NEXSAN

WHITEPAPER

STORAGE IN A WORLD OF REGULATORY CHANGES

ADDRESSING THE CHALLENGES OF STORING CUSTOMER CALL CENTER DATA

AVERAGE COST FOR ORGANIZATIONS THAT EXPERIENCE NON-COMPLIANCE PROBLEMS IS $14.82 MILLION.

*(*According to the Ponemon Institute.)*

THE CHALLENGES OF STORING CUSTOMER CALL CENTER DATA IN A WORLD OF REGULATORY CHANGES

The list of compliance regulations is increasing, with each new requirement becoming an additional challenge to be met. It's no longer just about storing information—being able to remove personal data without risking the storage and integrity of other data is now equally important. A few of the regulatory compliance guidelines that call centers may need to adhere to include GDPR, CCPA, SEC-17a4, PCI DSS, CJIS, HIPAA, SOX, and more. Because regulations are frequently updated, call centers need to stay up-to-date on the changes and show that they are meeting all of the new requirements as they come into effect. In addition, call centers must always assess whether they are prepared for new customers with new requirements, and also whether they have the required agility to work within their existing framework for compliance.

No one wants to believe that their organization will be the target of compliance auditors and potential fines and penalties for non-compliance, but that threat is real and increasing. Studies have shown that over half of organizations have failed at least one regulatory audit within a five-year period. According to the Ponemon Institute*, the average cost for organizations that experience non-compliance problems is $14.82 million, a 45% increase from 2011.

LET'S START WITH HIPAA

Organizations that manage and/or store any type of healthcare information—including insurance, telemedicine, and call centers—are required to comply with Health Insurance Portability and Accountability Act (HIPAA) regulations. The U.S. Department of Health and Human Services (HHS) defines integrity controls in 45 CFR § 164.304 "as the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system." This requires that electronic personal health information (ePHI) is not modified in any technical or non-technical way. Many believe that traditional SAN or NAS storage does this; however, the standard is actually much stricter than this interpretation. The rules stipulate that:

- Audit trails need to be protected. Call centers and other regulated organizations need to provide and have immediate access to complete and accurate access audit logs. In a 2018 Data Breach Investigations Report by Verizon, researchers found that 68% of breaches took months or longer to discover. This is one reason why it is vital to be able to prove when someone accessed the information during the audit trail.
- Identification of unauthorized changes and access. This is a very interesting challenge, as today the industry is exploding in petabytes or even exabytes of data. Access logs are needed to show not only approved access, but unauthorized access attempts to data, as well as any changes to the file and the full access history.
- Authenticity of data. The frequency of monitoring for integrity isn't specified by the National Institute of Standards and Technology (NIST) or HIPAA guidelines. However, real-time monitoring can be crucial in protecting from data loss, ransomware attacks, or data theft.

A LOOK AT PCI DSS REQUIREMENTS

At a high level, the Payment Card Industry Data Security Standard (PCI DSS) requirements are focused on the protection of cardholder data and the encrypted transmission of cardholder data across open, public networks. It seems fairly simple, but as you dig into the requirements, they become much more detailed—as do the storage requirements to meet them. The PCI DSS guidelines that relate to data storage include PCI DSS 3.1 to 4.1, which specifically focus on:

- Keeping cardholder data to a minimum by implementing data retention and disposal policies, procedures, and processes
- Security policies and operational procedures for protecting cardholder data
- Encryption, including key management policies, procedures, and documentation processes to protect and manage encryption keys
- Encryption of data both at rest and during transmission across open, public networks

WHAT MAKES GDPR MORE CHALLENGING?

The General Data Protection Regulation (GDPR), often referred to as "the right to be forgotten," went into effect on May 25, 2018 across EU member countries. GDPR is a game changer in that it requires all organizations to take their data-handling responsibilities more seriously through greater accountability. As such, it is important to have documented policies in place to enable staff to have a clear understanding of what is required of them. Moreover, the GDPR's new accountability principle should encourage organizations to have something ready to show to regulators in the event of problems. Any such policy should at least satisfy the following six broad questions:

1. Which categories of data does the policy cover?
2. Who has responsibility for those categories of data, and who has specific obligations under the policy?
3. Other than data protection laws, what other rules, codes, or practices should be considered?
4. Subject to the above, when should data be retained and when should it be deleted?
5. When should certain data be made exempt from the general deletion principles (i.e., 'litigation holds')?
6. When should certain data be made exempt from the general retention principles (i.e., individuals exercising their right to be forgotten)?

CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

CCPA—THE NEW KID ON THE BLOCK

The California Consumer Privacy Act (CCPA) is the latest in data protection regulations and will go into effect on January 1, 2020. The three basic goals of CCPA are to:

1. Protect what information corporations may collect about individuals.
2. Ensure that an individual's personal information is not shared or sold to other organizations
3. Ensure businesses that do need to collect personal information take necessary precautions to keep it safe.

So, what are the consequences under CCPA? Twice per year and free of charge, consumers gain the right to know all data that has been collected by a business. The law also gives consumers the right to sue companies that collect their data, in the event that the consumer's data is stolen or disclosed due to an unauthorized data breach. If the data wasn't protected properly by encryption or if there weren't reasonable security policies and procedures in place, the organization is at risk of liability for any data breach.

Here is a list of many of the types of information that will be included in CCPA:

- A job application, resume, or CV
- An employment contract or independent contractor agreement
- A performance review or disciplinary record
- A photo used for an identification badge or organizational chart, marketing, or website
- Biometric data used for timekeeping or facility access
- Backup files
- Information from company devices or vehicles, including geolocation data
- Browsing or search history
- Information used for payroll processing and benefits administration
- Internal or external contact information maintained in the electronic onboarding, HRIS system, or Active Directory
- Information captured from video, audio, systems, or other forms of monitoring or surveillance

RANSOMWARE ANOTHER DATA PROTECTION CHALLENGE

The biggest consequences of ransomware are data loss and downtime, resulting in potentially millions of dollars in lost revenue in addition to decreasd customer trust.

MULTIPLE REGULATORY COMPLIANCE REQUIREMENTS

A twist on maintaining compliance is that many of these situations have more than one regulatory guideline that must be followed based on the type of data that is being captured. As an example, a customer service call that requires HIPAA compliance may also include rules for Personally Identifiable Information (PII), CCPA, GDPR, and/or PCI DSS. Many if not all of the on-call services require authentication to ensure that the patient calling can be verified against an actual policyholder, using key identifiers such as parent names, home address, email address, last four digits of social security number, and more. In rare cases, patients are asked to provide a co-payment, which is generally less than an office visit but requires a credit card to continue. Transactions and interactions like these blur the lines of responsibility for compliance. Based on the advice of internal legal counsel, organizations will need to set their storage retention and disposition policies accordingly.

YET ANOTHER DATA PROTECTION CHALLENGE—RANSOMWARE

Ransomware and other types of malicious software programs (also known as malware) can disrupt any environment. These programs infiltrate a network, propagate through connected devices and systems, and encrypt data, which disables user access, software, and IT assets. There are many types of ransomware that have infected organizations throughout the world, wreaking havoc and costing business their reputation by exposing sensitive data.

Although there's a high financial cost for the actual ransom payment, the biggest consequences of ransomware are data loss and downtime. Both of these ransomware outcomes are very costly for businesses, with significant downtime resulting in potentially millions of dollars in lost revenue in addition to decreased customer trust.

EVALUATING STORAGE PRODUCTS

So how does an organization evaluate a storage product to ensure it complies with all relevant regulations? The evaluation process begins based on the client being served today and their compliance requirements. How can an organization cost-effectively store the data to meet all requirements and have the flexibility to change the system as regulatory agencies add new requirements? When evaluating compliant storage systems, it's important to understand what is inherently built into a system versus what may be required for custom programming. Flexibility in configuration is the key to having not only a system that meets today's requirements, but additionally has the capability to be easily configured as other regulations such as GDPR or state trusted systems come into play.

SILENT DATA CORRUPTION IS A SERIOUS RISK

CERN REPORTED THAT APPROXIMATELY

1 OUT OF EVERY 1,500 FILES

HAD BECOME CORRUPT IN A MATTER OF WEEKS DURING THEIR TESTING

Data is valuable. If we're afraid to lose the data and also have to provide proof and processes of compliant storage and audit trails, the risk of data loss is even greater. With this in mind, shouldn't a key feature of storage be data protection? If an organization fails to ask the right detailed questions, it may not receive sufficient data protection in storage. Not all storage will protect data from integrity issues or silent data corruption. And what about the ability to do real-time audits for integrity checks? It's critical to ensure that the system will never overwrite an original file, and will keep the original intact so that nothing, including malware, can alter that data.

