Report

EXONAR

How to strengthen information security with data discovery

How to strengthen information security with data discovery

Today, every company is a data company. Every business, no matter which sector it claims to be in, is producing extraordinary amounts of data which is growing in size every day. We are all operating in the information age and data has become the most valuable commodity a business owns. There's so much value locked away within it.

With massive increases in data comes risk too. And when nowadays there's no longer a perimeter to protect, maintaining a strong security posture is challenging.

The problem most organisations have is getting visibility of their data at scale, right across the organisation. The sheer volume and complexity of data is a huge challenge. It's easy enough to find the data held in one data store, particularly when it's structured. Most storage comes with rudimentary data discovery. But it's perceived as impossible to get visibility of structured and unstructured data across multiple data stores for the purpose of securing it.

The reality is that the management of data is a concern for data security and governance professionals. With remote working becoming the norm since Covid-19, getting visibility of devices, users and who owns them is almost impossible. Which means nowadays, a lot of the burden of privacy and protection relates to securing the data that's held by the organisation, so getting to grips with it is crucial.

> **In this report we will show you how to gain visibility of your data at scale right across your data estate, so you can govern what's sensitive and use what's valuable.**

A key priority for security and data leaders in 2020

We were recently joined by data security and governance specialists, from leading UK companies in a roundtable discussion to identify their challenges. They said that insider threats and the need to lock down data at source was one of their major priorities. To read the report written after the event, **click here**.

> *"When I'm working on stuff, I ask where's the trust in the employee? Where do you draw the line saying, 'I trust you as the employee', because you have to?"*
>
> European Data Privacy Officer for a bank specialising in wholesale assets

Security Threats

All it takes is one mistake. Sensitive customer data saved in a spreadsheet on a local drive. A written down password. A file wrongly shared...

The average size of a data breach increased 1.8% to more than 24,000 records compared to the previous year.

Source: The Ponemon Institute

Data security remains a top business priority for good reason, because a single small mistake can lead to lasting reputational damage that's costly to repair.

In the ideal world organisations would be able to protect themselves against a breach happening at all. But everyone knows that there's data lying unprotected all over any business leaving it exposed and vulnerable.

Therefore, for organisations to ensure that their data is adequately protected, they need to know what data they've got, at scale, right across their estate including structured and unstructured information.

Once the data is discovered, organisations can lay the foundations for comprehensive data security.

So in an age where securing the perimeter becomes redundant, where should the security focus be?

The insider threat

The biggest threat to data is your people. 66% of cyber breaches are caused or enabled by employee negligence or malfeasance.

World Economic Forum

In simply performing their jobs, employees can become the 'unintentional internal terrorist' because they negligently keep and store high-risk information, and leave it unprotected in the wrong place.

More common is employees sending sensitive data outside the business by accident, in the process of trying to get their jobs done. However, businesses cannot expect their employees to understand data management or how to protect data in huge detail, especially when nearly everyone is working from home. A basic understanding of data protection: yes. But expecting people to adhere to the highest standards and intensive detail around data governance is unrealistic.

There is a balancing act to be undertaken to weigh the merits of robust data protection against productivity. The internal environment needs to be opened up so people can work effectively and efficiently whilst at the same time protecting data.

Not all data is stored in locked down databases. Yes, there will be a number of CRM and storage systems in place for sales, finance and HR that keep everything ordered and structured - some on-premise, others in the cloud.

But what about all the emails that are sent, and the documents that teams creates every day, which aren't maintained in organised databases? And the fileshares such as SharePoint and OneDrive, the company intranet and personal folders?

It's this unstructured data that is the point of weakness, leaving organisations vulnerable and exposed. Our research suggests that a typical organisation's unstructured information contains:

- **42% confidential information.**
- **1% sensitive personal information.**
- **9% personally identifiable information.**

Therefore, it becomes the responsibility of the company to put systems and processes in place to protect its data. Businesses need to provide the right methodology, technology, and processes that enable the workforce to continue to operate without having to follow undue data process and procedure. And this starts with knowing your data.

Things to think about...

- **Do you know what data is in your estate?**
- **Do you know where all your data – particularly unstructured – is stored?**
- **Do you know who has access to your data?**

The external actor

Every CISO knows that it's not a case of 'if' there's a breach, but 'when' hackers try to break into the data estate from the outside.

