Int Tec Solutions

Cybersecurity in the Public Sector

Cybersecurity and the Persistent Digital Threats

Cybersecurity and data breaches are a looming threat for businesses in any industry. As quickly as IT tools are developed to combat data threats, new and increasingly sophisticated attack methods are developed and implemented on a global scale. These attacks target businesses across many industries, and often cause significant damage.

For organisations in the public sector, the stakes are even higher, and these institutions need the highest level of complete protection that is available. Along with the Energy Industry and SME's - Healthcare, Higher Education and other Government Agencies represent the top 5 industries that are most vulnerable to cyber-attacks[1].

Staying One Step Ahead

In the USA, Homeland Security has reported a 10-fold increase in the number of cyber incidents reported to the Department of Human Services between 2006 and 2015 that impacted the public sector. Moreover, with the rapid proliferation of an expanding number of digital devices combined with the increasing level of interconnectedness, cyber threats are constantly-evolving and becoming progressively more elaborate.

The challenge here lies in ensuring a comprehensive cybersecurity plan is implemented; this means it should be one step ahead of any potential threats. Any plan must embrace a holistic approach that includes common best practices, employee engagement and training, and extensive knowledge of threat risks and mitigation actions.

Operating within the Victorian Protective Data Security Framework (VPDSF)

Because public sector information is so valuable and targeted, the Victorian Protective Data Security Framework was created for public sector organisations operating in Victoria and compliance is mandatory. This framework was developed as a means to help these organisations improve their data security practices and policies, manage risk and promote innovation that can lead to increased productivity. The agency behind the VPDSF, the Office of the Victorian Information Commissioner, has outlined a 5-step action plan that includes specific mandatory documents to be completed and policies implemented. Once a comprehensive Protective Data Security Plan has been adopted, regular reporting and review of the plan is required.

While this framework is a huge asset in planning to ensure the integrity of data is safeguarded in the best manner possible, it can be a daunting process for many organisations. The framework includes 18 high-level mandatory standards, each with 4 distinct protocols. In addition to this, OVIC will oversee the compliance and monitoring activities related to the VPDSF, which may include audits.

Achieving the goals laid forth by the VPDSF can be intimidating any sized organisation, which is why the professionals at Int Tec Solutions can assist with every component to ensure full compliance is achieved. This service can begin during the planning process with the Risk Profile Assessment and carry through the entire process, during which only reporting and mandatory reviews are required. Despite the low level of requirements that are formally dictated by the VPDSF once the Protective Data Security Plan has been adopted, Int Tec Solutions will continue to be a proactive party that seeks out new vulnerabilities in a rapidly changing data landscape and working to ensure that these threats are properly accounted for.

[1] CD Networks. (2018, February 16). The 5 Industries Most Vulnerable to Cyber-Attacks.
2. US Department of Homeland Security. (2018, May 15). US Department of Homeland Security Cybersecurity Strategy.

The Int Tec Solutions Advantage

Int Tec Solutions has the high-level of expertise necessary to provide a full range of IT services to those operating in the public sector. Int Tec Solutions also recognises that governmental agencies also serve as trustees to public funds, which is why Int Tec's commitment to cost-effectiveness becomes a significant factor their ability to provide superior service to those operating in the public sector.

While there is no miracle solution or silver bullet that can prevent any attack, Int Tec Solutions' strategy is based on a multi-tiered approach to security that can often reduce the threat level as well as increase an organisation's ability to mitigate the threat and in the event of a successful data breach, minimise the amount of damage that can occur.

Solutions Made Simple

There are many benefits in selecting Int Tec Solutions as a trusted partner that can assist with all of your cybersecurity needs. By letting our professionals handle the day-to-day tasks that ensure security is at its peak performance, you can trust that the threat of a data breach (and its corresponding adverse impact on reputation) will be minimised. Int Tec Solutions can provide a hand-on approach that applies the 6 Points of Comprehensive Cyber Security to your organisation. This safeguards your organisation from noncompliance and provides enhanced internal security practices. With regular monitoring and continuous identification of emerging and evolving threats, Int Tec Solutions can address these vulnerabilities quickly and respond accordingly. By contacting our experts, you can rest assured that your organisation's IT security measures are ahead of the game.

Int Tec Solutions 6 Points of Comprehensive Cyber Security

Identification	Vulnerability	Disruption	Mitigation	Response	Stabilisation
Audit network environment Prioritise threats as they are detected Educated on new threats and vulnerabilities Security awareness Security training	Identify risk factors Create comprehensive security road map Train employees on threat response Ensure all network components are up-to-date and appropriate patches are installed Test security routinely to identify weaknesses Review access to ensure data is accessed by only those who need it	Install and update all anti-virus, anti-spyware and anti-malware programs Develop and implement a real-time monitoring plan Identify and implement appropriate response Coordinate with other agencies if necessary Cooperate with law enforcement when criminal activity is detected Facilitate communication between response team members to ensure a rapid and effective response	Create situation-based response plans that can be enacted quickly Assist with backing up all necessary data to migrate a massive data loss Communicate with team members to get systems restored quickly Communication with business leadership to ensure compliance to public reporting requirements Analyse past data breaches and successful attacks to identify areas for improvement	Maintain an active role in network assessments Work with in-house IT team to identify the best solutions to meet the intended business function Conduct thorough research on new network elements to identify any potential weaknesses	Develop security policies Train staff on best practices Advise on IT strategies that will facilitate the long-term business goals Choosing an SEO expert (identifying key indicators of knowledge, experience and depth) Continue assessing and re-assessing to ensure that the best solutions are in place Develop long-term preventative maintenance plan/schedule

1. Risk identification

As experts with decades of experience, the professionals at Int Tec Solutions stay up to date on established threats that continue to evolve as well as new, emerging cyber threats. The breadth of knowledge allows them to rapidly and effectively identify and prioritise cyber threats so that prevention and response measures can be executed quickly.

2. Vulnerability reduction

By employing all available security measures and empowering employees within the organisation with the knowledge necessary to reduce cyber threats, clients can be assured that their level of vulnerability is greatly reduced.

3. Disruption and prevention of attacks

With their extensive level of threat intelligence, the professionals at Int Tec Solutions can quickly detect data corruption and configuration anomalies that are red flags of a cyber-attack. This ability to quickly recognise an attack is the biggest factor in preventing data breaches.

4. Mitigation of incidents

Despite providing the best security measures available, no organisation is 100% immune from a cyber-attack, which is why Int Tec Solutions also works with their clients to develop mitigation plans so that data losses and downtime are reduced or eliminated.

5. Respond to changes in the network

With the rapid progress of digital technology, the only constant has been persistent change. As new applications and infrastructure solutions are developed, the older ones are replaced. The rise in cloud computing and the rapid proliferation of the Internet of Things (IoT) is also contributing to the fluidity and mutable nature of network environments. Int Tec Solutions is committed to providing the highest level of security for the unique network needs of their clients, no matter how much those needs may change.

6. Work to stabilise the entire cyber landscape

As the cyber security plan begins to take shape, the key to ensuring long-term security is empowering organisations in their ability to create policies and education on the importance of maintaining security. In this role, clients can depend on Int Tec Solutions to serve as a trusted and knowledgeable advisor that will help to develop successful strategies that support long-term cyber security.