Netwoven

eBook

Data Security and Governance

6-Steps to kick start your initiative

Create a Data Security and Governance Strategy for your business or lose your business

Data breaches are not new, and I am sure you have heard about it in the news frequently. Just to refresh your memory, organizations experience data breach incidents in many scenarios. According to statistics, the top three causes of data breaches are

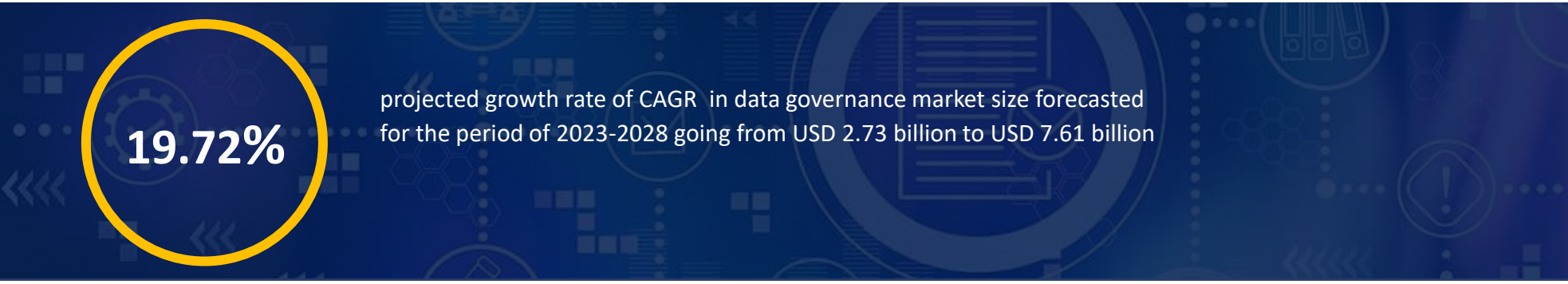
- Threat actors attack on company with the intent of stealing sensitive information
- Unintentional error by an insider
- Malicious insider accessing confidential and sensitive information.

The average cost of a data breach incident across companies worldwide is 4.45 million U.S. dollars. This includes detection, business losses, post-breach response, and notification.

Your sensitive data could reside in any of the repositories below:

- Cloud Repositories like Dropbox, Box, OneDrive, and Google Drive
- On-Prem Repositories like NetApp File shares
- On-Prem Applications with Databases
- Cloud SaaS Applications
- Digital Products you provide to your customers

Technology has matured significantly to offer solutions to the problem of data protection and governance irrespective of where it resides or how it is being acted upon.



6-Steps to jump start your data security and governance initiative

Gartner defines data security governance (DSG) as “a subset of information governance that deals specifically with protecting corporate data (in both structured database and unstructured file-based forms) through defined data policies and processes.”

