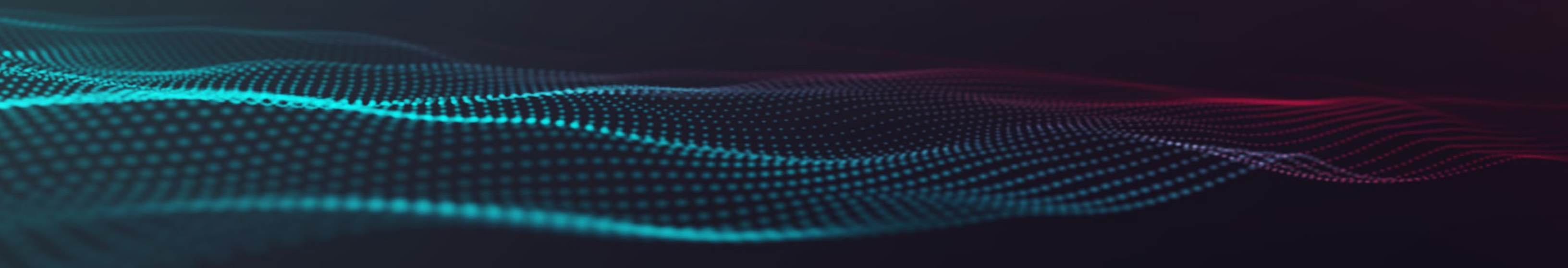
Enterprise Strategy Group | Getting to the bigger truth.™



ESG WHITE PAPER

Effective Cyber Resiliency

A Comprehensive Approach to Ransomware Preparedness with Carbonite Data Protection

By Christophe Bertrand, Practice Director

August 2022

This ESG White Paper was commissioned by OpenText and is distributed under license from TechTarget, Inc.

Contents

Market Landscape and Key Trends

Cybersecurity initiatives are driving IT spending in 2022 as organizations race to secure digitally transformed data and processes and safeguard newly hybridized workforces. Over half (54%) of the IT security professionals polled for the ESG/ISSA Cybersecurity Process and Technology Survey indicated they had experienced one or more security incidents over the past two years, including system compromise, malware incidents, DDoS attacks, targeted phishing attacks, and data breaches. These incidents inflict quantifiable damage on an organization, including lost productivity (51%), time-consuming incident remediation (39%), and disruption to business processes (37%).[1]

While organizations face a broad range of cyber-threats, one in four (26%) rank ransomware as their most important business priority, and over half (53%) place it in their top five.[2] The concern for ransomware is greater now than two years ago for over eight in ten organizations, and this has elevated ransomware readiness to a top business priority.[3] Senior leadership in nine out of ten organizations now plays a role in determining ransomware strategies. The costs for organizations that don't sufficiently invest in cybersecurity defenses continue to mount, including payments to cyber-adversaries, higher cyber insurance premiums, and government regulatory penalties and fines. Correspondingly, two-thirds of IT decision-makers (69%) said their organization would increase cybersecurity spending compared to last year.[4]

Cloud (62%) and data security (58%) top the list of planned cybersecurity spending increases in 2022. Cloud infrastructure security (56%), network security (55%), and endpoint security (50%) round out the top five spending spots, emphasizing the broad and rapid adoption of cloud services and the need to protect cloud-resident data assets.[5]

Data is now being generated at unprecedented rates, and the ability to collect, manage, process, analyze, monetize, and protect data are business-critical priorities. Over half of organizations (57%) plan to increase their 2022 data protection budget compared to last year. Protection for endpoint devices (48%), data and applications residing in the public cloud (48%), and implementing cyber resilient data recovery capabilities (47%) topped data protection budget plans.[6] As digital transformation initiatives mature and customer expectations for cloud-based services grow, organizations will increase data protection spending to mitigate the risk from highly sophisticated cyber-threats.

Organizations realize they can no longer pin their hopes on keeping the bad guys out. A layered, defense-in-depth approach that prioritizes cloud security, data security, network security, and endpoint security can deliver a more holistic and resilient defense.

