MOORE

CYBERSECURITY RISK

Safeguard your business
with our services

Moore Hong Kong

WHY MOORE?

At Moore, it's not about us. It's all about you. When it comes to providing personalised and commercially astute audit, accounting, tax and business advisory services, it simply can't be anything else.

With over 30 directors and a team of over 300 staff, we offer a wide range of audit, assurance tax, and advisory services to our clients. Our global family of 30,000 professionals in more than 110 countries allows us to share expertise, knowledge, and best practices to ensure our clients receive the highest quality of service, no matter where their work takes them.

As your genuine professional partner, we will not only advise you but also challenge you to meet your goals and objectives for the future. With our team's personal qualities, skills, and experience, we are confident in our ability to support your group's development.

Cyber strategy and planning.

In today's digital age, cybersecurity is not just a necessity; it's a strategic imperative. Effective cyber strategy and planning are the cornerstones of a proactive defence against evolving threats.

Why cyber strategy and planning matters?

Cyber threats are constantly evolving, making it crucial for organisations to stay ahead of potential risks. A well-defined cyber strategy and robust planning process are essential for:

Risk mitigation

Identifying and mitigating potential vulnerabilities and threats before they escalate.

Compliance and governance

Ensuring adherence to regulatory requirements and industry standards.

Business continuity

Safeguarding critical assets and maintaining operations in the face of cyber incidents.

Resource optimisation

Allocating resources effectively to maximise cybersecurity investments.

Strategic alignment

Aligning cybersecurity efforts with overall business goals and objectives

Approach to cyber strategy and planning

Every organisation is unique with distinct risks and priorities. Our experienced team works closely with your stakeholders to develop customised cyber strategies that align with your business objectives.

Our approach includes:

Risk assessment

Comprehensive evaluation of your organisation's cybersecurity risks and vulnerabilities.

Strategic roadmap

Development of a tailored cybersecurity road map aligned with your long-term goals

Incident response planning

Establishing protocols for rapid and effective response to cyber incidents.

Training and awareness

Educating employees on cybersecurity best practices to enhance overall resilience

Cyber strategy and planning are fundamental pillars of a robust cybersecurity posture, enabling organisations to navigate the complex cyber landscape with confidence and resilience. By embracing strategic planning practices, organisations can proactively mitigate risks, strengthen defences, and safeguard their digital future.

Cyber threats intelligence

In the ever-evolving landscape of cybersecurity, organisations face a myriad of digital threats that can compromise their critical assets and operations. Cyber threat intelligence (CTI) serves as a powerful tool in identifying, analysing, and mitigating these threats.

Importance of CTI

CTI plays a crucial role in enabling organisations to proactively defend against cyber threats by gathering and analysing information on potential threat actors and their tactics. By understanding and anticipating these threats, organisations can strengthen their cybersecurity defences and protect their critical information assets.

The CTI process flow involves several key stages:

1 Planning and direction

Establishing goals and objectives for CTI activities, and aligning them with the organisation's cybersecurity strategy

2 Collection

Gathering relevant data and information from various sources, such as threat feeds, open-source intelligence, and internal security logs

3 Processing

Organising and filtering the collected data to identify relevant threat indicators and actionable intelligence

4 Analysis

Assessing the identified threats, understanding their potential impact on the organisation, and determining appropriate response measures

5 Dissemination

Sharing the analysed intelligence with relevant stakeholders, such as security teams, IT personnel, and management, to facilitate informed decision-making

Benefits of CTI

Proactive defence

Anticipate and respond to cyber threats before they materialise into attacks

Informed decision-making

Utilise intelligence insights to make data-driven decisions and prioritise cybersecurity efforts

Enhanced incident response

Improve incident response capabilities by leveraging intelligence to detect and respond to threats swiftly

Strategic planning

Tailor cybersecurity strategies and investments based on intelligence to address specific threats and vulnerabilities

Why choose CTI?

Cyber threat intelligence is not just about reacting to threats; it's about proactively identifying and neutralising potential risks. By harnessing the power of CTI, organisations can strengthen their cybersecurity posture, enhance resilience, and protect their digital assets from sophisticated cyber threats.

Cyber threat intelligence is a cornerstone of modern cybersecurity, providing organisations with the insights needed to navigate the complex threat landscape effectively. By embracing CTI practices, organisations can fortify their defences, mitigate risks, and safeguard their digital infrastructure from an array of cyber threats.

Cyber response

In the ever-evolving landscape of cybersecurity, organisations face a multitude of digital threats that can compromise their data, operations, and reputation. Cyber response is a strategic approach that equips organisations with the tools and techniques to detect, respond to, and recover from cyber incidents swiftly and effectively.

