GDT

Strengthen Your
Cyber Resilience:

5 Components
for a Proven
Ransomware
Defense Strategy

Strengthen Your
Cyber Resilience

Your Ransomware
Defense Strategy

1 **2** **3** **4** **5**

GDT for Cyber-Resilient
Infrastructure

Table of Contents

Strengthen Your Cyber Resilience

5 Components for a Proven Ransomware Defense Strategy

Comprehensive cyber resilience is absolutely critical in today's business environment. Data breaches have become a fact of life, with cyber incidents, including ransomware, topping the list of leading business risks for the last several years.[1]

Solidifying its reputation as a top cybersecurity threat, ransomware has impacted nearly 60% of organizations in the last year. The average recovery cost — excluding ransom payments — **$2.73 million**.[2] With ransom payments, the number is much higher. The average initial ransom demand is **$2 million**.[3]

59%

of organizations **experienced ransomware attacks in the last year.**

Unpatched vulnerabilities **&** **compromised credentials**

are the top causes of entry.

Ransom bills have

increased 5x

in the last year.[4]

[1] Statista. (January 2024). Leading Risks to Businesses Worldwide from 2018 to 2024.

[2] Sophos. (April 2024). The State of Ransomware 2024.

[3] Ibid.

[4] Ibid.

AND RANSOMWARE ONLY CONTINUES TO EVOLVE IN SOPHISTICATION AS NEW TECHNOLOGIES EMERGE.

Today's cybercriminals employ advanced social engineering and phishing campaigns, exploiting vulnerabilities in remote access tools and often spending weeks inside a target's networks before deploying ransomware. In addition, the rise of ransomware as a service has democratized access to sophisticated tools for the less technically proficient.

Taken together, the implications are enormous: Ransomware is everywhere. Attacks will happen, data breaches will occur, and the potential impacts are astounding. The question is, what are you doing to create a cyber-resilient data estate that's ready for any eventuality?

Strengthen Your
Cyber Resilience

**Your Ransomware
Defense Strategy** `1` `2` `3` `4` `5`

GDT for Cyber-Resilient
Infrastructure

Your Ransomware Defense Strategy: A Proven, 5-Part Framework

Prioritizing a comprehensive ransomware defense strategy has a twofold positive effect. First, it will help prevent ransomware attacks. Second, it ensures that when a data breach does happen, your organization is fully prepared to respond quickly to mitigate risk and costs and maintain business continuity.

To help you strengthen your cyber resilience strategy, GDT has developed a five-part ransomware defense framework. We use this framework to help our clients address growing ransomware threats while also maturing their overall security posture. In this ebook, we're making this framework available to you to help you build and execute a proactive approach to ransomware preparedness and response. The following outlines the five key parts of this framework and the major components within each.

1

Ransomware Resiliency Workshops

Assessing your organization's overall cyber resilience, including strengths and vulnerabilities, is essential in building a holistic ransomware defense strategy. Combine the following strategies to help identify and prioritize threats to your business.

THREAT INTELLIGENCE BRIEFINGS FOR YOUR INDUSTRY

Know thy enemy. It's essential to seek out threat intelligence briefings relevant to your field that take an in-depth look at your industry's unique challenges while also providing trends and insights for mitigating threats. For example, Trustwave releases threat briefings for industries such as technology, healthcare, and manufacturing.

ATTACK SURFACE MANAGEMENT (ASM) REVIEWS

An ASM review involves identifying, assessing, and mitigating vulnerabilities across your organization's digital footprint, including hardware, software, network infrastructure, and even human factors. This comprehensive review identifies potential attacker entry points. ASM reviews will help you prioritize risks, improve incident response, enhance employee awareness, and integrate and optimize existing security tools and measures to improve your overall strategy.

EMAIL SECURITY STRATEGIES AND REVIEW

Email is a primary vector through which ransomware attacks are initiated. Take the time to evaluate your email security strategies. Look at areas like email security, filter and quarantine methods for preventing infection, employee education programs, authentication practices, and compliance with security policies.

BEST PRACTICE POSTURE ASSESSMENTS

Reviewing your organization's procedures, methods, and practices provides a starting point for ensuring your organization has a systematic approach to identifying vulnerabilities that could be exploited by ransomware, prioritizing risks, and benchmarking against industry standards.

RANSOMWARE DEFENSE VALIDATION

Finally, validation testing can help your organization simulate various attack scenarios to assess your organization's resilience, identify vulnerabilities, and train staff in identification and response techniques.

Strengthen Your
Cyber Resilience

**Your Ransomware
Defense Strategy** `1` `2` `3` `4` `5`

GDT for Cyber-Resilient
Infrastructure

2

Ransomware Protection

Organizations must enact processes and policies to guard against ransomware attacks. Here at GDT, when we're helping an organization improve ransomware protection, we focus on these core components.

PATCH AND VULNERABILITY MANAGEMENT REVIEWS

Regular patch and vulnerability management reviews play an essential role in identifying vulnerabilities, prioritizing risks, ensuring timely patches and updates, and ultimately reducing the attack surface.