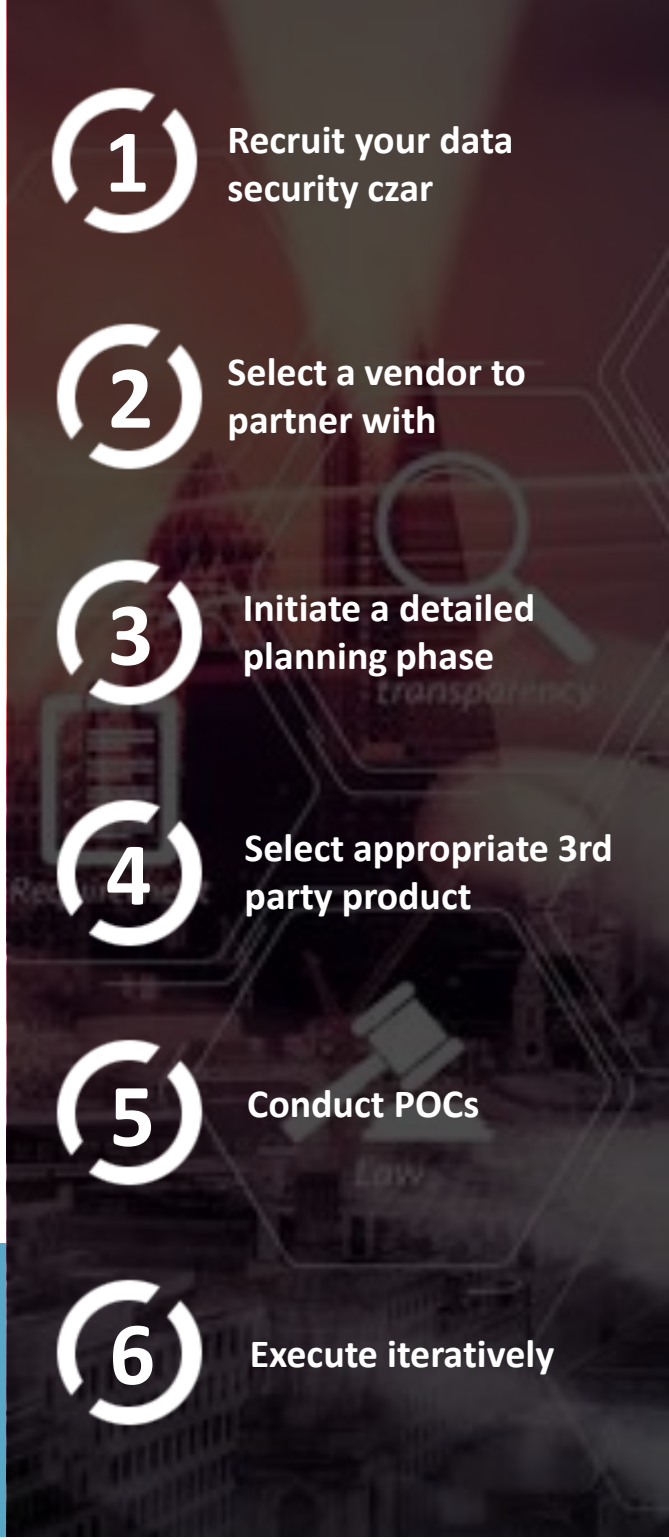
So, what is the best way to go about it?

The challenges are plenty. Enterprise data changes continuously in its form, size, usage and residence. It drifts in the cloud, crosses boundaries of business units, enterprises and glides everywhere.

The choice of technology today is so vast that picking up the right tool for your purposes could be daunting. Also, the internal team can easily get overburdened to define, execute and manage data security and governance activities.

You must identify your sensitive information, fortify your foundation, shield and protect your data and finally safeguard and govern those.

Netwoven, an accredited member of Microsoft Intelligent Security Association (MISA), recommends few key steps to be taken to secure and govern your data incrementally through a well-crafted program, designed from a practitioner’s standpoint.



4,100+

publicly disclosed data breaches ooccurred in 2022 equating to approximately 22 billion records being exposed

1. Recruit your data security czar

This is the first and most important step you can take for this initiative. This person should not be the typical data person or the security person but someone that has a strong data background and has developed security knowledge (It's hard to go the other way).

The responsibilities, for example, would include:

- Prepared to serve as the single point of contact and has knowledge and accountability for both technical and policy-oriented security issues and their solutions
- Any online business has data protection obligations with respect to third-party scraping. The security czar's role would be to identify and implement controls to protect against, monitor for, and respond to scraping activities, be it on the web or in social media
- In jurisdictions where the data scraping may constitute a data breach, the person would be responsible for notifying affected individuals and privacy regulators as required.

37%

of security professionals say lack of qualified staff is the biggest roadblock to faster adoption

28%

of enterprises consider security to be the most important criterion when picking a cloud vendor.

2. Select a vendor to partner for your Data Security and Governance

Data security initiatives are complex and require careful planning and execution. It requires knowledge of systems, data, security, infrastructure, and organization to define a plan that can be successfully executed. By partnering with external consulting organizations, companies can benefit from the experience and reduce risk. These consulting organizations can be of any size. There are several small companies specializing in data security that you can partner with. These companies are flexible, have the focus, and are specialists to deliver your projects successfully.

When selecting a cloud security provider, organizations say they look for:

- Cost effectiveness (63%)
- Ease of deployment (53%)
- Security tools are cloud native (52%)

It is also essential to build a synergistic relationship between your organization and the chosen 3rd Party vendor. The synergy must be holistic sharing each others knowledge and expertise in a wide array of areas like tools and technology, data management practices, regulatory compliance etc.

