FROST & SULLIVAN

Can Your Business Recover From Today's Cyber Incidents?

Improving Your Enterprise Cyber Resilience With Modern Data Protection

In partnership with

kyndryl / VERITAS

FROST & SULLIVAN EXECUTIVE BRIEF

frost.com

Introduction

Today's businesses face cyber threats that are increasing in frequency and sophistication, and most will experience numerous per year. According to Frost & Sullivan's 2023 Cyber Security Voice of the Customer Survey, some of the most common breaches involve personal identifiable information (PII). PII breaches can result in significant consequences for your business, including a loss of revenue and customers or a diminished corporate reputation.

With consequences this high, you need an approach that utilizes a modern data protection strategy capable of securing and protecting your critical data regardless of where it resides.

Traditional data backup services are insufficient when recovering from a cyber incident because the backups could have also been corrupted. This is primarily because such services do not store data on immutable storage, scan backup data for anomalies, or leverage network air gaps. These services also may not provide orchestrated recovery capabilities. To ensure that your business is protected and able to meet all applicable regulations—including new cyber resilience regulations like the Digital Operations Resilience Act (DORA) and the European Cyber Resilience Act (CRA)—your business must continually re-assess and test recovery procedures. This ensures that all critical data is protected and critical business operations are quickly recoverable in the event of an incident. Businesses need such functionality to recover rapidly and with the least possible impact.

In this executive brief, we will examine the business impacts of cyber incidents and explain why yesterday's data protection methods are no longer adequate. We will also discuss the need for continually testing and assessing data protection methods to ensure recoverability and why businesses need a more comprehensive approach to cyber resilience.

Most Businesses Overestimate Their Cyber Preparedness; Managed Service Providers Close the Gap

Though most businesses recognize that security is a critical IT area, many still treat it as a set-it-and-forget-it proposition. If the enterprise IT department implements a security service or application to protect data, the assumption is that it will work for all data, all the time. Some believe they are adequately equipped to recover from or mitigate potential threats.

The reality is that changes to business operations and the type of threats require frequent recovery plan tests and assessments. Regulatory changes also drive the need for reassessments and updates to meet compliance expectations. The stakes of nonconformity are high and may include anything from steep fines and sanctions to damaged business reputations. With respect to the California Consumer Privacy Act (CCPA), the penalties range from $2,500 per violation or $7,500 per intentional violation to €20 million or up to 4% of global gross annual revenue (whichever is higher). If you breach data handling rules in Japan, the Act on the Protection of Personal Information (APPI), the company and the individuals compromising the data are at risk. An organization's maximum fine is ¥100 million (roughly USD $815,000), while individuals can face imprisonment of up to a year or fines of up to ¥1 million (around USD $8,150).

Stats:

Despite feeling prepared to prevent an attack, **33%** perceive that they could be negatively impacted by an attack in the next 12 months.

41% of businesses struggle with the security and compliance of data and applications.

40% struggle to implement resiliency plans for data and apps.[1]

For firms with revenues **greater than USD $2 billion**, the average ransomware attack costs **USD $10.1 million** for the cost of a ransomware incident among large firms (revenue **greater than $2 billion**).[2]

[1] Frost & Sullivan 2023 Global Cloud End User Survey, Conducted Aug-Sep 2023

[2] Net Diligence's 2023 analysis of 9,000+ cyber insurance claims data: https://netdiligence.com/wp-content/uploads/2023/10/2023-NetDiligence-Cyber-Claims-Study_v1.1.pdf, accessed April 2, 2024

Threat Actors Will Target Business Data

Threat actors target your data daily, and these attacks can come from internal or external sources. Most businesses overestimate their ability to prevent an attack and recover from an incident.

Stats:[3]

In 2023, 91% of businesses self-rated their ability to prevent or mitigate cyberattacks as good, very good, or excellent.

