IBM Systems

Cyber resilience
An important new role for storage

Contents

Highlights

- Implement IBM Storage systems to build powerful cyber resilience solutions
- Deploy cybersecurity solutions designed specifically for your business
- Leverage the power of a broad portfolio of IBM Storage offerings
- Choose between flash, disk, tape, software-defined, and cloud object storage solutions

IBM Storage provides a broad spectrum of cyber resilience solutions

As information technology (IT) becomes more pervasive in our daily lives, and as more and more data is collected by businesses, governments, and individuals, cybersecurity rises as a key societal need. Every week brings public disclosure of a security failure within a well-known business or government agency, often with staggeringly large numbers of affected parties.

A July 2018 study by Ponemon Institute, sponsored by IBM Security reports that the average cost worldwide of a data breach in the preceding 12 months was USD 3.86 million, with the largest breaches reaching a cost of USD 350 million. The root causes of the data breaches included human error (27 percent), system glitches (25 percent), and malicious or criminal acts (48 percent). Nearly half of the surveyed events were due to malicious attacks, and the per-record cost of these attacks was 20 percent higher than the cost of other causes.[1]

A major risk to worldwide business

Deliberate attacks on IT infrastructure come in several forms, depending on the purpose of the attack. In some cases, installations are attacked to gain access to confidential data, such as credit cards or bank accounts. Ransomware is a form of malware that encrypts files and demands payment for a key to unlock data. The WannaCry outbreak in 2017 may have infected 200,000 computers, including systems in the UK National Health Service, causing hospitals to turn patients away.[2] Some attacks have nonfunctional, no payment functions or simply destroy data, indicating that the intent of the attack is to cripple a business or government.

Besides the threat of external malware as described above, there is also the threat of insider attack. Dishonest or disgruntled employees, including some with significant authority to harm IT operations, can misuse data or disrupt business operations.

Given the extreme dependence modern society has on IT and data, the World Economic Forum Global Risks Report 2019 rated cyberattacks as one of the most likely major risks to human welfare.[3] Clearly, with both the likelihood and cost of cyberattacks being high, IT organizations require a systematic approach to security.

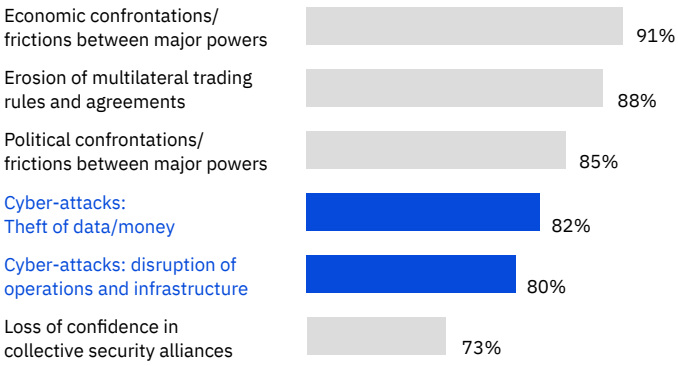

Figure 1: Top risks to human welfare, according to the World Economic Forum

Cyber security and cyber resilience

Whether data breaches result from an accident or malice, protection of IT operations and the data that sustains them is critically important. As business use of technology increases and includes more assets, such as mobile devices, the Internet of Things (IoT), and multivendor supply chains, and as attacks grow in sophistication, IT security will need to respond. There are already a number of methods available to protect organizations from disruptions or minimize the cost. The Ponemon study shows the value of implementing some of these security strategies. The most beneficial ones—creating an incident response team, using extensive encryption, employing business continuity management and improving employee training—can lower the cost of a successful breach by one-third.

To establish and maintain robust cybersecurity and related cyber resilience, a procedural approach should be employed to understand what data and system assets you have, what their value is, and what risks apply to them. In a world without budget or staffing constraints, you would want to make everything as secure as possible all the time. But because that is not how our real world operates, you will need to apply the disciplines of risk management, consider a range of possible tiers of implementation, and use tools to profile the current and desired security state of your organization.