The overall cost savings and the benefits derived for your organization by engaging a partner must stay focused on the following such that the vendor

- Provides substantial reduction in risk of breach-related costs
- Greatly reduces technology and licensing costs
- Eliminates staffing and training costs
- Utilizes up-to-date cyber security practices and technology
- Administers a scalable solution
- Provides continuity of support

3. Initiate a Data Security and Governance planning phase

Planning phase of a data security and governance initiative requires defining the overall goals, and success metrics of the initiative with the CISO. It also requires meeting with stakeholders from various business functions such as legal, finance, HR, IT, supply chain, engineering, security, and operations to collect relevant information about business processes, types of applications being used, data being collected and some insight into any past security breaches that may have occurred. Partnering with the vendor helps obtain standard templates, procedures, best practices, and tech stack knowledge to accelerate your project and avoid any pitfalls. Upon completion of the planning phase, one should have a clear idea of the business benefits, and roadmap that can be executed iteratively.

It may be worthwhile to take a note of the industry standard framework that is available to undertake such activities.

Source: DataGovernance

It is also important that risks are prioritised so that security efforts are focused on business priorities rather than their own.

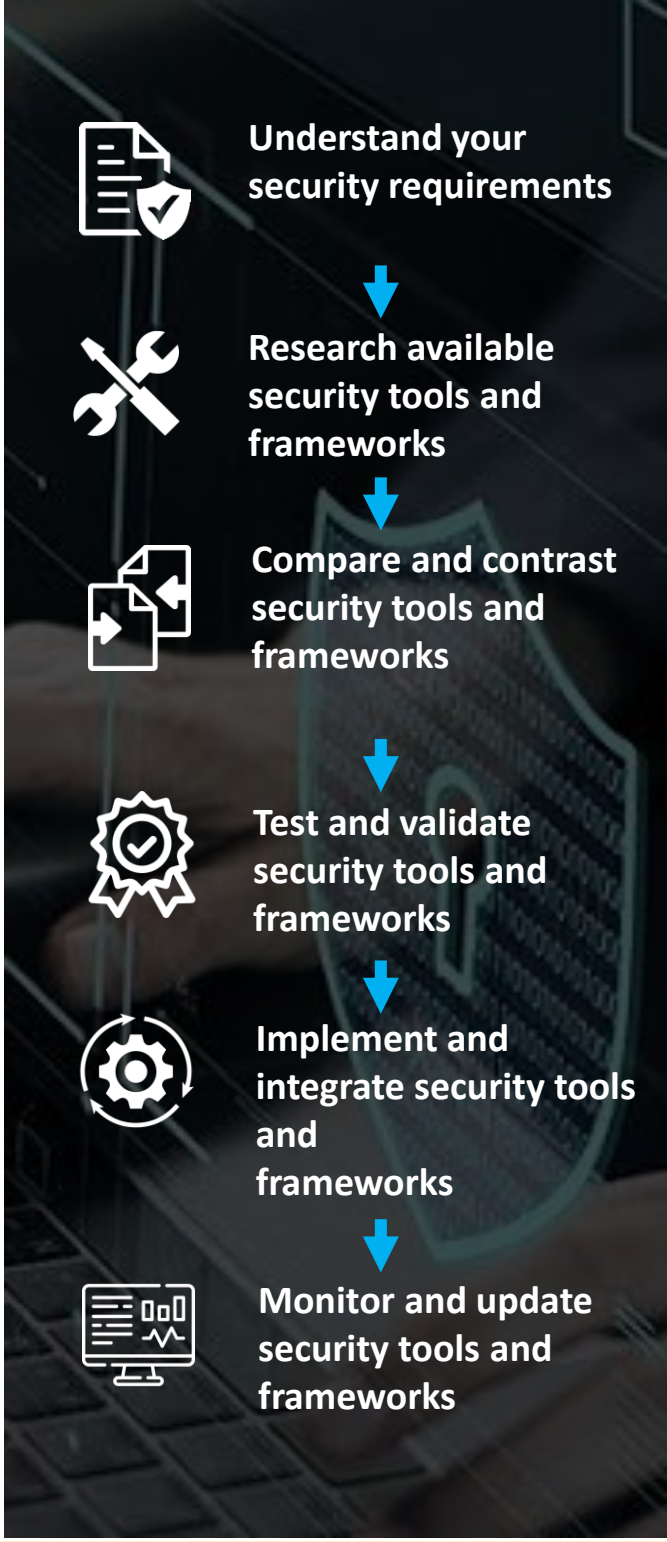
84% of digital transformation initiatives in business enterprises fail

