PRAGMA

SECURING YOUR DIGITAL FUTURE

Business Overview

By proactively investing in cybersecurity measures, you can protect your assets, your reputation, and your bottom line. Don't wait for a disaster to happen, act today and secure your digital future.

- Geoff and Manish, co-founders of Pragma

PRAGMA
SECURING YOUR DIGITAL FUTURE

Our Credentials

01
Cyber & Regulatory Consultancy

02
Incident Response

03
Cyber Security as a Service

04
Security Testing

Securing Your Digital Future.

Pragma is a global provider of cybersecurity and regulatory solutions. We help organisations strengthen cyber resilience and safeguard valuable information assets with a pragmatic approach.

Currently, Pragma is the trusted partner of some of the world's most successful organisations across a wide range of industries, including 4 of Forbes's Most Valuable Brands, 3 of Singapore's Hottest FinTechs, and the Best Global Crypto Exchange and 10 of the Top 100 Insurance Companies.

Headquartered in Asia and Europe and with regional offices worldwide, we provide Cyber and Regulatory Consultancy, Incident Response, Managed Security services, and Security Testing services.

We have been awarded two new Singapore Cyber Licences and according to the Financial Times, Pragma is one of the fastest-growing cyber companies in Asia.

CREST

aws partner network
Select
Consulting Partner

Microsoft Partner

C|EH™
Certified Ethical Hacker

OSCP

CISSP.