Threat actors have something that none of us do: **time.** The average dwell time of a hacker who gains access to a network is 10 weeks. Generally once on the inside, they can move around with relative ease. They observe behaviour and activity before they grab the goods.

A large organisation can have literally thousands of systems and storage facilities. And keeping on top of them all is a huge challenge. Over time they can be forgotten. Unless they are known about and constantly secured, they are vulnerable to hackers determined to get inside and who are prepared to exploit the tiniest vulnerability to do so.

The risk is that forgotten systems may contain valuable or sensitive data that nobody is aware of and which represents a risk.

Data discovery: the enabler of more effective information security

So what's a business to do?

It's a fine balancing act. On one side, organisations must lock the business down to secure the data and protect it from harm. But on the other side, they need to open up the business to provide greater access to the information people need to do their jobs.

The answer lies in the data.

The fact is, no business can protect itself from an insider or external data breach until they get a handle on all of their data – both structured and unstructured. The first step has to be to discover what's there, where it's stored and whether there's sensitive data within it.

When an organisation has visibility over its data, they acquire the insights to determine what needs to happen to that data to protect it – whether that's nothing because appropriate controls are already in place, or taking remediation actions to either move the data or delete it with confidence.

Then by wrapping the right methodology, technology, and processes around the data, the business empowers its employees to continue working in any way they choose, without having to follow undue data process and procedure. And the business doesn't need to worry, because if people start to do something risky with the data, they'll be nudged to do the right thing, in the moment.

By gaining visibility over all the data lying within the estate, a business can prioritise its risks, take action to protect the data at source, and in addition reveal the value in its data too.

> *"Data should be used to protect and power organisations and the people they serve. When an organisation becomes information intelligent, it's able to secure data, extract its value and manage the ongoing complexity of its data estate."*
>
> **Danny Reeves, CEO, Exonar**

Laying the foundations of a model for stronger information security

The journey towards effective security must encompass people, process and technology. The following is a model that we've created, which helps organisations to successfully lay strong foundations to build a more effective information security strategy:

