**MSPEI Playbook for Data Breach/Theft**

**Key Members and Roles:** [**https://www.mspei.org/about/**](https://www.mspei.org/about/)[**https://www.mspei.org/contactus/**](https://www.mspei.org/contactus/)

**MSPEI Leadership Team:**

* Dr. Krista Cassell, President
* Dr. Scott Cameron, Chair
* Dr. Padraig Casey, Past President

**External IT Security Partner:**

Require the service of reputable IT security firm. Designate a primary contact person from the external partner to be part of the incident response team.

**Financial Team:**

* Economics Advisor: Derek Law
  + Mr. Law is the financial representative responsible for providing insight on potential financial impacts of a breach and reporting requirements during and after a breach.
* Finance Manager: Doug Carr
  + Mr. Car is overseeing all the payable and receivables of the organization and will act as Derek’s backup if he must be absent.

**Communication team:**

* Associate Director of communications: Sheila Kerry
  + Mrs. Kerry oversees strategies for managing the organization’s reputation during and after an incident. She will establish clear lines of communication especially with the media, potential affected patients, healthcare stakeholders, regulatory bodies, and financial partners.

**Incident Response Coordinator (IRC):**

Appoint an Incident Response Coordinator from within the organization, responsible for managing communication and coordination during data breach incidents. The IRC will be the constant point of contact and work closely with the external IT partner, Sheila Kerry from the Communication team and relevant stakeholders. In MSPEI position, the coordinator should be Scott Cameron (Chair). He will relay any development to the president. Each time you will be encountering the IRC in the present document, know that we refer to Scott Cameron. It is possible that the name of M. Scott and the IRC may duplicate because he holds two positions. Namely the Chair and the IRC. MSPEI has been advised to appoint an official IRC, but until they do, M. Scott will hold the position.

**NIST 7 Steps Risk Management Framework** [**https://csrc.nist.gov/Projects/risk-management/about-rmf**](https://csrc.nist.gov/Projects/risk-management/about-rmf)

**Step 1 Preparation:**

Identify the key members and roles within the incident response team:

**MSPEI Leadership Team:**

* Dr. Krista Cassell, President
* Dr. Scott Cameron, Chair
* Dr. Padraig Casey, Past President

**External IT Security Partner:**

* Reputable IT security firm (primary contact designated)
* Reputable Cyber Forensics firm

**Financial Team:**

* Economics Advisor: Derek Law
* Finance Manager: Doug Carr

**Communication Team:**

* Associate Director of Communications: Sheila Kerry

**Incident Response Coordinator (IRC):**

* Dr. Scott Cameron (Chair)

**Step 2 Categorize:**

Engage with outside third parties such as the above-mentioned IT security firm and the forensics firm

**Step 3 Select:**

Prepare for incident response (see last page for a detailed incident response plan):

* Ensure the incident response team is familiar with MSPEI systems and operations.
* Establish clear communication channel among team members and stakeholders.

**Step 4 Implement:**

identify and verify data breach incidents:

* Collaborate with the external IT partner to detect and verify data theft incidents through proactive monitoring and analysis.

**Step 5 Assess:**

Coordinate and execute incident response actions:

* Isolate affected systems and devices under the direction of the IRC and the external IT partner.
* Eradicate the root cause of the incident in collaboration with the external IT partner.

**Step 6 Authorize:**

Obtain approval for recovery and remediation actions:

* Restore affected systems and services in consultation with the external IT partner, the IRC and the forensics third party.

**Step 7 Monitor:**

Continuously assess the incident response process:

* Conduct a post-incident analysis with input from the external IT partner and a third-party cybersecurity forensic partner.
* Collaborate with Derek Law to analyze the financial impact and incorporate insights into recommendations for improvement.

**Recovery and lesson learned from NIST RMF**

**Communication and Escalation:**

* Notify all affected parties, including members, MSPEI Leadership (Dr. Krista Cassell, Dr. Scott Cameron, Dr. Padraig Casey), regulatory bodies, with guidance from the external IT partner, Sheila Kerry and oversight by the IRC.
* Escalate the incident to the MSPEI Leadership Team (Dr. Krista Cassell, Dr. Scott Cameron, Dr. Padraig Casey) for decision-making.

**Reputation Management:**

• Discuss strategies for managing the organization's reputation during and after an incident, emphasizing clear and consistent communication, with Sheila Kerry playing a vital role in communication strategies.

**Documentation and Follow-up:**

**Record Keeping:**

* Maintain an incident log detailing actions taken, including collaboration with the external IT partner, supervised by the IRC.

**Continuous Improvement:**

* Regularly update the playbook based on insights from the external IT partner, Sheila Kerry, the IRC, and third parties.

**NIST Steps for Incident Response:**

1. **Preparation**

* Establish a response team including MSPEI Leadership (Dr. Krista Cassell, Dr. Scott Cameron, Dr. Padraig Casey), the external IT partner, and the Incident Response Coordinator (IRC).
* Ensure the external IT partner and the IRC have a good understanding of MSPEI's systems and operations.
* Make sure that all the procedures are well known from all parties.

1. **Identification:**

* Collaborate with the external IT partner (with the guidance of the IRC) and Sheila Kerry to detect and verify data theft incidents through proactive monitoring and analysis.

1. **Containment:**

* Isolate affected systems and devices in coordination with the external IT partner (under the direction of the IRC).
* Utilize backup systems to maintain critical operations.

1. **Eradication:**

* Work with the external IT partner (under the supervision of the IRC) and Sheila Kerry to identify and eliminate the root cause of the data theft incident.
* Implement security patches and updates with IT partners and/or IRC approval.

1. **Recovery:**

* Restore affected systems and services in collaboration with the external IT partner (in consultation with the IRC).
* Validate the integrity of the restored environment with a reputable third-party cybersecurity forensic partner.

1. **Lessons Learned:**

* Conduct a post-incident analysis with input from the external IT partner, the IRC, Sheila and the forensics third-party to identify vulnerabilities and recommendations for improvement.
* Document lessons learned for future incident prevention and response.
* Collaborate with Derek Law, the Economics Advisor, to analyze the financial impact of the incident and identify cost-effective measures for improving incident prevention and response strategies. Incorporate his insights into the recommendations for improvement.