BBI ehf., Dengsi ehf., and Noona Iceland ehf[4]. Míla ehf. is identified as the largest single counterparty[6]. Contact: +354 550 6000, email format: firstname.lastname@siminn.is.

B. Leadership and Key Personnel

Board of Directors: Jón Sigurðsson (Chairman), Sigrún Ragna Ólafsdóttir (Vice Chairman), Bjarni Þorvarðarson, Arnar Þór Másson, and Valgerður Halldórsdóttir[7].

Executive Management: María Björk Einarsdóttir (CEO), Berglind Björg Harðardóttir (Director of Consumer Division), Logi Karlsson (Director of Technology Development), Birkir Ágústsson (Director of Media), Hjörtur Þór Steindórsson (CFO), and Sæunn Björk Þorkelsdóttir (Director of Business Division)[7].

CEO María Björk Einarsdóttir's public Facebook profile reveals she was born in 1989, is married to Ellert Arnarson, and has two young children including a son named Einar Örn. This personal information, while publicly shared, represents a significant OPSEC vulnerability enabling targeted social engineering attacks.

C. Infrastructure & Technology

Síminn uses AWS EC2 for hosting and operates three DNS servers (ns1.simnet.is, ns2.simnet.is, ns3.simnet.is)[8]. Subdomain enumeration revealed 2000+ subdomains, many following the pattern "mobile-out-133-*.siminn.is" for bulk SMS/MMS messaging infrastructure.

Email services include Microsoft Exchange/365 (corporate), Amazon SES (automated notifications), MailChimp and Marketo (marketing), and Salesforce SPF (customer service).

Critical vulnerability: The website uses jQuery version 3.5.1 (five years old), which narrowly avoids severe XSS vulnerabilities but remains outdated. The frontend combines jQuery, React, Redux, Underscore.js, and Modernizr (13+ years old)—suggesting fragmented development teams and no unified security architecture.

Employee LinkedIn profiles disclosed infrastructure details: Cisco routers and Fortinet firewalls for network security, and React/REST/Redux.js for frontend development. While shared to demonstrate professional experience, these disclosures provide attackers with valuable intelligence about security infrastructure.

D. Digital Presence

Síminn maintains active social media on Facebook (facebook.com/siminn.is/), YouTube (youtube.com/user/SiminnIsland), Instagram (instagram.com/siminn.island/), and X/Twitter (x.com/siminn).

E. Incidents, Outages and Regulatory Actions

Data Privacy Violation (2011): Persónuvernd filed its first-ever police complaint against Síminn for illegally collecting personal information about thousands of competitors' customers. The regulator called it "gross misuse of personal information" and noted the unprecedented scale[9].

Anti-Competitive Pricing (2012): Samkeppniseftirlitið ruled that Síminn engaged in illegal price squeezing, structuring prices to disadvantage retail competitors in violation of competition law[10][11]. Síminn appealed.

Service Outage (2021): Nationwide outage affecting mobile and broadband services. Síminn attributed it to human error during routine maintenance, not cyber attack[12]. This reveals vulnerabilities in change management and quality assurance processes.

These incidents demonstrate a pattern: regulatory compliance issues, competitive behavior violations, and operational reliability problems stemming from internal processes rather than external threats.

IV. Plan of Attack

Based on the intelligence gathered, we have identified a multi-vector approach that exploits Síminn's publicly exposed vulnerabilities without engaging in illegal activities. This theoretical attack plan focuses on three primary vectors: technical exploitation of outdated software, social engineering targeting key personnel, and competitive intelligence gathering.

A. Technical Vector: Frontend Exploitation

jQuery 3.5.1 presents exploitation opportunities. While narrowly avoiding the most severe XSS vulnerabilities, it remains five years outdated. The overlapping JavaScript frameworks (React, Redux, jQuery, Underscore.js, Modernizr) likely create compatibility issues where input sanitization fails.