The NIST framework

The US National Institute of Standards and Technology (NIST) has published a *Framework for Improving Critical Infrastructure Cybersecurity* as advice to business and government operators of critical infrastructure. The document defines "critical infrastructure" by citing the USA Patriot Act of 2001: "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." A business can replace the references to the "US" or "national public health" with concern for the viability of its own operations, so the Framework can be seen as a guide for IT shops of any size in any industry.

The Framework begins with the process of risk management to identify, assess, and manage the risks facing an organization's IT operation. The Framework is made up of three parts—the Framework Core, Framework Implementation Tiers, and Framework Profiles.

The Framework Core is a set of five cybersecurity functions that helps organizations:

- *Identify*: Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- *Protect*: Develop and implement appropriate safeguards to ensure delivery of critical services.
- *Detect*: Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- *Respond*: Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- *Recover*: Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

When considered together, these functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk.

Framework Implementation Tiers describe four maturity levels of cybersecurity functions, with a view into processes, implementation of a management program, and consideration of external relationships, such as partial, risk-informed, repeatable, and adaptive. These Tiers reflect a progression from informal, reactive responses to approaches that are agile and risk-informed.

Framework Profiles represent cybersecurity outcomes based on business needs. Profiles can be used to identify opportunities for improving a company's cybersecurity posture by comparing a current profile, the "as is" state, with a "target" profile, the "to be" state.

The Framework begins with the process of risk management to identify, assess, and manage the risks facing an organization's IT operation.

Planning for cyber resilience

Through the use of the NIST Framework, business leaders can determine their current security posture and plan future improvements. Vendors, such as IBM, use the NIST Framework to identify best practices and leading-edge technology, and explain the integration of product functions into an overall security position.

Within the overall discipline of cybersecurity lies a subset practice of cyber resilience, a relatively new idea. *Bjorck* and the team offer a definition: "Cyber resilience is defined as the ability to continuously deliver the intended outcome despite adverse cyber events."[4] The discipline acknowledges that an accident or attack may well penetrate security protections, and a mature IT organization will prepare for these events with methods that limit damage and provide for rapid recovery. When providing a service of great public importance, or simply running the daily operation of a business, IT infrastructure should be robust even in the event of successful intrusion.

For example, in cases of data theft, malware seeks to remain undetected and interfere as little as possible with normal operations, with intrusions continuing undetected for perhaps hundreds of days. For newer types of attacks, including ransomware and wiper attacks, the goal is not theft of data but interfering with normal business operations. The term logical data corruption (LDC) is used for the damage this type of malware seeks to do. In both cases, the target is the data used by business applications. To ensure business resilience, IT infrastructure must preserve copies of active data which are current enough to be a viable recovery point in the event of attack.

The role of storage infrastructure

Storage has for a long time played the role of "data custodian" in enterprise operations. In addition to providing containers where data goes when not in main memory, the system storage layer has traditionally provided protection functions that help organizations recover from unusual events. Over time, the range of these functions has grown:

- *Backup*. From the 1960s on, storage has allowed application users to save a version of data on separate media to protect it from accidental deletion, corruption, or primary device failure.
- *High availability*. From the early 1990s on, storage has provided designs to create multi-path access, multi-server access, and duplication of on-line copies of data within a machine room.
- *Disaster recovery*. From the late 1990s on, storage has provided designs to create replicated copies of active data at distances sufficient to protect from power outage or regional disasters like earthquakes, floods, or fires.
- *Fast online data recovery*. From the 2010s on, storage has provided snapshot copies of data for rapid recovery from accidental deletion or data corruption.

In each case, the new function was introduced in storage systems, management software, and operational processes to address the specifics of the risk case.

The threat of LDC through cyberattack, specifically ransomware or wiper attack, presents a new set of protection considerations. To provide the needed level of resilience, solution providers can borrow some of the storage tools already in place for backup and disaster recovery (DR), but some new storage functions are also needed to address the new threats.