eLearnSecurity Junior Penetration Tester
eJPT

GIAC Certified Forensic Examiner
GCFE

SINGAPORE

2016 - Pragma was established by Manish Chawda and Geoff Leeming

LONDON

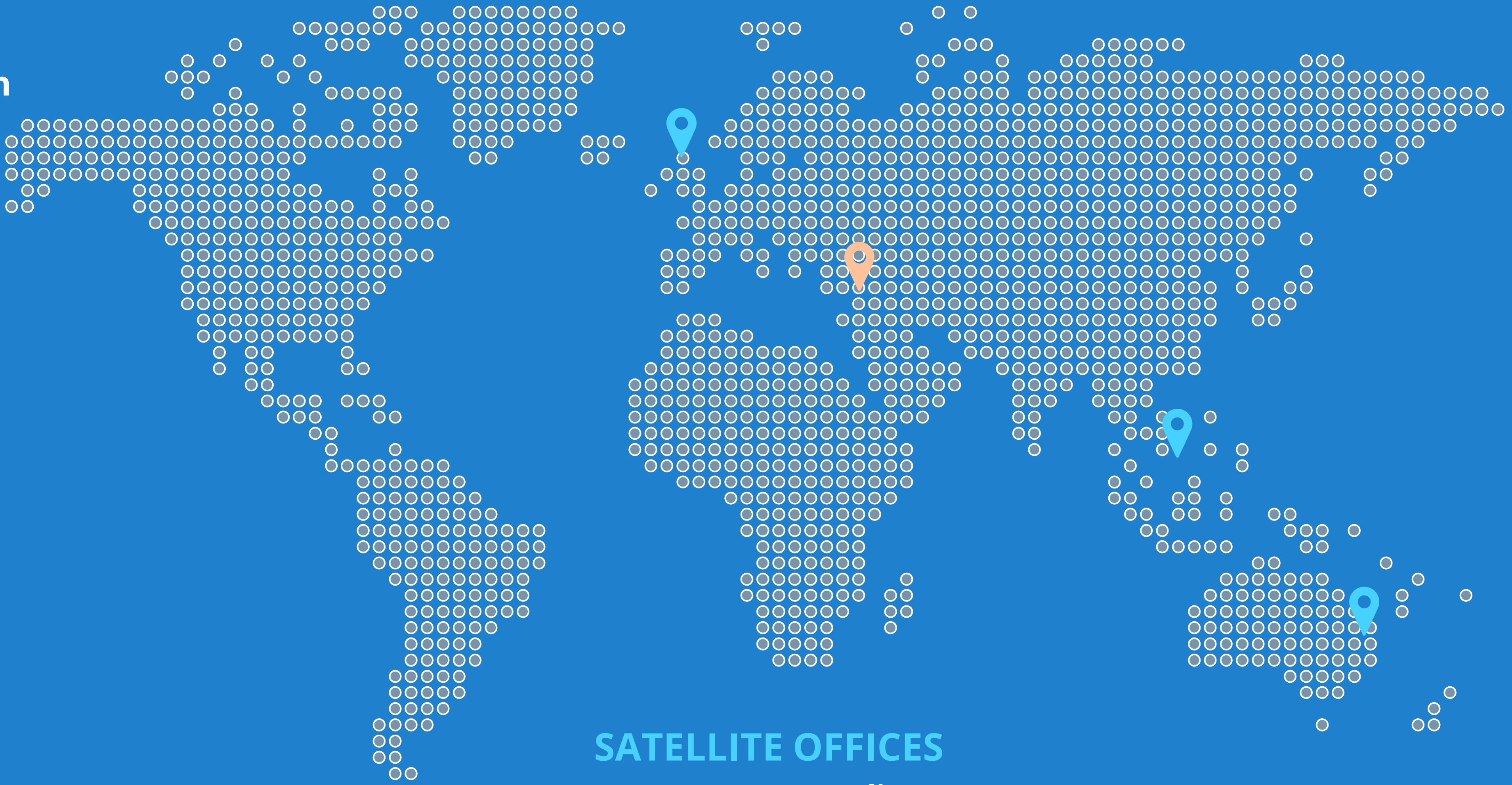
2020 – EMEA HQ established

SYDNEY

2022 – ANZ HQ established

DUBAI

Opening in 4Q23



SATELLITE OFFICES

Myanmar	India
Pakistan	Malaysia
Philippines	Indonesia

PRAGMA
SECURING YOUR DIGITAL FUTURE

Our Clients and Partners

ADDX previously iSTOX
Adenza
BABEL FINANCE
PURPLE NEXT
paradine
canopius
Charles Taylor

CIMB
CLSA
CMC cmc markets
cobo
coinbase
currensea
bambu

Europcar
FULLERTON HEALTH
GIC
headlam group plc
hoolah
ICICI Bank
broadpeak

JLL
LittleLives
Marriott
MM
MIZUHO
MSIG
NX NIPPON EXPRESS

Ochre HEALTH
OSM MARITIME
OrangeTee.
Parkway Hospitals SINGAPORE
Pionex
pnb
PRUDENTIAL

QBE
SALO. accounting . finance . business
Shareable Asset
SHOPBACK
sparrow
standard chartered
STATE COURTS SINGAPORE

switchcraft
TECHCOMBANK
V.Ships

PRAGMA
SECURING YOUR DIGITAL FUTURE

We are Here to Help

01

Transparent Competitive Fees

We get our cost structure right so that the fees proposed to you are **transparent** and **competitively priced** without impairing our objectivity and quality.

02

Custom-Built Solutions

We understand that no one business is identical. Our solutions are bespoke and aims to empower your business with the right tools and technology to grow.

This means having a **collaborative approach** while working with your team and listening to you.

03

Dedicated Expertise

The team dedicated to you has **deep cybersecurity knowledge** and experience across financial services, technology, media, telecommunication and government agencies.

PRAGMA

SECURING YOUR DIGITAL FUTURE

Our Services

01 Cyber & Regulatory Consultancy

Your Partner in Secure Digital Transformation

COMPLIANCE MANAGEMENT

- ISO 27001
- MAS TRM
- PCI DSS
- NIST 800
- SOC2/SOC3

- Gap analysis and assessments
- Policies and procedures
- Implementation
- Internal and third-party audits
- Reporting

FINANCIAL INSTITUTION LICENCE APPLICATION

- Licencing support for Singapore, Hongkong, Dubai, UK, Germany, Australia, and the US
- Creation of the policies and procedures required to support obtaining the license
- Support with end-to-end technical compliance

CONDUCT RISK AND COMPLIANCE

- Drafting of compliance; AML/CFT/KYC/CDD frameworks, policies, and procedures
- Sanctions Monitoring Manual
- Transaction Monitoring Manual
- Enterprise-wide Risk Assessments
- Reg/Risk health checks
- Ad hoc regulatory advice

OUTSOURCED RISK AND COMPLIANCE MANAGEMENT

- Supports companies in running their day-to-day risk management activities
- Level of involvement can be tailored based on company-specific needs
- Compliance and Risk as a Service

01 Cyber & Regulatory Consultancy

Your Partner in Secure Digital Transformation

IT AUDIT

- Pragma complements and enhances existing Internal Audit processes, including the overall Internal Audit risk assessment and plan.

