Cybrilliance — NeuShield Strengthens DORA Compliance

Digital Operational Resilience Act

The EU Digital Operational Resilience Act (DORA) aims at strengthening the IT security of financial entities such as banks, insurance companies and investment firms and making sure that the financial sector in Europe is able to stay resilient in the event of a severe operational disruption.

DORA brings harmonisation of the rules relating to operational resilience for the financial sector applying to 20 different types of financial entities and ICT third-party service providers.

DORA entered into force on January 16, 2023 and is set to take effect in January 2025, bringing significant implications for organizations operating within the financial sector. Under DORA's mandate, financial entities and their critical third-party technology service providers must implement stringent ICT system guidelines by January 17, 2025. This initiative aims to establish a universal framework for managing and mitigating ICT risk across the financial landscape.

The regulations are designed to ensure compliance, and penalties for non-compliance can be costly. These penalties can include:

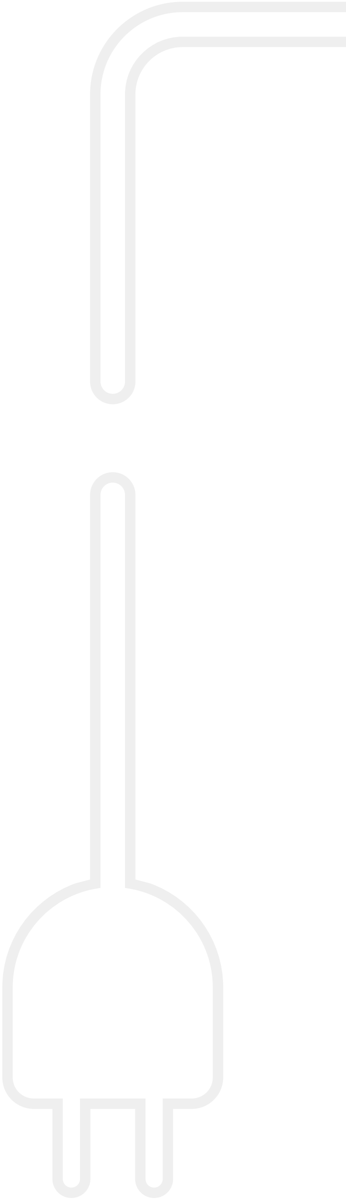
- Financial penalties that amount to the equivalent of one day of trading revenue
- Criminal charges against companies and individuals who do not adhere to DORA

Cybrilliance have identified the following sections from the final text[1] of DORA, indicating existing technology, techniques and policies (TTPs) and highlighting the additional value delivered by NeuShield Data Sentinel.

.

[1] - https://www.digital-operational-resilience-act.com/DORA_Articles.html

Table of content



Preamble (48)

Efficient business continuity and recovery plans are necessary to allow financial entities to promptly and quickly resolve ICT-related incidents, in particular cyber-attacks, by limiting damage and giving priority to the resumption of activities and recovery actions in accordance with their back-up policies. However, such resumption should in no way jeopardize the integrity and security of the network and information systems or the availability, authenticity, integrity or confidentiality of data.

Existing TTPs

Recovering data using existing 3-2-1 backup strategies, originally developed for traditional disaster recovery scenarios do not deliver the recovery time objectives (RTO) that align to 'always-available' financial services organisations. Cyber-attacks will compromise on/off-site data copies and any snapshots to hinder recovery operations, requiring organisations to be dependent on an off-site immutable copy for data restoration. Notification of a cyber-attack necessitates the removal of all internal/external networks to contain the spread/effects of the attack.

NeuShield Policy

- All data required to recover device/ data operations already exists and is protected on the devices. This negates any need to use traditional backup copies to rebuild compromised data that may have deleted or encrypted as part of the execution by the cyber malware.
- NeuShield RTO can be >90% faster than recovering data using traditional backups. This is because NeuShield does not need to transfer data to rebuild the data. NeuShield only need to delete the data update/compromise to make the original data available.
- NeuShield doesn't jeopardize network integrity and allows recovery of data without introducing possible malware. NeuShield recovery can be performed by the end user or IT administrator. If executed by the end user, no network connections (LAN, WAN, wi-fi, etc.) are required to restore device operations. If the IT administrator performs the recovery, a network connection is only required to send a NeuShield command.

Preamble (51)

The propagators of cyber-attacks tend to pursue financial gains directly at the source, thus exposing financial entities to significant consequences. To prevent ICT systems from losing integrity or becoming unavailable, and hence to avoid data breaches and damage to physical ICT infrastructure, the reporting of major ICT-related incidents by financial entities should be significantly improved and streamlined.