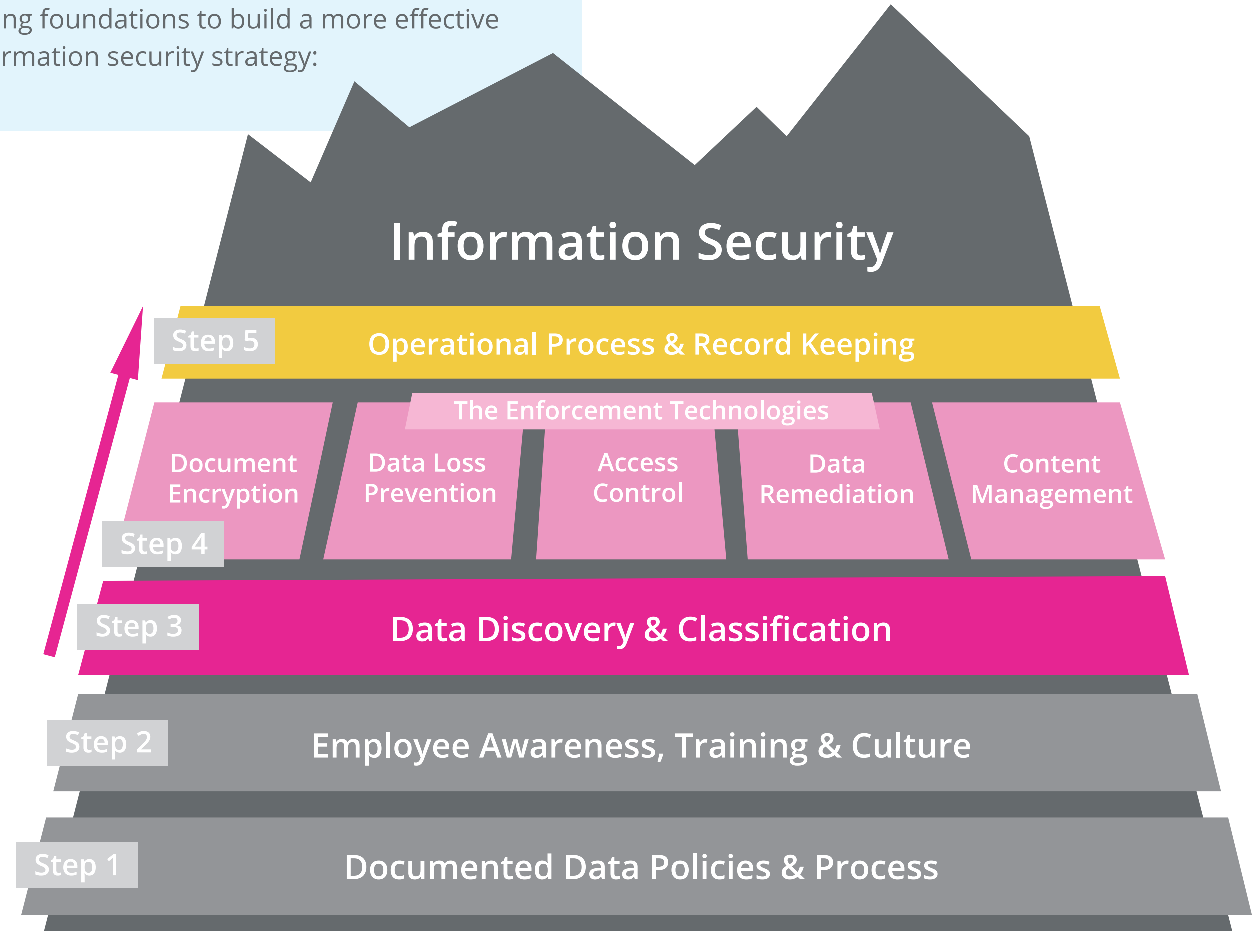

Information Security
Step 5
Operational Process & Record Keeping
The Enforcement Technologies
Document Encryption
Data Loss Prevention
Access Control
Data Remediation
Content Management
Step 4
Step 3
Data Discovery & Classification
Step 2
Employee Awareness, Training & Culture
Step 1
Documented Data Policies & Process

Figure 1: *Laying the strong foundations of the 'information security architecture model' enables organisations to build and maintain a strong security posture to protect data inside the estate.*

Step 1: Documented data policies and process

The first step towards a stronger security posture inside the data estate is to create the policies and processes that set out the intentions for how the organisation will deal with its data. These lay the bedrock for successful data security and governance.

From speaking with several data and security professionals, we're finding that while most organisations have documented data protection and privacy policies in place, a lot were simply a way of ticking the GDPR compliance box. When it comes to enabling business-as-usual, these policies fail to support people in carrying out their day-to-day duties. One of the biggest areas of concern this leads to is retaining data 'just in case' because people don't have the confidence to delete.

> *"One of the biggest challenges we have is how long data is kept for. Some people don't want to let go of it in case it has value in the future."*
>
> Digital Data Director
> Quoted in 'The Great Data Conflict'

By taking the time to evaluate their current policies and processes, organisations have the opportunity to re-think data privacy and how it can be ingrained into business-as-usual in a way that helps their employees to do the right thing with data.

Things to think about...

- **When was the last time you reviewed and updated your privacy policy?**
- **How confident are you that data is always handled in accordance with your policies?**
- **Do you know who has access to your data?**

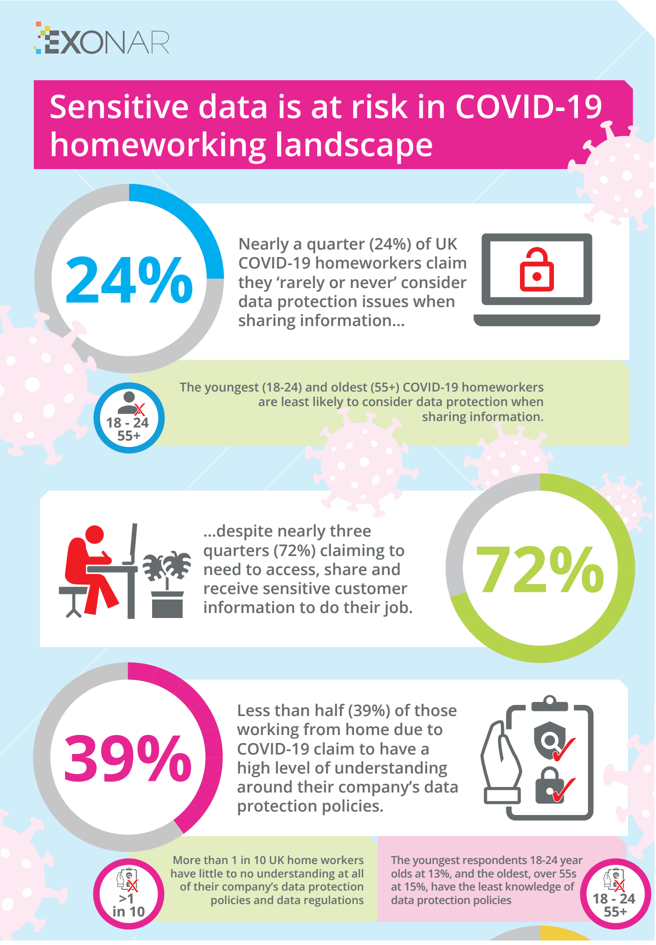
Step 2: Employee awareness, training and culture

