opentext™

Critical content protection and risk mitigation guide

Zero Trust Information Governance

opentext™

Contents

Introduction

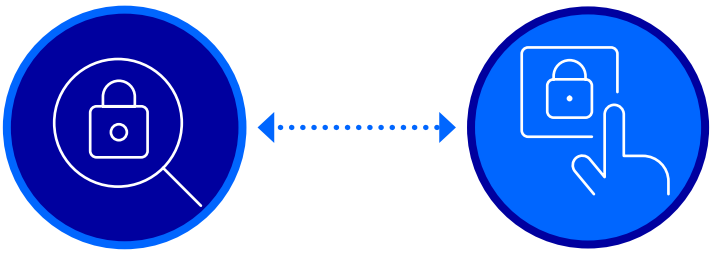
The gradual shift to an information-based economy has increased IT threats and organizational risks. Security professionals have made many advances in cybersecurity infrastructure, from two-factor authentication to deployment of intelligence and analytics in the realtime detection of threats. These improvements in cybersecurity have created strong perimeter defenses and intelligent, proactive threat detection for organizations, leading to common frameworks such as the NIST Cybersecurity Framework[2] and Zero Trust Architecture.[3]

> **"Zero Trust"** – A security practice that individually validates identity and grants the least functional level of access to each resource (such as applications and resources) and does not trust anyone from inside or outside the system.

Cybercriminals continuously evolve their techniques, relying on social engineering, phishing, ransomware and procedural vulnerabilities to access otherwise highly secure networks. In particular, vulnerabilities and threats such as ransomware are specific to content, such as access to email, documents, images, records or data. Zero Trust practices contrast with cybersecurity efforts that focus solely on a role, identity, resource or region, leaving the protection of atomic units of data or content up to the users. Application-level trust models are insufficient to cope with the current threat level.

Leaking or mishandling content and data can lead to high-profile and costly consequences for organizations that include fines, sanctions, job loss and even the organization's very existence at risk.

Improving risk/vulnerability assessment or management is the top strategic initiative for information security in 2022.[1]



A record 1,862 data breaches occurred in 2021, with 22% of breaches occurring through ransomware attacks.[4]

Threat vectors expand with each new application, integration, upgrade or digital transformation project, often in ways that are not readily apparent. Adopting information governance best practices can greatly reduce these risks while improving productivity. This guide provides a foundation for reviewing the intersection of governance and cybersecurity, as well as recommendations to reduce the risk profile of information.

As a first step, consider the following questions:

- What is missing from the organization's approach to network security?
- How are information repositories threatened independent of the network?
- How is security systemically applied to content?
- What information governance policies referencing security are in place?
- What steps will proactively to reduce risk and secure content?

A fully implemented and well-equipped information governance system helps to strengthen a security posture for an organization's content. Knowing where risky content exists on the network, classifying and preserving that content according to a detailed records policy, and placing an active governance automation system in place are essential to a complete cybersecurity plan and mastering information protection.

opentext™

Considerations from the NIST Cybersecurity Framework

The **NIST Cybersecurity Framework Core** establishes essential activities of cybersecurity infrastructure. Highlighted below are some of the key activities that can drive secure information governance policies and proactive automation, ensuring better protection of organizations' content.

Identify	Protect	Detect	Respond	Recover
Asset management	Access control	Anomalies and events	Response planning	Recovery planning
Business environment	Awareness and training	Security continuous monitoring	Communications	Improvements
Governance	Data security	Detection processes	Analysis	Communications
Risk assessment	Information protection processes and procedures		Mitigation	
Risk management strategy	Maintenance		Improvements	
	Protective technology			

Including governance solutions in the cybersecurity mesh

A modern trend in cybersecurity is the concept of the "cybersecurity mesh," a technique that establishes security in more atomic and purposeful domains at the service and server level, in addition to endpoints and the network perimeter. Gartner research VP Peter Firstbrook recently cited cybersecurity mesh[5] as a top trend in security and risk management. Another long-running trend that speaks to practice of "zero trust" is building security controls as close to the data as possible.

A robust content services infrastructure combined with attention to governance, privacy and process-centric handling of content can fundamentally improve cybersecurity and reduce the organization's risk profile.

opentext™

How can organizations apply these principles to the totality of their information assets, including their documents, images and other unstructured data?

