



# Data Defence

How To Protect Your Business From Ransomware

**Si2SYSTEMS**  
[www.sisystems.com.au](http://www.sisystems.com.au)

**EMC<sup>2</sup>**  
BUSINESS  
PARTNER

# overview

Ransomware is a rapidly growing threat. This malicious software takes control of your business systems and locks or encrypts your data, enabling attackers to demand a fee in return for handing over the keys.

Despite the increasing notoriety of ransomware, many businesses remain ill-equipped to deal with an attack. A recent Malwarebytes survey found more than a third of businesses will simply pay the ransom rather than dealing with the impact. While this might seem like the easiest option, it strengthens the position of cybercriminals with no guarantee that your data will be returned.

The rise of ransomware highlights a significant cybersecurity skills gap, with many businesses lacking the necessary experience to protect their organisation from attacks. According to a Mimecast survey, 40 per cent of IT decision makers feel unprepared to deal with malicious attacks, even though more than half have experienced a recent breach.

Ransomware is particularly insidious, as it often arrives disguised as an everyday email like an unpaid bill notification or parcel delivery. Any one of your employees could open a compromised email without a second thought, but the consequences can be significant and far-reaching.

A ransomware attack seriously impacts business productivity, threatening profitability and reputation. A recent high-profile incident affected the business operations of a large hospital for more than a week, forcing staff to divert patients to other hospitals and fall back on paper records and faxes, before finally paying a ransom fee of \$17,000 to attackers. Newer forms of ransomware also contain additional threats like leaking customer data to the public.

As ransomware becomes increasingly sophisticated and complex, you need a robust and multifaceted strategy to avoid downtime and data loss. Is your business sufficiently protected?

---

**// If you're not prepared for ransomware, you face the unenviable choice of paying up or working against the clock to minimise downtime and data loss. //**

---

# Statistics

## Data protection is essential for businesses of all shapes and sizes.

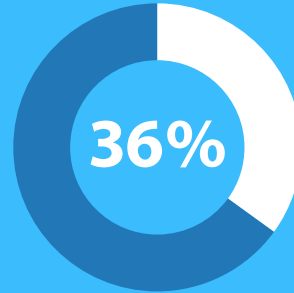


52% have suffered unplanned system downtime in the last twelve months



29% have suffered data loss in the last twelve months

## Security breaches can have significant and long-lasting consequences.



36% of organisations have suffered unplanned system downtime and/or data loss in the last year due to a security breach



The average cost to those organisations in the last 12 months is more than \$1.1 million AUD

## Many businesses are unprepared to protect themselves from an attack.



71% of organisations are not very confident they can meet SLAs to fully recover systems and data



Less than 20% of organisations are confident that their data protection solutions will meet future business challenges

## The cloud is changing the game when it comes to data protection.



84% of organisations believe central visibility for data protection across cloud environments is essential



47% believe that not all their data stored in the cloud is protected





# Dealing with Ransomware

Unlike more targeted cyberattacks like phishing or email hacking, ransomware is not about gaining access to company data. Instead, attackers are focused on freezing access and using scare tactics to extort money. This poses a serious threat if your business doesn't have an effective recovery plan in place, especially if it would quickly feel the impact of being out of operation.

That's why healthcare, government and finance are common targets but all businesses are at risk – and the growing rate of incidents highlights the need to take the issue seriously. If your organisation provides an online service, or stores a significant amount of critical or confidential data, you're a prime candidate for a ransomware attack.

**Here are three ransomware challenges your business needs to be aware of:**



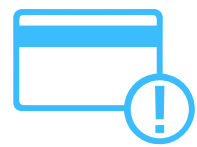
## DIFFICULT TO CONTROL

While other security threats will target your data directly, ransomware usually arrives in the form of a seemingly innocuous email. Anybody in your business can open it and, if that employee has access to a large number of files on a local server or cloud drive, that data can be locked or encrypted within minutes. With ransomware spreading to smartphones and other mobile devices, the associated risks are being amplified.



## WHOLE BUSINESS IMPACT

Ransomware can quickly spread across your systems, affecting shared folders inside and outside of your organisation. Once a user has opened an infected link or attachment, malware spreads almost immediately, accessing network drives and other endpoints like OneDrive or Dropbox. This has a significant impact on business productivity and can shut down business operations for days if the issue isn't dealt with swiftly.



## PAYMENT IS NO GUARANTEE

To recover data quickly, many businesses will simply pay the ransom fee – particularly if it's comparatively low compared to the cost of downtime. Yet paying up doesn't actually guarantee that your data will be decrypted. Worse still, it increases the incentive for cybercriminals to pursue other organisations while positioning your business as a prime target for further attacks.

