Case Study

Supplier Security Assessments

Customer: **Elsevier**

Industry: **Information Analytics**

Services: **Supplier Security Assessments**

Challenges:

- A global organisation with dependence on more than 40+ suppliers dispersed in several countries with unknown levels of protection for confidentiality, integrity and availability of data.

Outcomes:

- CyberCX successfully conducted all supplier security assessments identifying gaps and issues specific to each supplier.
- Remedial action has been carried out by the suppliers to improve security and align controls, resulting in significant improvement of overall resiliency for Elsevier as part of the program.

The challenge

Our long-term client is a world leader in information and analytics for customers across the global research and health ecosystems.

As part of their standard operations and service delivery, they are reliant on specific suppliers across the globe to fulfil production process requirements. Elsevier recognise that utilisation of external parties can introduce additional risk to the protection of data and service provision.

Part of our engagement was to determine the approach for assessing such a vast number of suppliers in a controlled and consistent manner that was scalable and cost effective.

"We have worked with CyberCX for a number of years so we were confident about the security controls we have in place. However, we work with over 40 suppliers worldwide and were very aware of the risks this presented. A supplier resiliency program (SRP) was the natural next step and CyberCX did not fail to deliver."

– Zohar Zacks, Senior Director, Business Resilience, Elsevier

Our approach

Program Governance

CyberCX delivered a Supplier Resiliency Program (SRP) maturity and metrics report in line with the governance framework which defined the resiliency objectives, performance metrics and reporting dashboard for each supplier and presented monthly to the executive steering committee demonstrated the business commitment to risk management.

Assessments

Elsevier determined which suppliers were critical to their global production process and CyberCX were able to use this in scoping their assessment for each supplier's cyber resiliency status and identification of the control gaps. Each assessment covered business continuity, IT disaster recovery, information security, technical infrastructure and data protection. Gap assessments for each included the following:

- External, internal, wireless and physical penetration tests;
- Server configuration reviews and password audits;
- Assessment of business continuity capabilities, including incident management plans and ability to shift work to alternate locations;
- Disaster recovery capability assessment and testing;
- Policy and procedure gap analysis against the information security ISO27001 standard;
- Gap analysis against the regional data protection and privacy laws.

The CyberCX team compiled a comprehensive report for each supplier which provided an overall risk and security maturity rating along with full details of what remedial action was needed. The assessments uncovered a number of risk issues which were resolved immediately.

Remediation

CyberCX worked directly with suppliers that required mitigating actions and provided advice and guidance to ensure continued security control improvement. Our goal was for both us and Elsevier to have confidence that the suppliers had the adequate protection of data and preparation for the organisation in adverse events that ensured the provision of their services against contract and/or service level agreements to Elsevier.

Validation

The CyberCX team re-assessed each supplier following the completion of remediation actions to ensure all had been effectively implemented. This ensures the supplier, as part of the SRP, will maintain its cyber resilience maturity. The ongoing validation each year provides assurance which benefits Elsevier, the supplier and their other clients.

The outcome

CyberCX successfully carried out all Supplier Assessments providing Elsevier with the peace of mind that all their critical suppliers have the required standard security and resilience practices in place which protect the confidentiality, integrity and availability of their organisation's data and services.

The program has also enhanced the suppliers' reputation by giving their customers and business partners confidence that they are committed to information security and have robust systems and procedures to safeguard sensitive data in place.

The benefits of the supplier assessments have been recognised internally at Elsevier by managing supply chain risk as well as externally in the market and it is now carried out on an annual basis as part of an ongoing program.

About CyberCX

CyberCX is a leading independent cyber security services company with offices across the UK, US and Australia, unifying the most trusted cyber security brands and the experts who built them.

CyberCX delivers end-to-end cyber security services and the best cyber security talent with the most comprehensive range of cyber security services to business, enterprise and government.

Contact us to find out how CyberCX can help you with proactive Supplier Security Assessments to better understand and manage the risks you face.

UK: +44 (0) 1865 504 032
US: +1 212 364 5192
www.cybercx.com