SERVICE DESCRIPTION

Ransomware Readiness Assessment

Overview

Trustwave's Ransomware Readiness Assessment ("**Service**") provides a lightweight NIST CSF-based review of Client's ability to prevent and respond to a ransomware attack. Trustwave will deliver a report with tactical and strategic recommendations directed at potential shortcomings in Client's preparedness for a ransomware attack and its consequences. Trustwave will also advise Client on the common motivation, methodologies, and emerging trends in ransomware attacks.

The following description sets out the parameters of the Service, as may be further modified by an applicable SOW or Order Confirmation between Trustwave and Client.

Delivery Phases

The Service consists of the following phases:

Phase 1 – Ransomware Readiness Information Collection

Trustwave will collect information on Client's current state of ransomware readiness using a questionnaire developed by Trustwave. Client will complete this questionnaire. Trustwave will use Client's responses to measure the maturity of Client's ransomware-related controls against industry standard frameworks (such as NIST CSF).

Phase 2 – Assess Identify Controls

Trustwave will assess the overall effectiveness of Client's 'Identify' controls. 'Identify' refers to the categorization of controls in the corresponding NIST CSF function, insofar as those controls relate to Client's establishment of foundational measures to assist in the detection of a ransomware attack in its environment. This may include reviewing some or all of the following (at Trustwave's discretion and based on the applicable domains, their relevance, and Client's responses to the Phase 1 questionnaire):

- Existence and coverage of a vulnerability management program, including any evidence of treatment of identified vulnerabilities by Client
- Scope and output of Client's external and internal penetration testing activities
- Presence of any commonly exposed and vulnerable services (such as remote desktop protocol or virtual private network services)
- Data classification policies or practices addressing the protection of critical data assets

Phase 3 – Assess Protect Controls

Trustwave will assess overall effectiveness of Client's 'Protect' controls. 'Protect' refers to the categorization of controls in the corresponding NIST CSF function, insofar as those controls relate to Client's mechanisms to defend against ransomware attacks. This may include reviewing some or all of the following (at Trustwave's discretion and based on the applicable domain, relevance, and Client's responses to the Phase 1 questionnaire):

- Existence and coverage of a vulnerability management program, including any evidence of treatment of identified vulnerabilities
- Existence and content of security awareness training programs
- Phishing simulation campaigns to augment staff awareness levels
- Use of multi-factor authentication
- Implementation and quality of a backup strategy
- Quality of restrictions for system access privileges, particularly for critical data assets

Phase 4 – Assess Detect Controls

Trustwave will assess overall effectiveness of Client's 'Detect' controls. 'Detect' refers to the categorization of controls in the corresponding NIST CSF function, insofar as those controls relate to Client's mechanisms to build on foundational 'Identify' controls to detect ransomware attacks. This may include reviewing some or all of the following (at Trustwave's discretion and based on the applicable domain, relevance, and Client's responses to the Phase 1 questionnaire):

- Presence of next generation firewalls
- Use of sandboxing technologies
- Presence of next generation anti-virus/endpoint solutions
- Use of enterprise detect and respond tools
- Use of intrusion protection & detection tools
- Presence of security incident event monitoring systems along with use cases and capabilities (e.g., related to data exfiltration)

Phase 5 – Assess Respond Controls

Trustwave will assess overall effectiveness of Client's 'Respond' controls. 'Respond' refers to the categorization of controls in the corresponding NIST CSF function, insofar as those controls relate to Client's ability to respond effectively in the midst of a ransomware attack. This may include reviewing some or all of the following (at Trustwave's discretion and based on the applicable domain, relevance, and Client's responses to the Phase 1 questionnaire):

- Existence of Client's incident response playbooks and processes relating to ransomware attacks
- Coverage of Client's crisis management plans
- Coverage of disaster recovery plans

Phase 5 – Assess Recover Controls

Trustwave will assess overall effectiveness of Client's 'Recover' controls. Recover refers to the categorization of controls in the corresponding NIST CSF function, insofar as those controls relate to Client's ability to resolve a ransomware attack and recover data lost during such attack. This may include reviewing some or all of the following (at Trustwave's discretion and based on the applicable domain, relevance, and Client's responses to the Phase 1 questionnaire):

- Efficacy of backup, recovery tools, and processes (including online vs. offline tools, test restoration frequency, and related documentation)
- Use of local systems for sensitive data storage
- Quality of business continuity processes
- Presence of ransomware and related insurance policies

<u>Phase 6 – Summary Assessment Report</u>

Trustwave will develop a summary report including:

- An executive summary providing an overview of Client's security-related weaknesses and strengths
- A summary of Trustwave's recommendations for addressing such weaknesses aligned to the NIST CSF and suggested priority for remediation
- Current maturity by security domain (aligned to the NIST CSF domains – Identify, Protect, Detect, Respond, and Recover)
- Discussion of commonly asked questions about modern ransomware attacks, including likely future ransomware trends, common ransomware attack vectors, and preferred prevention methods and tactical response measures to put in place in the event of a ransomware compromise

Client Obligations

For Trustwave to provide this Service, Client will:

- establish contact with and remain available for communications from Trustwave
- establish communication and escalation plans with Trustwave
- provide contact details of and access to relevant stakeholders within Client's organization
- provide logistics support for booking meetings and arranging access to required documentation or personnel
- provide the necessary documentation and interview access so as to support off-site delivery of the Service by Trustwave who may be based in the same or different countries to the Client
- make available resources needed for Service activities
- participate in and understand materials explained during calls, meetings, interviews, workshops, discussions, facilities inspection, and controls analysis.

Client acknowledges:

- the Service may consist of onsite and remote consulting activities (at Trustwave's discretion)
- the Service does not include technical testing, penetration testing, social engineering testing (including phishing testing), or other forms of technical testing or assurance of Client's security controls
- the Service does not include verification by Trustwave of control implementation and effectiveness beyond the information provided to Trustwave by Client
- the Service does not include visits to third parties or vendor sites
- Trustwave will perform the Service in the English language
- Trustwave will not create or modify Client documentation as part of the Service
- Trustwave will not provide remediation services as part of the Service
- Trustwave will not offer any legal guidance or regulatory advice
- the quality and accuracy of the Service is dependent on the provision of accurate information to Trustwave by Client.

Client is responsible for:

- the accuracy of information provided in response to Trustwave's data gathering questionnaire

- making its own business decisions about technology security
- assessing its risks and deciding the most appropriate security solution
- having personnel who have the ability to assess the advice received from third parties as it relates to Client’s business
- its own security and access management
- its data backup, retention, and deletion
- its data recovery, disaster recovery and business continuity management
- making decisions on location of data and transferring data, particularly in relation to personal information
- its redundancy of networks or systems and support obligations.

Trustwave Obligations

For this Service, Trustwave will:

- allocate a consultant to deliver the Service
- establish contact and remain available for communications from Client
- establish communication and escalation plans
- schedule and conduct kickoff, periodic status, and closeout meetings, as appropriate
- deliver the Service and document the findings of the Service in a report
- present the report to Client electronically.

Definitions

All capitalized terms not defined in this document have the meanings ascribed to them in Trustwave’s Master Terms and Conditions available at https://www.trustwave.com/en-us/legal-documents/contract-documents/ or in the applicable Statement of Work or Order Confirmation between Trustwave and Client.