CONSULTANCY

- Review Security Architecture, Configurations, and Code
- Compliance with regulatory standards
- Prompt and reliable support on security matters
- Support client to achieve ISO 27001and SOC certifications

SECURITY IMPLEMENTATION

- Network Security (Juniper Networks, Fortinet)
- Endpoint Security (Sophos)
- Cloud Security (AWS and Azure)
- Password-less Multi-Factor Authentication (Hypr)
- 24/7, cloud backup solutions and disaster recovery

AWARENESS TRAINING

- Bespoke Cyber Awareness Training
- World-class Gamified Training Platform (Right-Hand)
- Cloud Based Platform with games, videos, and phishing simulations
- Scheduled Phishing Training

PRAGMA
SECURING YOUR DIGITAL FUTURE

02 Incident Response

Recover With Minimal Disruption

PRE-LOSS CYBERSECURITY SERVICES

- Security Software
- Awareness Training
- Compliance Audit
- Incident Management Plan creation

CYBER INCIDENT RESPONSE

- Our Incident Response Specialist will guide you through the process of containment, eradication, and recovery from the attack
- Common incidents: Phishing attack, Unauthorised access, ransomware, DDoS

RECOVERY AND REMEDIATION

- Rapid Recovery to the Cloud
- On-site System Recovery, Restoration from Backup
- Rebuilding of Systems and Technology
- 24/7 Dedicated IT Support Team

CYBER FORENSIC INVESTIGATION

- Malware and Malicious Code Analysis
- Compromised Machine Analysis
- Policy Violations or Improper Usage
- Forensics Imaging (including mobile devices)
- Fact-finding, Live Interviews and Evidence Collection

AIG

PRAGMA
SECURING YOUR DIGITAL FUTURE

Our Partnerships:

Allianz, canopius, QBE, Crawford, Kennedys, Charles Taylor
Clyde&Co, DUAL, delta, AIG, wotton kearney

02 Incident Response

Recover With Minimal Disruption

SECURITY STRENGTHENING

- Antivirus programs
- advanced firewalls
- AI-driven threat scanning

RETAINER SERVICES

- A specialist who is guaranteed to be available when you need them
- Your designated specialist to respond rapidly to any security event
- A streamlined response process

RANSOMWARE RESPONSE

- Facilitated Ransom Payments
- OFAC Sanctions list checks
- Negotiations with cybercriminals
- Decryption assistance by Pragma’s Forensics Lab:

MANAGED DETECTION AND RESPONSE (MDR)

- Proactive threat hunting, intrusions detection, malware, and malicious activity in their network and assists in rapid response to eliminate and mitigate those threats

Coverage and Capabilities

Be assured that you are covered and taken care of in the event of an incident.

QUALITY

CREST

As a CREST-approved Incident Response provider, you can be assured of the quality of the organisation and the technical capability of staff in the information security industry.

COVERAGE

85+

Countries

Our service coverage extends to over 135 countries across Africa, Asia Pacific, United Kingdom and Europe.

EXPERIENCE

120+

Years

Our incident response team has more than 120+ years of collective experience in investigating and resolving cases of varying complexity.