Essential foundations to protect content through governance

ARMA Generally Accepted Recordkeeping Principles®

Starting with a documented and defensible recordkeeping foundation is essential to an effective information governance program. Organizations planning their governance program should refer to ARMA International's Generally Accepted Recordkeeping Principles®.

The principles are as follows:[6]

- **Accountability** – a senior executive or equivalent is accountable to the plan
- **Transparency** – the plan is documented and verifiable
- **Integrity** – there is a reasonable guarantee of authenticity and reliability
- **Protection** – protect assets that are private, privileged or business-critical
- **Compliance** – the plan complies with laws, authorities and policies
- **Availability** – information retrieval is timely, efficient and accurate
- **Retention** – information is retained for an appropriate time
- **Disposition** – information is disposed of securely and with documentation

Modernizing recordkeeping programs to promote information protection and security

With fully capable information governance solutions, organizations can more easily adopt recordkeeping principles and build a robust information protection program. Organizations must consider the entire information lifecycle while building such a program and should seek out proven, complete information governance solutions that support the following information protection fundamentals:

Know where and what information you have

It's nearly impossible to tailor the security of an organization's information without knowing exactly what that information is, how it is incorporated into processes and the specific compliance requirements for each record type. Effective classification requires that relevant and consistent metadata can be discovered and applied and that a meaningful process exists to action on a records policy.

opentext™

Did you know?

Organizations can face substantial fines for retaining information longer than necessary. In a single recent case, authorities in three different jurisdictions entered into a **$500,000** settlement with a website operator who held personal information beyond the allowed retention period.

Comply with evolving data protection and privacy regulations

Ensure that written policies adhere to all privacy and data protection requirements for the jurisdictions in which the information is processed. This can be a complex, and sometimes even contradictory, series of requirements that apply differently based on jurisdiction, region and regulatory authority.

Regulations evolve rapidly and should be reviewed regularly by both legal and risk professionals. Modifications to records policy and automation rules must be kept up to date.

Proactive and accurate classification of content can trigger automatic controls and encryption, such as digital rights management, and save the organization from hefty fines.

Implement retention policies and follow through; don't over-retain content

Many organizations are still holding onto terabytes, or even petabytes, of legacy files because they do not have enough context assigned to the content to decide what to dispose of and what to keep. Paralyzed by lack of classification, they hold risky assets in perpetuity, creating ongoing information risks.

Dispose of information in a defensible manner

When it is time to discard information, the organization must ensure that content is disposed of in a defensible manner. That means that the reason for the disposal should be logged, and all copies of the information—no matter where they are kept—should be destroyed. The only exception to this is when information has a valid and documented legal hold.

A common error is assuming that the content has been disposed of appropriately through a records repository while failing to remove convenience copies that have accumulated through content sprawl and careless handling (e.g., on user laptops).

Automate access control to the content

The goal is to have the most accurate access control assigned to each document possible. Manual efforts result in incomplete and inaccurate access controls in large user populations.

Establishing more accurate access control is best accomplished through templates and automation that grant access to content based on a "need to know" approach. The focus should be on roles and groups rather than individuals whose roles may change over time. This can protect the organization against systematic attacks on "loose content" and ransomware. Granting public access to content may seem convenient, but it is almost never an appropriate approach.

Manage access vertically and horizontally with security markings

While a bottom-up ("need to know"), automated approach to granting access to content is essential, another check on content is a security marking, which should align content types to roles within the organization.

For example, even when granting broad access to content within a folder, it is advisable to mark content containing sensitive data, such as personally identifiable information (PII) or personal health information (PHI), as a further check on a folder-based access control template.

opentext™

Did you know?

Under the GDPR, a severe violation of the GDPR for failure to protect personal data can result in a fine of up to **€20 million**, or up to **4% of the organization's total worldwide annual turnover of the preceding financial year, whichever is higher.**[7]

Protect content in flight

Content is meant to be shared, but protecting that content beyond the firewall, or even within it, can be nearly impossible if it is shared unencrypted (as "plain text"). Attaching and enforcing security from within the file through digital rights management provides an additional security measure. When accurately applied, it protects against data leakage and even certain social engineering and phishing attacks.

Secure content when it is being handled or processed by third parties

As the primary custodial entity for information, organizations may be exposed to increased legal liability for careless handling of sensitive data by partners and contractors.