As the ones on the frontline, it's an organisation's people who need to follow and enforce these policies as part of business-as-usual. Data security and governance should be so ingrained into people's thinking that it sits front and centre in their minds every day.

And yet our own research indicates that during COVID-19, 1 in 10 UK home workers have little to no understanding of their company's data policies, while 1 in 4 claim they 'rarely or never' consider data protection issues when sharing information.

When a policy is treated as a tick-box exercise, it's destined to sit in a fileshare gathering dust. Never looked at, never thought about, never enforced.

But when it's ingrained into a company's DNA, it becomes a part of the culture. When people understand why data protection and privacy is important, they actively want to take better care of it. In one of our roundtable events, the data governance and security professionals concluded that when an organisation talks about its data in terms of the people it represents, everybody – from the senior leadership team right through to the frontline staff – understand why it's so important and needs protecting.



EXONAR

Sensitive data is at risk in COVID-19 homeworking landscape

24%

Nearly a quarter (24%) of UK COVID-19 homeworkers claim they 'rarely or never' consider data protection issues when sharing information...

The youngest (18-24) and oldest (55+) COVID-19 homeworkers are least likely to consider data protection when sharing information.

...despite nearly three quarters (72%) claiming to need to access, share and receive sensitive customer information to do their job.

72%

39%

Less than half (39%) of those working from home due to COVID-19 claim to have a high level of understanding around their company's data protection policies.

More than 1 in 10 UK home workers have little to no understanding at all of their company's data protection policies and data regulations

The youngest respondents 18-24 year olds at 13%, and the oldest, over 55s at 15%, have the least knowledge of data protection policies

Read the research...

> *"When you engage with people, it's a different conversation."*
>
> Data quality and analytics expert
> Quoted in 'Managing data as an asset and a risk'

Things to think about...

- **If you asked an employee at random, would they know where to find your data policy?**
- **How confident are you that people are following that policy while working remotely?**
- **Do you believe data security and privacy is always front of mind?**

Step 3: Information discovery and classification

In the information age, organisations produce extraordinary amounts of data, which continues to grow in size every day. And while some of this data is neatly structured in protected systems and databases, the majority of it is lying unstructured across the estate, potentially unprotected against a breach.

Therefore, the priority for organisations is to identify exactly what data they have within the estate, because once they know what's there, where it is and who has access to it, appropriate remediation actions can be taken to:

- **Secure data:** keeping sensitive confidential and personal information secure.
- **Extract value:** mining intellectual property, research or insight within information and data.
- **Manage complexity:** managing the volume, such as migrating data to the cloud.

With Exonar, we've focused on how to provide unprecedented visibility of organisational data at scale, coverage and detail.

COVERAGE

Connect to all the most relevant data stores across your estate, no matter where or what it is, to get a truly organisation-wide view.

SCALE

Exonar Reveal creates an index of billions of items of your structured and unstructured data so you can search everything instantly.

DETAIL

Drill down to find the sensitive content of every item of information including the text in documents, not just the metadata.

Firstly, we do this by enabling our technology to index any data set within any type of data repository, so it becomes instantly searchable.