Attack method: Create XSS payloads targeting customer-facing interfaces (login portals, customer service chat, payment pages). Automate testing across the 2000+ identified subdomains—legacy systems often receive less security attention. Successful XSS enables session hijacking, credential harvesting, or malicious code injection.

Timing: Target the end of financial quarters when IT focuses on availability over security monitoring, or during major Icelandic holidays when staff is reduced.

B. Social Engineering Vector: Executive Targeting

CEO María Björk Einarsdóttir's public Facebook information enables highly personalized spear-phishing. Knowledge of her children's names, husband's basketball team, and career history allows convincing emails purporting to be from her son's school, her husband's team, or former colleagues. The email format (firstname.lastname@siminn.is) makes constructing her corporate address trivial.

Timing: Strike during quarterly earnings when executives are distracted, or use personal details about young children to create urgency.

Other targets: CFO Hjörtur Þór (fake invoices), CTO Logi Karlsson (fake security alerts), Compliance Officer Eiríkur Hauksson (fake regulatory communications). LinkedIn profiles provide role-specific attack vectors for each executive.

C. Infrastructure Reconnaissance

Knowing Síminn uses Cisco routers and Fortinet firewalls allows targeted monitoring of vendor vulnerability disclosures. When patches are announced, there's a window before large organizations apply them.

The 2000+ subdomains present an enormous attack surface. Many in the "mobile-out-133-*" messaging infrastructure may receive less security scrutiny. Systematically probe for exposed administrative interfaces, unpatched vulnerabilities, or misconfigured services.

AWS EC2 with custom DNS suggests a hybrid cloud model. Scan for misconfigured S3 buckets, overly permissive security groups, or publicly accessible databases.

D. Timing and Resources

Optimal timing: Financial quarter-ends (March, June, September, December), major Icelandic holidays (Christmas, July-August vacation period), or immediately following service outages when attention focuses on restoration rather than security.

Resources required: Subdomain enumeration and vulnerability scanning tools (freely available), email infrastructure for phishing (minimal cost), cloud capacity for large-scale scanning, penetration testing tools, and expertise in network security and cloud infrastructure. The extensive public intelligence reduces reconnaissance time, allowing focus on exploitation.

E. Legal Attack Strategies: Regulatory Pressure and Market Competition

F. Legal Attack Strategies

GDPR Audit Campaign: File complaints with Persónuvernd requesting audits of current data handling, citing the 2011 "gross misuse" incident as establishing a pattern. Complaints must be investigated, creating regulatory burden and negative publicity.

Competition Monitoring: Use the 2012 price squeezing ruling to justify ongoing complaints about current pricing. Systematically document practices and file new complaints forcing Síminn to defend and potentially modify strategies.

Operational Transparency Demands: Leverage the 2021 "human error" admission to question change management procedures. Use freedom of information requests for incident reports. Reference during future outages to question competence.

G. Competitive Disruption: Whitepaper and Advertising

Publish a whitepaper documenting Síminn's regulatory history: the 2011 privacy violation ("gross misuse of personal information"), the 2012 anti-competitive pricing, the 2021 outage (human error), and technical vulnerabilities (outdated jQuery, fragmented architecture). Format as objective research, cite all sources, distribute to media and consumer organizations.

Advertising Campaign: Position competitor as the antithesis:

- Privacy-first messaging: "Your data is yours" (contrasts 2011 violations)
- Guaranteed uptime with SLAs: "99.9% uptime guarantee" (contrasts 2021 outage)
- Pricing transparency (contrasts 2012 anti-competitive ruling)

Timing: Launch immediately following Síminn service outages (72-hour advertising blitz), upon quarterly/annual report releases, during shareholder meetings, or at contract renewal periods.

Resources: Whitepaper (ISK 2-3 million), PR distribution (ISK 1-2 million), advertising campaign (ISK 10-15 million across digital, print, outdoor).

