Prevalent™

Third-Party Ransomware Assessment

Prevalent

Contents

Prevalent

Document Purpose

This document provides example questions that can be leveraged to assess the ransomware risk among the third parties (e.g., vendors, partners, suppliers, etc.) providing services to your organization. Questions are provided as either multiple choice, free text, or single selection. The question set below focuses on identifying immediate gaps which impact the readiness of your organization to react to ransomware threats.

Sample Questions – External Third-Party Assessment

	Question	Potential Responses
1	Has the organization been impacted by a ransomware attack? (*Please select a single response)*	☐ Yes, we have been impacted as a result of a ransomware attack. ☐ No, we have not been impacted as a result of a ransomware attack.
2	If yes to question #1, what is the impact to the organization as a result of this ransomware attack? *(Please select a single response)*	☐ There has been a significant impact to our company operations, and loss of sensitive data. Please describe the impact caused: ☐ There has been a high-level impact to our company operations, and loss of sensitive data. Please describe the impact caused: ☐ There has been a low-level impact to our company operations, and loss of sensitive data. Please describe the impact caused:
3	Does the organization have an incident investigation and response plan in place? *(Please check all that apply)*	☐ The organization has a documented incident management policy. ☐ The incident management policy includes rules for reporting information security events and weaknesses. ☐ An incident response plan is developed as part of incident investigation and recovery. ☐ Incident response planning includes escalation procedures to internal parties, and communication procedures to clients. Please upload a copy of your incident management policy.

	Question	Potential Responses
4	Who is the person responsible for managing and/or communicating on incident response and resolution? (*Free text field)*	
5	What methods do the organization apply when responding to ransomware attacks? (*Please check all that apply)*	☐ Any affected systems are isolated to prevent further spread of the ransomware. ☐ The malware is quarantined to allow for investigations to analyze the infection and identify the exact strain of ransomware responsible. ☐ Automated maintenance tasks such as temporary file removal and log rotation are disabled on affected systems.
6	Does the organization have a disaster recovery plan, and are ransomware attacks considered as part of a risk assessment? (*Please check all that apply)*	☐ Our organization has implemented a disaster recovery plan. ☐ The disaster recovery risk assessment does include the threat of ransomware attacks. ☐ The disaster recovery plan includes communication trees to inform relevant internal and external parties.
7	Which of the following prevention controls has the organization designed and applied to minimize the risk of a ransomware attack? *(Please check all that apply)*	☐ Regular back-ups are performed on critical or sensitive data. ☐ Employee awareness and training is provided to make staff aware of how to identify and report suspected ransomware attacks. ☐ Software is regularly patched and kept up to date. ☐ Permissions including privileged access is regularly reviewed, and local administration rights are removed.

	Question	Potential Responses
8	Please describe the approach taken to manage data backups. *(Please check all that apply)*	☐ Backups are stored off-line. ☐ Backups are stored in an off-site location. ☐ Testing is conducted to validate successful backups.
9	Do remote workers employ endpoint security protection and preventative technologies and processes? *(Please check all that apply)*	☐ The organization has deployed file-based malware protection. ☐ The organization utilizes intrusion detection and prevention protection to detect and block malicious activity. ☐ The organization centralizes audit logging to enable investigation and remediation response to dynamic incidents and alerts.
10	Does the organization regularly assess its security controls and prevention techniques to ensure they remain up to date? (*Please check all that apply)*	☐ Internal audits are conducted on a periodic basis to validate that security controls are implemented and effective. ☐ External assessments are conducted on a periodic basis by independent parties.

Prevalent

About Prevalent

Prevalent takes the pain out of third-party risk management (TPRM). Companies use our software and services to eliminate the security and compliance exposures that come from working with vendors, suppliers and other third parties across the entire vendor lifecycle. Our customers benefit from a flexible, hybrid approach to TPRM, where they not only gain solutions tailored to their needs, but also realize a rapid return on investment. Regardless of where they start, we help our customers stop the pain, make informed decisions, and adapt and mature their TPRM programs over time.

To learn more, please visit www.prevalent.net.