Existing TTPs

There are various reporting requirements that financial organizations must comply with. The biggest challenge for any organization is to fully appreciate the depth of the data breach as part of their incident response (IR) activities, ensuring they can report correctly. In many occurrences financial organizations need to report to the local regulatory office (DPC, ICO, etc.) within 72 hours of becoming aware of the breach.

NeuShield Policy

- NeuShield will not allow exfiltration for Microsoft SQL Databases. If the IR team determine that the data breach is focused on their database system, they will be able to confirm with confidence that no data left the MS SQL environment.
- When the IR team are confident that they have contained the malware used in the attack, NeuShield will allow every protected device to be re-enabled simultaneously within 30-60 minutes.

Article 9 – Protection & Prevention - Para 2

Financial entities shall design, procure and implement ICT security policies, procedures, protocols and tools that aim to ensure the resilience, continuity and availability of ICT systems, in particular for those supporting critical or important functions, and to maintain high standards of availability, authenticity, integrity and confidentiality of data, whether at rest, in use or in transit.

Existing TTPs

A combination of aligned security and data recovery TTPs remain the standard when designing and implementing levels of maturity to protect an organization's infrastructure and data. Endpoint, network, boundary and communication tools remain the most effective way to detect and mitigate cyber-attacks. When an attack is missed/overlooked, there are no further tools available to stop active data and devices from being compromised. Backup and recovery tools can stop malware from compromising a copy of the backup data by storing this data on immutable storage media. This policy play's no part in protecting an organization's active data or devices.

NeuShield Policy

- NeuShield protects all an organization's active and inactive structured/unstructured data and system data/files continuously. NeuShield's Mirror Shielding patented architecture is impenetrable, guaranteeing protection of data during all operations.
- NeuShield protection is not reliant on the detection of a specific malware vector, it will protect your data from known/unknown/file/fileless and zero-day attacks, where that attack is focused on compromising your data.
- No longer do organizations need to depend on rebuilding compromised data from backups which may take days/weeks to complete. NeuShield's RTO can be >90% faster as no transfer of data is required.

Article 9 – Protection & Prevention - Para 3

In order to achieve the objectives referred to in paragraph 2, financial entities shall use ICT solutions and processes that are appropriate in accordance with Article 4 (principle of proportionality). Those ICT solutions and processes shall:
(b.) minimise the risk of corruption or loss of data, unauthorized access and technical flaws that may hinder business activity;
(c.) ***prevent the lack of availability, the impairment of the authenticity and integrity, the breaches of confidentiality and the loss of data;***
(d.) ensure that data is protected from risks arising from data management, including poor administration, processing-related risks and human error.

Existing TTPs

Current TTPs provide organizations with the capability to duplicate systems and data during standard operating activities, offering the capability to fail-over to maintain levels of availability . In addition, data management tools such as Data Loss Prevention (DLP) attempt to stop data from being shared without authorization and file encryption impairs the unauthorized recipient of data from opening/reading the data.

During cyber (exceptional) incidents, the attackers have proved they have the ability to compromise primary and fail-over devices and also production data, backup data and VSCs.

NeuShield Policy

- NeuShield does not allow direct update of protected data. All file updates are separated from the protected data, ensuring any update can be verified before committing as a valid update.
- Access to the NeuShield portal is allowed via multi-factor authentication. Organizations can build access to NeuShield into their overall Zero-Trust Identity and Access Management (IAM) TTPs.
- NeuShield retains versions of the operating system and application data, allowing the IT administrator to roll back instantly if a software patch or cyber-attack attempting to compromise the device occurs.

Article 9 – Protection & Prevention - Para 4

As part of the ICT risk management framework referred to in Article 6(1), financial entities shall:
(f.) have appropriate and comprehensive documented policies for patches and updates.

Existing TTPs

Organizations will have a change management process in place to determine the process that should be followed when patch updates and new software versions need to be applied. Using standard RMM tools these changes are pushed out to devices and applied once the device is active. Any prior testing is undertaken on a test/development environment, that imitates the production environment.

NeuShield Policy

In the event of a failed/faulty patch update, organizations can adjust their documented TTPs to include the use of NeuShield One-Click Restore feature that will instantly roll-back the OS/Applications to a prior point deemed stable. This feature can be executed centrally via the NeuShield portal or locally by the user. The latter is especially useful if the device is located in an air-gapped or non-network connected environment.