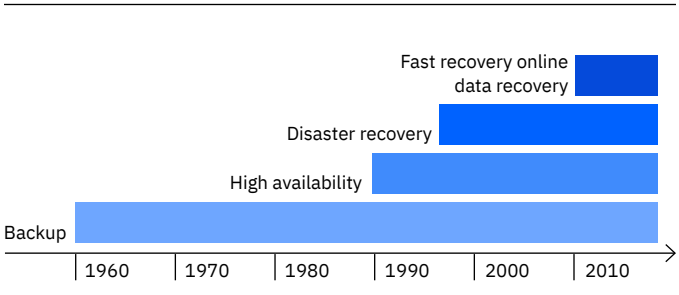

Figure 2: Storage protection functions over time

For example, in the event of a successful LDC attack, the storage layer must have a way to protect data from what would normally be routine operations. Writing to files, blocks, or objects could now be the act of malware that is encrypting or destroying valuable data—creating new backups could be a way to quickly expire good backups and replace them with backups of corrupt data. A mechanism is needed that combines storage functions and operational processes to preserve current recovery copies of data, even in the face of a sophisticated malware attack. Once the attack has been detected and a response mounted, these preserved copies can be used to restart applications and resume normal service. The IBM Redpaper *DS8000 Safeguarded Copy* identifies three new capabilities needed to create preserved copies: [5]

- *Granularity*: Organizations must be able to create multiple protection copies in order to minimize data loss in case of a corruption incident.
- *Isolation*: The protection copies must be isolated from the active production data so that they cannot be corrupted by a compromised host system (this is also known as an "air gap").
- *Immutability*: The copies must be protected against unauthorized manipulation.

In *Five Key Technologies for Enabling a Cyber-Resilience Framework*, Phil Goodwin and Sean Pike of IDC add two additional considerations which, while not unique to LDC attack resilience, are part of a best practice list: [6]

- Automation and orchestration for recovery of platforms and applications
- Regulatory reporting and assurances

A mechanism is needed that combines storage functions and operational processes to preserve current recovery copies of data, even in the face of a sophisticated malware attack. Once the attack has been detected and a response mounted, these preserved copies can be used to restart applications and resume normal service.

Using the NIST framework to design data resilience solutions

The specific technologies used to accomplish LDC resilience vary considerably in performance and response time, overall time to recover, and cost. In the vocabulary of the DR discipline, implementations will have different recovery point objectives (RPO) and recovery time objectives (RTO). The NIST Framework and a risk assessment methodology are useful guides for the design of an overall cybersecurity posture. A complete plan might include the following steps:

- *Identify*: Use a risk management method to list key applications and data assets and determine the appropriate protection policies for each. Which are mission critical? Which have high rates of data change? Which could be rebuilt from external sources? What time to recover (RTO) and allowable degree of data loss (RPO) is required? What cost for protection is appropriate for each data asset?
- *Protect*: Evaluate additional security protections within the production environment, such as restriction of privileged access. Establish a process to create backup copies of data at a rate required by the desired RPO. Select appropriate homes for the copies, including protection of the copies through network isolation, storing the copies in immutable format, and preventing their deletion by software or administrative action. Provide automation to create the backups so they are not dependent on human intervention. Establish a response plan, including response teams and process steps or run books, to recover specific applications or servers—or the entire infrastructure.
- *Detect*: Include mechanisms to identify the presence of malware, hackers, or rogue privileged users and suspend corrupted servers or applications to minimize damage.
- *Respond*: Activate response teams, including skilled personnel, to take action to protect backups, identify affected assets, and plan recovery actions. Identify the source of the attack and modify protections to prevent recurrence.

– *Recover*: With skilled people in place and backups created through automation, begin the process of creating a recovery environment. Backups should be used as the source of secondary copies and not directly mounted to applications that might still be corrupt. If systems are still functional, a forensic analysis can determine the areas affected and guide recovery actions. The scope of recovery will vary depending on the degree of damage. Surgical recovery can address corruption of specific files or applications; catastrophic recovery of complete systems is needed when damage is extensive.

The design of a business resilience plan must be unique to each business, with specific needs identified through its risk assessment process. The plan should establish a view of a current state or profile and identify areas of improvement or investment based on a "to be" profile. The resilience plan should be updated as changes are made to infrastructure, new business processes are created or new types of threats are identified. In most cases, cyber resilience will be combined with products and processes used for the more traditional practices of backup and DR.