SPEED

~60

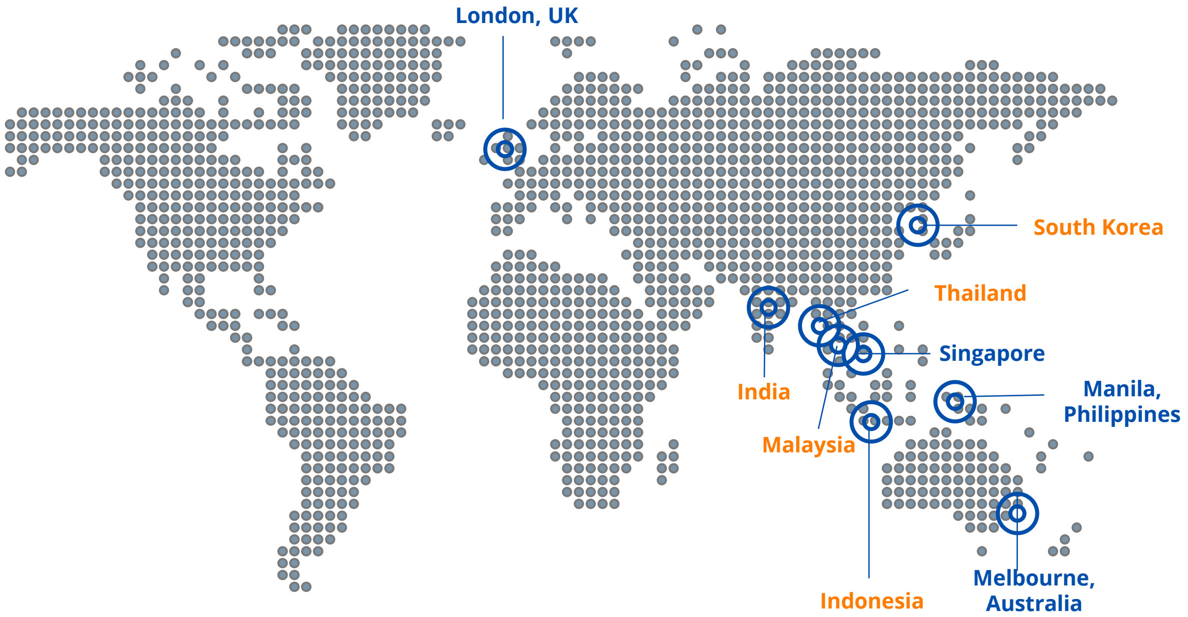
Minutes

We are committed to responding to incidents within the hour, no matter where you are.

PRAGMA
SECURING YOUR DIGITAL FUTURE

Incident Response Network

Our global offices and network of incident response partners ensure 24/7 response and support.



◎ Pragma Office

◎ Partner's Office

03 Cyber Security as a Service

Realise the full value of the cloud safely and cost efficiently.

MXDR SOLUTION

- User and Entity Behaviour Analytics
- Attacker Behaviour Analytics
- Endpoint Detection & Response (EDR)
- Security Incident & Event Monitoring (SIEM)
- Automated Response

MXDR SOLUTION

- End-points
- Servers
- Cloud workloads
- Networks

CLOUD CONTROL

- Secure, scalable, and regulatory-compliant hosted cloud environment
- Continuously monitors for vulnerabilities and automatically recovers the cloud environment upon detection of threats to minimise downtime
- Provides standardised regulated support that helps the organisation comply with local regulatory standards

CLOUD SECURITY SERVICES

- Cloud Security Consultation
- Cloud migration
- Architecture Assessment
- Cloud Security Gap Assessment
- Cloud Security Technical Assessment
- Vulnerability Assessment and Penetration

Our Partnerships:

SOPHOS

aws partner network Select Consulting Partner

Microsoft Azure

Secureworks

RAPID7

VEEAM

PRAGMA SECURING YOUR DIGITAL FUTURE

04 Security Testing

Tailored and Cost-Effective Testing

CREST

RISK ASSESSMENT

- Active Directory Review
- Network Data Security Review

SOURCE CODE REVIEW

- Static Analysis
- Dynamic Analysis
- Manual Analysis

VULNERABILITY ASSESSMENT

We can test the following classes of system:

- Servers/NW Devices
- Websites
- Cloud Environments
- SCADA
- IoT

PENETRATION TESTING

We can test the following classes of system:

- Servers/NW Devices
- Websites
- Cloud Environments
- SCADA
- IoT

Our Partnerships:

ImmuniWeb® AI for Application Security · tenable · PortSwigger · RAPID7

PRAGMA
SECURING YOUR DIGITAL FUTURE

PRAGMA

SECURING YOUR DIGITAL FUTURE

Case Studies

Case Study: Bank Negara Malaysia Risk Management in Technology (RMiT) Compliance| Banking

Supporting a Large Malaysian Bank to Comply with Bank Negara Malaysia RMiT

Pragma signed up with the client as they needed a partner with expertise in technology risk and cybersecurity to support them in achieving compliance with RMiT

BACKGROUND

The Bank is a leading ASEAN universal bank and one of the largest commercial banks in Southeast Asia, with a presence in 17 countries. The bank must comply with the Bank Negara Malaysia Risk Management in Technology (BNM RMiT) guidelines, which set the standards for managing technology risks in the banking industry. The bank seeks to implement effective risk management practices to ensure compliance with the BNM RMT guidelines.

