# Cyberattacks and Ransomware Accentuate the Need for Rapid Recovery

by DCIG Principal Storage Analyst & Partner, Ken Clipperton

**COMPANY**

Arcitecta

**LOUISVILLE OFFICE**

357 South McCaslin Blvd.
Suite 200
Louisville CO 80027
USA
+1 720 583 4006
talk@arcitecta.com

**MELBOURNE OFFICE**

15 Little Bakers Lane
Northcote, Victoria 3070
Australia
+61 3 9029 3437
talk@arcitecta.com

**arcitecta.com**

**INDUSTRY**

Data Management Software

**SOLUTION**

- Mediaflux
- Point in Time Ransomware Rapid Recovery Solution

What would it cost your business if it lost access to critical business data and applications for a few days? What if that disruption lasted a few weeks, or months?

What would that disruption do to your customers?

This nightmare has become all too real for thousands of businesses that have fallen victim to ransomware. According to many reports[1], material business disruption averages about 21 days, with full recovery from a ransomware incident taking more than six months.

## Many Sources of Downtime

There was a time when most businesses ran on small data, printouts, and many manual business processes. Today, most business processes depend on IT. Therefore, an extended disruption will have a major impact on the business.

Common sources of data loss and downtime include:

- accidental deletion or overwriting of files
- computer viruses and malware
- equipment theft
- fires
- floods
- hardware/system failures
- malicious acts
- other human errors
- power surges and outages
- ransomware
- software errors
- spills

Prudent business leaders take action to reduce the likelihood of experiencing any of the common causes of data loss and downtime. Nevertheless, failures will occur. The key to achieving business resiliency is the ability to rapidly recover from any incident.

> ***"The key to achieving business resiliency is the ability to rapidly recover from any incident."***

## Cyberattacks and Ransomware are Now the Primary Causes of Downtime

While there are many sources of downtime, cyberattacks have become a major source of risk to businesses of all sizes and across all industries.

Cybercriminals have figured it out: Your data is valuable. Disrupting business operations by denying access to data or threatening to release sensitive data to others can unlock large ransom payments from the victims of these attacks.

Cyberattacks can also result in payments to customers whose data is stolen by criminals. For example, thieves stole more than 447,000 patients' names, Social Security numbers, and sensitive medical information from a Florida healthcare organization. In response to a class-action lawsuit, it agreed to pay up to $7,500 per SSN that was stolen.

Cyber insurance is one tool organizations can use to protect themselves from financial losses. Ironically, some cybercriminals now seek information about their victims' cyber insurance coverage so they can tune their ransom demands to that coverage.

## Startling Statistics from Recent Ransomware and Cyberthreats Reports

Many enterprise technology providers and security experts have compiled data about the impacts they are seeing from recent ransomware attacks and other cyberthreats.

Commissioned by and licensed to Arcitecta with unlimited, unrestricted, perpetual, global distribution rights.

## Q: *Why do cybercriminals target business data with ransomware attacks?*

## A: *Because that's where the money is.*

### According to Acronis' 2022 Year End Cyberthreats Report

> *"Ransomware continues to be the number-one cyberthreat for businesses, including government, healthcare and other critical organizations."* [2]

> *"No one is safe—email-borne attacks are targeting virtually all industries."* [3]

> *"More than 100 million accounts were breached in the third quarter of 2022, as found in a recent Surfshark survey."* [4]

And these attacks are increasingly costly to their victims.

> *"The global average total cost of a data breach is now $4.35 million, having increased by another $110,000 this year. In the United States, the average total cost is nearly $9.5 million."* [5]

> *"No matter the size or industry, data breaches can absolutely devastate an organization. In addition to the immediate impact on business operations, companies must contend with severe reputational damage and potential regulatory fines."* [6]

### From Cisco's Security Outcomes Report, Volume 3: Achieving Security Resilience

Nearly two-thirds of respondents reported suffering major security incidents that jeopardized business operations. The leading types of incidents were network or data breaches (51.5 percent), network or system outages (51.1 percent), ransomware events (46.7 percent) and distributed denial of service attacks (46.4 percent)." [7]

These incidents cause wide-ranging costs to affected businesses. These include downed systems, response and recovery costs, brand damage, and legal costs or penalties. (Figure 1.)