IBM Storage systems deliver a broad spectrum of features that can be used to build IT operations that are resilient in the face of LDC attacks or accidental disruption.

Storage infrastructure solutions from IBM

IBM Storage systems deliver a broad spectrum of features that can be used to build IT operations that are resilient in the face of LDC attacks or accidental disruption. Comprehensive IBM solutions can combine storage functionality, network configuration, administrative controls, and physical security. Some of the key cyber resilience solutions and technologies provided by IBM Storage are introduced below.

Traditional snapshot-based backup and recovery
Snapshots, such as the IBM FlashCopy® function, have become one of the best performing and most cost-efficient methods to address the requirements of traditional backup. IBM DS8000® data systems, IBM Storwize® family arrays, IBM SAN Volume Controller, IBM FlashSystem® 9100, FlashSystem A9000 and FlashSystem A9000R software defined storage implementations with IBM Spectrum® Virtualize, IBM Spectrum Scale, IBM Spectrum Accelerate and IBM Spectrum NAS all support FlashCopy functions. Space-efficient, read-only data copies provide cost-effective recovery points that can be used for quick restores of prior versions of data. Using snapshots to recover from accidental deletion or corruption has become a widespread practice. Various FlashCopy solutions are well documented in IBM Redbooks® and Redpapers.[7,8,9] The existence of data backups can provide a recovery point for some LDC malware attacks, but without additional consideration exposure to sophisticated attacks still exists.

Protected snapshots using IBM Storwize and IBM FlashSystem solutions

Starting with the snapshot functionality available in Storwize or FlashSystem arrays, you can configure even more resilient LDC protection solutions by deploying software facilities that automatically invoke snapshots at regular intervals in the storage arrays. The frequency of the snapshots determines the RPO of the data being protected, with lower RPO using more storage resources. The number of backups kept determine how far back in time you must go to find an uncorrupted version of data. The policies for specific applications should be identified through the risk assessment process. Software solutions for this purpose include IBM Copy Storage Management, IBM Spectrum Copy Data Management, and IBM Spectrum Protect Snapshot.

In addition to snapshot automation, there is the question of protecting the snapshots. One approach is to replicate storage volumes from the production system to a secondary storage system of the same type. Periodic snapshots can then be used as recovery copies on the secondary array. The replication and snapshot function should be automated through software. The non-production storage system should not be connected directly to any application servers, and the only storage data connection active should be the port or ports through which backup copies arrive. The administrator sign-on should have a different password and be managed by a different person than the production system. And the administrator of the non-production system should be a member of the cyber resilience response team.

The physical separation between the systems is a matter of implementation design; closer proximity, even in the same data center, provides better performance and lower network costs, and the non-production storage solution can be included in a remote facility used for DR.

In the event of an LDC malware attack or a test of a recovery action, data copies stored on the non-production system should be used as the source of recovery copies that could be moved back to the production storage system. The use of a non-production storage system provides a logical air gap between production and protected copies. The physical separation between the systems is a matter of implementation design; closer proximity, even in the same data center, provides better performance and lower network costs, and the non-production storage solution can be included in a remote facility used for DR.

Protected snapshots with IBM Spectrum Scale

File system data is often part of mission-critical operations and must also be included in a cyber resilience plan. The approach described on the left, using protected snapshots of active data, can also be applied to implementations of IBM Spectrum Scale.

IBM Spectrum Scale supports DR configurations with a primary site for production and a secondary recovery site. In a true DR scenario, these systems should be separated by distances appropriate to the type of disaster risk, such as a local flood, power outage, or earthquake. For the purposes of cyber resilience, physical separation is not necessary, but a cyber resilience solution can be combined with a DR one. IBM Spectrum Scale maintains a copy of file data at both sites; the underlying technology is data replication between the sites, as described in the IBM Redbook *Spectrum Scale (Formerly GPFS)*.[10]

Snapshots that represent backups can then be taken at the secondary site and used for recovery in the event of a malware attack. As described above, the secondary system should have no host attachment and a different admin sign-on from the primary admin sign-on. The secondary admin should be a member of the cyber response team.

