Nicholas Petrovich
GRC Analyst (or Cybersecurity Strategist)
Date: July 14th, 20252

Title: Risk Analysis – ICC Cybersecurity Breach (July 2025)
Frameworks: NIST CSF + MITRE ATT&CK

Purpose: Demonstrate application of cybersecurity governance frameworks to real-world geopolitical events.

Disclaimer: This report is an independent analysis conducted for educational and professional demonstration purposes. It is based solely on publicly available information. The author has no affiliation with the International Criminal Court and does not claim access to internal systems or data.

1. Executive Summary

In July 2025, the International Criminal Court (ICC) experienced a targeted cyber intrusion—its second in under two years. This incident occurred during ongoing legal proceedings involving senior political and military leaders from Russia and Israel. Given the ICC's role in prosecuting war crimes, and the lack of financial motive or public attribution, this breach likely reflects a strategic espionage operation by a state-aligned threat actor. This report maps the incident to the NIST Cybersecurity Framework and MITRE ATT&CK, and outlines key governance failures, attack vectors, and corrective recommendations.

2. NIST Cybersecurity Framework Mapping

Nist Function	**Observed or Missing Controls**	**Commentary**
Identify	Limited third-party Governance; unclear asset inventory	Potential entry via outsourced systems or vendors without strong contractual controls
Protect	Weak access controls; no evidence of Zero Trust	High-value legal data likely stored without RBAC, encryption-at-rest, or identity segmentation
Detect	Delayed breach notification; unclear detection timeline	No signs of effective SIEM/logging or proactive monitoring from internal or external sources
Respond	Minimal public IR disclosure; no IOC sharing	Lack of transparency suggests absence of a formal response plan or external coordination
Recover	No evidence of backup activation or BCDR posture	ICC operations impact not clarified; may lack recovery maturity or reporting structure

3. MITRE ATT&CK Mapping

Phase	**Technique ID + Name**	**Description / Likely Use**
Initial Access	T1566.001 – Spearphishing via Service	Entry via compromised vendor, helpdesk, or legal correspondence
Execution	T1059 – Command and Scripting Interpreter	PowerShell or macro-based initial execution post-phish

Persistence	T1505.003 – Web Shell	Maintain access through vulnerable web-facing system
Privilege Escalation	T1068 – Exploitation for Privilege Escalation	Exploit of unpatched OS/app privilege misconfigurations
Defense Evasion	T1070 – Indicator Removal on Host	Wipe logs or disable auditing to cover tracks
Collection	T1119 – Automated Collection	Target legal documents, emails, case notes, and communications
Exfiltration	T1048.003 – Exfiltration Over Encrypted Channel	Transfer files securely to avoid detection
Impact	T1499.001 – Endpoint Denial of Service / T1531 – Account Access Removal	Potential goal: delay, disrupt, or sabotage legal operations

4. Governance Commentary

The ICC breach highlights a systemic failure in basic governance controls. Vendor risk management appears insufficient, with no evidence of contractual enforcement around cybersecurity standards. Role-based access, data segmentation, and encryption policies were either missing or poorly implemented. The absence of transparent incident response procedures suggests a lack of tested playbooks, board-level cyber oversight, or integration into global threat intelligence communities. These gaps represent not just technical exposure but critical weaknesses in governance maturity.

5. Recommendations

1.) Implement Role-Based Access Control (RBAC): Restrict case file access by legal role and clearance level to reduce exposure.

2.) Adopt a Zero Trust Architecture: Prevent lateral movement and privilege escalation in case of breach.

3.) Enforce Vendor Security SLAs: Require third-party systems to meet minimum compliance baselines (e.g., ISO 27001, NIST 800-171).

4.) Integrate into Threat Intelligence Sharing Alliances: Establish regular participation with INTERPOL or EUROPOL cyber fusion centers.

5.) Run Annual Incident Response Drills: Simulate politically motivated attacks to prepare legal and technical teams for coordinated response.

6. Conclusion

This breach reflects more than a technical failure — it is a direct threat to judicial independence in the digital age. Institutions handling politically sensitive information must be treated as high-priority cyber targets and protected accordingly. Without proactive governance, even the world's most powerful legal bodies are vulnerable to silent sabotage.