DATA PROTECTION ASSESSMENTS

This involves evaluating current data protection strategies and working with organizations to provide a custom approach and roadmap to data protection.

32%
of attacks start with an unpatched vulnerability.

70%
of attacks result in data encryption.

32%
of data encryption victims had data stolen.[5]

2 Ransomware Protection
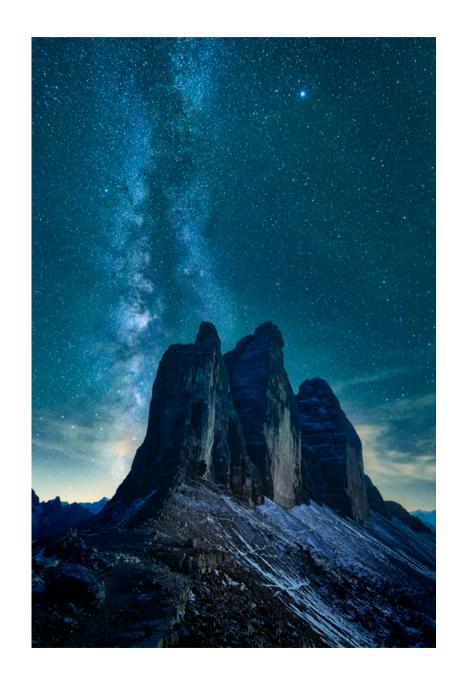
IDENTITY ACCESS MANAGEMENT (IAM) MATURITY

IAM maturity contributes to ransomware protection by providing a comprehensive framework for managing and securing digital identities. For example, implementing role-based access control helps ensure users can access necessary resources for their roles. Implementing multi-factor authentication adds an extra layer of security. Regular IAM reviews ensure unnecessary permissions get revoked promptly while also contributing to maturing an organization's security posture.

MICROSEGMENTATION

Microsegmentation comprises a critical component of a Zero Trust security model. Segmenting a network into smaller, isolated parts — each with its own security protocols — helps protect other parts of a network by containing a ransomware attack, preventing its spread to different areas of the network, and limiting its impact. It also enforces granular access controls, reducing the attack surface. Other benefits include enhanced monitoring and detection, rapid isolation and response, and increased regulatory compliance.

GOVERNANCE FRAMEWORK MODELS AND COMPLIANCE REVIEWS

Governance framework models and compliance reviews provide a structured approach to ensuring adherence to compliance best practices. These models protect organizations against ransomware attacks by establishing policies, controls, and procedures to increase resilience and lower risk.

Strengthen Your
Cyber Resilience

Your Ransomware
Defense Strategy   1 2 **3** 4 5

GDT for Cyber-Resilient
Infrastructure

3 Ransomware Detection

As the nature of ransomware attacks continues to change, a robust detection solution that uses AI and machine learning is a vital part of any defense strategy. At GDT, we find strong results focusing on the following areas.

MANAGED DETECTION AND RESPONSE (MDR)/ EXTENDED DETECTION AND RESPONSE (XDR)

MDR and XDR services provide organizations with advanced detection and incident response capabilities, combining AI and other technologies with human expertise. Capabilities include continuous network monitoring, proactive cyberthreat hunting, rapid response to contain threats, and root-cause analysis with an eye toward prevention.

INSPECTION STRATEGIES AND NETWORK SECURITY INFRASTRUCTURE

Organizations can further enhance ransomware detection and overall security posture by layering inspection strategies with a more robust network security infrastructure. Inspection strategies can include signature-based detection and behavioral analysis to detect anomalies. Network security infrastructure strategies include network traffic analysis, intrusion detection, file integrity monitoring, and network segmentation.

CLOUD SECURITY POSTURE MANAGEMENT (CSPM) SERVICES

CSPM automates identifying and mitigating misconfigurations and security risks across hybrid and multicloud environments. These services may include continuous real-time monitoring of cloud resources, detecting misconfigurations, providing automated mitigation recommendations, risk and compliance monitoring, and DevOps integration.

DARK WEB MONITORING

Dark Web monitoring focuses on the hidden online marketplace where cybercriminals buy and sell stolen and leaked information. It scans for indicators of compromise to support early threat detection and delivers threat intelligence to mitigate or prevent ransomware attacks. Additional benefits include identifying emerging threats and targeted attacks and prompt identification when sensitive information falls into the wrong hands.

Strengthen Your
Cyber Resilience

**Your Ransomware
Defense Strategy** `1` `2` `3` **4** `5`

GDT for Cyber-Resilient
Infrastructure

4

Ransomware Remediation and Response

While robust ransomware identification, prevention, and detection strategies help lower risk, they don't eliminate it. That's why every business must adopt strong ransomware remediation practices and have a practiced, comprehensive incident response plan.

DISASTER RECOVERY PLANS

A robust disaster recovery plan can help streamline recovery and contain the costs and operational impacts of a ransomware attack. A plan must include steps like identifying impacted assets, damage control, network isolation, variant identification, choosing the right remediation approach, and implementing preventative measures.

