Crowe

Cybersecurity Overview

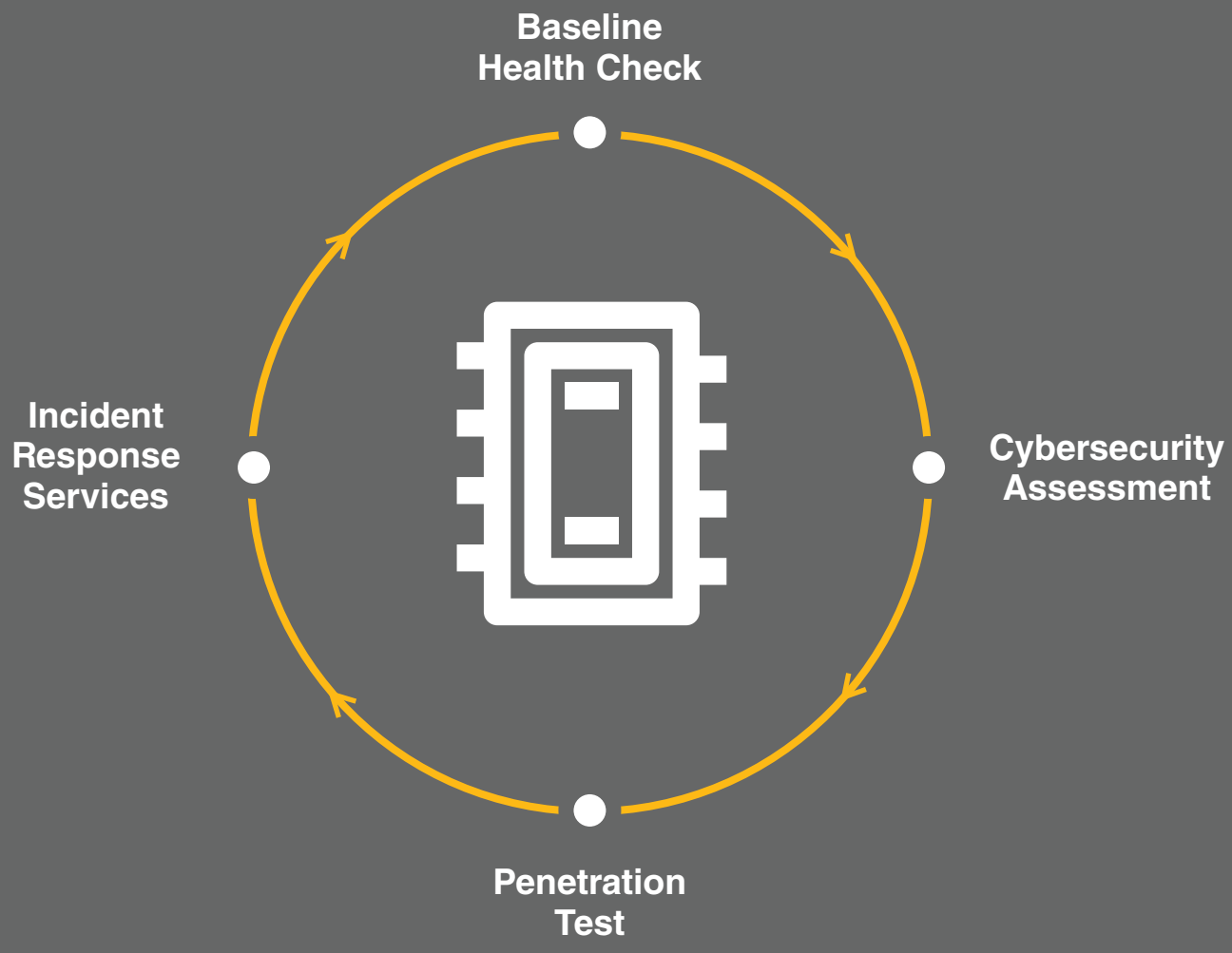
Audit / Tax / Advisory

Smart decisions. Lasting value.

Fortify your cyber resilience and secure your critical assets.

The risk of exposure to cyberattacks are constantly evolving and poses an ongoing challenge for business in ensuring that their sensitive information remain secure, through the maintenance of a robust cybersecurity infrastructure.

Through our deep capabilities in technology audit, Crowe is well-placed to assist in advising you on how to resolve vulnerabilities that may exist, through a comprehensive cybersecurity review, as well as to help plan, prepare and test your organization's approach to cybersecurity resilience.