Ensure that when information flows to partners and third parties, they have a contractual obligation to adhere to published policies on the data they possess. Alternatively, contractually obligate them to process data only within a closely monitored, protected environment that the organization manages according to the policy.

Ensure complete and accessible auditing

Having complete, meaningful and ready access to audit trails is essential to good information governance. Monitoring, event investigation and documentation of events require robust audit trails.

Proactive steps to achieve Zero Trust Information Governance

With comprehensive content services that combine a secure infrastructure with intelligent automation and proven governance controls, organizations can implement a robust information protection regimen and instill zero-trust principles into business processes. Capabilities that indicate an organization's content services can achieve this level of protection include:

1 Organize content management controls around meaningful business events

Standardizing business practices and content organization by well-understood, repeatable business entities such as clients, projects or events can help an organization deliver predictability and enhance user participation and compliance.

When the organization has an established, repeatable process that demands secure handling of content, the system should be able to naturally apply appropriate information protection controls. Automating content classification and access control within such business processes is much simpler and far more reliable than depending on user compliance.

2 Fully engage robust governance controls

It is essential to proactively and accurately classify content and oversee its lifecycle. All information should be under management, even long forgotten information, that is more likely to be leaked. Keeping PII and other sensitive data beyond its necessary retention period puts the organization out of compliance. Ensure that written records policies are automated, and when possible, connected to sources of business transactions that can trigger on time and accurate disposition.

opentext™

Did you know?

Pre-built AI models can help identify many types of risky content and take action:

- Personal information, such as IDs, credit card info or tax data
- Sensitive data, such as racial or ethnic origin or political opinions
- Potentially inflammatory images, such as violence, alcohol or firearms

3 Extend governance controls with active rights management

Ensure that security clearances and markings are relevant by employing digital rights management explicitly driven by the organization's governance policy and classification system. Content services should retain and fully embrace security controls within systems that they integrate with, such as Microsoft 365®.

4 Assess risk continuously with intelligent content analysis tools

Content must be constantly monitored for compliance, and policy must be assessed for gaps in coverage. The volume of information to be reviewed likely requires automated tools to facilitate ongoing assessment and drive content and policy review priorities. AI, natural language processing, image analysis and more integrated content analytics can help identify and measure risk levels and areas to investigate further.

5 Bring unmanaged content into compliance and under a proactive security plan

Legacy network file shares and repositories with terabytes of unmanaged content represent an unacceptable risk to any organization. Organizations should initiate a program to bring all unmanaged content under the control of governance.

Strong auto-classification, data mapping and discovery tools can help remove redundant, obsolete and trivial (ROT) content and preserve only necessary business records. This proactive control helps protect against disruptions caused by ransomware as well.

opentext™

Additional resources

- Webpage: Information Governance
- Webpage: Privacy Management
- Webpage: OpenText™ Magellan™ Risk Guard
- Blog: Master modern work with stronger information protection

Strengthen content protection through governance

Developing a strong cybersecurity infrastructure for an organization requires evaluating risk wherever it arises. Certainly, there are many external threats that must be addressed with the most modern cybersecurity practices and tools. However, much of the risk in many organizations can be measured in the unnecessary and unwitting exposure caused by unprotected personal and sensitive data.

Strong governance practices and intelligent automation can strengthen an organization's cybersecurity posture and reduce the organizational risk. By mastering information protection, organizations can remain in compliance with constantly evolving regulations related to data privacy and security. They can also adapt quickly to other emerging risks.

Master information protection with OpenText

About OpenText

OpenText, The Information Company, enables organizations to gain insight through market leading information management solutions, on-premises or in the cloud. For more information about OpenText (NASDAQ: OTEX, TSX: OTEX) visit: opentext.com.

Connect with us:

- OpenText CEO Mark Barrenechea's blog
- Twitter | LinkedIn

1 Kennedy, D., Key Security Trends 2022: Recent Research from VotE: Information Security. (2022)

2 NIST, CyberSecurity Framework

3 NIST, Zero Trust Architecture. (2020)

4 Identity Theft Resource Center, Annual Data Breach Report. (2022)

5 Gartner®, The Top 8 Security and Risk Trends We're Watching. (2021)
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

6 ARMA, The Principles®. (2017)

7 GDPR.EU, "What are the GDPR Fines?". (2022)