The bank required a partner with expertise in technology risk, cybersecurity, and regulation to support them in achieving compliance with Bank Negara Malaysia RMiT.

THE PROCESS

Risk Assessment: The first step was to conduct a comprehensive risk assessment of the bank's technology systems, processes, and controls. This involved identifying potential technology risks, evaluating their impact and likelihood, and prioritising them based on the level of risk.

Policy and Procedure Development: Pragma helped the bank develop a comprehensive policy and procedure manual that outlines the bank's approach to managing technology risks in line with the BNM RMT guidelines. This manual includes incident management, disaster recovery, and business continuity planning guidelines.

Technology Infrastructure Upgrade: The bank upgraded its technology infrastructure to ensure that it is secure, reliable, and resilient. This involved implementing firewalls, intrusion detection and prevention systems, and encryption technologies to protect against cyber threats.

Training and Awareness: Pragma provided training and awareness programs to its employees to educate them on the importance of technology risk management and the measures they can take to minimise risks.

Monitoring and Review: The bank established a system for monitoring and reviewing its technology risk management practices. This involves regular audits and assessments to ensure that the bank's risk management practices are aligned with the BNM RMT guidelines.

THE RESULTS

By implementing these measures, The Bank was able to comply with the BNM RMT guidelines and minimise its technology risks. The bank's technology systems and processes are now more secure and resilient, and the bank is better equipped to manage technology risks effectively.

Complying with the BNM RMT guidelines is an important step for the Bank in ensuring the security and stability of its technology systems. By implementing effective risk management practices, the bank has improved its technology infrastructure and reduced its exposure to technology risks.

Note: Due to non-disclosure agreements with our clients, we are unable to disclose clients' real names.

Strengthening the Security Posture through System Hardening

Due to local regulations requirements and concerns over the fast change of technology, the Client engaged Pragma to help in making system security hardening tasks efficient.

BACKGROUND

A large financial services company that offers a wide range of insurance and investment products to individuals and businesses. Founded in 1875, the client operates in the United States and several other countries, serving customers worldwide. With the fast change of technology and uncertainty in technological regulations, the client engaged Pragma for security hardening task assistance. Having consistently secure configurations across all systems ensures minimal risks to those systems. Another requirement is to ensure that any new system created will be equally designed in terms of security.

THE PROCESS

The client's IT environment consists of multiple systems with various operating systems and ensuring all the systems are hardened securely and consistently became daunting. This is especially challenging for newer or niche operating systems, as there is limited reference to establishing a security hardening standard.

Pragma worked with the client to create and write security hardening standards for various enterprise operating systems and developed a tool to audit the existing system configuration and automate the implementation tasks based on the established standards.

The process of defining security hardening involves several steps:

We performed a Risk assessment: This involves identifying the assets that need to be protected, the threats they face, and the impact of a security breach on the organisation. This step provides a foundation for the security hardening process and helps to prioritise the measures that need to be taken.

We developed a Policies: This involves creating policies and standards for securing technology systems and devices. The policies were based on regulatory and industry good practices and tailored to meet the organisation's specific needs.

The organisation performed the technical implementation: This involves implementing the security hardening policies and procedures, and scripts

The security hardening process for technology is ongoing and regularly reviewed to ensure that it remains effective and up-to-date in protecting the organisation from security threats.

THE RESULTS

Our recommendations and tool enabled the client to assess the system security posture efficiently and strengthen the system if required within a few clicks. This allows them to keep pace with continuous compliance activities.

PRAGMA
SECURING YOUR DIGITAL FUTURE

Note: Due to non-disclosure agreements with our clients, we are unable to disclose clients' real names.

Enabling Business Continuity & Disaster Risk Recovery for a Global Logistics Enterprise

The Client is a Japan-based logistics enterprise with a global reputation and a network of over 300 locations worldwide.

