Hewlett Packard Enterprise

Case Study

Origin Energy achieves cyber security transformation

HPE Security Services drives Origin Energy Security Transformation Programme success

Objective
To achieve better visibility of the security environment across its widespread production and operational assets

Approach
Origin Energy initiated a Security Transformation Programme, seeking a partner to deploy the cyber security solution

IT Matters
- Managed IT risks effectively, efficiently and proactively
- Ensured alignment with the longer term Cyber Security Transformation Programme
- Minimised the likelihood and impact of cyber security-related threats and incidents

Business Matters
- Improved crisis management response in the event of cyber security incidents
- Prevented unauthorised access and the risk of adverse impacts on safety and business operations

Origin Energy initiated a Security Transformation Programme to achieve better security visibility across its business. Hewlett Packard Enterprise deployed a Managed Security Services capability including HPE ArcSight SIEM, McAfee® network IPS and anti-malware to help execute the expanded IT risk and security strategy.

Connecting resources to market vision
Origin Energy is Australia's leading integrated energy company with a rich heritage in gas exploration and production, power generation and energy wholesaling and retailing. It has more than 4.2 million customers throughout Australia and New Zealand, approximately 6,000 employees.

Origin Energy is the largest owner of natural gas-fired power stations in Australia and also produces power from coal, wind, solar, pumped water storage and cogeneration plants. The company has major offices across four state capital cities, as well as regional sites.

> "Cyber security is key to each of our business units, and our management approach has to be holistic to make sure we protect what is important to the organisation, while enabling us to take advantage of and leverage more technology in a safe manner."
>
> — Christoph Strizik, head of IT risk and information security, Origin Energy

The company's vision is to connect resources to markets while striving to create more valuable social, environmental and economic outcomes for society. This vision is supported by a philosophy that recognises the energy supply chain is being shaped by a growing global demand for energy, technological innovations and climate change concerns; all against a background of the need for greater energy efficiency.

Christoph Strizik, head of IT Risk and Information Security for Origin Energy, explains, "Our operation is centred on two business units. The energy markets business focuses on retail and wholesale energy, our renewable energy portfolio such as solar and wind, and also our online digital presence. The second part of our business is integrated gas which focuses on conventional and non-conventional gas exploration and production.

A challenge common to the energy industry is adopting and using information technology to enhance business operations and to help create a competitive edge. "One example would be smart metering, where customers can see real-time consumption of energy and the associated costs, enabling them to make decisions based on this information," Strizik said.

"Another example is how the industry connects to its customers, not just in the traditional way by phone and email, but by creating online and mobile channels that give customers more choice in the way they interact with us."

In the upstream part of the energy business, "The digitisation of our operational assets essentially allows us to manage those assets safely and more efficiently."

Managing security and reducing risk

Cyber security is central to all three examples. "Cyber security means different things for each of our business units and our management approach has to be holistic to make sure we protect what is important to the organisation, while enabling us to take advantage of and leverage technology in a safe manner.

"It has to be holistic because high risk environments can have a significant impact on the organisation if they are unavailable for any reason. There are a range of different health, safety and legislative requirements operating at different sites in different states, adding a degree of complexity and cost that is really quite challenging."

Origin Energy initiated a Security Transformation Programme to put a foundation in place to give them better visibility of security across the business. "We were looking for a cyber security programme where we could see security activities and events that were occurring and one that would position us for a future of increasing cloud services, more BYOD capability, plus anything else likely to introduce new classes of risk."

Global cyber security innovation

Hewlett Packard Enterprise has partnered with Origin Energy since 2011. "We were able to leverage a range of support services from HPE in our IT environment, and this definitely simplified the process for us," Strizik said. "HPE brings a great deal of innovation and investment around global cyber security to the table. It was attractive to us to be able to leverage that investment and expertise locally. I don't think organisations could afford, nor achieve a similar investment around cyber capabilities so fast. The ability to consume these services in a mature fashion is very compelling."

Another factor that made the HPE solution appealing was the ability to use and re-use existing processes. "We didn't have to reinvent change control or reengineer our service management capabilities," Strizik said. "This simplified the deployment and roll-out process."

In mid-2014, HPE deployed a Managed Security Services capability to help execute the expanded IT risk and security strategy that made up a key part of Origin Energy's cyber security programme. The programme covers HPE ArcSight based Security Incident & Event Management (SIEM); Managed Network Security Services, including Intrusion Detection (IDS) and Prevention (IPS) Systems; end point encryption and anti-malware for Operations Technology (OT); plus Cyber Security Incident Management.

"HPE's ability to deliver the overall cyber security programme project on time and within the budget was an important factor," Strizik said. "Senior management recognised and appreciated the fact that HPE immediately understood Origin's environment very well, and as a result was able to handle a very challenging schedule, and still deliver on time."

The HPE solution leverages HPE security operations centres in the UK and delivery centres in Australia, Malaysia and India which monitor and operate Origin Energy's security capability. The SIEM service provides end-to-end visibility whereby security logs are centrally collected, aggregated and passed through HPE's intelligent correlation engine to detect security events of interest.

Case study
Origin Energy

Industry
Oil and Gas
Energy Sector

Customer at a glance

Application
Cyber Security & Risk Management

Software
- HPE ArcSight SIEM

HPE services
- HPE Financing
- HPE Managed Security Services
- HPE Security Information and Event Management
- HPE Managed Network Security
- HPE Endpoint Security Services

"HPE ability to deliver the cyber security project on time and within the budget was an important plus. They were able to meet what was a challenging programme schedule."

— Christoph Strizik, head of IT risk and information security, Origin Energy

Full integrated service
"One of the major benefits is the fact that we are now able to leverage a managed security service that is delivered to us by HPE via its centralised security operations centre (SOC)," Strizik said. "The SOC actively monitors the SIEM console 24x7 and has a robust process in place to triage and escalate as required. This delivers an end-to-end perspective in terms of seeing and collating events and then having the capability to analyse the information and provide an understanding of when to escalate incidents.

"These are connected to our existing HPE service desk and are assigned to the relevant groups within HPE for action. This fully integrated service is an important benefit because it gives us 24x7 coverage, while saving us time and expense."
Strizik cites the improved crisis and emergency management response capability in the event of cyber security incidents and a real-time capability to prevent hacking attempts as another critical business benefit. This is complemented by the ability to detect unauthorised access and abuse of privileged activities on key internet-facing systems. "The solution enables us to prevent unauthorised access at primary production sites which would otherwise adversely impact production and safety systems."

Strizik adds, "There is a high degree of complexity in our business and HPE understands Origin Energy's environment very well and was able to deliver on what was a challenging programme schedule."

Learn more at
hpe.com/services/security

Sign up for updates

★ Rate this document

Hewlett Packard Enterprise

4AA6-4983EEW, April 2016