**Introduction**

The news of data breaches and online frauds has become a matter of regular occurrence, which gives a constant reminder of how organizations need a robust strategy for fraud prevention and cyber security. Though the private sector usually grabs the headlines, it often goes unnoticed that the public sector is facing similar incidents. Working in the public sector requires you to serve the public and citizens can have access to healthcare, education, parks, libraries and more. Likewise, judicial system, law enforcement, defense and other government levels are vital components of society. Because of their critical role, these public sector departments and organizations have now become key targets for cyber-criminals. High-profile events such as elections and Olympics have also been victims of fraud attacks in recent years, pressing government authorities to prioritize cyber security.

**Current State of Cybersecurity in Public Sector**

According to a research published by Freedom of Information in 2019, about eighteen percent respondents from different public sector organizations in U.K reported more than 1000 cyberattacks in the previous year (which were about 14 percent more than in 2017). Among these, 95 percent respondents were using antivirus, firewall and malware protection. On the other hand, about 38 percent of respondents said they had not experienced any cyberattacks at all, compared to 30 percent the year before that.

The types of attacks mostly faced by the respondent organizations included phishing (95 %), malware (86 %) and ransomware (54%). Other attacks such as targeted attacks from insiders or malicious cybercriminals were faced by only 3 percent of respondents. This explains why the typical defenses used by these public sector organizations were antivirus software and firewalls. However, other critical defenses were still lacking where approximately only 70 percent organizations were using log management or network traffic analysis, tools that can help monitor unexpected activity.

**Common Threats Faced in Public Sector**

Phishing, ransomware and email malware are common threats faced by public sector organizations. Loss of personal data as a result of criminal intelligence is used to commit online frauds and identity thefts. The sector is also at risk from illegal cryptomining, cyber espionage, and software supply chain attack.

Although these threats may have a significant impact, there are other areas of concern such as data leakage, with seemingly lesser impact but greater importance in terms of public eye. Occasionally, employees may pose serious threat by losing important data in tablets, memory sticks or laptops left in public trains or by using public WiFi access points. Moreover, successful cyber frauds are mostly the result of insider mistakes such as opening phishing emails, zero-day attack and third-party errors.

What is even a bigger problem is the failure of public organizations to fix known vulnerabilities. According to Ponemon institute, only 28 percent of public organizations had a very high ability to “recover” from cyber attacks and only 19 percent had a very high ability to “prevent” attacks.

**Importance of Cyber security awareness and Preparedness in Public Sector**

The importance of awareness of potential frauds in the public sector needs to be taken very seriously. It is essential for public organizations to promote and aware internal staff and public about potentially fraudulent activities and how they can be identified and stopped. Governments should establish a general fraud awareness program which can then be implemented across all public organizations. We have seen so many instances where organizations rush into implementing fraud protection systems right after suffering a breach or attack. This reactive approach usually results in unsuccessful fraud protection and puts the organization’s innovation pipeline in jeopardy. Furthermore, companies that don’t apply a proactive strategy to prevent fraud risk their reputation as being irresponsible and incompetent, which can result in revenue loss and compromised organizational image.

**How can Public Sector Guard Against the Threats?**

**Cybersecurity policy based on established Guidelines and Standards**

State governments need to implement federal frameworks (for instance NIST Cybersecurity Framework) to provide means of baselining effective and strong cybersecurity state policy. These frameworks provide strategic and high-level view of cybersecurity risk life cycle to allow states to be in better position to understand fraud risk and apply the best practices. This can enable them to manage risk and improve security of their critical services and infrastructure.

**Establish cybersecurity council with industry and academia**

As academic disciplines and industry sectors hold better expertise in cybersecurity and fraud prevention, their experts are likely to be eager to share their knowledge to formulate public sector fraud management policy. These assets can be coordinated to develop strategies for the government to help respond to real and potential threats.

**Create cybersecurity culture**

In most of the cases, whether public or private organizations, the weakest link in information leakage and security compromise is careless or uninformed personnel. Employees should be empowered with skills to be proactive and ready to face increasing threats. In order to reduce risk from cyber fraud and related attacks, there needs to be a culture of cybersecurity that can only prevail when public organizations implement robust cybersecurity training programs for all their employees.

**Integrate fraud prevention into every step of strategic planning**

In addition to protection of IT assets from online frauds, there needs to be a focus on making public services resilient in times when an attack actually happens. This can not only ensure security of public departments but also create opportunity to create long-term, comprehensive strategies to set them on path to digital transformation.

**Consider cyber insurance for protection of public assets**

Public sector can complement its cyber risk management process with cyber insurance for risks that cannot be completely mitigated. Cyber insurance benefits are not just financial, but also indirectly forces organizations to meet a certain criteria of security practices in order to be able to qualify for the insurance.

**Conclusion**

There is no denying that cyberattacks can cause financial, regulatory and organizational image issues. In some cases, it becomes practically impossible to recover from large scale professionally planned fraudulent attacks, especially for public sector. Hence, the government needs to stop considering fraud prevention methods as burdening expenses and take them as necessary measures for growth and longevity of public sector organizations.