FLEXENTIAL®

Ransomware defense readiness assessment

Reduce ransomware risks and increase protection, detection, response and recovery capabilities

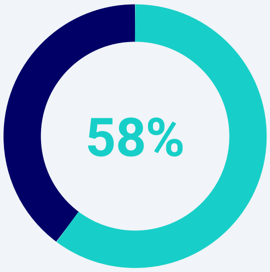
Internal security teams face increasingly sophisticated, rampant, and costly ransomware threats. To successfully protect against, detect, respond and recover from ransomware attacks, organizations must proactively understand and mitigate ransomware risks and continuously enhance their response and recovery capabilities for when they experience a ransomware incident.

Before you experience a ransomware attack, IT needs to identify weaknesses, identify how you will stop an attack when it occurs, protect your environment by mitigating those weaknesses, and prepare your response team and users.

- **80% of organizations** who paid a ransom were victims of one or more subsequent ransomware attacks
- **68% who paid a ransom** were hit again in less than one month—and the ransom demand increased

When a ransomware attack occurs, IT must quickly detect, respond, and recover all data and systems. Detection and response speed and effectiveness can directly limit the extent, losses and damage of cyber attacks. Recovery capabilities, including backup and disaster recovery, can provide organizations with the means to recover all data—without paying a ransom.

- **78% of organizations** that did not pay a ransom fully restored systems and data without a decryption key
- **46% reported** that they paid the ransom to restore data
- **Only 4%** of those that paid the ransom got all their data back



58% of US organizations were hit by ransomware in the last year

Ransomware defense readiness assessment

Our highly certified and experienced professional services' cybersecurity and risk team partners with your team to assess and improve your protection, detection, response and recovery capabilities needed for today's ransomware threat landscape.

Deliverables include detailed, actionable, and prioritized, guidance to improve your cybersecurity posture and reduce ransomware risk.

Protect

Objective: Ensure there are defense capabilities in-house before a ransomware incident occurs

- Assess the security of access controls, external perimeters, and email threat protection
- Assess effectiveness of critical asset segmentation
- Assess endpoint security, including whitelisting, endpoint protection, hardening, and patch management.
- Assess the user training program for recognizing suspicious activity
- Assess the user training program for quickly communicating possible security issues to the appropriate IT contact.

Detect

Objective: Ensure there are ransomware detection capabilities

- Assess monitoring and alerting capabilities for critical assets, including email, file shares, and databases
- Assess monitoring and alerting capabilities for intrusion detection
- Assess endpoint detection and response capabilities

Respond

Objective: Ensure ransomware response capabilities that allow for maximum containment that limits exposure and losses

- Assess ability to quickly contain a ransomware attack to a limited number of systems
- Assess capabilities to quickly notify the response team of a possible ransomware incident
- Assess incident response capabilities for responding and containing the incident as quickly as possible.

Recovery

Objective: Ensure there are ransomware recovery capabilities for recovering from a ransomware attack quickly and avoiding ransom payments

- Assess backup and snapshot methodologies and capabilities
- Assess disaster recovery plan and capabilities
- Assess ability to meet business expectations for recovery requirements and availability
- Assess the ability to recover without paying a ransom

Deliverables

- Technical guidance for preventing and responding to ransomware attacks
- Technical report with detailed, actionable, and prioritized recommendations
- Executive summary of identified ransomware risks to share with IT and executive leadership
- Presentations of findings with discussion of recommendations
- Knowledge transfer to security and risk teams

Sources:
(1) The State of Ransomware 2022, Sophos
(2) Ransomware: The True Cost to Business 2022, Cybereason

Problems we solve

- Unknown and unaddressed ransomware risks
- Ad-hoc or reactive ransomware incident response approaches
- IT teams that are unsure of how to defend, respond, or recover from ransomware
- Uncertainty on why and how to prioritize actions
- Lack of cybersecurity or ransomware knowledge
- Insufficient tools and training

Outcomes we create

- More effective ransomware defenses
- Know what to do and in which sequence to improve ransomware protection, detection, response, and recovery
- Visibility and documentation for improving ransomware defense readiness
- Prioritization of ransomware risk reduction activities to protect critical operations and data
- Increase in IT staff preparedness and knowledge
- Higher confidence in IT team's ability to respond and recover from a ransomware attack