Technology Report

DCIG

Identifying and Deploying the Right Cyber Resilience Solution

By DCIG President & Founder, Jerome Wendt

DCIG

TECHNOLOGY REPORT

Identifying and Deploying the Right Cyber Resilience Solution

Contents

Complacency a Risky Option

All organizations—public, private, profit, non-profit, small, large, and anywhere in-between—recognize ransomware poses a risk to their operations. Further, many of these same organizations have already experienced a ransomware attack.

A recent survey of over 1,100 information and operational technology professionals found 80 percent had experienced a ransomware attack. Of those, over 60 percent paid a ransom with 52 percent of them paying a ransom of at least $500,000.[1]

Ransomware's pervasiveness presents an imminent threat to all organizations regardless of their classification or size. It indiscriminately finds its way into organizations often creating untold anxiety, frustration, and costs once it attacks.

Adding to organizational stress levels, ransomware continues to evolve to escape detection by cyber security software. This makes an attack more likely. This combination of the inevitability of a ransomware attack and the devastating impact it can have make complacency a risky option.

Mounting a Defense Against Ransomware

In response, organizations must defend against ransomware attacks by implementing the right combination of cyber security and cyber resilience technologies that work well together.

Cyber Security Definition

"The art of protecting networks, devices, and data from unauthorized access or criminal use and the practice of ensuring confidentiality, integrity, and availability of information."

– Cybersecurity and Infrastructure Security Agency (CISA)

Cyber Security

On the cyber security side, many organizations embrace a zero-trust or minimal trust security model. This model controls access to corporate IT systems and their digital assets. It relies upon multi-factor authentication (MFA), role-based access, or both to authenticate system and/or user access.

Cyber security technologies such as antivirus software and firewalls then get used to defend data and systems from ransomware attacks. Users and systems access cyber security software using MFA and role-based methods.

Source: DCIG

Cyber Resilience

Organizations must augment their cyber security technologies with the appropriate cyber resilience offerings. Products that provide cyber resilience primarily differ from cyber security focused offerings in the following manner: they reduce and mitigate the organizational risk once a ransomware attack occurs.

Organizations primarily turn to cyber resilience solutions after a ransomware attack occurs. These offerings should withstand an attack and continue to operate, though they may operate in a degraded state.

Cyber Resilience Definition

"The ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."

– National Institute of Standards and Technology (NIST)

Existing disaster recovery (DR) and business continuity (BC) plans help organizations identify their core cyber resilience technologies. These plans document how they will recover from a ransomware attack or any type of outage or disruption. Any software or technology they use as part of their DR/BC plan they should classify as cyber resilient. Once classified this way, they should proceed to evaluate how well it measures up as a cyber resilient offering.

The Four Goals Cyber Resilience Products Should Ideally Meet

Classifying products as core to an organization's cyber resilience strategy does not immediately make them cyber resilient. Organizations should determine how well each software or technology meets the four cyber resilience goals the NIST lays out.[2] How well each one meets these goals helps organizations establish the overall viability of their broader cyber resilience strategy.

Cyber Resilience Goal #1: Anticipate

DCIG finds it almost a statistical certainty that every organization will at some point experience a ransomware attack. This likelihood of an attack translates into the need for cyber resilience software and technologies to expect an actual attack to occur. In anticipation of an attack, these products should continually take steps to defend themselves.

These preparations may show up in various ways. They include:

- Utilizing third party, cyber security providers to monitor and alert on ransomware attacks occurring regionally, nationally, or globally.
- Monitoring hardware and network resources for any unusual or suspicious activity.
- Taking steps to scan and analyze the data under their management for ransomware.

In short, the products should continually monitor their health and operating environment to prepare to act appropriately.

Cyber Resilience Goal #2: Withstand

Organizations should operate on the assumption that they will experience a ransomware attack. They should also assume an attack may occur undetected over a period of hours, days, weeks or even months. This puts the onus on organizations to implement software and technologies that can withstand both overt and covert ransomware attacks.

Overt ransomware attacks, while potentially disruptive and devastating, do have one potential advantage over covert attacks. These attacks may immediately disrupt IT and business operations. Software and technologies core to a cyber resilience strategy simply need to survive and remain operational during this time. Organizations also may want to take these systems offline or air gap them to secure them.

In the case of covert attack, organizations may fail to recognize it in a timely manner. As such, organizations must ensure their cyber resilience software and technologies continually protect themselves. These products should secure and monitor all activity on them to withstand covert attacks. Otherwise, if and when a covert attack becomes overt, organizations may find their cyber resilience solutions irreparably compromised.

