STRIDE + DREAD Threat Modelling

| Threat (STRIDE) | D | R | E | A | D | AVG |
| --- | --- | --- | --- | --- | --- | --- |
| Spoofing | 8 | 7 | 6 | 8 | 6 | 7.0 |
| Information Disclosure | 9 | 8 | 6 | 9 | 7 | 7.8 |
| Elevation of Privilege | 9 | 8 | 7 | 9 | 6 | 7.8 |
| Tampering | 7 | 6 | 5 | 6 | 5 | 5.8 |
| Denial of Service | 5 | 7 | 5 | 5 | 6 | 5.6 |
| Repudiation | 6 | 4 | 4 | 5 | 6 | 5.0 |

Score Scale

Each DREAD element is scored from 1 (Low) to 10 (High) based on:

* Damage Potential
* Reproducibility
* Exploitability
* Affected Users
* Discoverability

The average score is used to rank threats as:

* High (7–10)
* Medium (4–6.9)
* Low (<4)

Threat 1: Spoofing

Average DREAD Score: 7.0 → High Priority

Damage Potential (8): An attacker impersonated a senior regulatory officer, enabling unauthorized access to sensitive communications and control threads.

Reproducibility (7): Once a phishing email bypassed filters and credentials were captured, the attacker repeated spoofed interactions over multiple days.

Exploitability (6): Exploitation relied on user error and public information about officers—made easier due to optional MFA and legacy email clients.

Affected Users (8): Law enforcement officers, applicants, and internal IT staff were misled by the spoofed identity.

Discoverability (6): The spoofed activity went unnoticed for nearly six days due to weak email monitoring and no real-time alerts.

Justification:  
Spoofing succeeded due to gaps in user authentication (MFA optional), attacker social engineering, and system monitoring. This posed direct risks to operational integrity and trust with external stakeholders.

Threat 2: Information Disclosure

Average DREAD Score: 7.8 → Top Priority

Damage Potential (9): Exfiltrated documents included licensing approvals, audit schedules, and internal communications — exposing regulatory workflows.

Reproducibility (8): Once the attacker had inbox access, it was easy to browse, forward, or auto-export sensitive emails.

Exploitability (6): Moderate technical skills were required; the attacker used cloned domains and spoofed license processing alerts.

Affected Users (9): Citizens, auditors, IT, and law enforcement agencies—all became vulnerable to follow-on attacks or data misuse.

Discoverability (7): Despite known gaps in alerting, some signs were eventually detected — but only after six days.

Justification:  
Sensitive internal data was exposed and potentially distributed publicly or to threat actors. This poses regulatory, reputational, and operational risks — and would trigger mandatory disclosures under Jordanian data laws.

Threat 3: Elevation of Privilege

Average DREAD Score: 7.8 → Top Priority

Damage Potential (9): Gaining additional internal privileges could allow system reconfiguration, administrative actions, or expanded access to backend services.

Reproducibility (8): Attack logs show the impersonator attempted to manipulate internal IT communications more than once.

Exploitability (7): Access to the officer’s email enabled the attacker to potentially request access changes or mislead IT staff.

Affected Users (9): IT administrators, compliance officers, and anyone relying on that account’s authority.

Discoverability (6): Some privilege escalation attempts were stopped due to workflow anomalies—but not before several were forwarded.

Justification:  
Privilege escalation risks system-wide compromise. While some defenses worked, they depended on human judgment rather than robust automation or zero-trust enforcement.

Threat 4: Tampering

Average DREAD Score: 5.8 → Medium Risk

Damage Potential (7): Sending fake license approvals with embedded malware undermines DPSR’s legitimacy.

Reproducibility (6): Once credentials were obtained, fake responses could be sent multiple times.

Exploitability (5): Required some technical setup—malware injection into official templates.

Affected Users (6): Targeted citizens and applicants—possibly introducing malware to personal devices.

Discoverability (5): Detected only after reports from confused recipients.

Justification:  
The attacker weaponized official communication templates. While impactful, this threat was contained faster and had more external detection pathways.

Threat 5: Denial of Service (DoS)

Average DREAD Score: 5.6 → Medium Risk

Damage Potential (5): Email system downtime and redirection to alternative channels disrupted daily work.

Reproducibility (7): A spam or malware campaign could recreate the problem.

Exploitability (5): Somewhat technical—requires high-volume access or inbox flooding.

Affected Users (5): Primarily internal staff; law enforcement operations were delayed.

Discoverability (6): Disruption was clear after internal escalation.

Justification:  
This wasn’t a system crash but rather disruption through misuse. Though less damaging long-term, it affects operational continuity.

Threat 6: Repudiation

Average DREAD Score: 5.0 → Medium–Low Risk

Damage Potential (6): Attackers may deny sending malicious emails or requests, making legal tracing difficult.

Reproducibility (4): Depends on absence of logging and audit trails.

Exploitability (4): Requires attacker to anticipate investigation techniques.

Affected Users (5): Primarily affects legal/audit teams and accountability measures.

Discoverability (6): Lack of EDR and alerting makes action attribution harder.

Justification:  
Poor email and activity logging create risk in audits and compliance. While not immediately destructive, it complicates accountability.