After working with many different customers and organizations in the data storage and data compliance industries, here are some key points that we have learned at Nexsan:

- From a compliance and data protection perspective, the way that organizations store data for compliance has evolved in many ways. Initially, organizations flocked to WORM technology systems for protection against accidental deletion and security. Many of these systems were cumbersome and required costly APIs that ended up costing more than the best Tier-1 storage systems. Many WORM disks could not guarantee that the information was removed when the retention period was completed, which therefore left organizations at risk for storing the data longer than required.
- Unable to use WORM effectively, many organizations decided to store on traditional SAN or NAS systems for ease of use. But this too left companies at risk, because the snapshot data or backup is not guaranteed for retention and timely, proven disposal since there were multiple backup and snapshot copies stored.
- Tape makes no guarantees that the data originally placed on it will be available due to handling, media quality, and the software that originally saved it. While typically marketed as the best, most inexpensive medium for long-term archive, tape also doesn't allow for easy disposition for various regulations.
- DeDupe and Disk-to-Disk both extol the virtues of their systems. But it's notable that they will not guarantee data integrity due to the software that is sending them the information and known disk issues.
- Silent Data Corruption is a serious risk. CERN, a world-renowned particle physics lab, reported that approximately 1 out of every 1,500 files had become corrupt in a matter of weeks during their testing. What's worse, this can happen right under a company's nose—and there are no effective ways to verify corruption other than a full end-to-end integrity check. Some of the largest manufacturers in the disk storage market have published bit error rates and known file integrity issues, since they lack full integrity check capabilities.

ORIGINAL FILE INGESTION

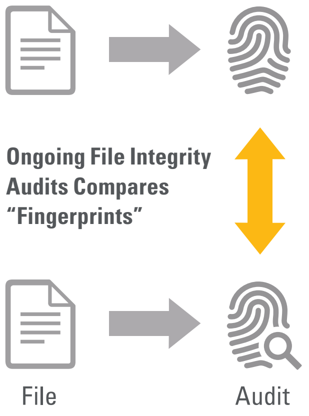

Figure 1: *Unique fingerprint enables recurring checks for corrupted files.*

Figure 2: *Unity Assureon Archive's unique file serial numbers enable easy identification of missing files.*

NEXSAN ASSUREON HELPS MEET REGULATORY COMPLIANCE

Nexsan Assureon® is a proven system that has been protecting data for over 12 years. Designed originally for meeting the strict requirements of medical and financial regulatory needs, the Assureon has evolved to become one of the most secure and reliable data protection systems on the market today. Assureon meets stringent compliance regulations along with other challenges such as ransomware and silent data corruption. So what are the benefits of deploying a Nexsan Assureon replicated system?

- **Original Data or Call Recording Preserved.** Whenever data is written, Assureon immediately creates a digital fingerprint for both the original file and the associated metadata. These secure copies are then leveraged to preserve image integrity for the duration of the retention period.
- **Retention Period.** Assureon includes auditing, integrity, and self-healing features that let call centers and other organizations easily implement multi-decade retention times if needed. It keeps two copies of each file in independently protected object stores, and applies two cryptographic hashes—like unique digital fingerprints of the file contents—that are separately stored in a hardened blockchain internal to the device. Additionally, Assureon issues a globally unique consecutive serial number to each file so that it can be tracked throughout its lifetime.
- **Automated Integrity Audits.** Assureon protects data from viruses, silent data corruption, and incidental or intentional tampering. On a regular basis, Assureon audits validate the integrity of all archived data by comparing the files stored in the archive to the original fingerprint. If any discrepancies are discovered, Assureon automatically restores the study to the original state and logs the action. This ensures that the data stored is the same as the data received. Simply put, any archive solution that lacks this integrity checking cannot credibly claim to offer secure archiving...period.
- **Data Availability.** Regular Assureon availability audits continuously validate the presence of all data. If any files are missing, Assureon automatically restores the study from the duplicate original file and logs the action.
- **Integrated System Protection.** Hardware layer protection prevents the deletion of RAID sets or volumes.