The Inevitability of Ransomware

Ransomware attacks are pervasive, and their impact is felt across all types of organizations. ESG surveyed 620 IT and cybersecurity professionals involved with the technology and processes associated with protection against ransomware. Four out of five responding organizations (79%) report experiencing a ransomware incident within the last year, with 73% indicating the attack was successful. Indeed, paying the requested ransom rarely resulted in the retrieval of all data held hostage by attackers. Over half of victims of successful attacks indicated the data included sensitive infrastructure configuration information.[7]

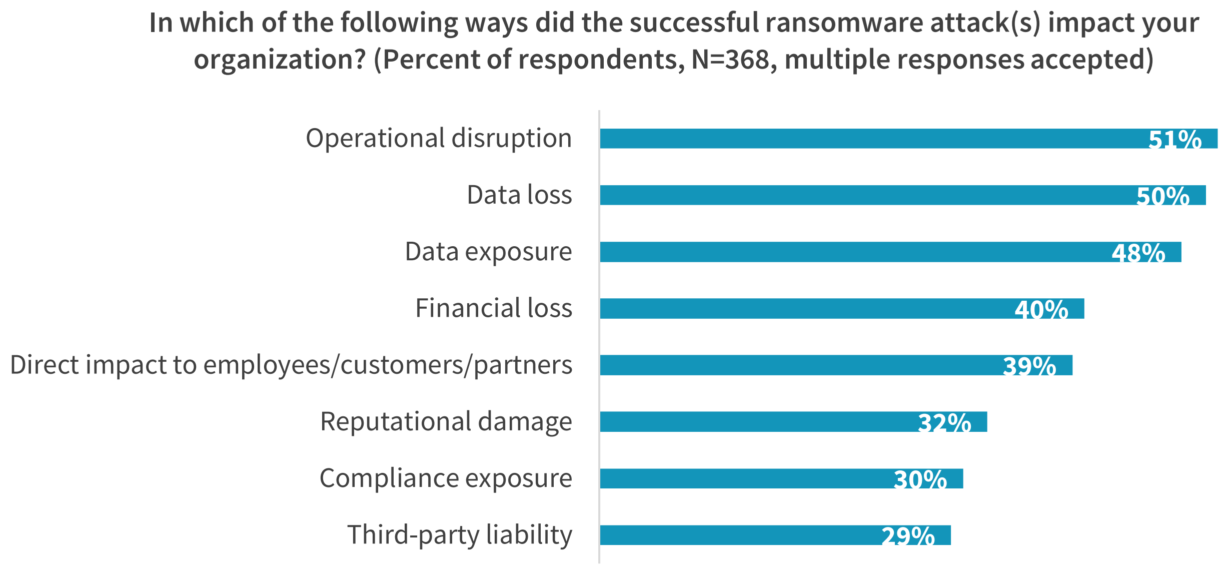
[1] Source: ESG Complete Survey Results, *ESG/ISSA Cybersecurity Process and Technology Survey*, June 2022.
[2] Source: ESG Brief, *Cybersecurity Spending Trends for 2022*, March 2022.
[3] Source: ESG Complete Survey Results, *2022 Technology Spending Intentions Survey*, November 2021.
[4] Source: ESG Brief, *Cybersecurity Spending Trends for 2022*, March 2022.
[5] Ibid.
[6] Source: ESG Complete Survey Results, *2022 Technology Spending Intentions Survey*, November 2021.
[7] Source: ESG Research Report, *The Long Road Ahead to Ransomware Preparedness*, June 2022.

Ransomware attackers have become more adept at evading defenses and more discerning in the data they target. Regulated data (55%), sensitive infrastructure configuration data (53%), and intellectual property (49%) were the top categories of data held for ransom.[8]

This emphasis on attacking high-value data assets is reflected in the success of ransomware attacks. More than half of surveyed organizations (56%) admit to paying the attacker's ransom. Additionally, extortion rarely stops after a single attack. 87% of organizations experienced further extortion attempts after the first successful attack, although only 61% paid more to the attackers. Many organizations have found that paying the ransom does not guarantee the recovery of their data. Only 14% were able to fully recover all data affected by an attack.[9]

Ransomware attackers commonly target data hosted in storage systems (40%) and the cloud (39%), but an organization's IT infrastructure, including the data protection infrastructure (36%), is increasingly a focus.[10] When primary data is corrupted or lost during an attack, backup copies are traditionally used for recovery. The ability to frustrate a cyber-criminal's goals by mitigating or negating a ransomware attack (see Figure 1) has made the data protection infrastructure a target. Nearly nine in ten organizations (87%) are concerned that a ransomware attack could corrupt their backup copies.[11]

Figure 1. The Impact of Successful Ransomware Attacks



Source: ESG, a division of TechTarget, Inc.