The average business was negatively impacted by a successful security attack 26 times in the last 12 months.[4]

Most common negative impacts of attacks include:

- Disruption of system/workload availability—experienced by 39%
- Lost productivity—experienced by 30%
- Personally identifiable information breach—experienced by 28%

What You Need

You need a cyber resilience program to help you anticipate, protect, withstand, and recover quickly from attacks. This requires two components:

1. A reliable underlying technology that can protect your entire environment, including on-premises infrastructures, cloud-based resources, and services/data at the edge.

2. A managed services provider with expertise managing complex mission-critical business data and processes. Look for a partner that can protect data, detect cybercrime, and mitigate attacks that successfully breach your defenses. This is your company's best bet to protect its business comprehensively.

[3] Frost & Sullivan 2023 Cyber Security Voice of the Customer Survey, Conducted Feb-March 2023

[4] Frost & Sullivan 2023 Cyber Security Voice of the Customer Survey, Conducted Feb-March 2023

What You Need in a Managed Services Provider

When searching for a cyber resilience partner, look for a provider that:

- Assesses your current data security posture and compliance adherence
- Doesn't push a one-size-fits-all all solution
- Takes time to understand your business goals, risk tolerance, and compliance requirements
- Brings the latest technology into the optimal solution
- Provides ongoing testing/assessments to ensure your plan works at the time of deployment and into the future
- Possesses capabilities to support a wide range of complex, mission-critical infrastructures and regulated environments

The Last Word

With cyber threats increasing in frequency and changing in nature, businesses must constantly evaluate whether their resilience strategy goes far enough to protect business-critical assets. Just as threat actors leverage the latest technologies to target and breach critical data, businesses must stay one step ahead by leveraging the latest technologies coupled with strategic expertise.

With the complexity of today's IT landscape, it's rare to make unbiased assessments about data protection and implement a holistic data protection strategy alone. Engaging with trusted partners enables your business to protect, secure, and implement compliance for your most valuable asset—data—regardless of the changing regulatory and threat landscape.

Kyndryl, the world's largest IT infrastructure services provider, and Veritas Technologies, the leader in secure multi-cloud data management, have partnered to extend Kyndryl's framework of cyber resiliency services with joint offerings including: Kyndryl Data Protection Risk Assessment with Veritas and Kyndryl Incident Recovery with Veritas.

ABOUT VERITAS

Veritas Technologies is the leader in secure multi-cloud data management. Over 80,000 customers—including 91% of the Fortune 100—rely on Veritas to help ensure the protection, recoverability, and compliance of their data. Veritas has a reputation for reliability at scale, which delivers the resilience its customers need against the disruptions threatened by cyberattacks, like ransomware. No other vendor can match Veritas' ability to execute, with support for 800+ data sources, 100+ operating systems and 1,400+ storage targets through a single, unified approach. Powered by Cloud Scale Technology, Veritas is delivering today on its strategy for Autonomous Data Management that reduces operational overhead while delivering greater value. Learn more at Veritas.com. or http://www.veritas.com/partners/kyndryl. Follow us on X at @VeritasTechLLC.

ABOUT KYNDRYL

Kyndryl (NYSE: KD) is the world's largest IT infrastructure services provider, serving thousands of enterprise customers in more than 60 countries. The company designs, builds, manages and modernizes the complex, mission-critical information systems that the world depends on every day. We are deeply committed to advancing the critical infrastructure that powers human progress. We're building on our foundation of excellence by creating systems in new ways: bringing in the right partners and working side by side with our customers to make the right technology investments to achieve business outcomes and unlock potential. Our alliances with market leading technology partners empower us to innovate and co-create an integrated cyber resilience approach to help our customers anticipate, protect against, withstand and recover from adverse cyber events. For more information, visit https://www.kyndryl.com/alliances/veritas. Follow us on LinkedIn

YOUR TRANSFORMATIONAL GROWTH JOURNEY STARTS HERE

Frost & Sullivan's Growth Pipeline Engine, transformational strategies and best-practice models drive the generation, evaluation, and implementation of powerful growth opportunities.

Is your company prepared to survive and thrive through the coming transformation?

Join the journey. ➔