What is cyber response?

Cyber response encompasses a set of proactive measures and reactive strategies aimed at preventing, detecting, responding to, and recovering from cyber threats and incidents. It involves a coordinated effort to protect your organisation's digital infrastructure, data, and reputation from malicious actors.

Key components of cyber response

Threat detection and monitoring: Utilising advanced threat detection technologies to identify and respond to cyber threats as they emerge.

Incident response planning: Developing comprehensive incident response plans to guide actions in the event of a cyber incident.

Forensic analysis: Conducting in-depth investigations to understand the scope and impact of cyber incidents.

Recovery and remediation: Implementing measures to recover systems, data, and operations post-incident and prevent future occurrences.

Benefits of cyber response

Enhanced security posture

Strengthen your organisation's security posture and resilience against cyber threats

Rapid incident response

Enable quick identification and response to cyber incidents, reducing potential damage

Regulatory compliance

Ensure adherence to data protection regulations by implementing effective cyber response measures

Reputation protection

Safeguard your organisation's reputation and trust among customers and stakeholders by demonstrating a proactive approach to cybersecurity.

Why choose cyber response?

Cyber response is not just a reactive measure but a proactive strategy that empowers organisations to stay ahead of cyber threats. By investing in cyber response, you are investing in the security and resilience of your organisation's digital assets.

In an era where cyber threats are constantly evolving, cyber response is a critical component of a comprehensive cybersecurity strategy. By embracing cyber response practices, organisations can effectively mitigate risks, respond to incidents decisively, and protect their digital assets from malicious actors.

Cyber assessments and recovery

In today's interconnected world, cybersecurity threats loom large, posing risks to organisations' data, operations, and reputation. Cyber assessments and recovery are essential components of a robust cybersecurity strategy, enabling proactive risk management and effective response to cyber incidents.

Understanding cyber assessments

Cyber assessments involve thorough evaluations of an organisation's cybersecurity infrastructure, policies, and practices to identify vulnerabilities and assess the overall security posture. Through comprehensive assessments, organisations can gain valuable insights into potential risks and areas for improvement in their cybersecurity measures.

Key components of cyber assessments

Vulnerability assessment: Identifying weaknesses in infrastructures and applications that could be exploited by cyber attackers.

Penetration testing: Simulating cyberattacks to assess the effectiveness of existing security controls and identify potential vulnerabilities.

Risk analysis: Assessing the likelihood and impact of potential cyber threats to prioritise risk mitigation efforts.

Compliance audits: Ensuring adherence to regulatory requirements and industry standards to maintain cybersecurity compliance.

Navigating cyber recovery

Cyber recovery involves developing and implementing strategies to recover from cyber incidents swiftly and minimise their impact on business operations. By establishing robust recovery plans, organisations can mitigate downtime, data loss, and financial repercussions resulting from cyberattacks.

Key components of cyber recovery

Incident response planning: Preparing incident response playbooks to guide the organisation's response to cyber incidents.

Data backup and recovery: Implementing regular data backups and recovery procedures to safeguard critical information.

Business continuity planning: Developing continuity plans to ensure essential business functions can continue in the event of a cyber incident.

Post-incident analysis: Conducting thorough post-incident reviews to identify lessons learned and enhance future incident response strategies.

Benefits of cyber assessments and recovery

Proactive risk management

Identify vulnerabilities and mitigate risks before they are exploited by cyber threats

Enhanced resilience

Develop strategies to recover quickly from cyber incidents and minimise their impact

Regulatory compliance

Ensure compliance with data protection regulations and industry standards through regular assessments and recovery planning

Stakeholder confidence

Demonstrate a commitment to cybersecurity best practices, fostering trust among customers, partners, and stakeholders

Why choose cyber assessments and recovery?