Article 10 – Detection

Financial entities shall have in place mechanisms to promptly detect anomalous activities, in accordance with Article 17 (incident management process), including ICT network performance issues and ICT-related incidents, and to identify potential material single points of failure.
All detection mechanisms referred to in the first subparagraph shall be regularly tested in accordance with Article 25.

Existing TTPs

A combination of aligned security and data recovery tools utilize malware engines, penetration testing and threat intelligence insights to detect vulnerabilities and anomalous activities across an organization. The majority of these tools focus on pre-breach activities, apart from backup tools that are only effective in post-breach activities, identifying malware embedded with their data copies.

If the pre-breach tools are evaded by a cyber-attack, these tools play no further part in protecting your active environment.

NeuShield Policy

NeuShield does not replicate the detection capabilities of current pre-breach tools. NeuShield will instantly alert and continually protect data when the pre-breach tools have been evaded. Without NeuShield organizations will need to wait until program failure or user notification of any breach.

Article 11 – Business Continuity

Financial entities shall implement the ICT business continuity policy through dedicated, appropriate and documented arrangements, plans, procedures and mechanisms.

Existing TTPs

A well tested and documented process should exist for all DR/BC activities. The organization’s backup and recovery tools and all data retained within its systems are the primary recovery mechanisms for BC/DR activities.

NeuShield Policy

Although NeuShield has been built specifically to address time-sensitive incidents such as a Ransomware attack, NeuShield can be utilized in a DR/BC event to complement existing backup and recovery tools. NeuShield does not transfer data off a device, but where the active data is replicated to an offsite device for use during BC/DR, organizations will be protected and able to engage operations very effectively.

Article 12 – Backup Policies and Procedures - Para 1,2,3,5

1. *For the purpose of ensuring the restoration of ICT systems and data with minimum downtime, limited disruption and loss, as part of their ICT risk management framework, financial entities shall develop and document:*
   (a.) backup policies and procedures specifying the scope of the data that is subject to the backup and the minimum frequency of the backup, based on the criticality of information or the confidentiality level of the data;
   (b.) restoration and recovery procedures and methods.
2. *Financial entities shall set up backup systems that can be activated in accordance with the backup policies and procedures, as well as restoration and recovery procedures and methods. The activation of backup systems shall not jeopardise the security of the network and information systems or the availability, authenticity, integrity or confidentiality of data. Testing of the backup procedures and restoration and recovery procedures and methods shall be undertaken periodically.*
3. *When restoring backup data using own systems, financial entities shall use ICT systems that are physically and logically segregated from the source ICT system. The ICT systems shall be securely protected from any unauthorised access or ICT corruption and allow for the timely restoration of services making use of data and system backups as necessary.*
   For central counterparties, the recovery plans shall enable the recovery of all transactions at the time of disruption to allow the central counterparty to continue to operate with certainty and to complete settlement on the scheduled date.
   Data reporting service providers shall additionally maintain adequate resources and have back-up and restoration facilities in place in order to offer and maintain their services at all times.

Article 12 – Backup Policies and Procedures - Para 1,2,3,5

5. Central securities depositories shall maintain at least one secondary processing site endowed with adequate resources, capabilities, functions and staffing arrangements to ensure business needs.
The secondary processing site shall be:
(a.) located at a geographical distance from the primary processing site to ensure that it bears a distinct risk profile and to prevent it from being affected by the event which has affected the primary site;
(b.) capable of ensuring the continuity of critical or important functions identically to the primary site, or providing the level of services necessary to ensure that the financial entity performs its critical operations within the recovery objectives;
(c.) immediately accessible to the financial entity's staff to ensure continuity of critical or important functions in the event that the primary processing site has become unavailable.

Existing TTPs

Data backup policies tend to align to a version of the 3-2-1 backup strategy, originally developed for traditional disaster recovery scenarios. These data copies will be a mixture of incremental, differential and full copies taken at daily, weekly, monthly and quarterly intervals. In addition to recognized backup & recovery products, organizations will also complement these with Microsoft Snapshot copies, retaining up to 64 Virtual Shadow Copies (VSCs) for immediate recovery purposes. The use of a secondary site / clean room are also accessible as a method to recover an environment quickly or to act an active alternative Point of Processing (POP).

Article 12 – Backup Policies and Procedures - Para 1,2,3,5

NeuShield Policy

- Two of the data copies stored from backup and recovery tools using the 3-2-1 policy are immediately susceptible to compromise (along with VSCs) when a cyber attack occurs. This renders these two copies of data redundant. NeuShield does not suffer from this type of compromise.