Cyber Resilience Goal #3: Recover

Achieving the first two goals to ready and secure their cyber resilience software and technologies does not prevent a ransomware attack. Ransomware may still circumvent their cyber security solution and encrypt part or all their production environment.

Meeting these first two cyber resilience objectives only positions organizations to recover. They provide no guarantees as to the success, speed, completeness, or outcome of the recovery.

"Organizations need to configure their cyber resilience solution to place the right data on the right storage media for recoveries."

For example, DCIG knows of a ransomware attack that compromised production systems. The organization first had to replace its production hardware and software before it could restore its applications and data.

In another example, the only 'good' or clean backups an organization possessed resided on tape. Unfortunately, these tape backups were not viable for recovery. The restorations took too long to complete plus the data was outdated for recovery purposes.

Organizations need to configure their cyber resilience solution to place the right data on the right storage media for recoveries. This placement ensures they can recover as quickly as they need. This media may include the cloud, disk, flash, tape, or some combination thereof. They also must test their recovery processes to account for either covert or overt ransomware attacks.

Cyber Resilience Goal #4: Adapt

This last goal represents perhaps the most difficult one for organizations to consistently achieve. Driven by business, technical, and regulatory requirements, organizational IT environments change with great regularity. Aggravating the situation, these changes may occur with little notice and without consideration for the impact they have on the cyber resilience solution.

To keep a cyber resilience strategy viable, organizations must identify ways to monitor and track changes to their IT environment. Only by doing so can their cyber resilience solution adapt to these changes as they occur.

Organizations may still find it impractical for their cyber resilience solution to adapt in real time as production changes occur. However, by monitoring changes to their production environment they can update their cyber resilience solutions in a timely manner.

New Premium on Data Protection Offerings

Organizations must accept the critical role that cyber resilience plays in recovering from ransomware attacks. This requires they place a premium on the data protection software and technologies they use as part of their cyber resilience strategy.

Organizations too often treat data protection software and technologies as a "check box". They put them in place to meet specific best practices, compliance, or regulatory requirements. However, they could not validate how well they met cyber resilience standards since NIST only recently defined them.

Now that these standards do exist, organizations must verify if their existing data protection software and technologies meet them. To do so, they should answer the following questions:

- ***What measures do these products take to anticipate attacks?*** Do the offerings check the data under their management for ransomware? Do they monitor their logs as well as ransomware attacks occurring regionally, nationally, and/or globally?
- ***How well do they withstand attacks?*** Do they offer air gapped and immutable storage options? Do they integrate with existing organizational cyber security technologies?
- ***How quickly can they recover and bring production systems and data back online?*** Can they back up and recover the systems when and where they need them to meet their recovery time and point objectives? What media do the products manage? Do the products offer instant recovery capabilities?
- ***How viable is the organization's DR plan?*** Does the organization's overall DR plan satisfy these four cyber resilience goals? Do all software and technologies used as part of the DR plan meet these objectives?

Organizations should evaluate their existing cyber resilience solution using questions like these. More strains of ransomware target organizational backups, backup software, and backup storage targets. Hackers recognize that compromising any component of an organization's cyber resilience solution may result in the organization paying a ransom.

"To mitigate these advanced forms of ransomware attacks, data protection software and technologies must restrict and monitor access to them and their data."

Data Protection Software and Technology

To mitigate these advanced forms of ransomware attacks, data protection software and technologies must restrict and monitor access to them and their data. This begins by first authenticating users that access them. Ideally, they will use role-based access control (RBAC), multi-factor authentication (MFA), or both to authenticate user access.

Once logged in, backup software and technologies will ideally monitor and log all user actions while validating some of them. For instance, they should monitor for and authenticate any changes or deletions to backup schedules or data. Some changes, such as unscheduled deletions of backups, may even require a second user to authenticate the action.

They should also offer options to forensically analyze backups. This analysis may include the ability to scan backup data for unusual data change rates between backups as well as analyze it for the presence of ransomware. Finally, they should store backup data in an immutable format so one cannot delete or encrypt the data accidentally or maliciously.

The DR Plan's Viability

Multiple organizations have experienced ransomware taking out their entire production environment. In one case, DCIG spoke to a company whose DR plan failed to account for how ransomware has evolved. When the company was attacked, the ransomware encrypted its on-premises backups residing on network filers. This made it impossible for the firm to use these backups for recovery.

This evolution in ransomware attacks makes it imperative that organizations verify the viability of their DR plans.

Organizations should also ensure their DR plan accounts for how ransomware has changed. This requires examining each underlying software and technology upon which their DR plan relies. Should the DR plan fail to account for these changes in how ransomware attacks, even a tested DR plan can fail when a ransomware attack occurs.