25% of respondents say length of the project/delivery time is the most significant challenge

4. Select appropriate third-party products

Several tools will be required to implement your data security and governance solution. These will include tools like classification tools, scanning tools, DLP tools, and encryption tools. Your vendor should help you define your requirements to help identify and select the right tools. These tools will remain with you for quite some time so it's important to select them properly. Your selected vendor should have templates, and best practices to help with the selection process.

1. Understand your regulatory compliance requirements well. These are the standards, regulations, and policies that apply to your organisation, such as GDPR, PCI-DSS, HIPAA, or ISO 27001 or anything else.
2. identify the threats, risks, and vulnerabilities that your enterprise faces, such as data breaches, denial-of-service attacks, or malicious insiders.
3. Look for all the functionalities that you need, such as encryption, authentication, auditing, or monitoring. Do some due diligence using online reviews, blogs, forums, or podcasts to learn about the pros and cons of different security tools and frameworks.
4. Compare and contrast the alternatives based on various criteria, such as functionality, compatibility, performance, usability, scalability, cost, support, or documentation. You should focus on the basic metrics such as return on investment (ROI), total cost of ownership (TCO), or security maturity model (SMM) to quantify and measure your comparison.
5. Use methods such as proof of concept (POC), pilot, or sandbox to test and validate the shortlisted security tools and frameworks in a controlled environment.
6. Evaluate the details of installing, configuring, and connecting the security tools and frameworks with your existing infrastructure, and processes.
7. Look at the effectiveness of the facilities of tracking, measuring, and improving the performance, and security of the proposed security tools and frameworks.



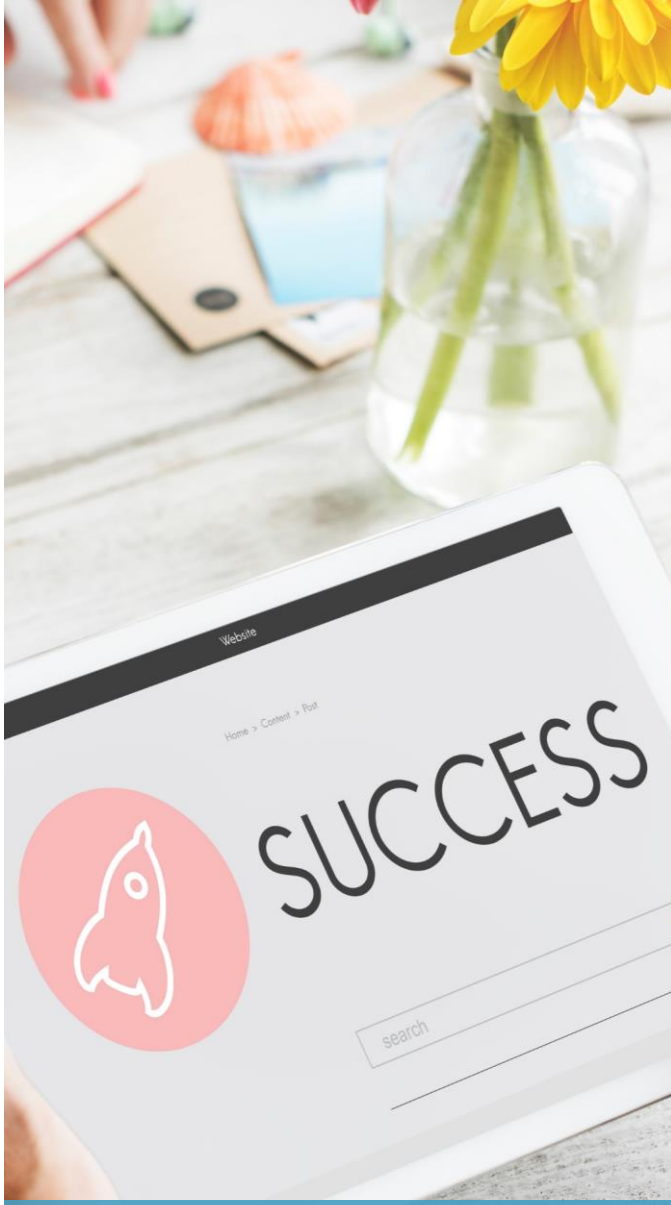
5. Conduct PoCs

Conducting PoCs is always a good best practice. Once the tools are selected, a POC environment should be created with test data and test users to prove out the solution, and its results. The PoC phase helps refine the overall approach and increases the chances of project success.