THE BACKGROUND

After being a target of a massive cyber breach and malicious activity, the client realised their business continuity programme was insufficient. The operational and financial impact of a disruption brought about by a cyber incident has cost millions of dollars and thousands of hours in lost productivity and valuable data.

Pragma was required to help put technology or solution in place to recover business-critical applications quickly if another incident ever occurs. The answer needs to be able to scale and support twelve countries supporting the client's network of more than 500 locations. The critical applications need to be available with a Recovery Time Objective (RTO) of less than one hour, 365 days a year.

THE PROJECT

Pragma presented and implemented a 4-stage business continuity programme and disaster recovery system that is ISO22301 Business Continuity Management compliant – specially developed for the client's critical system across twelve regional hubs in three months. Pragma had also set up a fully managed 24/7 Disaster Recovery Infrastructure on the cloud using Veeam's Backup & Disaster solution, enabling a cost-efficient recovery without the need to allocate additional workforce or resources. The cloud-based solution can restore critical client systems within one hour and allow access to all applications for all users from any location.

The system also institutionalises a regular Disaster Recovery testing regime conducted in all regional hubs that involve the simulation of different disaster scenarios and documented disaster recovery tests, ensuring that the backup lifecycle is maintained properly.

Pragma supported the client during the ISO implementation phase by documenting the procedures and policies and ensuring the DR testing met the criteria set by the ISO.

THE RESULTS

With the help of Pragma's Security Architecture Team and several workshops with the client's IT, team, across the ten countries, a tailor-fit Business Continuity Plan focused on the client's critical system was rolled out across the entire organisation and certified by both regulatory and local auditing bodies on each regional site. A bi-annual review and disaster recovery testing are performed with additional cyber security awareness training for the management staff. The solution has met businesses' requirements, giving them access to their critical systems 24/7 securely from any location. The system protects from ransomware attacks and unauthorised threats.

Note: Due to non-disclosure agreements with our clients, we are unable to disclose clients' real names.

Case Study: Cybersecurity Audit: Risk Assessment and Penetration Testing | Telecommunications

Assessing and Implementing Security Protocols for a Telecom company

The client who is a leading telecom giant engaged Pragma to analyse potential threat models and to reinforce security protocols.

BACKGROUND

The client is a prime European telecommunications company with a regional hub in Singapore to spearhead the expansion of telecom's global enterprise operations in the APAC region. The client also provides managed communication services to several leading multinational corporations.

With networks operating across the globe and teams operating worldwide, this telecommunication giant has won several prestigious accolades.

THE PROCESS

The client experienced multiple attempted hacking in their offices and data centres. Pragma was engaged to investigate the presence of threat factors and to fortify security protocol. We performed cybersecurity risk assessments on their Data centres, laptops, mobiles and telecom technology, mapping out threat models. Our on-premise investigations also involved interviewing 20 plus staff, hacking Wi-Fi 2 SSID and conducting network security analysis. Our technology-driven Penetration Testing services helped detect the technology risks in two data centres and offices. We also examined the 120 company's process analyses, policies and procedures.

THE RESULTS

Amongst many recommendations, we suggested the client exercise the use of Multi-factor Authentication besides the existing VPN. We also advised suitable measures to prevent data loss from laptops, which were vulnerable to access through USB keys.

Consequently, Pragma's recommendations and assessments enabled the client to secure funding from the board to address the security gaps in the system and establish a robust environment. We provided a prominent three-year strategy for the company's people, process, and technology.

Note: Due to non-disclosure agreements with our clients, we are unable to disclose clients' real names.

Case Study: Security Assessment and Documentation| Digital Bank

Helping a Global Retail Bank Launch a New Digital Bank

Pragma was chosen to perform a security assessment and help with detailed process documentation to be compliant with regulatory cyber requirements.

BACKGROUND

We helped a large global retail bank launch a new digital bank by performing its security assessment and ensuring compliance with regulatory cyber requirements. Regulations such as MAS Guidelines on Information Security Management require financial institutions to implement information security management systems. The aim is to establish a secure environment for the protection of customers' personal data, banknotes, and monetary instruments.

