Data-Centric Cyber Risk Management

Security leaders have long agreed that implementing a well thought-through defense-in-depth strategy can significantly reduce an organization's risk of data loss and prevent successful cyber-attacks. A multi-layered approach to security acknowledges that a cyber-attack involves multiple stages. This means that even after getting initial access to an enterprise network, an attacker needs to go through multiple stages to get to their end goal, which in most cases is data exfiltration.

By placing multiple layers of defense across their internal networks and endpoints, organizations can stop attackers – if not at the perimeter, then at one of the later stages of attack.

Data protection at the core of security

For defense-in-depth to be effective, however, security teams need to start with the data. One of the core components of a strong defense-in-depth strategy is data protection, which is more complex now than ever before because of increasing data sprawl. With sensitive data dispersed across computing environments and geographical locations, finding and classifying this data has become more difficult.

Data is essential for routine company operations, but it can easily become intractable if organizations don't regularly monitor where it resides, what its sensitivity level is, and who has access to it. The process of identifying, classifying and protecting data is best accomplished using a combination of reliable technology and human input. The human element requires education to understand the different types of sensitive information relevant to an organization and then design and implement policies and controls to handle sensitive and business-critical data.

Data Protection-focused Security and the Zero Trust Model

The pace of digital transformation and cloud migration over the past decade has brought significant operational and productivity benefits to organizations, but it has also exposed enterprise networks and devices to new attack vectors and created security gaps. With data storage extending into environments that organizations aren't aware of or have no visibility into, securing data has become a challenge.

Sensitive Data is everywhere

Sensitive data is everywhere – file shares, personal drives, email, database, cloud storage, backups – and access control to such data is often inadequately implemented.
With a globally distributed workforce, organizations need to make data available to employees working in different locations and timezones, and to devices not directly controlled by the enterprise. This data needs to be safeguarded, but it also needs to be accessible when it's needed. Additionally, organizations need to comply with an ever-growing array of industry standards and regulations.

This has necessitated the adoption of security models that center around the data, with a focus on granular, attribute-based access controls that ensure that no unauthorized entity gets access to business-critical data.

The landmark US Executive Order (EO 14028) on "Improving the Nation's Cybersecurity", released in May 2021, talks about the necessity to advance toward Zero Trust Architecture to meet current security challenges. "The Zero Trust security model eliminates implicit trust in any one element, node, or service and instead requires continuous verification of the operational picture via real-time information from multiple sources to determine access and other system response." The data-centric zero trust model assumes that a breach is inevitable or has already occurred, and limits users' (including devices and applications) access to only the data or resources that they need to do their jobs. Every access decision needs to be based on the principle of leave privilege and access control enforcement needs to be as granular as possible.

CISA's Zero Trust Maturity Model, created in response to the 2021 EO says, "Zero trust presents a shift from a location-centric model to a more data-centric approach for fine-grained security controls between users, systems, data and assets that change over time." As a first step, organizations should inventory, categorize, and label data and protect this data on devices, in applications, and networks.

Why network-centric security is not enough

Security experts agree that breaches are now inevitable and more a matter of "when" than "if". What this means from a security perspective is that organizations need to be prepared to

protect their crown jewels from attackers who bypass perimeter controls and are already inside enterprise networks.

Traditional approaches to security would focus primarily on responding to external threats and regulatory compliance needs. Additionally, preventive controls and perimeter defenses designed to keep threat actors out of internal networks were the central component of security programs. The threat landscape today, however, is completely different from what it was a decade ago. Organizations are becoming more reliant on cloud-based applications and data handling, and workloads have moved from centrally managed devices on-premise to employee-controlled BYOD laptops, tablets and smart phones.

More organizations are adopting hybrid and flexible work models. Because enterprise systems and operations are no longer restricted to a specific physical location and a single network, network-centric security models can't meet present-day security needs. While network controls remain the first line of defense and are important to the success of a well-rounded security program, it is the data that is the key asset to secure, not the network.