To obtain meaningful PoC results, you should pay attention to the following:

- Understand the needs of your company's Lines of Business (LoBs) and the stakeholders who need the security solution capability
- Agree on the goals
- Select important use cases that are complex enough to present a challenge
- Determine the scope and key performance indicators to measure the success of the PoC
- Perform an objective measurement of the vendors' efforts based on a clear set of rules and an appropriate checklist
- Drive vendors to install and deliver the PoC in your test environment, not on an artificial demo landscape
- Set a competitive but reasonable PoC timeframe in accordance with your use case
- Gain internal support, time, commitment and focus
- Ask the vendor for reasonable documentation and knowledge transfer. This will support you to entirely test and evaluate the delivered PoC

Proceeding this way, a meaningful PoC verifies that the proposed solution can meet the specified challenges and address the use cases in your environment. This brings your stakeholders on-board and provides confirmation before you sign contracts and close the deal. Thus, a PoC reduces your risk of selecting the wrong IT solution.



50%

And more of Proof of Concepts fail

6. Execute iteratively

In this phase, one should refine the roadmap created during the planning phase with inputs from the PoC phase. Each iteration should be well defined with the user requirements, detailed design, and execution plan along with a rollout plan. Each iteration could be geography based or business unit based depending on your organization.

The value of an iterative execution methodology lies in recognizing the following.

- Major requirements are defined at the onset, but some functionality may evolve over time
- Most risks can be identified during iteration and higher risks can be dealt with as an early priority
- Goals are subject to change over time
- Time-to-market is critical for success
- Innovative technology is involved, and some unforeseen issues are expected
- Progress is easily measured
- An operational artefact is delivered with every iteration
- It allows an organization to organically grow its security governance structure
- Customer feedback is based on working products rather than technical specifications

Case Study

Data Governance Transformation at a Global Electronic Manufacturing Company

Company embarked on a data governance program and contracted with Netwoven to help define a data governance strategy and use Microsoft Purview to implement it since they owned Microsoft Purview.

Read the case study

Why Netwoven?

Data Protection execution is full of challenges, but you can overcome them using Netwoven's proven methodology and experience.

- Implemented a comprehensive Information Protection program to protect sensitive data for a Fortune 1000 company
- Migrated 45000 Mailboxes and migrated M365 tenant for a large Fortune 1000 hospital

Microsoft Solutions Partner
Security

Specialist
Identity and Access Management
Information Protection and Governance

Microsoft Solutions Partner
Microsoft Cloud

Member of
Microsoft Intelligent Security Association
Microsoft

"The client has taken a comprehensive approach to protecting sensitive information both inside and outside the organization while ensuring there was no impact on collaboration. Netwoven's extensive technical expertise and willingness to work with Microsoft's product engineering combined with their unique approach to designing solutions with a business-centric view allowed them to make the best use of Microsoft's offerings to meet the company's information protection needs. "

Enrique Saggese
Principal Program Manager, Microsoft

Next Steps

Book a complimentary security workshop with our experts to understand the Microsoft security stack and learn how you can modernize your security infrastructure and improve your security posture.

+1 877 638 9683

info@netwoven.com

netwoven.com

About Us

Netwoven

We shepherd organizations safely through the cloud transformation journey by unraveling complex business problems.

By partnering with us, our clients securely collaborate globally, improve business operations, build new products and solutions with deeper insights, and reduce cyber security risks.

Acknowledgement

- cshub
- Titanfile
- mordorintelligence
- purplesec
- ispartnersllc
- Dataservicesinc
- datagovernance
- Webinarcare
- gartner
- Linkedin
- Seeburger
- one-beyond
- sapphireventures