Beyond taking snapshots, IBM Spectrum Scale has the ability to copy data to Write Once Read Many (WORM) tape as an additional safeguard. As described in the IBM Redbook *Active Archive Implementation Guide with IBM Spectrum Scale Object and IBM Spectrum Archive*, IBM Spectrum Scale supports multiple storage pools that are mapped to distinct physical storage.[11] One supported storage type is tape, which is presented as an Linear Tape File System (LTFS) mounted into an IBM Spectrum Scale storage pool. Linear Tape Open (LTO) tape can be deployed as WORM media, creating an additional immutable copy that is safe from malware action. In the event of an attack that compromises primary operations, the response team can determine which copy to use for recovery at the secondary site.

DS8800 Safeguarded Copy

To provide a higher degree of automation, better protection, and a deeper history of backups, the Safeguarded Copy function was introduced into the IBM DS8880 storage array family in September 2018. Safeguarded Copy is a special version of FlashCopy; it creates space-efficient, read only copies that cannot be mounted to an external server or deleted by an administrator. Up to 500 copies per DS8880 volume can be created, giving users the option of creating a long history of protected data. Administrators need at least two interfaces in order to create, enable, and manage the Safeguarded Copy—DS8880 DS CLI or DS GUI to provision backup capacity and IBM Copy Services Manager to enable and manage Safeguarded Copy tasks. Copies can be kept in the same production storage system or copied to a remote DS8880 array that is the target of synchronous or asynchronous replication.

As discussed earlier, the secondary DS8880 storage system should be isolated to minimize the attack surface that it presents. It should not be attached to application servers and the only storage data connection active should be the port or ports through which backup copies arrive. The administrator sign-on should have a different password and be managed by a different person than the production system. And the administrator of the non-production system should be a member of the cyber resilience response team.

For more details on the design of DS8880 Safeguarded Copy solutions, planning, and operation, see the IBM Safeguarded Copy Redpaper.[12]

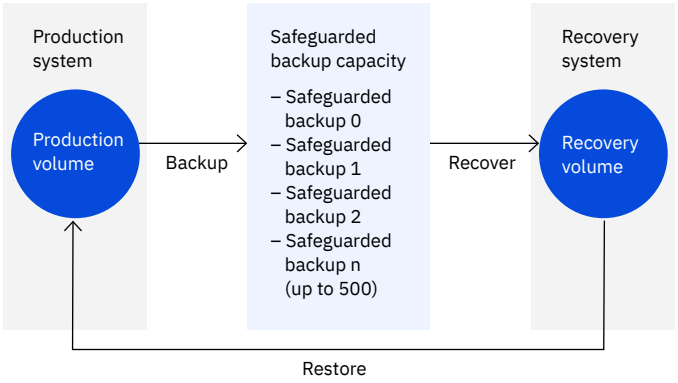

Figure 3: DS8800 Safeguard Copy process

Cyber resilience management solutions

IBM provides specific management solutions for cyber resilience, including awareness and management of the overall replication topology, as well as server integration. These solutions include the IBM GDPS® logical corruption protection capability for IBM Z® servers and the IBM i PowerHA® toolkit.

Protected backups with WORM media

IBM Spectrum Protect provides a highly functional backup and archive software system. It can move full copies of data into a managed storage space, and using an incremental-for-ever design, maintain backup versions by storing changed data. IBM Spectrum Protect can be configured to manage a collection of storage pools, including flash, disk, object storage, or physical and virtual tape.

For the purposes of protecting recovery copies, WORM media can be useful. The IBM TS1100 and LTO families of tape drives offer the added protection of fully disconnected media with no programmatic access except through the control of the library function. Tape cartridges can be identified as WORM and used to write recovery copies that are protected from overwrite by the tape drive. Once committed to a WORM cartridge, no type of malware in application or management servers can destroy the backup copy. Consideration for physical protection is of course necessary. The TS7700 Virtual Tape system provides a logical WORM function enforced by the storage controller.

Unlike space-efficient snapshots, full copies written to tape require time to move data and restores are much slower than what can be achieved with snapshots. Designs should be customized to the needs of each business, but it may be desirable to create a full defense in depth, with a snapshot-based recovery augmented by a backup that places data on offline media. For more details, consult IBM Spectrum Protect product documentation.[13]

Protecting data on IBM Virtual Tape
IBM TS7700 Virtual Tape systems offer a Logical WORM (LWORM) capability that provides a software version of WORM on physical tape. This prevents data on an LWORM volume from being overwritten and, once the volume is created, it can only be appended to or expired, but not modified.