Top 3 Prioritized Threats (Based on DREAD Averages):

1. Information Disclosure (7.8)
2. Elevation of Privilege (7.8)
3. Spoofing (7.0)

2.5.2

Define Level 5 Variables

Contact Frequency (CF)

Data: 5 spear-phishing emails/month → 60/year; 18–24 whaling attempts/year

Min: 5

Most Likely: 18

Max: 24  
Justification: Logs show ~18–24 whaling attacks/year targeting senior staff; phishing volume ~5+/month.  
Confidence: Medium

Probability of Action (PoA)

Min: 0.1

Most Likely: 0.19

Max: 0.42  
Justification: Phishing simulation click rates dropped from 42% → 19%; attacker used real officer names and license codes.  
Confidence: Medium

Threat Capability (TCap)

Min: 0.6

Most Likely: 0.9

Max: 1.0  
Justification: APT actor with cloned domains, VPN, SSL, and advanced phishing methods.  
Confidence: High

Resistance Strength (RS)

Min: 0.2

Most Likely: 0.48

Max: 0.6  
Justification: MFA is optional, phishing filter blocks only ~48%, legacy email clients still used.  
Confidence: Medium

Loss Magnitude

Primary Loss (PL)

| Type | Min | Most Likely | Max | Justification |
| --- | --- | --- | --- | --- |
| Productivity Loss | $10,000 | $20,000 | $30,000 | Email outage + delays |
| System Replacement | $15,000 | $25,000 | $40,000 | Legacy system upgrade |
| Incident Response | $60,000 | $90,000 | $120,000 | Forensics, audits, EDR |

Secondary Loss Event Frequency (SLEF)

Min: 0

Most Likely: 0.3

Max: 0.5  
Justification: 2-week delay in breach disclosure caused public scrutiny. Citizens and media expect strict confidentiality.  
Confidence: Medium

Secondary Loss Magnitude (SLM)

| Type | Min | Most Likely | Max | Justification |
| --- | --- | --- | --- | --- |
| Regulatory fines | $0 | $75,000 | $250,000 | Due to exposed personal data |
| Reputation damage | $30,000 | $60,000 | $100,000 | Public/media backlash |
| Legal response (lawsuits) | $5,000 | $20,000 | $50,000 | Data privacy & trust cases |

2.6

| Function | Relevance to Phishing Incident | DPSR Evaluation | Improvement / Recommendation |
| --- | --- | --- | --- |
| Identify (ID) | Determines what assets, data, and personnel are critical, and defines roles and responsibilities. | DPSR had gaps in understanding critical assets. MFA was optional for senior staff, and asset protection responsibilities were unclear. | Conduct full asset inventory and role-based access classification. Define cybersecurity responsibilities clearly for all staff levels. |
| Protect (PR) | Encompasses access control, training, and security policies. Critical for preventing unauthorized access. | Weak implementation: legacy email clients, optional MFA, 48% phishing filter effectiveness. Senior staff less aware of phishing risks. | Mandate MFA for all staff, upgrade email systems, and enhance phishing training — especially for leadership. |
| Detect (DE) | Identifies anomalies and potential security events quickly. | Ineffective: 6-day delay in detecting the phishing breach shows poor anomaly detection and monitoring. | Implement real-time monitoring with SIEM tools and establish alert thresholds. Include behavioral analysis for unusual access. |
| Respond (RS) | Guides containment and mitigation of incidents. | Response was delayed and lacked preparedness. Disclosure to citizens took two weeks. | Develop and test an Incident Response Plan (IRP). Run regular tabletop drills for faster and more coordinated response. |
| Recover (RC) | Ensures systems return to normal operations while minimizing damage. | Response involved server replacement and audits, but no clear recovery strategy or post-incident improvements were highlighted. | Build a formal recovery plan with defined roles, timelines, and communication protocols. Incorporate lessons learned into future operations. |

2.7

Application of the Jordan National Cybersecurity Framework (JNCSF) and Jordanian Cybersecurity Regulations to the DPSR Phishing Incident

The Jordan National Cybersecurity Framework (JNCSF) sets the national vision for securing cyberspace by institutionalizing risk management, enhancing national capabilities, promoting awareness and training, enforcing cybersecurity economics, and enabling collaboration across sectors. Its core objectives include establishing governance structures, enforcing regulatory compliance, and ensuring readiness to detect, respond to, and recover from cyber threats.

Two key Jordanian regulations directly apply to the DPSR phishing incident:

Cybersecurity Law No. 16 of 2019: Mandates that public institutions like DPSR implement protective measures, maintain incident response readiness, and coordinate with the National Cybersecurity Center (NCSC) for threat handling and information sharing.

Personal Data Protection Law No. 24 of 2023: Requires explicit consent for data use, proper data handling protocols, and timely notification of data breaches to affected individuals and authorities (typically within 72 hours).

Based on the scenario, DPSR only partially aligned with these regulations. While the department did notify citizens after the phishing attack, the 2-week delay violates expected standards under the PDPL. Additionally, incident detection lagged for six days, revealing gaps in monitoring and response capabilities. The continued use of legacy email clients and the absence of enforced multi-factor authentication (MFA) for senior staff further highlight non-compliance with both technical controls and governance best practices under JNCSF and the Cybersecurity Law.

To achieve compliance and strengthen its cybersecurity posture, DPSR should:

Mandate MFA for all users, especially those in leadership roles;

Upgrade to modern email and monitoring systems, ensuring real-time detection and alerting;

Conduct mandatory phishing awareness training, targeting executive-level staff;

Align breach notification processes with PDPL requirements to issue alerts within 72 hours;

Engage with the NCSC to report, analyze, and respond to threats in a nationally coordinated manner.