CASE STUDY: The Department of Education and Early Childhood Development (DEECD)

State of Victoria's DEECD partners with IPSec to protect Privacy and Information Security around the clock

State Government Victoria Department of Education and Early Childhood Development

Annual Budget	$11.6Bn (2013-2014)
Employees	75,000
Founded	1872
Headquarters	East Melbourne
Market Vertical	Education
URL	www.deecd.vic.gov.au

Client Profile

Founded more than a century ago, Victoria's Department of Education and Early Childhood Development (DEECD) is responsible for the education of more than 550,000 students. DEECD manages one of the largest network infrastructures in Australia with their IT group overseeing service delivery to more than 1800 schools located at urban and rural sites. Like all State Government entities, they are under constant pressure to rein in costs while improving levels of service delivery and embrace emerging technology. As user demands have grown, the IT Department must constantly innovate, invest in new technology and provide high levels of security to screen and protect their users from potential harm.

Photo Credit: Mark Calleja

Executive Summary

Protecting the security of DEECD's stakeholders is a daunting task for the department's dedicated Information Technology team. The organisation must secure 450,000 devices, meet child protection guidelines while complying with onerous Federal and State compliance mandates. To add further complexity to the mix are 4 internal and 6 external annual audits conducted by the department and Victoria's Auditor General's office. To help solve this business challenge, DEECD selected highly respected Managed Security Service (MSS) provider IPSec to tailor a monitoring and management service to meet their unique requirements. IPSec provides DEECD with industry leading response times of 15 minutes if a severe threat or fault is detected supported with granular reporting to enable forensic incident management analysis.

- Protect the privacy of stakeholders in compliance with Victoria's Information Privacy Act 2000
- Deliver around-the-clock protection with industry leading response times of 15 minutes
- Provide a pivotal piece of DEECD's risk management and business continuity strategy at a lower cost than resourcing the role internally
- Independently audit and monitor security, offering granular and forensic reporting capabilities while providing DEECD administrators with real-time visibility into operating parameters
- Consult with IPSec's certified engineers to exchange knowledge and regularly review DEECD's overall security posture

> "We needed a Security Partner who was highly skilled, responsive and flexible. IPSec have exceeded our expectations"
>
> Gavin Russell
> IT Operations Manager – DEECD

Business Driver

The DEECD is under the constant scrutiny of numerous authorities responsible for operational oversight to ensure stakeholder privacy and intellectual property is protected. Prior to IPSec assuming responsibility for providing DEECD's Managed Security Services (MSS), the increasing demands were proving too challenging for the incumbent vendor to keep pace with. Providing in-house services was proving difficult with highly paid IT Security staff in great demand and prone to making frequent career changes. A further concern for the IT management team was that contractors could not be contacted or were unavailable when an incident was detected: they needed an organisation that could learn their environment, understand their security challenges and provide around the clock monitoring and escalation services if the severity of the risk warranted this response.

IPSec Business Solution

The DEECD clearly defined their business needs for monitoring and managing their security infrastructure. When the engagement began a complete security audit was undertaken with all appropriate hardware checked for correct configuration and software, firmware and patching verified or updated. This was followed by a password refresh coupled with device and application hardening to improve resilience and reduce the surface area exposed to possible threat. With the baseline established, an industry leading service level response time of 15 minutes was established and risk reduction targets were set to identify and mitigate security risks. The most important deliverable was granular reports that drilled down to zones and devices permitting unprecedented insights into security operations in real-time. This simplified trend analysis and rendered greater meaning from the previous logging and reporting systems.

Summary

Managing Information Security is an enormous task for every enterprise. Providing an organisation with high level security skills and providing 24*7 protection is demanding and extremely costly. By partnering with IPSec, the burden of protecting stakeholders is shared and knowledge exchanged at prescribed intervals. IPSec is a critical contributor to the department's risk mitigation strategy providing security expertise on call to ensure DEECD's operating environment is continuously protected.

Scope of Engagement

IPSec's managed security service monitors core infrastructure at DEECD's data centre and corporate headquarters. Incidents are logged and correlated by Security Incident Event Management (SIEM) software with anomalous behaviour flagged and remediation escalated if conditions are outside of acceptable operating parameters. If any incidents pose a threat to the integrity of DEECD's network or service availability, the IPSec Security Operations Centre (SOC) alerts DEECD within a 15 minute period in strict compliance with their service level agreement and remediation actions are commenced.

Services

- Comprehensive security audit and remediation
- Device hardening and auditing
- Managed Security Service (MSS) 24*7*365
- Incident event response time of 15 Minutes
- Vulnerability Identification, Intrusion Detection and Prevention (IDP)
- Application and firmware updates applied within hours of their release
- Continuous Security Improvement Program (CSIP)
- Highly secure log file storage and archiving services

Reporting

- Secure management portal providing real-time visibility into security operations and incident remediation
- Compliance with service level agreements
- Monthly review and knowledge transfer meetings
- Incident management ticketing system updates and estimated task remediation time-line

ipsec

Please call us on 1300 890 902

About Us

IPSec specialise in protecting your information assets and mitigating security risks. Our team of highly skilled professionals design, implement, audit, and manage every aspect of your information security environment. By applying industry best practice to business processes, IPSec offer unrivalled service levels that protect your organisation and improves your overall security posture.

To find out more visit our website www.ipsec.com.au

Photo Credit: Flickr