valencia

September 27, 2024

The Byte Stops Here

When Canadian Federal Departments Exercise Cybersecurity Preparedness

Exercising the Physical and Virtual

This week, we revisited the results of a cybersecurity exercise conducted last fall across federal government departments. The October 2023 Cy-Phy Exercise was planned for over two years and involved over 150 private and public sector organizations. They were allowed to explore the relationship between cyber and physical realities and to improve their knowledge of organizational security measures. The purpose? Improve the exchange of risk-based information, identify best practices, improve cross-sector interdependency awareness, and assess incident response capabilities.

Layered Lessons: Training, Partnerships, Decision Making, and Information Sharing

The exercise provided valuable insights for the participants, but also for Canadian organizations writ large. We saw this in looking at the report's observations.

1. Participants witnessed, and found taxing, the cascading effects of cyber incidents on physical infrastructure and the complexities involved in addressing both fields. The need for ongoing training to give staff skills needed to effectively tackle cyber and physical security challenges and enhance policies for business continuity.
2. Pitfalls were seen when public and private sector groups were meant to collaborate, pointing to the need for a holistic approach integrating cyber and physical security. The exercise showed that protocols for timely information sharing with law enforcement and regulatory bodies were essential when responding to incidents.
3. Participants struggled with aligning on priorities and sharing intra-departmental information. Legal experts' roles were affirmed, highlighting the importance of their timely involvement during an incident response process.
4. There were delays in sharing sensitive information, pointing to a need for timely updates to facilitate decision-making. Gaps were seen in participants' communications plans and outreach contingencies.

Ultimately, the exercise effectively identified key opportunities for enhancing resilience within the Canadian critical infrastructure community in the face of cyber threats with physical repercussions. Marked gap in preparedness and training in organizations was acknowledged, highlighting the need for early commitment and active involvement in planning exercises.

Resilience Reboot: What Can We Learn From This Exercise?

We were encouraged to see that the federal government sponsored and organized this exercise. Information and operational technology are increasingly intertwined, but we have seen similar dynamics to those highlighted in the report in the tabletop exercises we conduct. Incident response is essential nowadays, we advise the following simple steps to stay away from the grasp of attackers:

1. Training. Staff members are your first line of defense against cyberattacks. Make sure that they have opportunities to continuously improve their knowledge of cyber threats and the complexities of their own domains. Foster a culture of cyber awareness: make sure staff know who to speak to for cybersecurity and be open to feedback.
2. Define roles and collaborate. Ensure that members of your incident response team know how to react and what to do. Test how well you collaborate and codify teams' responsibilities in incident response, disaster recovery, and business continuity plans. Establish clear roles and responsibilities to enhance coordination during incidents. Socialize incident response plan contents with those involved.
3. Don't forget third parties. Know which regulatory bodies and law enforcement agencies you should talk to, when, and with how much detail in the event of an incident and codify it in your documentation. Know which third parties, including legal representatives, public relations firms, and insurance brokers, you should engage at which point in time.
4. Test, test, test. Regularly conduct incident response exercises that simulate real-world scenarios to identify weaknesses in your policies, plans, and protocols. Make sure that simulations test all aspects of your incident response readiness.
5. Keep learning. Integrate findings from conducted simulations, threat landscape changes, and procedural changes in your plans, policies, and processes. Regularly review your plans to ensure that they remain relevant and actionable.