### From IBM's Cost of a Data Breach 2022 Report

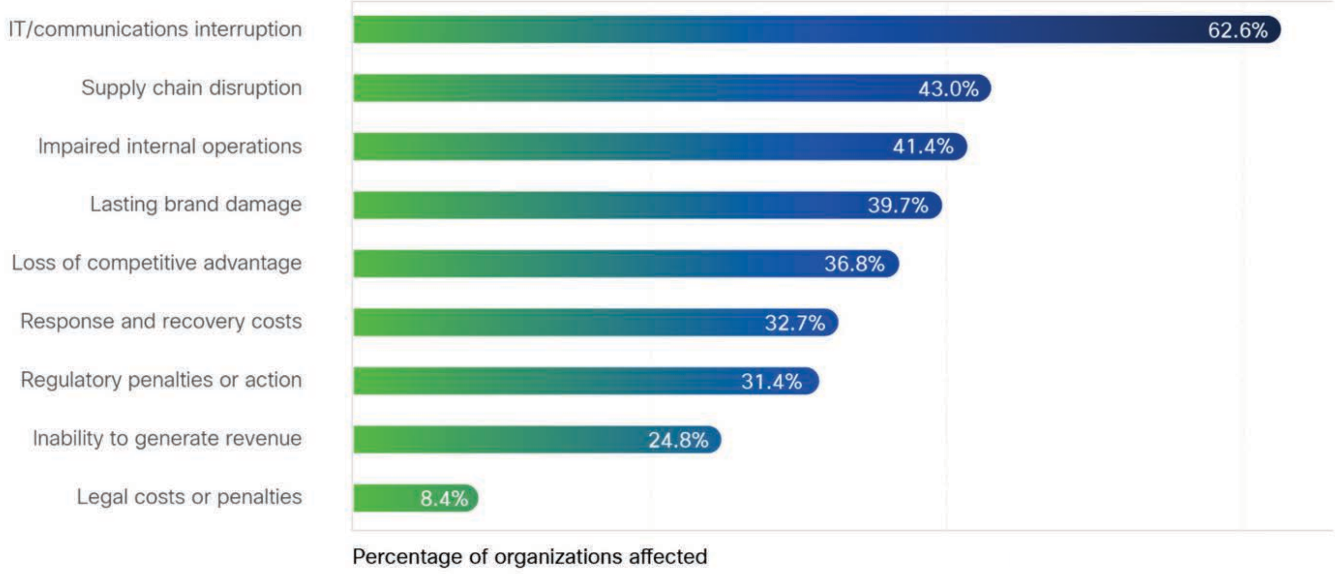
> *"For 83% of companies, it's not if a data breach will happen, but when. Usually more than once. When detecting, responding to, and recovering from threats, faster is better. Organizations using AI and automation had a 74-day shorter breach lifecycle and saved an average of USD 3 million more than those without."* [8]

*Source:* Canva

### From Entara

> *"Entara was deployed to recover a 450-server environment that had about 50% of its LUNs backed up with snapshots. The customer was able to operate its most critical, revenue-driving business applications in a few days because they had partial snaps. We spent the next few weeks restoring the remaining high-priority systems used for functions like monthly batch reporting. The whole project took no more than one month, while the customer with traditional storage and no snapshot capabilities took 3-4 months."* [9]

