Enterprise Strategy Group | Getting to the bigger truth.™

BUSINESS JUSTIFICATION BRIEF

How to Protect Against the Impacts of a Ransomware Attack with DXC Technology and Dell Technologies:

Creating a Secure Vault to Help Protect Your Business-critical Information from Cyber Criminals

Author: Vinny Choinski, Senior Analyst

AUGUST 2021

The Challenges of Ransomware Incidents and Impacts of Downtime

Ransomware represents a serious threat to organizations of every size. According to ESG research, a combined 70% of respondent organizations reported experiencing ransomware attacks over the previous year. Most indicated they'd dealt with ransomware attacks on either a daily, weekly, monthly, or sporadic basis. 42% of respondents reported that they were being attacked on a weekly basis or more frequently. Alarmingly, 18% faced ransomware threats *daily*.[1] ESG research also found that 82% of respondent organization believe that cyber-risk in general has increased over the past two years.[2]

Ransomware Challenges and Business Downtime Impacts

70%
reported that they experienced a ransomware attack over the last twelve months

42%
reported that they were being attacked on a weekly basis or more frequently

46%
identified loss of employee confidence as an impact to their business that could result from application downtime or data loss

45%
identified diversion of IT resources from long-term or business-critical projects as an impact to their business that could result from application downtime or data loss

The consequences of ransomware-related downtime can be very negative to a business and its customers. IT downtime affects organizations in several ways—but it almost always negatively impacts operational efficiency, employee morale, and consumer confidence. In fact, staff is so important to today's organizations, that loss of employee confidence (34% of respondents) was a more commonly cited response as an impact to business than loss of revenue was (32% of respondents).[3] Remember, costs still accrue when those staff members are idle.

Cyber-resilient Solutions Delivered as-a-Service from DXC and Dell

In an age where businesses have been forced to become micro focused on data protection solutions that can deliver cyber-resiliency, organizations are looking for agile, modern solutions that can keep pace with evolving cyber-threats. Organizations are looking to become more cloud-like in their consumption of infrastructure and services whether their data lives on-premises or in the cloud. And when it comes to this type of data center modernization, ESG research indicates that improving backup and recovery is the most commonly cited area in which organizations expect to make the most significant investments over the next 12-18 months. Additionally, improving security and employee productivity are the most common considerations that research respondents believe will be most important in justifying IT investments to their organization's business management team over the next 12 months.[4] DXC and Dell Technologies help customers drive growth by dramatically improving their ability to anticipate and respond to change. They work collaboratively with your team to develop powerful business continuity strategies, apply industry-recognized innovations, and manage foundational technologies as-a-Service such as a secure air-gapped vault of critical data that is isolated from ransomware yet accessible to the business.

[1] Source: ESG Research Report, *Tape's Place in an Increasingly Cloud-based IT Landscape,* January 2021.
[2] Source: *Cyber in the C-Suite and Boardroom*. Multi-client 2020
[3] Source: ESG Research Report, *Real-world SLAs and Availability Requirements,* October 2020.
[4] Source: ESG Master Survey Results, *2021 Technology Spending Intentions Survey,* December 2020.

Why DXC and Dell?

We provide end-to-end security solutions with 3000+ security professionals, including both advisory services and managed services.

Together, we have a rare combination of deep IT and security expertise to prevent incidents and guide response in the event a recovery is needed.

DXC's vault capability provides a lower risk of impact from ransomware and the ability to recover business operations more quickly.

DXC delivers a pay-as-you-go model that includes hardware, management, and additional expertise as-a-Service.

DXC's Vault leverages Dell Technologies' industry-leading, field-tested, data-proven, end-to-end infrastructure and data protection solutions. But most importantly, when it comes to cyber-resilience, DXC and Dell offer a joint solution with the ability to:

