GOTHAM
technology group, LLC

RANSOMWARE READINESS ASSESSMENT

***Gotham's Ransomware Readiness Assessment** works with your IT department to bring ransomware security gaps, posture, and misconfiguration into focus with detailed analysis, experience, and insight.*

In 2019, Verizon found that 87% of breaches were financially motivated and 27% involved ransomware. Meanwhile, IBM reported that 70% of small businesses have no experience managing ransomware attacks.

Unfortunately, ransomware isn't going away any time soon. Cybercriminals know that encrypting data can be highly profitable, and that there are numerous ransomware packages available for their use.

Organizations need to be confident that their IT environment and assets are protected against ransomware and other types of malware.

It's important to understand the specific security controls needed to successfully fend off ransomware attacks, and organizations must continually adjust to the increasingly complex and challenging ransomware and malware

THE ASSESSMENT

Using an online survey, we collect data about your current security controls, including:

- End point protection
- Vulnerability management
- Browser and email protections
- Security awareness training
- Network admission controls
- Firewall policy and remote access
- Privileged account management
- Logging and alerting
- Incident readiness

After the survey is completed, we interview your IT and cybersecurity teams to drill down into each of the security control categories. As we work through each control, a complete picture of your organization's security posture and ransomware readiness comes into view.

Based on this information, we create and present a Ransomware Readiness Report that includes the current status of your security controls and gaps as well as recommendations for remediation.

To get started on your assessment or for more information, contact your Gotham Account Manager.