It's a bit like a reference book. Rather than start at the beginning every time to search for a precise piece of information (assuming the user even knows what this piece of information is), Exonar unlocks the power of the index. Now every piece of data is identified and recorded, with the technology constantly re-indexing the data to identify what's changed, what's new and to understand the context of the data.

We then enrich this index by adding content and meta data descriptions, before augmenting the index through:

- **Pattern matching:** resolves number and text patterns to identify information, like credit card numbers, government IDs, or phone numbers.
- **Natural language processing:** understanding and extracting the context of words, such as names, ethnicity and places.
- **Machine learning:** identifies or resolves additional contexts such as topics and types of document such as contracts or CVs.

It's the power of Exonar's indexing capability, along with the scale it can achieve with hundreds of billions of items across structured and unstructured data, that makes it unique in the data discovery space.

Organisations can't start to protect something until they know it exists, and only Exonar has the ability to identify ALL data sets – both structured and unstructured – allowing users to query the data in any way they choose and produce real-time search results.

Exonar is the layer in the technology stack that allows organisations to get the most out of their enforcement technologies. Because Exonar is focused on discovering data at scale, it's specifically built to plug into third-party systems to carry out the appropriate remediation actions, so users retain full control of their data estate and reduce the security threat.

Things to think about...

- **Do you know what proportion of your data estate is unstructured data?**
- **Can you identify risky data in your estate right now?**
- **If you have a data discovery tool in place already, does it enable instant, detailed search across all your data?**

Step 4: The enforcement technologies

There are 5 main categories of enforcement technologies that we see our customers using, alongside many others:

1. **Document encryption:** a powerful tool when organisations need to protect a single file, like an employee or client contract.
2. **Data loss prevention:** the ability to apply rules that are designed to prevent accidental loss, for example classifying confidential information so it's not shared outside the organisation.
3. **Access control:** assigning roles and responsibilities to individuals, which govern what data they're allowed to view, and the way they're allowed to interact and handle that data.
4. **Data remediation:** the ability to categorise, move or delete data at scale, to effectively 'spring clean' it and remove anything toxic from the estate.
5. **Content management:** enforcing what the organisation's policy allows to happen to its data, these tools support how to collect, process and share information within the business and externally with third-parties.

Having continuously evaluated the competitive landscape for well over a decade, we are yet to discover a 'one size fits all' data-related technology. Instead, different vendors focus on developing the best technology within their niche – whether that's data discovery or enforcement technologies – which is why organisations need to take a blended approach. By opening up the APIs and integration packs, organisations can build a bigger and better architecture that delivers effective information security with data discovery.

Action!

To discover more about the technologies covered in this section, watch our on-demand webinar:

'Why data discovery matters in a zero trust world'

Things to think about...

- **What enforcement technologies does your business use?**
- **How well do they integrate and support each other?**
- **Would you risk your job on them securing you against a breach?**

Step 5: Operational process and record keeping

Having discovered what data is within the estate, and integrated other technologies to take appropriate remediation actions, the final step on the path to becoming an information secure organisation involves adding a layer of operational process and record keeping.

Once the organisation starts to record KPIs for internal auditing purposes, it enables the business to monitor and better understand its data on an ongoing basis so it can identify areas for continuous improvement.

> *"Group wide, our programmes are all dependent upon having clean, accurate, up to date information to enable the business to drive its commercial goals."*
>
> Privacy business analyst
> Quoted in "Turning data governance policy into practice in 2020"

In reaching this point, an organisation has achieved an effective security architecture that starts with the data, balancing the need for security and increased access to information.

Things to think about...

- **What KPIs do you measure when it comes to data?**
- **Do you know where your business could improve its security posture today?**
- **Have you implemented a mechanism to ensure continuous improvement?**

Discover your data. Strengthen data security.

Taking a step-by-step approach to add layer upon layer of good data management and security practices, organisations establish the modern architecture they need to strengthen data security in the information age because it enables them to:

- **Secure data:** ensuring that sensitive, confidential and personal information is programmatically kept private and secure.
- **Extract value:** mining intellectual property, research or insight within the information so they can use their data to drive competitive advantage.
- **Manage complexity:** tackling the volume and complexity of data at scale, so it can be organised and migrated intelligently.

Using data policies and process, organisations can lay a strong foundation, before turning those policies into practice through employee awareness, training and culture.

Then by discovering and classifying all the data across the estate, organisations can better implement the enforcement technologies to take appropriate remediation actions to secure data.