# Is Your Business Vulnerable?

**Cybersecurity is becoming an increasingly important part of doing business – and waiting until a threat presents itself is a bad strategy. Here's a checklist of potential vulnerabilities that could leave your business open to ransomware:**

- Are your employees aware of ransomware and how it presents?
- Are your firewalls and malware protection up to date?
- Do you have remote access enabled when it's not needed?
- Are you using legacy software or business systems?
- Do you have a bring-your-own-device policy?
- Does your backup plan include real-time and offline or offsite backups?
- Are your operating system and application patches up to date?
- Do your employees have more file rights on network drives than necessary?
- Is there an effective backup and disaster recovery solution in place?



**You can't modernise your business without modernising data protection**

- Dell EMC Global Data Protection Index Research Study



# How to Ensure Your Business is Protected

While ransomware attacks are difficult to prevent, an effective backup strategy is the best way to protect your business. The ability to recover data quickly and easily without resorting to ransom payments means you can minimise downtime and data loss. A robust backup and disaster recovery plan will also make your business less of a target in the first place, as cybercrime groups look to identify organisations with vulnerable security setups.

**So what does an effective backup solution look like? Consider these qualities to ensure your business is as secure as possible:**



## **SPEED**

The ability to back data up quickly, and as regularly as possible, is crucial. This ensures that you can restore infected files in the case of an attack and be confident they're completely up-to-date. Fast restoration of data is also essential because newer versions of ransomware will permanently delete files every hour the fee isn't paid.



## **SCALE**

As your business grows, so do your backup requirements. Your solution should scale as your needs change, without losing significant space or time. This will ensure that your security standards don't slip as backup requirements become more complex. Remember, storing larger volumes of critical data increases your risk of becoming a target.



## **FLEXIBILITY**

A backup solution should be easily inserted into your existing environment with little change to your current processes and systems. It should also integrate with other archive and recovery applications, allowing you to build a multi-faceted security solution that protects your business from any breach or threat.



## ISOLATION

Recovering servers doesn't guarantee you'll remove the infection from your network altogether. Your backup strategy should include isolated recovery, where locking down systems used for recovery will ensure data is only visible to your business. This also creates an air gap between the recovery and production systems, making the recovery target inaccessible to the network and restricted from any users who aren't cleared.



## OFFLINE

Having backups stored in offline and offsite locations will ensure that your files are safe even if your entire network is compromised. An effective disaster recovery strategy includes storing one or more copies of your data externally, so the right backup solution will allow you to easily and quickly replicate data from one system to a secure offsite location.



## PRECISION

In the case of malware infections, restoration of an endpoint or server will be most effective when you have the ability to select a specific moment in time and restore applications instantly to that point. This ensures that data is as up to date as possible. Crash consistent copies will also allow you to validate your recovery, comparing it to the most recently copied version and invalidating corrupted versions, triggering isolated recovery.



**You need to be confident in your protection readiness**



- Dell EMC Global Data Protection Index Research Study

# How SI Systems Can Help Protect Your Business

SI Systems recommends an isolated data centre, disconnected from your network, to keep out ransomware threats and other types of cyber-attacks. This involves locking down systems used for backup and recovery, and limiting exposure to create an air gap between the recovery zone and production systems.

We provide consulting services for the implementation of an Isolated Recovery solution. This can be delivered in a range of ways including On-Premise or As-a-Service.

## ON PREMISE

SI Systems can provide expert advice to assist with the implementation of a successful on-premise Isolated Recovery solution. This can then be delivered as a package on-site with certain components disconnected from your network, helping to keep cyber threats away from your data.

## AS-A-SERVICE

A range of As-a-Service solutions are available from SI Systems. This includes replication of backup data to SI Systems' Isolated Recovery Solution. This also offers extra protection as this copy of your data is hosted on a separate site. SI Systems also offer standby compute for hydrating backups within an isolated environment.





# About

## Dell EMC Data Domain

SI Systems' recommended technology for the implementation of an Isolated Recovery Solution is Dell EMC's Data Domain appliance, the industry's most scalable, reliable and cloud-enabled isolated protection storage. Dell EMC's Data Domain allows you to protect your data wherever it lives in the most efficient way possible, with an air-gapped data protection device that never has an active unsecured connection.

The Data Domain disk backup system is able to be off the grid most of the time, making the recovery target inaccessible to the network and restricted from all users who are not cleared to access it. The air gap is created by closing ports when not in use, and limiting the open ports to those needed to replicate data. RecoverPoint can then be used with Storage to handle replication and provide crash consistent copies, which helps to validate copied versions and trigger corruption alerts. With seamless integration and reliable access, your business can ensure your data is protected at all times.

# About SI Systems

SI Systems is a systems integrator that provides IT services to a wide range of customers. We specialise in IT infrastructure, data protection and software development. We're passionate about delivering innovative industry-leading solutions to meet our customers' needs. SI Systems have a Backup-as-a-Service, Disaster Recover-as-a-Service and Isolated Recovery-as-a-Service platform which enables us to provide a full range of offerings to ensure your data remains protected.

Contact us today to reduce your risk of being impacted by ransomware.  
Discuss the right recovery strategy or 'as-a-service' solution to protect your data.

**[sales@sisystems.com.au](mailto:sales@sisystems.com.au) • +61 3 9013 0029**