LWORM can be combined with the TS7700 retention hold capability to enable restoration of expired tape volumes back to a prior point in time. With retention hold, a volume is not reused until some specified time has expired. In addition, when integrated with tape systems, such as IBM TS4500 and TS7700 solutions, it offers the air gap between data and online hackers, providing a safeguard against cyberattacks.

Powerful tape air gap protection
Networks are designed to disperse information fluidly through an organization. It is precisely this efficiency in data communication that allows malware to penetrate and spread through the network very quickly, leaving organizations exposed internally and potentially externally, depending on the systems affected.

As noted earlier, the term “air gap” refers to physical or virtual insolation of systems or networks to avoid widespread corruption of data due to malware infection, system failures, or human error. The basic concept around an air gap is to bring secondary storage systems online periodically to incorporate the latest changes and then take them back offline. The solution approaches that use snapshot functions to create copies can be quickly mounted to recover damaged applications. But full protection of the copied data does have some limitations; in every case the repository of the copies has a network connection of some type.

The most complete protection approach, which provides no network or software access to protected copies, can be implemented using a tape library. The IBM TS4500, TS4300, and TS2900 libraries make the tape cartridges only accessible when mounted in a drive. The “offline by design” nature of tape offers a true physical air gap and provides one of the most secure protections to confront cybercrime. For more details on data protection with tape, including the use of air gap techniques, WORM, and other security capabilities, please refer to the *IBM Tape solutions provide modern and powerful data protection* solution brief.[14]

Networks are designed to disperse information fluidly through an organization. It is precisely this efficiency in data communication that allows malware to penetrate and spread through the network very quickly, leaving organizations exposed internally and potentially externally, depending on the systems affected.

Protecting data with IBM Cloud Object Storage
IBM Cloud™ Object Storage provides durable, secure, and cost effective cloud-based storage for archiving and data protection. IBM Cloud Object Storage maintains integrity in a WORM manner to protect data against deletion or modification. Definition of policies allows the flexibility to specify the default, minimum, and maximum retention periods that help govern data retention requirements. A legal hold can also be applied at the object level, preventing data deletion until the completion of a specific audit activity. Retention periods and legal holds can be applied to a single object or multiple objects during data ingest into IBM Cloud Object Storage. Objects cannot be deleted until the retention period has expired and all legal holds are removed.