IMMUTABLE BACKUP STRATEGY

An immutable backup is crucial as it prevents data backups from being altered or deleted, even by administrators. It ensures data can be restored during remediation efforts and helps organizations meet data retention compliance and governance requirements.

94%

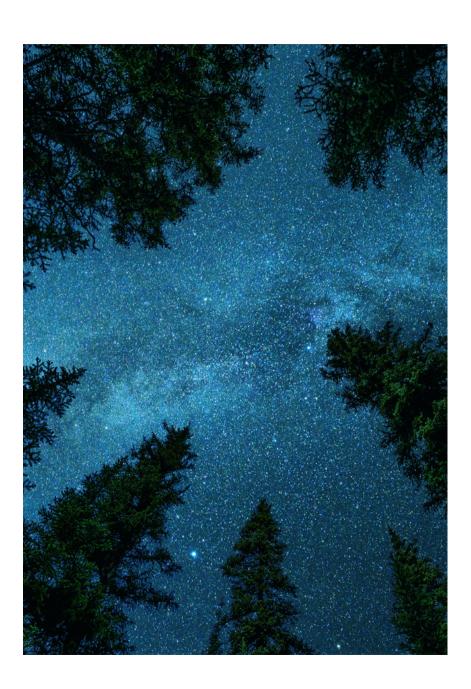of ransomware victims said attackers targeted backups.

57%

of backup compromise attempts in the last year were successful.

34%

of organizations impacted by a ransomware attack took over a month to fully recover.[6]

[6] Ibid.

Strengthen Your
Cyber Resilience

**Your Ransomware
Defense Strategy**   `1`   `2`   `3`   **`4`**   `5`

GDT for Cyber-Resilient
Infrastructure

`4` **Ransomware Remediation and Response**

INCIDENT RESPONSE RETAINER

You won't want to spend precious time finding qualified incident response support and negotiating contracts when a ransomware attack happens. That's why it's essential to incorporate an incident response retainer as part of your ransomware incident response plan, with professionals ready to support you at a moment's notice. In addition to swift engagement and immediate help when a ransomware attack occurs, an incident response retainer enables proactive planning and crisis preparation, expert guidance and support from seasoned experts, and flexible usage options for changing needs.

REGULAR UNIT TESTING

Testing program components in isolation ensures that vulnerabilities and weaknesses in code are identified and mitigated early in the development process, thus reducing the attack surface. Regular unit testing allows for quick code adjustments while also validating the reliability of data backups should they be needed for ransomware recovery efforts.

Strengthen Your
Cyber Resilience

**Your Ransomware
Defense Strategy** `1` `2` `3` `4` `5`

GDT for Cyber-Resilient
Infrastructure

5

Tools Consolidation and Maturity

Finally, the proper tooling and integration points play a crucial role in your ransomware defense strategy. As industry challenges increase in complexity, an integrated tool set that provides the proper cross-functional view is important. The ability of SOC teams and security organizations to respond quickly without bottlenecks is key.

BLACK KITE RANSOMWARE SUSCEPTIBILITY INDEX (RSI) SCORING

Black Kite's RSI helps organizations quantify the likelihood of a ransomware attack by assessing factors like email security, remote access ports, outdated systems, and other factors. This scoring provides organizations valuable insights into opportunities to strengthen their defenses and make proactive system updates. The RSI score can also help organizations develop policies to reduce losses associated with ransomware attacks.

Strengthen Your
Cyber Resilience

Your Ransomware
Defense Strategy

1 **2** **3** **4** **5**

**GDT for Cyber-Resilient
Infrastructure**

GDT for Cyber-Resilient and Ransomware-Ready Infrastructure

While there's no silver bullet to completely prevent ransomware attacks, much can be done to mitigate threats and maximize cyber resilience across the organization. Working with a holistically minded partner like GDT can help you identify the right next steps for your organization and implement strategies that deliver the business outcomes you need.

Our comprehensive approach to cyber-resilient infrastructure includes services spanning assessment, implementation, and support, plus our deep partnership with leading-class data center technology providers offers the best in data storage and protection. Whatever your current security posture, we'll help you align IT operations to support comprehensive and sustainable ransomware readiness and data protection outcomes.

WE'LL HELP YOU:

- ☑ **Assess** current-state data protection and ransomware readiness.
- ☑ **Adopt** modern storage and data protection infrastructure.
- ☑ **Identify and remediate** risks and close security gaps.
- ☑ **Implement** ransomware detection and response.
- ☑ **Define** effective backup/disaster recovery protocols.
- ☑ **Elevate** incident response strategies.
- ☑ **Ensure** regulatory compliance.

Start With a Data Center Strategy Workshop

Our complimentary Data Center Strategy Workshop is designed to help you get a clear picture of your existing infrastructure strengths and weaknesses and help you create a strategy to address them. Our experienced data center professionals will work with you to identify and prioritize opportunities for strengthening security, data protection, compliance, and processes to help ensure your data center is future-proof and secure.

AVOID DOWNTIME, DATA LOSS, AND THE NIGHTMARE OF RANSOMWARE.

Get your dream defense with GDT. Learn more and discover how to get started with a no-cost Data Center Strategy Workshop.

Learn More