Leveraging Ransomware Assessment to Craft a Solid Digital Defense

Keys to a Successful Ransomware Preparedness Strategy

No organization is completely immune from experiencing a ransomware attack, which only emphasizes the need for strict protocols and security processes. By incorporating a structured ransomware assessment process and adhering to cybersecurity best practices, companies can arm themselves with the most effective approach to protecting data assets and maintaining resilience against ransomware threats.

The IntraSystems methodology is based on maturity level and is cost-effective to fit your budget. Its flexibility enables the methodology to be easily replicated with the same results. This approach to ransomware preparedness is future-proof to guarantee that organizations stay ahead of constantly evolving threats.

Our prescriptive strategies and frameworks are designed to help organizations understand their current cybersecurity posture through a comprehensive assessment process. We focus on seven key pillars to evaluate current protocols and to provide a thorough analysis:

1. **Endpoint Protection** I Current security measures for all endpoints, including desktops, laptops, and mobile devices, are assessed to ensure they are protected against ransomware threats.

2. **Security Processes** I An organization's security processes, including regular audits, compliance checks, and continuous monitoring, are evaluated to identify gaps or weaknesses.

3. **Network Security** I Network security measures, such as firewalls, intrusion detection systems, and network segmentation,are reviewed to determine their effectiveness in preventing unauthorized access and containing potential threats.

4. **Data Center** I Security controls for physical and virtual data centers are examined to guarantee critical data is protected against ransomware attacks and other cyber threats.

5. **Incident Response** I The organization's incident response plans are analyzed to assess its ability to respond quickly and effectively to ransomware attacks, minimizing damage and providing a swift recovery.

6. **Backup and Recovery** I Backup and recovery strategies are evaluated to determine that data can be restored quickly and accurately in the event of a ransomware attack.

7. **Security Governance (Standard Offering only)** I The Governance framework is reviewed to define cybersecurity roles, responsibilities, and accountability, ensuring that all stakeholders are aligned and informed.

What is Ransomware Readiness?

Ransomware Readiness is a structured way to align IT security with business goals while managing risks specific to ransomware threats. While not a new concept, its importance has recently been elevated as companies contend with increasingly sophisticated ransomware attacks.

Express Offering

Topics Covered:

- Endpoint Protection
- Security Processes
- Network Security
- Data Center
- Incident Response
- Backup and Recovery

Two (2) Discovery workshops

Workshop Length
- 90 Minutes

Workshop 1
- Endpoint Protection
- Security Processes
- Network Security

Workshop 2
- Data Center
- Incident Response
- Backup and Recovery

Standard Offering

Topics Covered:

- Endpoint Protection
- Security Processes
- Network Security
- Data Center
- Incident Response
- Backup and Recovery
- Security Governance
- Ransomware Tabletop Exercise
- Documentation Review

Three (3) Discovery workshops

Workshop Length
- 90 Minutes

Workshop 1
- Endpoint Protection
- Security Processes
- Network Security

Workshop 2
- Data Center
- Incident Response

Workshop 3
- Backup and Recovery
- Security Governance

Additional items
- One (1) Tabletop Exercise (up to 3 hours in length)
- Limited Document Review (max 10 key documents)

Express Offering

Scope of Engagement

- Organizations with < 200 Employees
- Primary Data Center Only
- Single Active Directory Forest
- Information Security Policies at Headquarters Level
- Production Environment Only

Exclusions

- Document Review
- Implementation Services
- Custom Playbook Development
- Policy Writing
- Technical Testing or Penetration Testing
- Remediation Support
- Training Development/ Delivery
- Additional Workshops or Stakeholder Interviews
- Architecture Design
- Third-Party Vendor Assessments

Standard Offering

Scope of Engagement

- Organizations Up to 400 Employees
- Primary and One (1) Secondary Data Center
- Single Active Directory Forest
- Information Security Policies at Headquarters Level
- Production Environment Only

Exclusions

- Implementation Services
- Custom Playbook Development
- Policy Writing
- Technical Testing or Penetration Testing
- Remediation Support
- Training Development/ Delivery
- Additional Workshops or Stakeholder Interviews
- Architecture Design
- Third-Party Vendor Assessments

Benefits of the IntraSystems' Approach

- **Maximize Focus** | Enable focus on initiatives that matter via a business-aligned ransomware preparedness strategy and executable roadmap.
- **Justify Strategy** | Develop business cases with detailed current state and target-state financial models for ransomware defense.
- **Purposefully Execute** | Equip your team with a detailed architecture and implementation plan, with resources to execute ransomware preparedness measures.
- **Ensure Adoption** | Drive the program's success through organizational change management focused on ransomware awareness and prevention.