Pragma was called to perform and document security assessments for the client, ensuring compliance with the Monetary Authority of Singapore (MAS) Technology Risk Management and Cyber Hygiene regulations.

THE PROCESS

The process includes a review of the client's assessment and current documentation, including all project documentation, policies, and guidelines. We interviewed all vendors and performed an audit of their operational procedures to determine compliance. Pragma also designed the Risk Register and Risk Control Library with a consolidation of policies.

Pragma has created and updated detailed Level 3 procedures documentation, and an extensive database to support major financial processes throughout the organisation. This documentation is used in support of existing policies and standards based on the requirements of MAS TRM.

THE RESULTS

Working with the client allowed us to create over 40 standards and procedures that are compliant with the MAS TRM and Cyber Hygiene Regulations. Because of this detailed documentation, the client is on the path toward compliance with licensure and cybersecurity guidelines.

Note: Due to non-disclosure agreements with our clients, we are unable to disclose clients' real names.

PRAGMA
SECURING YOUR DIGITAL FUTURE

Case Study: Compliance and Cyber Risk Assessment | Global General Insurer

MSIG

Technical Review on Third-party Risks For Insurer

We helped a global general insurer perform assessments on the security and control environment of their service providers

> *"Pragma have always supported us with pragmatic advice and guidance on how to implement solutions that comply with the regulations. They have enabled us to become the example of gold standard in technology risk management."*
>
> - Chief Compliance Officer, MSIG

BACKGROUND

MSIG Insurance is one of Asia's leading general insurers, with a solid presence in Singapore. As large insurer, MSIG is subjected to regulators guidelines in multiple countries including Hong Kong Monetary Authority Technology Risk Regulations and Monetary Authority of Singapore Technology Risk Management guidelines and Outsourcing guidelines and the risks associated with using the outsourced service providers. Pursuant to the guidelines, MSIG is required to perform an assessment on there internal operations and their third-party service providers.

THE PROJECT

As a result, MSIG has requested Pragma to assess the security and control environment at several service providers and to report on the observations and associated risks for the services provided.

The scope of service for MSIG includes a security testing on their mobile application, backend server and web application, assessment of policies, procedures and process, architecture of third-party services and operational procedures that support MSIG. The assessment began with a thorough technical review of people, process, and technology, followed by a detailed report to illustrate the issues.

In total, we evaluated over 100 service providers and assessed the priority one material outsourced vendors against the HKMA Risk Management and Outsourcing guidelines, and MAS TRM guidelines and Outsourcing.

THE RESULTS

The recommendation we produced helped MSIG understand the risks of their service providers and allowed them to mitigate many of these risks through our recommendations and solutions. MSIG successfully reported the closure of the issue to the regulatory and are now important insurance company that the regulatory looks to for exemplary risk management.

PRAGMA
SECURING YOUR DIGITAL FUTURE

Case Study: MAS Payment Services Act Compliance| Cryptocurrency Exchange

coinbase

Supporting the Largest Crypto Exchange in MAS Payment Service Act Licence Application

Coinbase, the world's largest cryptocurrency exchange needed to apply for a Licence to operate in Singapore after the introduction of MAS Payment Service Act.

BACKGROUND

Coinbase is the world's largest cryptocurrency exchange, providing an easy and secure place to buy, sell, and manage digital currency. It has over 56 million users across 32 countries worldwide including Singapore.

In January 2020, the Monetary Authority of Singapore (MAS) implemented the Payment Service Act (PSA), a comprehensive regulatory framework for companies handling activities relating to digital assets. The new ruling means cryptocurrency-related services such as Coinbase need to obtain licences from MAS to continue their operations in Singapore.

THE PROCESS

One of the challenges faced by Coinbase was the lack of policies and procedures that are localised to suit the requirements of MAS. They also do not have in-house security compliance personnel or a team to assist in the application process.

Over a period of 2 months, Pragma provided advisory support in Coinbase's PSA application process in the aspects of security compliance and responding to questions related to technology risks raised by the authorities.