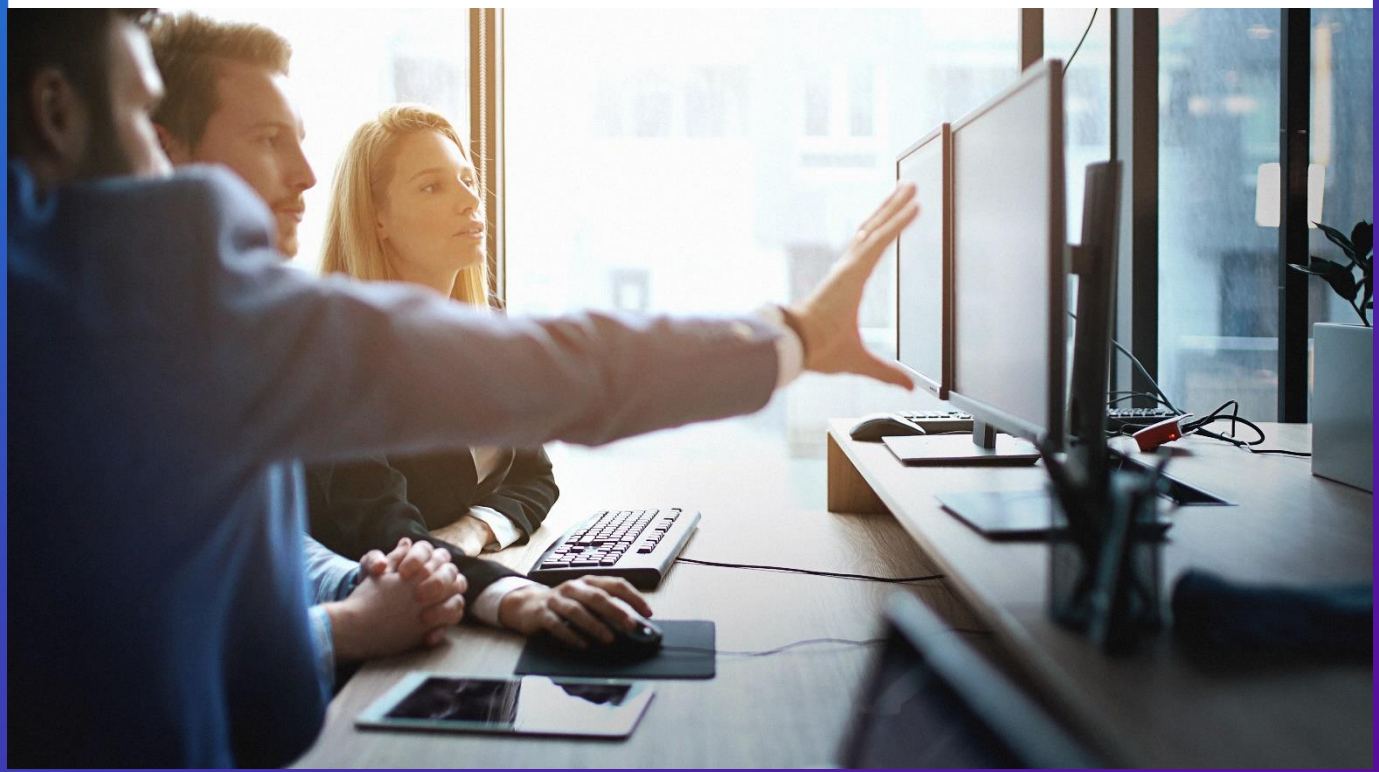
Cyber assessments and recovery are essential proactive measures that empower organisations to proactively manage cyber risks and respond effectively to incidents. By investing in these practices, organisations can enhance their resilience and protect their digital assets from evolving cyber threats.

Cyber assessments and recovery are critical components of a comprehensive cybersecurity strategy, enabling organisations to proactively manage risks and effectively respond to cyber incidents. By investing in assessments and recovery planning, organisations can enhance their cybersecurity resilience, protect their assets, and safeguard their digital future.

Why work with us?

- Our team includes professionals with practical and solid knowledge and experience.
- The team comprises charter holders or members of professional bodies such as CPA, CISA, CIA, ACCA, CIPP/and lead auditor for ISO/IEC 27001/27017/27018 & ISO/IEC 20000 (IRCA).
- We have extensive sector knowledge to provide customised advice to suit each client taking into account size, capabilities and goals.

Backed by our international network, we have the scope to provide clients with all solutions and expertise they require, wherever they choose to do business.



CONTACT US

Our IT and Cybersecurity practice offers a spectrum of services that help businesses to achieve a robust IT architecture and security framework through identifying vulnerabilities, threats, and areas for improvement.

For any enquiries, please contact our advisers directly.

PATRICK ROZARIO
Advisory Services Managing Director

T +852 2738 7769
E patrickrozario@moore.hk

KEVIN LAU
IT & Cybersecurity Principal

T +852 2738 4631
E kevinlau@moore.hk

At Moore, our purpose is to help people thrive – our clients, our people, and the communities they live and work in. We're a global accounting and advisory family with over 37,000 people in 558 offices across 114 countries, connecting and collaborating to take care of your needs – local, national and international.

MOORE