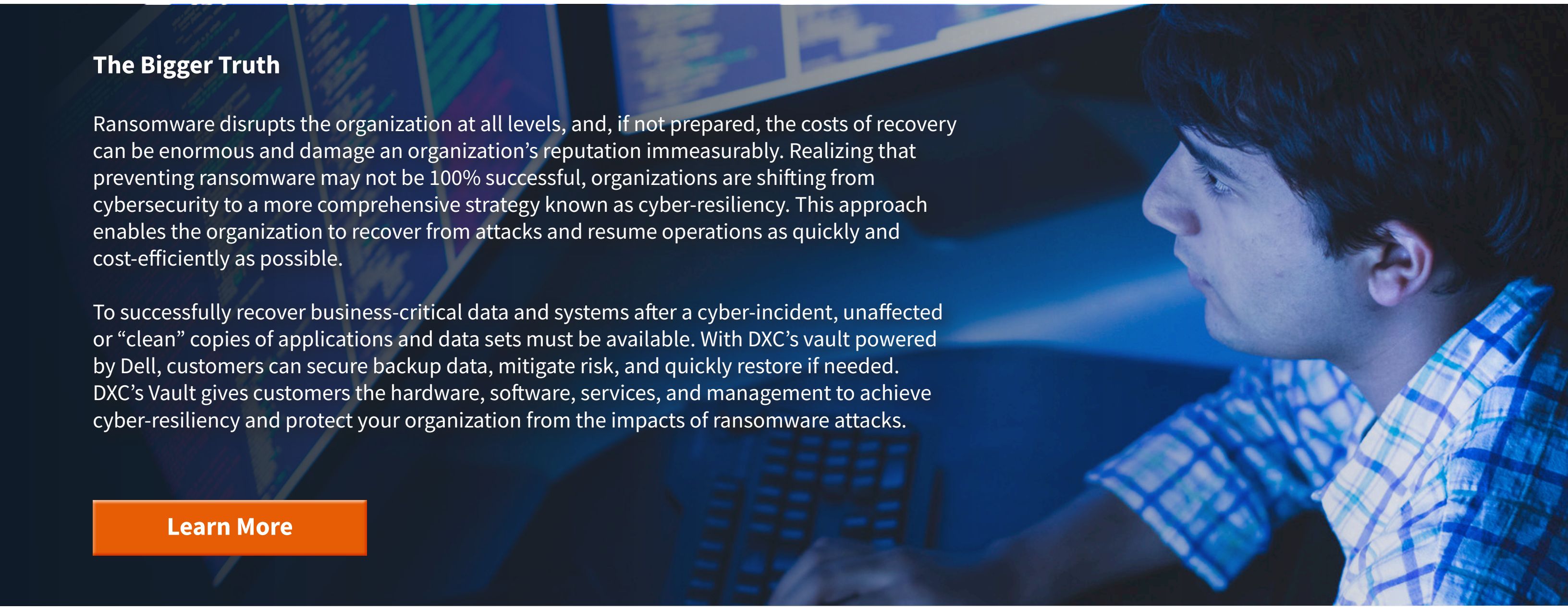
- Create an automated, orchestrated, logical air gap separate from the production environment to protect data.
- Create an immutable copy with compliance retention lock capability that meets with the 17a-4(f)(ii) standard. This locking capability cannot be turned off without a separate security officer password because an offsite copy alone does not provide a complete air gap.
- Deploy a physically- and logically-isolated location (called DXC's vault) that cannot be opened or controlled from the production side. This location is where cyber-recovery operations are conducted.
- Analyze and quickly identify corrupt data, the source of an attack, and a clean recovery point.

ESG Business Justification

Ransomware and other malware attacks are on the rise. The cyber criminals are getting more sophisticated. They are not only targeting production systems and data but also the data protection environments businesses depend on to protect against just such situations.

Data protection is a long-standing IT discipline that encompasses skilled people, sound processes, and solid infrastructure solutions, especially when it comes to creating and managing a cyber-resilient ecosystem. A business needs to know that it has a clean recovery point, infrastructure that can meet recovery SLAs, and skilled people to assure a successful recovery in in the event of a ransomware-type incident.

Together, DXC and Dell have crafted an as-a-Service solution that helps customers meet these cyber-resiliency challenges.



The Bigger Truth

Ransomware disrupts the organization at all levels, and, if not prepared, the costs of recovery can be enormous and damage an organization's reputation immeasurably. Realizing that preventing ransomware may not be 100% successful, organizations are shifting from cybersecurity to a more comprehensive strategy known as cyber-resiliency. This approach enables the organization to recover from attacks and resume operations as quickly and cost-efficiently as possible.

To successfully recover business-critical data and systems after a cyber-incident, unaffected or "clean" copies of applications and data sets must be available. With DXC's vault powered by Dell, customers can secure backup data, mitigate risk, and quickly restore if needed. DXC's Vault gives customers the hardware, software, services, and management to achieve cyber-resiliency and protect your organization from the impacts of ransomware attacks.

Learn More

ESG 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.

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 currentlyavailable 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.