Finally, establishing the operational process and record keeping, organisations gain the insights into how they can continuously improve to strengthen their security posture. And reveal the value in their data, enabling them to power the organisation for the benefit of the people they serve.

Should you need us...

When you're ready to start the data discovery process, you couldn't be in safer hands than with Exonar.

The Exonar smart index enables data to be used to protect and power the organisation - billions of items all viewable and manageable in one place, and instantly searchable via a user-friendly browser interface.

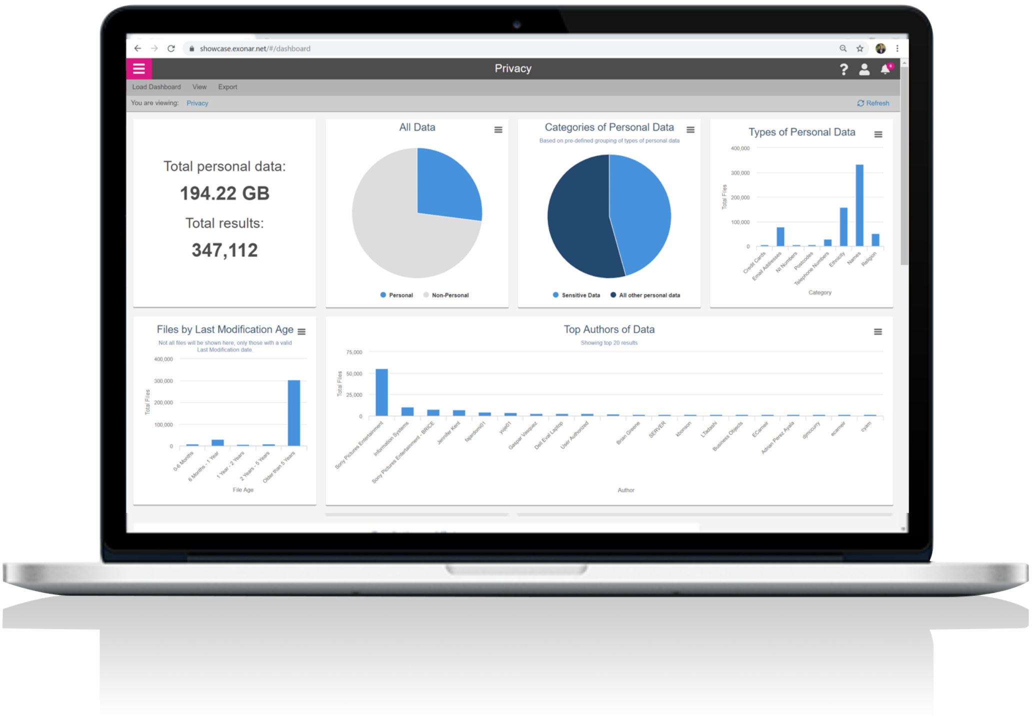
> *"Exonar's software is the most comprehensive and effective data discovery solution we've been able to find."*
>
> John Harris, CTO, Mundipharma

Start discovering your data today

Why don't you set up a time for one of our experts to give you a demo that's relevant to your business challenges and we will show you how Exonar can help.

Book at demo today

> *"Exonar is developing best-of-breed technology for its customers but only because the team is going the extra mile on a daily basis - whatever you need, Exonar is there. It's the best experience I've had of working with a solution provider in over 20 years."*
>
> **Dave Parker, Group Head of Data Governance, Arrow Global**



showcase.exonar.net/#/dashboard

Total personal data: 194.22 GB

Total results: 347,112

EXONAR

About us

Exonar

Exonar is the world-leading data discovery company building the crucial software organisations use to discover their data at scale, keep it safe and realise its value.

Every company faces the same problem; knowing what data they've got, and where it is stored. Exonar is the only software available today able to find and reveal billions of items of structured and unstructured information; enabling businesses to 'know the truth' about their data in order to reduce risk, uncover business value and deliver digital transformation.

Backed and funded by Beringea, Amadeus Capital Partners, Winton Ventures and Downing Ventures, Exonar boasts a growing list of large and well-recognised customers in the pharmaceutical, financial services and national critical infrastructure industries.

To find out more, visit us at **www.exonar.com**