Cyber Resiliency: The Future of Ransomware Preparedness

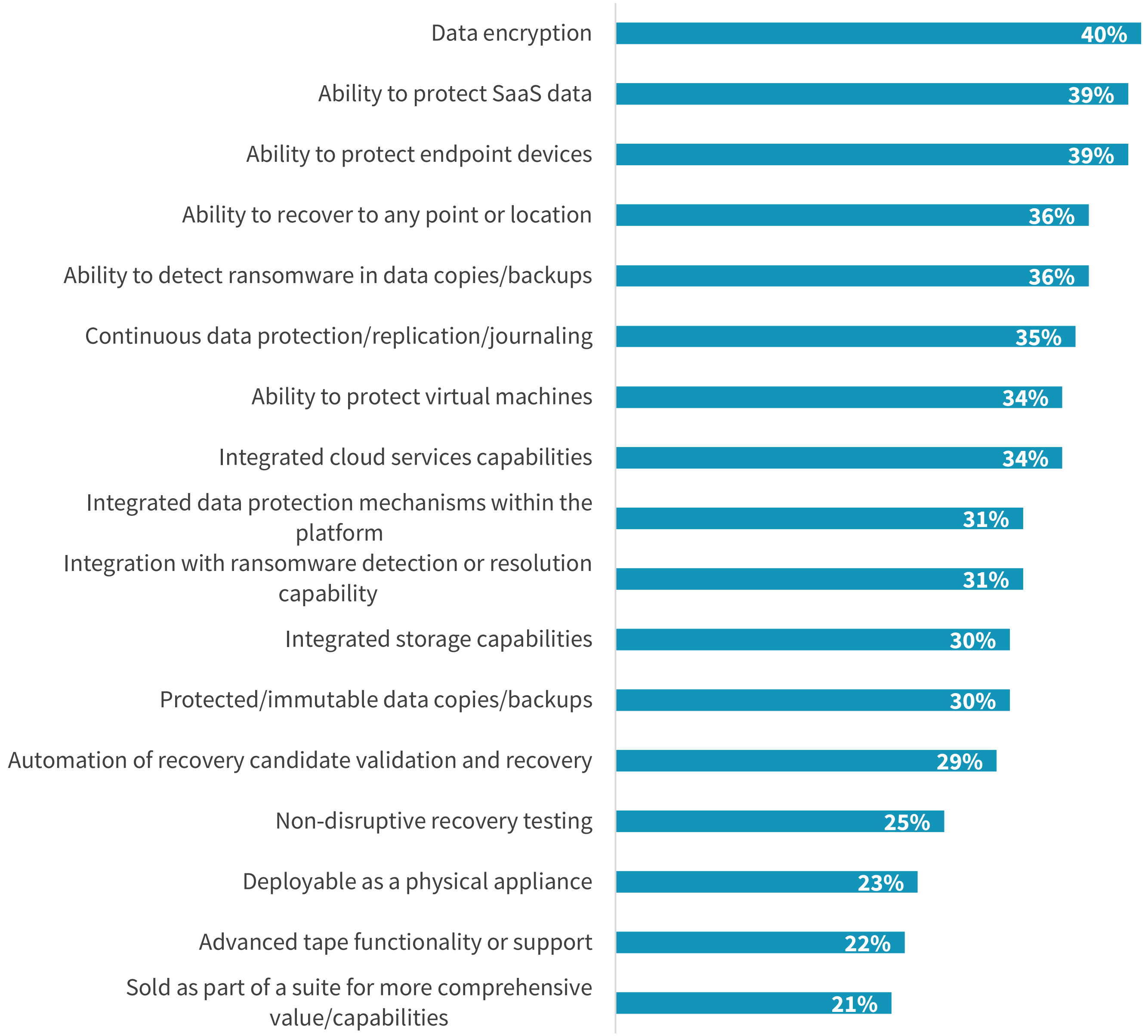
The difficulty in eliminating all exposure to vulnerabilities has broadened the scope of cyber defenses for every organization. Where cybersecurity traditionally focuses on securing an organization's attack surface—the network and endpoints of an organization that are reachable by external attackers—cyber resilience extends this definition and assumes breaches will happen.