The zero trust model works on the assumption that all networks are compromised, and brings security controls as close to the data as possible with granular access controls. The reason data-centric security works so well in current digital environments is that not only does it protect data against unauthorized access, it also allows authorized users to access the data they need without roadblocks and usability challenges.

You can't protect everything

Zero trust implementation in a number of security-focused organizations today starts with identifying their "protect surface", which is smaller than the "attack surface" in that it is made up of only the most critical and sensitive assets that need protection. By understanding industry context and business goals, and focusing on the crown jewels that are most important to them, organizations can design security and risk reduction programs that protect against the most probable attacks, as opposed to protecting against all possible attacks, which isn't viable.

Controlling Risk from the Inside Out

Identifying and classifying data and internal assets by criticality and designing granular security and access controls around these assets is also known as the “inside-out” approach to risk reduction. In addition to a focus on critical data, the inside-out approach looks at the human element within the enterprise.

Most data breaches start with human error or social engineering/phishing attacks. Attackers take advantage of human weaknesses, laxity in patching, system misconfigurations and a whole range of preventable factors to get initial access to internal enterprise environments.

By enhancing visibility into data, assets, vulnerabilities and configuration errors, creating awareness, proactively mitigating security weaknesses, and strengthening granular access controls, organizations can fortify their internal defenses and become more resilient against cyber attacks.

Implementing an inside-out cybersecurity strategy

To implement an inside-out, data-centric security model, organizations must start with locating, classifying and labeling data; followed by devising and implementing access controls around data at rest and data in transit; monitoring data access and use at each stage of the data lifecycle and tracking policy and regulatory
compliance.

- **Data classification:** Organizations must know what data they have, where it is stored and for what purpose, and classify it clearly to be able to make access decisions in relation to the data deemed sensitive or protected.

    - Data may be classified based on sensitivity, location, type and format, compliance requirements, and other attributes based on business context. There may be data categories that are relevant or meaningful to certain kinds of organizations and not to others.
    - When creating access policies around data, security teams must focus on the most high-risk and high-value data, i.e., data that has the highest chance of being stolen or has the highest monetary value in underground criminal marketplaces, or data that is most critical to business.
    - Sensitive or critical data that needs protection must then be mapped to the applications that generate, use or manage this data.

    - Additionally, there must be policies identifying data custodians or departmental authorities who will make decisions about labelling and classifying the data.

- **Protecting data:** Data needs to be protected throughout its lifecycle – when it is first created, while it is at rest, when it is on the move or being shared, and at the end of its life. Granular access controls need to factor in a variety of attributes and consider who can access the data, from where, when, how and why.

    - When implementing zero trust architecture, organizations can extend role-based access control to the more fine-grained attribute-based access control. For this, data must be clearly classified.
    - It's advisable to use a combination of human input and automation that factors in user mistakes. Access control policies may consider things like whether a user's or a device's security clearance matches what the data label is set to; whether 2FA or MFA is enabled; the specific device or network that access is being requested from; a specific time range (work hours in a specific time zone, for instance) and so on.
    - User privileges must change dynamically based on ongoing mission or business requirements and the operational needs of organizations.
    - Because most data is generated and managed through applications, access policies must apply not just to users but extend to applications as well.

- Monitoring and compliance: Finally, data access and use must be monitored across the information lifecycle including creation, sharing/distribution, and deletion, with alerts set up for actions that are anomalous or suspicious. Organizations with centralized activity tracking and trend analysis can also generate more detailed and useful reports for both internal performance improvement and to demonstrate compliance.

Getting started with sensitive data discovery

CISA's Zero Trust Maturity Model envisions the optimal level of data security as providing for the following:

- Data protection controls on devices, in applications, and on networks.

- Inventorying, categorizing, and labeling data, and protecting data at rest and in transit
- Continuous inventorying of data with robust tagging, tracking and categorizing
- Dynamic access to data supporting just-in-time and just-enough principles, and continual risk-based determinations.
- Encryption of all data at rest.
- Logging and analyzing of all access events for suspicious behaviors
- Enforcement of strict access controls for high-value data with all high-value data backed up regardless of its storage location.
- Automatic updating of data inventories.
- Data access authorizations defined using a fully unified approach that integrates data, independent of source.