- NeuShield has no dependency on existing backup and recovery products. In the event that an organization needs to recover their data and device following a cyber-attack, everything can be executed locally and simultaneously.

- NeuShield will not increase the vulnerability of the organization by requiring the network to be opened and the transfer of data from the immutable copy of the data (offsite).

- NeuShield allows an organization to retain between 0-30 copies (delta changes) of every file held on the device. In addition, five (5) copies of the OS/Application image are retained for instant recovery.

- Recovery of data and device files using NeuShield does not require the user to wait for IT support to manage the recovery. Deploying NeuShield means that remote users can recover their environments instantly and not lose any productivity that may be the case when users are reliant on IT support to manage their recovery actions.

Article 12 – Backup Policies and Procedures - Para 6

In determining the recovery time and recovery point objectives for each function, financial entities shall take into account whether it is a critical or important function and the potential overall impact on market efficiency. Such time objectives shall ensure that, in extreme scenarios, the agreed service levels are met.

Existing TTPs

Recovery Point Objectives (RPO) are aligned to the frequency with which an organization takes their data copies and also if the data copy is an incremental, differential or full copy as this will determine if the IT support team need to recover multiple instances of data. Recovery Time Objectives (RTO) have a number of dependencies; location of data copy, network accessibility, availability of device to recover data, etc. Service Level Agreements (SLA) specified for a data recovery RTO should not reflect the original time taken to perform the backup. The SLAs should be set to acknowledge that recovering data from an offsite location can take ~2 hours per Terabyte assuming all dependencies are available.

Unfortunately, the nature of extreme scenarios means that re-establishing a consistent network connection will not be accessible until the IR team are assured of the malware eradication.

NeuShield Policy

- NeuShield has no dependency on existing backup and recovery products. In the event that an organization needs to recover their data and devices following a cyber-attack, everything can be executed locally and simultaneously.
- NeuShield only requires a network connection for a limited period to enable the IT support team to send a command to the device. The network can be disconnected after the command is sent, ensuring all infrastructure remains air-gapped.
- NeuShield can 'instantly' revert a file, completing in seconds, never needing to introduce external data to the device. In addition, if the device is unresponsive, the user can put the device into Windows recovery mode and select the NeuShield OS/Application image to restore the device in ~20 mins.

Article 12 – Backup Policies and Procedures - Para 7

When recovering from an ICT-related incident, financial entities shall perform necessary checks, including any multiple checks and reconciliations, in order to ensure that the highest level of data integrity is maintained. These checks shall also be performed when reconstructing data from external stakeholders, in order to ensure that all data is consistent between systems.

Existing TTPs

There are multiple options available to organizations when they need to recover from an ICT related incident.

As these events tend to be exceptional events (not planned), the reliance on regularly tested TTPs and a demonstrable RTO are critical.

Validation of data can be time consuming to ensure that the infrastructure and data are consistent and capable of operating effectively without further delays.

NeuShield Policy

- NeuShield revert/recovery operations never introduce data from external stakeholders. All data used to restore operations had already operated cleanly on the device at a prior point of operations, ensuring that no rogue or malware embedded data or application can compromise your device.

- NeuShield Datacenter Edition will always ensure that when restoring an MS SQL Server that requires recovery, the entire system (database, data, logs, registries, directories, etc.) will always be restored at the same time. This ensures organizations have consistency for the database system, and also ensure any malware tampering is never retained.

Conclusion

The critical nature of the digital-first financial services industry to a country's economic and critical national infrastructure, necessitates compliance with a level of resilience rules.

Implementing DORA rules will be different for each financial organization based on the principle of proportionality, taking into account their size and overall risk profile, and the nature, scale and complexity of their services, activities and operations.

Implementing NeuShield Data Sentinel to assist with an organization's implementation TTPs for DORA, will significantly increase its data and security maturity level and elevate its overall cyber resilience status.

NeuShield is the only technology that guarantees continual protection of your production/active data from compromise, combined with the unique Mirror Shielding^{TM} capability to restore/revert data instantly.

cybrilliance

Empower Your Business with Cyber Resilience

Interested in Cybrilliance?

For more information visit: https://www.cybrilliance.com

Contact@CyBrilliance.com

CyBrilliance HQ

Burlington,
Ontario,
L7L 4C4.
Canada.

CyBrilliance EMEA

Covent Garden,
London,
WC2H 9JQ.
United Kingdom.

CyBrilliance Asia

Ulsoor,
Bangalore,
560008.
India.