Cybersecurity

PETRONAS Chemicals Group Berhad (PCG)

Released Date
July 2021

Cybersecurity

Why is this important?

Cyber crime is on the rise around the world, driven by global connectivity and the increasing use and reliance on digital services. Cyber attacks are an increasingly sophisticated and evolving danger to the business, as attackers employ new methods to circumvent traditional security controls. This presents new challenges to our businesses in ensuring the security of sensitive data. As PCG embraces digitalisation of systems and processes, the Company is increasingly exposed to cyber attacks and breaches. Protection of computer systems and networks from malware intrusions, safeguarding damage to the hardware or software and managing the misuse of data is critical. It is our corporate duty to protect the business and stakeholders from malicious cyber crime.

Cybersecurity

What is our approach?

Our cybersecurity efforts are guided by PETRONAS Enterprise Cyber Security Governance Framework (ECSGF), which aims to protect our systems and data from malicious attacks. Education is also a crucial part of our strategy to combat cyber crime, as it helps stakeholders understand the potential risks associated with utilising our network and applications. We educate our employees on simple social engineering scams to more sophisticated cybersecurity attacks designed to steal intellectual property or personal data. We empower our workforce with cybersecurity knowledge through structured Human Firewall Campaigns, specifically to raise cyber awareness and maintain cyber safe culture.

- Assign Board Risk Committee who oversee the cybersecurity strategy and appoint Executive Management Responsibility for overseeing cybersecurity
- Adopted the PETRONAS ECSGF, a single governance framework and standards for cybersecurity based on industry best practices and standards
- Actively monitor cyber threats and attacks in all our operations, which includes conducting vulnerability assessments to prevent possible attacks
- Organise campaigns to raise employee awareness on cybersecurity, including best practices on how to avoid cyber threats
- Performed phishing tests to exercise caution when using digital communication platforms and protect the company against phishing scams
- Continue to conduct Cyber Security Risk Management as part of our remediation against cyber risks and threats

Cybersecurity Board Level Responsibility

Board Responsibility

- The main roles and responsibilities of the Board are to review, approve and monitor the annual corporate plan, which includes information technology plan
- Board Risk Committee – Deliberated and recommended emerging risks to the Board which includes Cybersecurity
- Board Risk Committee – Review and endorse the Group's risk profile and risk appetite (where Cyber security is covered under Corporate Risk Profile)
- Board Audit Committee – Review the audit on PETRONAS Cybersecurity Programme and Activities implementation in PCG

Cybersecurity Executive Level Responsibility

Role of highest executive member in cybersecurity matters

- Responsible for the management of all financial and fiscal aspects of PCG and its subsidiaries as well as risk management, supply chain management, investor relations and information systems
- Responsible for ensuring the implementation and effectiveness of PCG Group risk management practices – via Risk Management Committee (cyber security as one of the key risk in Corporate Risk Profile)
- Align PCG's digital strategy and budget with PETRONAS Group Digital
- Create business value through technology
- Manage IT and focal team personnel
- Oversee information risk management
- Oversee the implementation and adoption of Enterprise Cyber Security Governance Framework, strategies, and standards