[8] Ibid.
[9] Ibid.
[10] Ibid.
[11] Ibid.

Like conventional business continuity planning, cyber resilience incorporates methods, best practices, and technologies that help an organization prepare for and mitigate the impact of a cyber-attack, including ransomware. Cyber resilience aims to ensure an organization can continue business operations during/after a breach. A defense-in-depth strategy incorporates cybersecurity and cyber resilience in a multi-layered approach to defending the organization (see Figure 2).

Figure 2. Important Considerations for a Ransomware Recovery Solution[12]

If your organization were to be the victim of a successful ransomware attack, what is its planned method of recovery for the impacted applications and data? (Percent of respondents, N=620, multiple responses accepted)



Source: ESG, a division of TechTarget, Inc.

[12] Ibid.

82% of organizations anticipate spending more on ransomware preparedness over the next 12 months. No single source dominates this spending, with organizations pulling from IT operations, cybersecurity/infosec, general IT, data protection, and executive level budgets to cover preparedness. Organizations reported that they regularly engage in various ransomware preparedness activities and processes, including data recovery testing, security awareness training, response readiness assessment, functional incident response exercises, and pen testing. The vast majority of organizations (96%) indicate that their ransomware preparedness is somewhat stronger or much stronger than it was two years ago.[13]

An Integrated Approach to Cyber Resiliency

Managing cybersecurity solutions from multiple vendors presents challenges, especially for smaller organizations with limited IT resources. Survey respondents cited the need for separate training for each vendor solution (45%), difficulty obtaining a complete picture of overall security status (36%), and not enough staff to manage security technologies appropriately (30%) as major obstacles associated with managing an assortment of security products from different vendors. Additionally, product integration is a significant consideration (37%), second only to cost (46%), when organizations purchase cybersecurity technologies.[14]

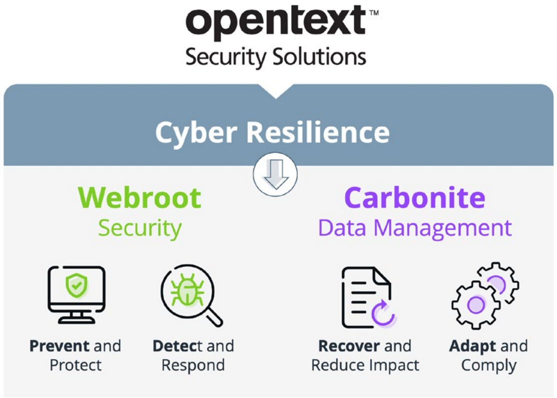
Product integration is significant, and when asked about the importance of integrating cybersecurity products, over 4 in 5 respondents (86%) indicated it was either important or critical.

When selecting cybersecurity solutions, a vendor's cybersecurity expertise and reputation (34%) were by far the most significant factor.

End-to-end Cyber Resiliency

Carbonite has a time-tested reputation for excellence in data protection and business continuity. In December 2019, OpenText acquired Webroot and its parent company, Carbonite, to add best-in-class cyber-resilience solutions to OpenText's existing security offerings. Then, with the Zix acquisition in December 2021, OpenText added leading SaaS-based email encryption, threat protection, and cloud compliance solutions to the existing Carbonite and Webroot portfolios. Together, OpenText, Carbonite, and Webroot provide a one-stop shop for cyber resilience, with a comprehensive, integrated approach that gives SMBs and managed service providers (MSPs) the cybersecurity, data protection, and recovery solutions they need to fight cybercrime and protect user data from loss (see Figure 3).

Figure 3. OpenText End-to-end Cyber Resilience



Source: OpenText

[13] Ibid.
[14] Source: ESG Complete Survey Results, *ESG/ISSA Cybersecurity Process and Technology Survey*, June 2022.

Within Carbonite data management, organizations have a wide choice of products including data protection and recovery, high availability, migration, and compliance.