**Figure 1: Types of resilience impacts caused by security incidents**

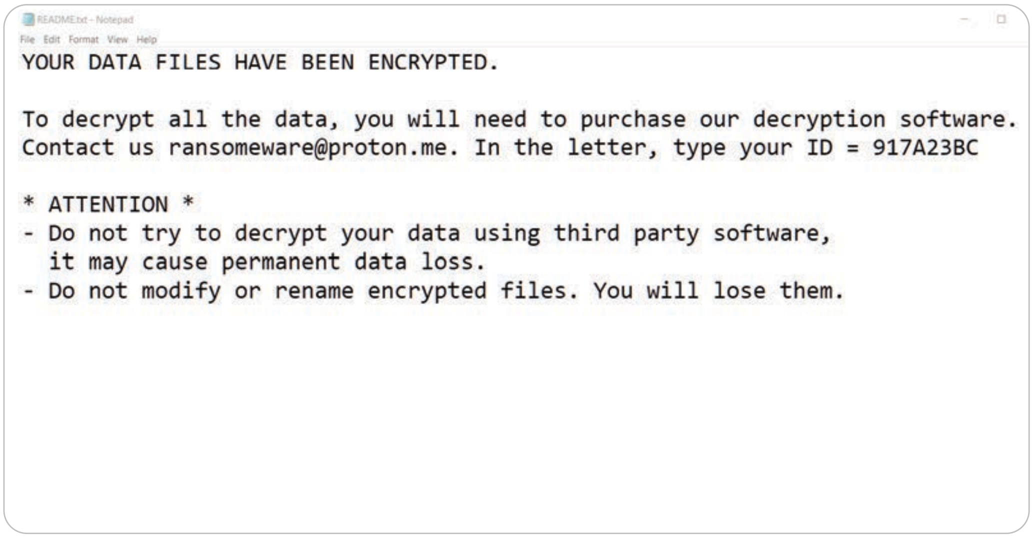


*Source:* Cisco Security Outcomes Report

## Every Business Needs a Rapid Recovery Strategy

The question is not if your business will experience a ransomware attack, but when. Therefore, every business must develop and implement a strategy for timely recovery from a successful cyberattack attack BEFORE DISASTER STRIKES.

## *Don't let a message like this ruin your day, week, month, or quarter:*



```
YOUR DATA FILES HAVE BEEN ENCRYPTED.

To decrypt all the data, you will need to purchase our decryption software.
Contact us ransomeware@proton.me. In the letter, type your ID = 917A23BC

* ATTENTION *
- Do not try to decrypt your data using third party software,
  it may cause permanent data loss.
- Do not modify or rename encrypted files. You will lose them.
```

Unfortunately, for organizations relying on traditional backup and recovery approaches, recovering from a ransomware attack in a few days would be considered a success. Recoveries often extend to weeks or months. Disruptions of these durations can easily result in business failure.

To be truly useful, a cyber resiliency strategy must recover the business to an operational state within the timeframes necessary to meet business continuity objectives. Ultimately, the recovery strategy must enable business resiliency.

## Create New Wins Through Proactive Data Management

Because this issue has executive-suite and board-level awareness, IT leaders should approach the creation or updating of their recovery strategy with a broader awareness of the needs of the business. IT leaders should look for opportunities to create new wins rather than addressing this risk by merely bolting on another layer of technology and expense.

Implementing an effective recovery strategy will probably entail significant costs. However, the right solution properly implemented provides opportunities to create new value from data, leverage AI/ML to cut or avoid costs, and address emerging edge data requirements.

A solution that enables proactive data management can benefit the business by enabling:

- greater data visibility
- optimal data placement
- improved data availability
- provable compliance
- consistent data governance
- data workflow automation
- policy-driven data management
- the extension of enterprise data management to the edge

A data management solution that enables end-user access and self-service tools will enable greater scalability and agility for the organization by freeing end-users from relying on IT interventions to complete their priority projects.

## Arcitecta Enables Business Resilience at Scale

Arcitecta is an excellent example of a company that addresses both cyber resiliency and data management at scale, enhancing overall business resilience.

Arcitecta is a data management company, not a storage company. Its Mediaflux product virtualizes multiple underlying storage systems to create an integrated data environment that enables continuous inline data protection at scale. Its Point in Time solution solves the rapid recovery problem by enabling IT and end users to rewind any file or file system to a specific point in time without performing a restore operation. Intelligent search facilities help to reduce the RTO to near zero, even at scale.

