STUDY:

Ransomware Pulse Survey 2021

A Research Study by:
Krista Macomber, Senior Analyst

PRESENTED BY Evaluator Group
July 2021
Table of Contents

Table of Figures ........................................................................................................................... 2

Introduction ................................................................................................................................. 3

Objectives and Scope of This Study ............................................................................................. 3

Executive Summary ....................................................................................................................... 3

Key Findings ................................................................................................................................. 4

Spending – Last 12 Months .......................................................................................................... 4

Spending – Moving Forward ....................................................................................................... 4

Best Practices – Ransomware Resiliency ..................................................................................... 4

Usage of Air Gapped Backups ..................................................................................................... 4

Security Audits ............................................................................................................................ 4

Recommendations for Vendors .................................................................................................... 4

Recommendations for End Users ................................................................................................ 4

Conclusion .................................................................................................................................... 4

Appendix ...................................................................................................................................... 4

Survey Demographics .................................................................................................................. 4

Company Size ............................................................................................................................. 4

Industry ......................................................................................................................................... 4

Area of Responsibility ................................................................................................................ 4

About Krista Macomber ................................................................................................................ 5

About Evaluator Group .................................................................................................................. 5
### Table of Figures

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Data protection spend over the past 12 months</td>
<td>4</td>
</tr>
<tr>
<td>2</td>
<td>Ransomware spending plans</td>
<td>5</td>
</tr>
<tr>
<td>3</td>
<td>Ransomware best practices</td>
<td>6</td>
</tr>
<tr>
<td>4</td>
<td>Air gapped backups</td>
<td>7</td>
</tr>
<tr>
<td>5</td>
<td>Security audit by third-party</td>
<td>7</td>
</tr>
<tr>
<td>6</td>
<td>Security audit over past 12 months</td>
<td>7</td>
</tr>
<tr>
<td>7</td>
<td>Company size</td>
<td>9</td>
</tr>
<tr>
<td>8</td>
<td>Industries represented</td>
<td>9</td>
</tr>
<tr>
<td>9</td>
<td>Area of responsibility</td>
<td>10</td>
</tr>
</tbody>
</table>

Included in full Research Study available with purchase
Introduction

Without a doubt, ransomware is a massive threat for enterprises across industries and across the globe. The recent Colonial Pipeline attack goes to show the critical role that data and recoverability has grown to play in our economy. Disrupted typical business operations and the massive shift to working from home due to COVID-19 have increased enterprises’ attack surfaces, against a backdrop of ever-more creative and resourceful organized ransomware gangs.

And as Evaluator Group observed from our “Enterprise IT Responds to Covid-19” Studies, cyber security topped the spending priorities this past year. However, the ability to recover data is the best defense against ransomware, throwing data protection into a strategic spotlight.

The threat is real, but what has been less clear is if customers are actually investing in data protection to bolster their defenses. And if so, where exactly they are spending, as ransomware protection and prevention crosses many disciplines.

Objectives and Scope of This Study

Evaluator Group fielded an online survey of 125 backup solution users and purchase influencers in May and June 2021. A variety of industries and organization sizes were represented. Additional detail on respondents’ roles and organizational demographics is available in the Appendix of this report.

The objective of this research was to understand if customers are spending from a data protection perspective due to the rise in ransomware. If so, Evaluator Group wanted to understand in what areas customers are spending, and roughly how much they are spending.

Executive Summary

Survey results show that the ransomware threat is materially impacting data protection initiatives and spending. Nearly all (96%) of respondents indicated having implemented some form of best practices for ransomware resiliency over the past 12 months, while more than half of respondents indicated having spent against data protection over the last 12 months due to the rise in ransomware. Meanwhile, 87% indicated that they plan to spend, or have budgeted to spend, against technologies for ransomware protection and prevention over the next 12 months.

Fundamental best practices like system patching, taking frequent backups, and auditing/testing backups and recoverability emerged were top-of-mind from respondents. Along the same vein, many respondents indicated that they have been taking a step back to assess their risk posture and develop an incident response plan; being prepared for the inevitable is key.

But, as responses showed, a comprehensive approach to ransomware resiliency goes further. Security controls like user access control and authentication, as well as end-user training initiatives, to inhibit malicious access to backups, have also become prominent.
Key Findings

- Spending – Last 12 Months
- Spending Plans Moving Forward
- Best Practices – Ransomware Resiliency
- Usage of Air Gapped Backups
- Security Audits

Recommendations for Vendors

Recommendations for End Users

Conclusion

Appendix

Survey Demographics

- Company Size
- Industry
- Area of Responsibility
About Krista Macomber

Krista covers data protection and management for Evaluator Group. She brings more than a decade of experience providing research and advisory services and creating thought leadership content, with a focus on IT infrastructure and data management and protection. Her vantage point spans technology and vendor portfolio developments; customer buying behavior trends; and vendor ecosystems, go-to-market positioning, and business models. Her work has appeared in major publications including eWeek, TechTarget and The Register.

About Evaluator Group

Evaluator Group Inc., an Information management and data storage analyst firm, has been covering systems for over 20 years. Executives and IT Managers rely upon us to help make informed decisions to architect and purchase systems supporting their data management objectives. We surpass the current technology landscape by defining requirements and providing an in-depth knowledge of the products as well as the intricacies that dictate long-term successful strategies.

Copyright 2021 Evaluator Group, Inc. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written consent of Evaluator Group, Inc. The information contained in this document is subject to change without notice. Evaluator Group assumes no responsibility for errors or omissions. Evaluator Group makes no expressed or implied warranties in this document relating to the use or operation of the products described herein. In no event shall Evaluator Group be liable for any indirect, special, inconsequential, or incidental damages arising out of or associated with any aspect of this publication, even if advised of the possibility of such damages. The Evaluator Series is a trademark of Evaluator Group, Inc. All other trademarks are the property of their respective companies.