Cyber Security Breach at a Water Service Station

Overview:

A water service station system was compromised when one disgruntled employee of the Contractor Firm that provided IT/ Control system technology to the Station. He was an "insider" with significant knowledge of the controls and with malicious intent. He launched an attack causing considerable damage and pollution to the neighbourhood.

The Challenge:

The service contract was deficient or inadequate concerning the contractor firm's responsibilities

- Management, technical and operational cyber security controls required
- Personnel security controls that applied to its employees such as background investigations and protection from disgruntled employees

A number of anomalous events occurred before recognition that the incidents were intentional.

- As a skilful adversary, Boden was able to disguise his actions.
- Extensive digital forensics were required to determine that a deliberate attack was underway

There were no existing cyber security policies or procedures.

There were no cyber security defences.

The Result : Attack

The former employee of the contractor firm used a stolen radio and a stolen computer to tamper with internal mechanism causing failure at many levels. Finally he caused spillage of raw sewage into parks, lakes and the entire neighbourhood causing pollution, stench and deaths to marine lives.

The Solution:

Most of the malicious activities could be arrested by the implementation of SP 800 53 controls.

Every organization should have cyber security policy and procedures. There are many discretionary and judgmental activities that require guidance. Common sense isn't sufficient; dos and don'ts need to be written down.

Neither the water station nor the IT/Control firm had cyber security policies or procedures in place. For example:

AC-18 Wireless Access Restrictions (i) establishes usage restrictions and implementation guidance for wireless technologies; and (ii) authorizes, monitors, controls wireless access to the information system. Such policy would have addressed the two-way radio that was used by the attacker.

It is prudent for to have a key personnel clause to protect the client from unilateral changes in key personnel by the contractor. In general, the contract should extend applicable Personnel Security controls to contractor employees. Determining which controls to apply to on-site contractor personnel may not be easy since it depends on the role played by the individual.

Personnel's need must be trained in preventing, recognizing, or responding to cyber-related incidents. Security awareness and training inform personnel of the information security risks associated with their activities and their responsibilities in complying with

Organizational policies and procedures designed to reduce these risks.

The communications and control components lacked sufficient audit capability to support fault determination or forensic analysis. Audit is concerned with collecting information that is significant and relevant to the security of the information system. Audit supports other control families such as incident response, access control, and flaw remediation.

Effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability

The Outcome

• **Continuous improvement:** the methods that determine what is being attacked and how to stop an attack, are constantly being monitored.

• **Identify at-risk users:** Account takeover, disgruntled employees, malware actions. Streamlined incident investigations – Immediate insights into risky user behaviours, action and activity history. 360°Analysis – Perform analysis of activities at the end point, insights from network data, and cloud activities. Identify Insider Threats

• **Single view of vulnerabilities:** Single centralised view of all vulnerabilities with their status and their context. Prioritise by threat and impact – Analyses threat intelligence, vulnerability status and network communications to assess true vulnerability risk.