3-2-1-1 Backup Strategy

A 3-2-1-1 backup strategy consists of the following:

- **3** Three copies of data (production data plus two backup copies)
- **2** Data stored on two different media types
- **1** One copy of data stored off-site for disaster recovery
- **1** One copy of data stored in an immutable format

Arcserve's Suite of Cyber Resilience Offerings

Arcserve focuses on delivering the underlying cyber resilience software and technology that organizations need to create an effective cyber resilience solution. Arcserve's offerings directly map to the current, stated goals that a cyber resilience strategy should meet. Consider:

- ***Arcserve Business Continuity Cloud*** offers organizations the flexibility to perform DR and BC in the Arcserve Cloud.
- ***Arcserve Continuous Availability*** provides continuous replication for files, folders, and physical and virtual machines. Using its Data Rewind feature, organizations may recover to a point in time that precedes the start of the ransomware attack.
- ***Arcserve OneXafe*** delivers on-premises object storage with data immutability capabilities. Using OneXafe, organizations may recover an unaltered copy of their backup data from an immutable store.
- ***Arcserve Unified Data Protection (UDP) Secured by Sophos*** grants organizations access to a proven, enterprise-caliber backup software offering. Arcserve UDP may store data in an immutable format on-premises, in the cloud, or both. It may store data on-premises on its immutable OneXafe storage offering. It may also store data in an immutable format in AWS S3 with Object Lock as well in other S3 compatible clouds that have a comparable Object Lock feature. Arcserve further protects the data by detecting and reversing incidents of ransomware encryption.
- ***Arcserve Appliances Secured by Sophos*** deliver ready-to-deploy appliances that contain both backup and cyber security software. As an all-in-one solution, it includes Arcserve UDP Secured by Sophos so organizations may quickly deploy and manage backup, recovery, and cyber protection.
- ***Arcserve UDP Cloud Hybrid*** builds on Arcserve's offerings to deliver an integrated cyber resilience solution that includes cloud backup, cyber security, and DR. It automatically replicates data from an on-premises Arcserve UDP recovery point server (RPS) to a corresponding RPS in the Arcserve cloud. The integrated Sophos Intercept X Advanced cybersecurity protects against known and unknown malware. Organizations then manage the entire process through the UDP console.

Arcserve builds on these core functions with multiple availability and DR options. For instance, Arcserve offers high availability through its Continuous Availability software. It also delivers DR through its Business Continuity Cloud, UDP Cloud Direct, and UDP Cloud Hybrid cloud offerings as well as on its Arcserve Appliances.

All Arcserve solutions such as Arcserve Appliances, Cloud Hybrid, and UDP, use and protect backup data with Sophos Intercept X, a leading antivirus software offering. Intercept X may scan data during backups and recoveries to proactively monitor and alert to the presence of ransomware. These scans ensure the integrity of backup data for successful recoveries and restores.

Arcserve also handles all aspects of storing and managing backup data. It may store and manage backup data onsite, offsite in another data center, or with multiple cloud providers. Arcserve's storage management capabilities extend to storing data on immutable storage on-premises or the cloud. Finally, it offers technical support for organizations to help ensure they continuously operate during any type of event.

Arcserve's cyber resilience offerings coupled with Sophos Intercept X collectively provide organizations a comprehensive, modern cyber resilience solution.

Company	**Arcserve**
Location	8855 Columbine Road Suite 150 Eden Prairie, MN 55347
Phone	(844) 765-7043
Website	https://www.arcserve.com/

An Effective Cyber Resilience Solution is a Necessity

No single cyber security solution guarantees 100 percent protection against ransomware. Too many examples exist of ransomware bypassing in-place cyber security solutions to compromise secured IT environments

Organizations must account for this eventuality and put in place an effective cyber resilience solution. This solution must, out of necessity, consist of the right combination of data protection software products and technologies. Each offering should ideally anticipate, withstand, recover, and adapt to avoid becoming the weak link in an overall cyber resilience solution.

Arcserve delivers the type of offerings that organizations should consider when building a comprehensive cyber resilient solution. Each Arcserve offering satisfies the four cyber resilience goals. In so doing, Arcserve's offerings do more than position organizations to defend against ransomware. Arcserve provides organizations with a high level of certainty they can successfully recover in a timely and effective manner. ■

Sources

1. https://claroty.com/wp-content/uploads/2022/02/Claroty_Report_State_of_Industrial_Cybersecurity_2021.pdf. Referenced 4/12/2022.
2. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf. Pg 26. Referenced 4/20/2022.

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.**