- **Right to Be Forgotten or Removal of Personal Information.** A unique Client-Triggered Expiration feature allows companies struggling with proper retention in the new rules of GDPR and CCPA to ensure that once deletion of data has been approved, Assureon will destroy the records within the system. All copies of the encryption key for the file, and the encrypted file itself, are irrevocably destroyed once the deletion cycle is complete. Optional deletion may be postponed for business or legal reasons. Administrators are no longer burdened with ensuring that copies left on backup tapes exist that could result in penalties within the new GDPR framework. Rather than managing two systems (software and hardware), the triggered expiration is directed by the organization's primary software platform, ensuring that once approved for deletion, the file is removed with an audit trail.
- **File-By-File Encryption.** Assureon provides a robust, industry-leading, fully automated encryption system that includes encryption at rest, secure multi-tenancy encryption, and encryption in-flight:
  - Encryption at Rest. Every file is encrypted with its own unique AES-256 encryption key, while many other archives either don't encrypt or use a single shared key across volumes or across controllers.
  - The keys themselves are transferred and stored in encrypted key containers. Those key containers are refreshed and re-encrypted each month automatically.
  - Files are encrypted at the Assureon Processing node and are transferred in encrypted format to the alternate Assureon site.
  - Secure Multi-Tenancy Encryption. In a multi-tenant environment, the root keys for each tenant are unique. Each file also has its own individual AES-256 encryption key underneath that. In short, there is a completely isolated encryption system for each tenant within a multi-tenant Assureon system.
  - Encryption In-Flight. Assureon can encrypt files as they are transferred between sites using an encrypted tunnel between clients/edges and the Assureon
  - Privacy Protection. Assureon protects the privacy of customer data through user access authentication. This ensures that data is quickly available only to authorized users.
- **File Access Audits.** Assureon records all attempts to access data, whether successful or unsuccessful. All file activities are recorded to provide absolute certainty that privacy has not been compromised.
- **Disaster Recovery with Real-Time Replication.** Whenever a recording or dataset is written, Assureon immediately replicates both the file and associated metadata to the remote site. Continuous file audits protect against corruption during replication.
- **Failover to Remote Site.** In the event of a failure at the primary site, Assureon will failover to the remote location enabling the facility to continue operations without interruption.

- **Automated Restore.** When a primary site is restored, Assureon self-healing technology automatically audits all data and settings to ensure consistency of data, policies, and settings between both sites.
- **Streamlined Disaster Recovery and Data Migration.** Following a major disaster, data migration is simplified through automated file auditing and fast shortcut restore. **Protecting the Data.** Data protection needs to include unauthorized or accidental changes or deletions of files by people, viruses, or ransomware that have escalated to super-user privileges or have compromised the Active Directory server in some way. Because Assureon resists attempts by privileged accounts to change or modify files, it helps remove the temptation for authorized users to make unauthorized changes; those users will be unsuccessful and will be caught. Any attempt to overwrite a file merely creates a new version. By default all versions are stored, but version-limiting options allow protection against DDoS attacks that attempt to consume all available storage space with unwanted and corrupt versions.

SUMMARY

Nexsan Assureon ensures that call centers and other regulated organizations will meet or exceed most, if not all, regulatory compliance requirements. By offering unmatched visibility into user activity via comprehensive audit trails, data retention, data destruction policies that meet strict regulatory guidelines, unmatched data archiving and redundancy capabilities, and flexibility in configurations settings, no other data protection solution is easier or more effective when it comes to setting up new rules for compliance.

ABOUT NEXSAN

Nexsan® is a global enterprise storage leader, enabling customers to securely store, protect and manage critical business data. Established in 1999, Nexsan has built a strong reputation for delivering highly reliable and cost-effective storage while remaining agile to deliver purpose built storage. Its unique and patented technology addresses evolving, complex enterprise requirements with a comprehensive portfolio of unified storage, block storage, and secure archiving. Nexsan is transforming the storage industry by turning data into a business advantage with unmatched security and compliance standards. Ideal for a variety of use cases including Government, Healthcare, Education, Life Sciences, and Media & Entertainment. Nexsan is part of the StorCentric family of brands along with Vexata, Drobo and Retrospect – and operates as a separate division to securely protect business information.

(Rev. 8/01/19)