## Broader Business Benefits of Dark Market Scanning as a Service

Every cyber-connected organisation in today's world is a legitimate target in the eyes of the modern cybercriminal and whilst many may postulate that cyber criminals are nuisance hackers only interested in large financial organisations focussing on online banking details, this couldn't be further from the truth.

Globally networked entrepreneurial organised crime syndicates work in seamless harmony to exploit every organisation no matter the size. They possess a greater appreciation of the value of data than most organisations appreciate. They continue to expand at a rapid rate without fear of getting caught for the reality is that most organisation is not reported to law enforcement and most countries lack the legislation and infrastructure to adequately support any prosecutorial action.

DMS provides benefits across the entire organisation in terms of being able to drive business outcomes, reduce risk and provide information to assist evidence-based decision making ultimately contributing to better business decisions.

Actionable intelligence possesses the capability to transform security propositions from one that is technology led and reactive to one that is intelligence led and proactive. Additionally, this intelligence can be used to facilitate value-adds across the entire spectrum of the business not only the IT domain as traditionally thought.

DMS looks to not only provide actionable intelligence in real-time but provide a Risk Assurance to any existing security technology. It is regarded by industry sources that on average it takes an organisation 206 on average to detect they've been breached. DMS provides an avenue to possibly reduce this exposure to mere days. Sometime intelligence can be utilised to neutralise a threat, other times it can be used to provide early warning, and other times it can be used to minimise harm.

Should one consider the standard cyber security maturity model then DMS intelligence can be utilised across that model to afford significant benefits:

**Leadership & Governance**

- Reduce risk across the broader business operating environment
- Improve operations across the Client environment
- Enhanced governance
- Reduced Project risk
- Migration towards a proactive state of readiness

**People**

- Removal or remediation of threats against the Client workforce
- Removal or remediation of threats against the Client Executive and Board
- Improved education programs
- More aware and cybersafe workforce
- Safer "work from home" practices leading to a more flexible workforce model
- Enhanced 3rd Party Risk Assurance
- Reduction of 3rd Party Risk

**Information Risk Management**

- Early identification of threats
- Proactive and more immediate remediation
- Protection of the Client brand
- Harm minimisation
- Risk reduction
- Enhanced state of readiness and response
- Reduction of breach costs
- Assist procurement in acquisition of safer equipment
- Improved business decision making
- Enhanced influence across the business

**Business Continuity & Crisis Management**

- Improved Incident Response
- Reduction of harm
- Reduction of business interruption
- Faster breach response time
- Enhanced business continuity
- Enhanced executive engagement

**Operations and Technology**

- Advanced warning of vulnerabilities
- Advanced warning of possible or impending attacks
- Enhanced maturity level of operations

**Legal and Compliance**

- Compliant state
- Reduction of risk for the Client Brand
- Improved response processes
- Argument for cyber insurance policy cost reduction

## Case Study Examples

**Malware**

Client is a major Australian brand incorporating many regional, local and national brand entities.

DMS identified a compromised server distributing a new malware that had three of the client's domains stipulated within the details of the malware. The purpose of the malware is as yet unknown but what is recognised is that the client organisation is specifically under attack and at risk.

**Insider Threat**

Client is a State based Public Sector entity.

DMS identified a suspected disgruntled employee or contractor who then sought to obtain assistance from criminal entities to cause harm to the client. Vitriolic language used clearly identified this entity as a serious threat both from a cyber and physical perspective. DMS has been engaged to conduct further covert investigations in order to identify the threat entity.

**Compromised eMails**

Client is a State Govt agency.

DMS identified 600 emails and passwords for sale. As a consequence, a forced password reset was ordered on the email accounts rendering the threat benign. The Client was to

conduct a forensic analysis to seek to identify the cause of the data breach in the first instance.

**Criminals Targeting Individuals**

Client is a financial entity.

DMS identified forum chatter between 2 entities discussing how they would seek to target and corrupt an employee inside the client environment. The Client interceded the employee and provided support, guidance and counselling to render any approach ineffective.

**Company Database for Sale**

Client is a Health Organisation

DMS identified part of the client's customer database for sale in the Dark Markets. DMS was able to act on behalf of the client and purchase samples of the database in order to confirm legitimacy and assist in identifying where the breach occurred within the client environment.

**CCS – Cultural Cyber Security Pty Ltd**
www.cultural cybersecurity.com
Brian Hay – 0404 492 220
bhay@culturalcybersecurity.com