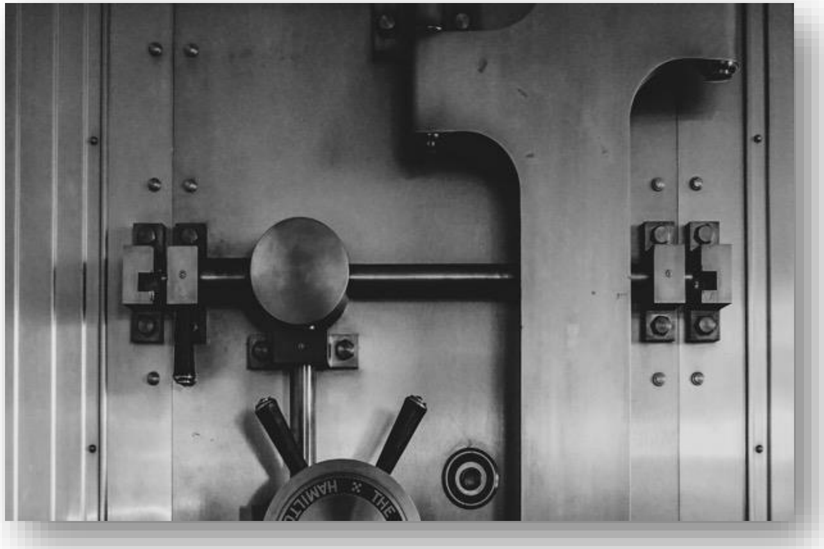
Given the complexity of the project and lack of an in-house security compliance team within Coinbase, Pragma worked closely with the client's Legal Counsel, Head of Compliance and Director for Security and Privacy to leverage their existing global policies and procedures, as well as align their service level agreements to meet MAS compliance requirements. We also interpreted the Act to ensure it's applicable for cryptocurrency exchanges.

THE RESULTS

Coinbase was able to submit their application and answer queries raised by MAS confidently with guidance from Pragma's security and compliance expertise. As a leader in the cryptocurrency exchange space, security is a priority. Through Pragma's recommendations, Coinbase now has better clarity from a security standpoint to implement technology and security controls.

Improving Bank's Security Posture Through Security Testing

A global bank underwent a series of assessments to verify the effectiveness of security controls on its payment servers.



BACKGROUND

ICICI Bank is India's largest private sector bank, with presence in 17 countries, including Singapore. ICICI Bank offers a wide range of banking products and financial services to corporate and retail. ICICI requested Pragma to conduct a vulnerability and penetration testing assessment of the FAST payment servers hosted in Singapore and to provide a report on the vulnerabilities found and associated risks.

The purpose of this assessment was to verify the effectiveness of the security controls put in place by ICICI to secure business critical information. The internal networks, including systems and application, are important to ICICI as they are utilised to process FAST payments. If accessed inappropriately, it could cause reputational damage and/or financial loss to ICICI and its management.

THE PROCESS

The nature of the testing performed was designed to replicate the threat of an attacker wishing to gain access to ICICI computer systems or data, through an unknown weakness in the systems and security mechanisms in place.

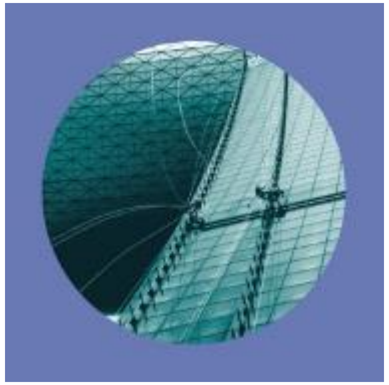
To test ICICI's ability to defend against direct attack, Pragma executed a comprehensive network vulnerability scan, including exploitation of weakened services, client-side attacks, and server-side attacks using Rapid 7 InsightVM.

THE RESULTS

The report represented the findings from the assessment and the associated remediation recommendations to help ICICI strengthen its security posture.

Pragma identified various issues, a few to be considered for remediation according to ICICI bank risk and patch management processes. Few issues could be remediated if desired, but do not by themselves represent a vulnerability.

Let’s work together



✉

Manish Chawda

manish@pragmastrategy.com

Learn more

https://pragma.ltd/

Singapore Headquarters

35A Keong Saik Road, 089142 #03-00 Singapore

London Headquarters

7 Bell Yard, London, United Kingdom, WC2A 2JR

PRAGMA
SECURING YOUR DIGITAL FUTURE