Our solutions to get you started.

Baseline Health Check

Our baseline health check services provide a baseline gap analysis for our clients to have a bird's eye view of their current cybersecurity posture. This covers IT Security Governance, Risk and Compliance. With this baseline health check report, you will be able to define and plan a cost-effective strategy to meet your compliance and cybersecurity objectives.

- Quick and accurate report under a week
- Cost-effective health check on current environment
- Identify maturity level of current information security posture

Cybersecurity Assessment

With evolving cybersecurity threats, it is critical for businesses to perform cybersecurity assessments periodically. A Cybersecurity assessment will help to identify potential vulnerabilities and threats that may exist in your current network. This activity also helps to identify weaknesses, so that we can work together with you to build a more resilient environment against threats.

- Evaluate current business process and policy
- Identify vulnerabilities and risks
- Review cybersecurity compliance according to your industry requirements
- Providing a risk matrix on current environment according to various international frameworks
- Aligning the organization with cybersecurity industry standards
- Comprehensive report including recommendation and remediations

Penetration Test

A holistic cybersecurity approach is multi-faceted, integrating various components together to deal with current threats. Penetration testing is one of the keys to the puzzle, which completes the cybersecurity total defense. A penetration test is a simulated attack done by qualified expert to exploit your network in a controlled manner, under noble intentions. By investing in a regular penetration testing regimen, an organization is able to reap many benefits such as:

- Evaluating how your current defense mechanism fares against simulated cyber attacks
- Quantifying, evaluating and prioritizing your cybersecurity investments
- Discovering hidden vulnerabilities and exploits
- Providing insightful reports on strength and weaknesses of the current infrastructure
- Vulnerability Assessment and Penetration Testing to get your TrustMark certification which can be used for your website and promotional materials

Red Teaming

As cyber threat actors are getting more creative, penetration testing alone at times is not enough to cater for large-scale sophisticated, targeted attacks. While the main objective of penetration testing is to identify as many vulnerabilities and exploits as possible of the targeted environment, the main focus of Red teaming is to sneak into the environment stealthily, bypassing detection, with a precise target. As an organization matures in their cybersecurity posture, this service is the next step forward upon conducting penetration testing.

- Access the organization's cyber mechanism to detect such attacks
- Providing the organization insights on the modus operandi that bad actors may deploy
- Giving the organization confidence in addressing such attacks

Incident Response Services

Preparedness is identified as one of the critical assets in a holistic cybersecurity defense mechanism. To effectively combat against any cyber threats, incident response plan and guidelines must be in place to contain, eradicate and recover during a cybersecurity incident. IT cybersecurity resources are scarce.

Therefore, our incident response service comes in to fill this critical gap due to the lack of available resources.

- Identify critical stakeholders during a cyber incident
- Define the roles and responsibilities in the organization during a cyber breach
- Assessment of our client's current critical business assets
- Provide a well-defined response plan during an incident
- Have an Incident Response team on contract for your Incident Response needs

Contact Information
Adeline Ng, Director
adeline.ng@crowe.sg

Alvin Neo, Director
alvin.neo@crowe.sg

Chia Shu Siang, Director
shusiang.chia@crowe.sg

Crowe Consulting (Singapore) Pte Ltd
9 Raffles Place
#19-20 Republic Plaza Tower 2
Singapore 048619

Tel: +65 6221 0338

For more information,
scan QR code below:

We are here to help you get there.

Crowe Horwath First Trust (Crowe Singapore) is a public accounting and consulting firm that provides audit, advisory, tax, outsourcing and fund administration solutions to a diverse and international clientele including public-listed entities, multinational corporations and financial institutions.

We are part of an international professional services network, Crowe Global. As a top 10 global accounting network, Crowe Global has over 200 independent accounting and advisory services firms in over 145 countries around the world.

www.crowe.sg

Crowe Consulting (Singapore) Pte Ltd is an affiliate of Crowe Horwath First Trust LLP. Crowe Horwath First Trust LLP is a member of Crowe Global a Swiss verein. Each member firm of Crowe Global is a separate and independent legal entity. Crowe Horwath First Trust LLP and its affiliates are not responsible or liable for any acts or omissions of Crowe Global or any other member of Crowe Global.
© Crowe Horwath First Trust