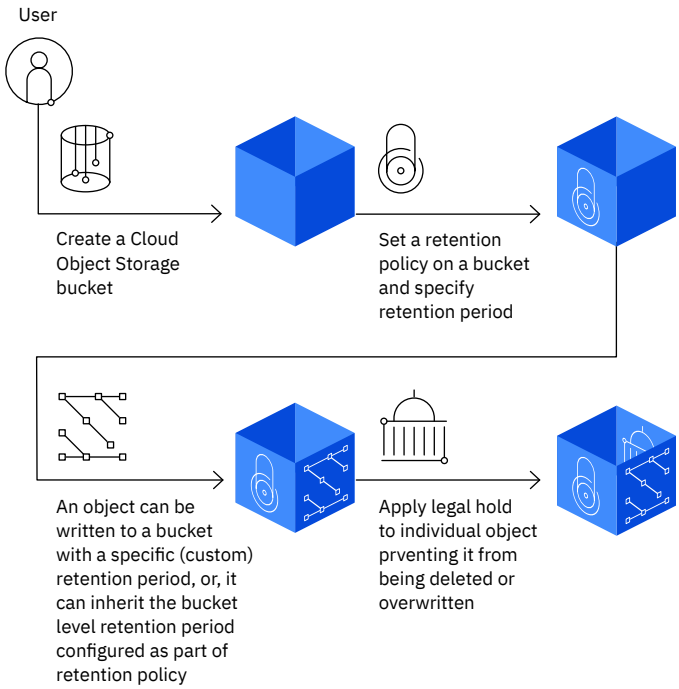

Figure 4: Protecting data with IBM Cloud Object Storage

Malware detection with IBM Spectrum Protect
IBM has added a feature to the IBM Spectrum Protect backup software to detect the actions of certain types of malware, including those associated with LDC attacks. When malware overwrites files with encrypted or corrupted versions, these changes are seen as updates and the new data is collected by IBM Spectrum Protect for backup. The solution keeps a history of normal operations and malware activity registers as a significant deviation from normal access patterns. In March 2018, with V8.1.5 of IBM Spectrum Protect Operations Center, a new alert feature was announced.[15] After every client backup session, statistics are analyzed for signs of ransomware infection. If signs are present, a warning message is displayed in the operations center. You can use the new security notifications page to view details for each security notification. This information helps you determine whether the client is infected with ransomware or if the notification is a false positive.

Cyber resilience for the 21st century

Cyberattacks designed to deny access to or destroy data are likely to remain a major business risk for the foreseeable future. The use of technology and operational processes for prevention of cyberattacks will be necessary, and measures to recover from successful attacks will also be an important part of a well-designed security posture. By leveraging proven technologies and approaches such as the NIST Framework and the discipline of risk management, IBM Storage offerings can be used to create and implement cyber resilience solutions that will help 21st-century businesses thrive well into this century.

References

1 “2018 Cost of a Data Breach Study: Global Overview.” *Ponemon Institute*, July 2018.

2 “Investigation: WannaCry Cyber Attack and the NHS.” *Report by the Comptroller and Auditor General, National Audit Office*, April 2018.

3 “Global Risks Report 2019, 14th Edition.” *World Economic Forum*, Geneva Switzerland, 2019.

4 Björck F., Henkel M., Stirna J., Zdravkovic J. (2015) Cyber Resilience—Fundamentals for a Definition. In: Rocha A., Correia A., Costanzo S., Reis L. (eds) New Contributions in Information Systems and Technologies. Advances in Intelligent Systems and Computing, vol 353. Springer, Cham

5 Alexander Warmuth, Robert Tondini, Michael Frankenberg, Nick Clayton, and Bert Dufrasne, “DS8000 Safeguarded Copy.” *IBM Corp*., November 2018.

6 Phil Goodwin and Sean Pike, “Five key technologies for enabling a cyber resistant framework.”, *IDC*, July 2018.

7 Bert Dufrasne, Francesco Anderloni, Roger Eriksson, and Lisa Martinez. “IBM FlashSystem A9000 and A9000R Business Continuity Solutions, A draft IBM Redpaper publication.” *IBM Corp*., November 2018.

8 Jon Tate, Rafael Viela Dias, Ivaylo Dikanarov, Jim Kelly, and Peter Mescher. “IBM System Storage SAN Volume Controller and Storwize V7000 Replication Family Services”, *IBM Corp*., March 2013.

9 Dino Quintero, “IBM Spectrum Scale (formerly GPFS).” *IBM Corp*., May 2015.

10 Dino Quintero, Luis Bolinches, Puneet Chaudhary, Willard Davis, Steve Duersch, Carlos Henrique Fachim, Andrei Socoliuc, and Olaf Weiser. “IBM Spectrum Scale (Formerly GPFS)”, *IBM Corp*., 2015.

11 Larry Coyne, Joe Dain, Khanh Ngo, and Aaron Palazzolo. “Active Archive Implementation Guide with IBM Spectrum Scale Object and IBM Spectrum Archive”, *IBM Corp*., 2016.

12 Warmuth et.al, Op.Cit.

13 “IBM Spectrum Protect Version 8.1.3 Tape Solution Guide.” *IBM Corp*., 2017.

14 “IBM Tape solutions provide modern and powerful data protection solution brief.”, *IBM Corp*., 2019. https://www.ibm.com/downloads/cas/Z5RV1AKP

15 “IBM Spectrum Protect V8.1.5 and IBM Spectrum Protect Plus V10.1.1 deliver increased performance and additional capabilities”, Product announcement letter, *IBM Corp.*, March 2018.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
October 2019

29025229USEN-03 | Thought Leadership White Paper