### Arcitecta's Point in Time Ransomware Rapid Recovery Solution

Arcitecta's Point in Time Ransomware Rapid Recovery Solution for media and entertainment studios enables studios to quickly restore their media assets after a ransomware attack, minimizing downtime and avoiding the risk of data loss. Point in Time works across existing production storage systems, such as Dell PowerScale, making it easy to implement and cost-effective since no additional storage systems are required.

### Wins That Go Beyond Ransomware Recovery

Arcitecta goes beyond ransomware recovery, addressing the challenges of data resiliency and effective data management at scale. Arcitecta bases its Mediaflux product on an XML-encoded object database (XODB) developed by Arcitecta to meet the data management requirements of research computing organizations. XODB is hyperscale database technology that integrates and operates on rich, arbitrary metadata.

Arcitecta and Mediaflux are proven in demanding at-scale data environments. Jason Lohrey founded Arcitecta in 1998. Arcitecta serves more than 300,000 active users at organizations in the life sciences, research, clinical, geospatial, media and entertainment, and defense industries. Mediaflux users generate multiple petabytes of new data each month and move many petabytes for analysis each month… with no data loss or outages exceeding 3 minutes.

## Guidance for Business and IT Leaders

Every business must develop and implement a strategy for timely recovery from a successful cyberattack attack before disaster strikes. Enterprising professionals will leverage this necessity to implement proactive data management that creates new opportunities for their organizations while mitigating the risks posed by ransomware. ■

### About Arcitecta

*Arcitecta is a creative and innovative data management software company. Founded in 1998, Arcitecta builds the world's best data management platforms, enabling thousands of users worldwide in some of the most demanding data-driven environments. Arcitecta's flagship Mediaflux platform began with the vision to provide organizations with extraordinary technology for handling all forms of data, from small to very large and complex. Today, it forms the foundation for managing the simplest and the most complex data for all sizes of organizations and global enterprises, empowering them to simplify data-intensive workflows and accelerate time to insight from their data to improve business and research outcomes.*

### Notes

1. https://www.ktvu.com/news/oakland-ransomware-attack-nears-2-months
2. https://dl.acronis.com/u/rc/White-Paper-Acronis-Cyber-Protect-Cloud-Cyberthreats-Report-Year-End-2022-EN-US-221212.pdf
3. https://www.acronis.com/en-us/blog/posts/acronis-cyberthreats-report-year-end-2022-data-under-attack/
4. https://www.acronis.com/en-us/blog/posts/acronis-cyberthreats-report-year-end-2022-data-under-attack/
5. https://www.acronis.com/en-us/blog/posts/acronis-cyberthreats-report-year-end-2022-data-under-attack/
6. https://www.acronis.com/en-us/blog/posts/acronis-cyberthreats-report-year-end-2022-data-under-attack/
7. https://www.cisco.com/c/en/us/products/security/security-outcomes-report.html
8. https://www.ibm.com/reports/data-breach
9. https://money.yahoo.com/preparing-inevitable-understanding-ransomware-mitigate-120000466.html

### About DCIG

The Data Center Intelligence Group (DCIG) empowers the IT industry with actionable analysis. DCIG analysts provide informed third-party analysis of various cloud, data protection, and data storage technologies. DCIG independently develops licensed content in the form of TOP 5 Reports and Solution Profiles. Please visit **www.dcig.com.**

DCIG

DCIG, LLC // 7511 MADISON STREET // OMAHA NE 68127 // 844.324.4552

Product information was compiled from both publicly available and vendor-provided resources. While DCIG has attempted to verify that product information is correct and complete, feature support can and does change and is subject to interpretation. All features represent the opinion of DCIG. No negative inferences should be drawn against any product or vendor not included in this report. DCIG cannot be held responsible for any errors that may appear. This report was commissioned by Arcitecta.