Key advantage: Every claim is documented and verifiable. Síminn cannot dispute regulatory findings, only argue they're historical—which invites demands for transparency about current practices.

V. Discussion & Reflection

Within hours, we compiled comprehensive intelligence on Síminn: technical infrastructure, key personnel, security vulnerabilities, and personal information about leadership enabling social engineering attacks. The most concerning finding is how effectively disparate public sources aggregate into a detailed intelligence profile.

Individual pieces seem innocuous—a LinkedIn profile showcasing professional experience, a CEO's Facebook celebrating family milestones, a five-year-old JavaScript library. Combined, they create significant vulnerabilities: network security infrastructure revealed, spear-phishing ammunition provided, XSS entry points identified.

This highlights a fundamental tension: social media encourages sharing for professional networking and personal branding, yet this openness creates exploitable vulnerabilities. The "defense in depth" security model assumes multiple protective layers, but OSINT systematically catalogs numerous small weaknesses that collectively constitute major threats.

The "detective mindset" requires thinking systematically about information flows, understanding that data shared for one purpose (networking, customer communication, regulatory compliance) can be repurposed for another (reconnaissance, social engineering, competitive intelligence). Effective OSINT needs patience, creativity to identify unexpected sources, and analytical skills to synthesize scattered facts.

Defensively, this demonstrates the importance of OPSEC awareness at all organizational levels. Technical security measures like firewalls are undermined when employees publicly disclose infrastructure details or executives share personal information enabling social engineering. Organizations must balance public engagement benefits against information disclosure risks.

For individuals, CEO María Björk Einarsdóttir's public Facebook profile allows strangers to learn about her family and interests. While she has every right to share this, the security implications for her organization suggest executive-level personnel may need higher privacy standards.

Ultimately, security is not solely technical—better software or stronger encryption won't help when an attacker can simply call the CEO pretending to be her son's school and convince her to provide credentials. It's a human problem requiring awareness, education, and cultural change within organizations.

References

[1] *Síminn hf. - company information*, Accessed: December 7, 2024, Síminn hf. [Online]. Available: https://www.siminn.is

[2] *Síminn (iceland telecom ltd.)* Accessed: December 7, 2024. [Online]. Available: https://www.siminn.is

[3] Iceland ETF, *Siminn*, en-US. Accessed: Dec. 4, 2025. [Online]. Available: https://icelandetf.com/siminn

[4] Síminn hf., *Condensed consolidated interim financial statements*, Q1 2024 Financial Report, 2025.

[5] *Síminn hf. - employee information*, Accessed: December 7, 2024, Síminn hf.

[6] Síminn hf., *Grunnlýsing - base prospectus*, Accessed: December 7, 2024, 2025.

[7] *Stjórn og rekstur - governance and management*, Accessed: December 7, 2024, Síminn hf. [Online]. Available: https://www.siminn.is/fjarfestar/stjorn-og-rekstur

[8] *Discover subdomains - siminn.is*, Accessed: December 7, 2024, Netlas, 2025. [Online]. Available: https://netlas.io

[9] *Persónuvernd kærir símann til lögreglu*, Accessed: December 7, 2024, 2011. [Online]. Available: https://www.visir.is/g/20111849523d

[10] *Ákvörðun 7/2012: Ólögmætur verðþrýstingur símans hf.* Accessed: December 7, 2024, Samkeppniseftirlitið, 2012. [Online]. Available: https://www.samkeppni.is/media/akvardanir-2012/Akvordun-7_2012_Ologmaetur-verdthrystingur-Simans-hf..pdf

[11] *Síminn kærður fyrir verðþrýsting*, Accessed: December 7, 2024, 2010. [Online]. Available: https://www.visir.is/g/20101485220d

[12] *Síminn outage was not cyber attack*, Accessed: December 7, 2024, Oct. 2021. [Online]. Available: https://www.ruv.is/english/2021-10-12-siminn-outage-was-not-cyber-attack