It is clear that data inventorying, tracking and categorization are critical to the success of a data-centric risk management strategy, and this starts with an organization locating sensitive data in its environment – whether it is in the cloud, on premise or within its email environment.

From an implementation perspective, this would involve scanning enterprise systems and devices for sensitive data like financial information, PII, credit card data, SSNs and more to find sensitive databases that may be stored in plaintext without the knowledge of business owners.

Modern risk management tools like CYRISMA allow security teams to conduct quick scans on selected systems and cloud environments (Office 365, Google Workspace, etc.) to find any sensitive data stored on them that needs to be protected. This data can then be graded and classified based on volume, type, and business impact, and either deleted or encrypted to protect against breaches and ransomware attacks. This allows organizations to find where sensitive data is located and take measures to protect it before it gets into the wrong hands.

CYRISMA's sensitive data discovery scans allow users to choose from 150 different file extensions in the cloud, on premise and within their own email environments. Security teams can select systems and machines/targets to run scans on, include or exclude file types and folders, and select specific data categories to look for from an extensive list of options.
With powerful data sensitivity scanning solutions like CYRISMA's, organizations can discover, understand, mitigate and manage vulnerabilities and security gaps arising from sensitive data stored in plaintext in enterprise environments, ultimately reducing risk and providing security

teams with the kind of data awareness they need to design more effective access controls, develop strong security programs and make wiser investments.

Data-centric risk reduction at a glance

To create the right mitigation plan to reduce risk, security teams need to look at the following attributes using technology, processes, and human input:

Questions to ask:

1. Where is company data located?
2. How can the data be classified?
3. Are there multiple versions of the data?
4. Who has access to this data?
5. Is access open to anyone at any time?
6. Do the devices hosting the data have vulnerabilities?
7. Are the devices hosting the data securely configured?
8. Do these devices have some level of host integrity?

Mitigation steps:

1. Assign accountability to data owners (e.g., Department Managers)
2. Reduce the sensitive Data footprint
3. Patch identified vulnerabilities on devices
4. Securely configure devices
5. Respond to host Integrity alerts
6. Continuous awareness and education

Organizations must think differently when designing a risk reduction strategy. They need to evolve and adapt as their internal data footprint changes and as the threat landscape evolves. By regularly monitoring the status of their data – where it resides, in what form, how it can be accessed – and mitigating security weaknesses, organizations can reduce risk and become more resilient against attacks.

Key takeaways

Rapid digital transformation over the past several years has changed the way organizations operate and handle data. With workloads distributed across geographies and computing environments, network perimeters have blurred. Network-centric security controls alone have become infeasible and are too inflexible to allow day-to-day operations while also protecting data. While network protection remains important and is usually an organizations' first line of defense, the primary focus today has shifted to devising and implementing controls to protect critical data.

- **Zero trust security architecture:** The zero trust security model assumes that enterprise networks are already compromised, and focuses on designing access controls and micro-segmented networks based on the principle of least privilege.
- **Data discovery and classification:** For data to be protected and secured effectively, organizations must know what data they have and classify it clearly. They must put processes in place to maximize visibility, discover sensitive data in their extended environments, and define policies to label and classify the data based on business context, type, sensitivity and criticality.
- **Dynamic, attribute-based access controls:** Security leaders are adopting dynamic, attribute-based access controls to allow or deny access to data based on evolving business requirements and the operational needs of organizations.
- **Protecting data across its lifecycle:** Data needs to be protected across its lifecycle, from creation and storage, to distribution and sharing, to deletion or destruction. This is best achieved by devising access controls using a combination of technology, human input and repeatable processes.

By putting data at the center of their security strategy and taking an inside-out approach, organizations can reduce cyber risk more effectively and minimize the chances of a successful attack.