Carbonite Server Backup

For backup and recovery, Carbonite Server Backup offers a robust, all-in-one backup and recovery solution that keeps physical, virtual, and legacy systems secure; minimizes downtime; and protects business operations. Backups can be stored onsite or in the cloud, ensuring higher levels of resilience against ransomware attacks. Carbonite Server Backup provides flexible recovery options and easy management to safeguard data and help businesses recover from data loss. The solution offers:

- Hourly Backups —Carbonite Server Backup administrators can configure hourly backup and retention settings. Carbonite Server Backup's immutable backup capability greatly decreases the risk of ransomware corrupting data. New monitoring, alerting, and reporting functions keep administrators fully informed of the progress and status of hourly backups, enabling them to manage any scheduling issues that may occur using a shorter backup window.

- Scan and Flag for Potential Ransomware—Carbonite Server Backup includes early warning alerts for ransomware based on anomalous activity with the option to review flagged backups, enabling improved detection and review of possible ransomware.

Carbonite Cloud-to-Cloud Backup

Carbonite Cloud-to-Cloud Backup offers comprehensive backup and recovery for SaaS applications including Microsoft 365, Google Workspace, Salesforce, Box, and Dropbox. The solution provides central management, granular restore, rapid recovery, and flexible retention options. As a purpose-built backup solution, it ensures IT administrators can recover as much or as little SaaS application data as necessary.

Carbonite Endpoint Backup

Carbonite Endpoint Backup is a comprehensive, automatic backup solution for all data on endpoint devices. It simplifies data protection administration and deployment across the organization, regardless of the environment's size, distribution, or sophistication. This enables organizations to better protect valuable data on employee devices, mitigate data loss and data breaches, back up data as frequently as every minute, and restore lost data quickly. If devices are lost or stolen, location services and remote wipe capabilities help organizations keep their data secure. Carbonite Endpoint Backup enhances cyber resilience through best-in-class protection to reduce risks from ransomware, user errors, and lost or stolen devices.

Cyber Resilience for MSPs and Resellers

Carbonite has a healthy ecosystem of resale and MSP partners who add additional layers of customer service and support to end-users. With the robust Carbonite data protection solutions, they are able to deliver end-to-end cyber resiliency to their SMB clients as a service. Benefits of end-to-end cyber resilience to partners:

- Complete: Proven and feature-rich platform to deliver on end-users' stringent modern data protection and cyber-resilience SLAs.
- Operational Efficiency: Easy to deploy, scale, and manage across one or many locations.
- Benefits: Rich with upfront deal registrations, renewal incentives, pre-sales engineering support, training, professional marketing and sales enablement materials, rebates and incentives, and flexible subscription plans.

The Bigger Truth

Defense in depth is fast becoming dogma in the enterprise. Ransomware attacks are no longer a question of if but when. Organizations of all sizes must be prepared for this eventuality with a multi-layered approach emphasizing vulnerability management and resilience.

The most common impacts of security incidents are lost productivity, the strain of remediating an attack, and the disruption of business processes. Ransomware can no longer be seen as just an IT problem. It is a real business risk that requires the focused attention of business leaders and corresponding IT investment.

Regardless of size, organizations face significant challenges heading off cyber-attacks, including understaffed cybersecurity teams (38%), the complexity of multiple siloed cybersecurity tools (22%), and a lack of cybersecurity skills (19%).[15] An integrated, single-vendor, cyber-resilient approach to security can alleviate these challenges by reducing the burden on IT and ensuring organizations are prepared for a ransomware attack.

As smaller and mid-sized organizations face these unprecedented cybersecurity challenges, investing in the right technology has never been more critical. The OpenText Security Solutions portfolio offers operational efficiency, ease of deployment, and scale. The platform is designed from the ground up for service delivery. It provides operational advantages for service providers who may leverage it to deliver cyber-resiliency services and organizations that run the solutions internally.

Whether deployed and managed internally or through a service provider, the OpenText Security Solutions portfolio delivers a broad set of solutions that form a strong foundation for effective and integrated cyber resilience.

All product names, logos, brands, and trademarks are the property of their respective owners. Information contained in this publication has been obtained by sources TechTarget, Inc. considers to be reliable but is not warranted by TechTarget, Inc. This publication may contain opinions of TechTarget, Inc., which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget, Inc.'s assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget, Inc. makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

a division of TechTarget

Enterprise Strategy Group is an integrated technology analysis, research, and strategy firm that provides market intelligence, actionable insight, and go-to-market content services to the global IT community.

www.esg-global.com ✉ contact@esg-global.com ☎ 508.482.0188

[15] Ibid.