**Ransomware / Cyber Resiliency**

**Email 7: How to Develop a Ransomware Remediation Plan**

Subject line A: Ransomware Remediation Best Practices

Subject line B: How to Develop a Ransomware Remediation Plan

Header: How to Develop a Ransomware Remediation Plan

Hi [name],

[Incall to modify copy incorporating earlier conversation with customer here.]

Paying a ransom should not be your only option when ransomware strikes. Learn how to develop a strong remediation plan so you can better prepare your business against ransomware.

Download our best practices guide to learn how to:

* Construct your remediation plan.
* Assess your options in the case of a ransomware attack.
* Secure your environment against future threats.

Download eBook here.

**Email 5: ESG Technical Review: Rubrik Data Management Platform and Immutable Architecture For Ransomware**

Subject line A: Are your backups ransomware-resistant?

Subject line B: \*Get immune to ransomware\* ESG Review explains how.

Header: Safeguard your backups

Hi [First Name, Default: friend],

[Incall to modify copy incorporating earlier conversation with customer here.]

Cybercriminals are increasingly targeting backups, leaving organizations with no option but to pay the ransom.

Learn how Rubrik can safeguard your backups in this Technical Review.

IT analyst firm ESG examines how Rubrik protects data from ransomware attacks and accelerates the post-attack recovery process with its immutable architecture.

Button: [[GET THE REPORT]](https://www.rubrik.com/en/resources/Analyst-Reports/20/esg-report-immutable-architecture)