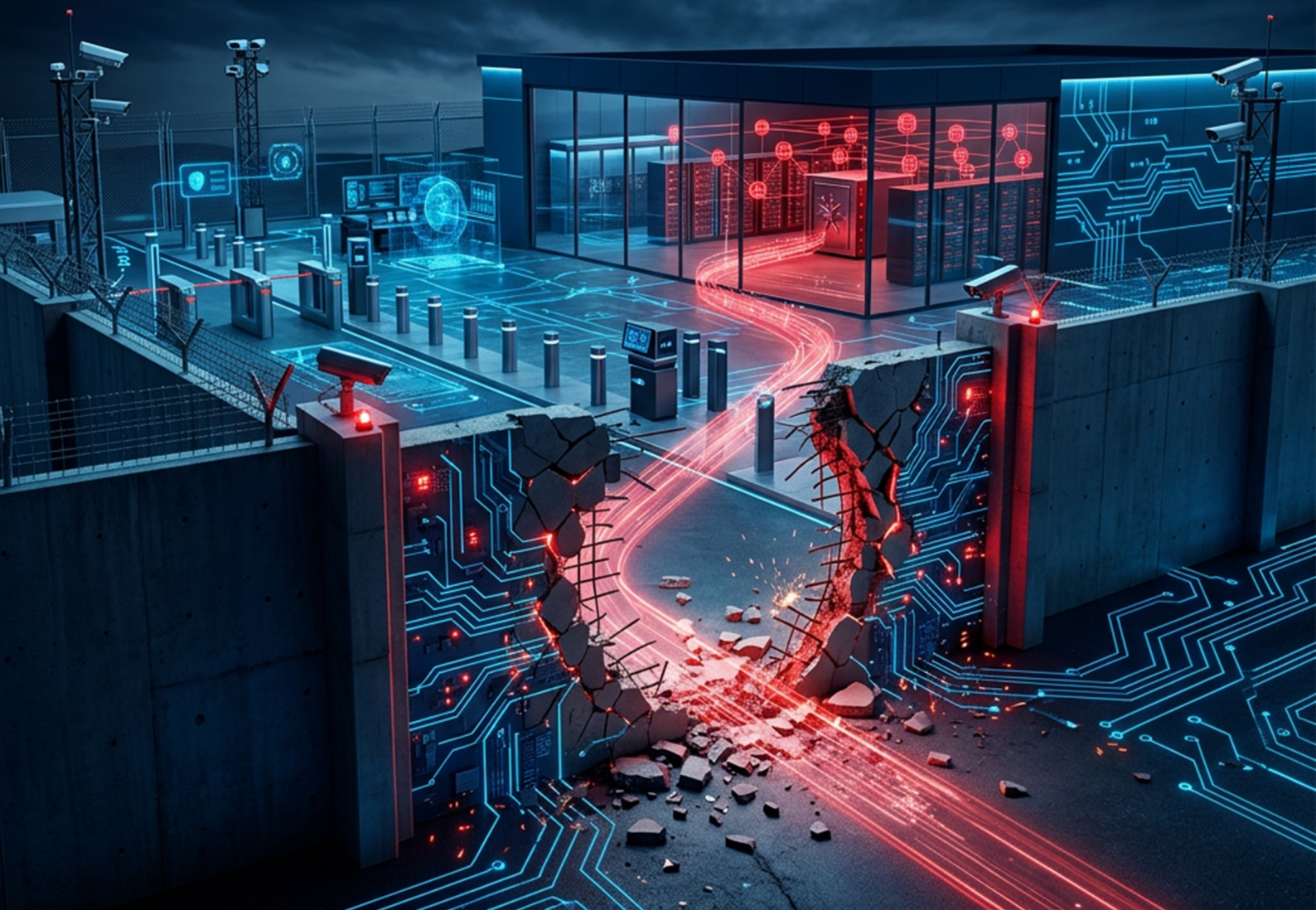
ezescan.
making digital work

When Prevention Fails

Why Information Exposure Determines Cyber Resilience



Executive Summary

- Cyber security controls reduce the likelihood of a breach but cannot eliminate the possibility.
- The impact of a breach is determined by the information exposed, not the attack method.
- Information risk management is frequently underfunded because organisations lack visibility into their information landscape.
- Information discovery, remediation and continuous monitoring provide organisations with the visibility and control required to reduce information risk and improve cyber resilience.
- Organisations that understand their information before a breach occurs are better positioned to respond when one does.

Table of Contents

The Question Every Executive Leader Needs to Consider

Government organisations continue to strengthen their cyber security posture through significant investments in security technologies, governance frameworks, staff awareness programs and operational controls.

These investments are essential. Yet as recent breaches continue to demonstrate, strong defences alone do not determine organisational resilience.

Despite billions of dollars invested globally in cyber security technologies and programs each year, breaches continue to occur. The question executive leaders must ask is no longer whether a breach is possible, but what happens when prevention fails.

Attackers are becoming more sophisticated, digital environments are becoming more complex, and human behaviour remains one of the most difficult risks to manage.

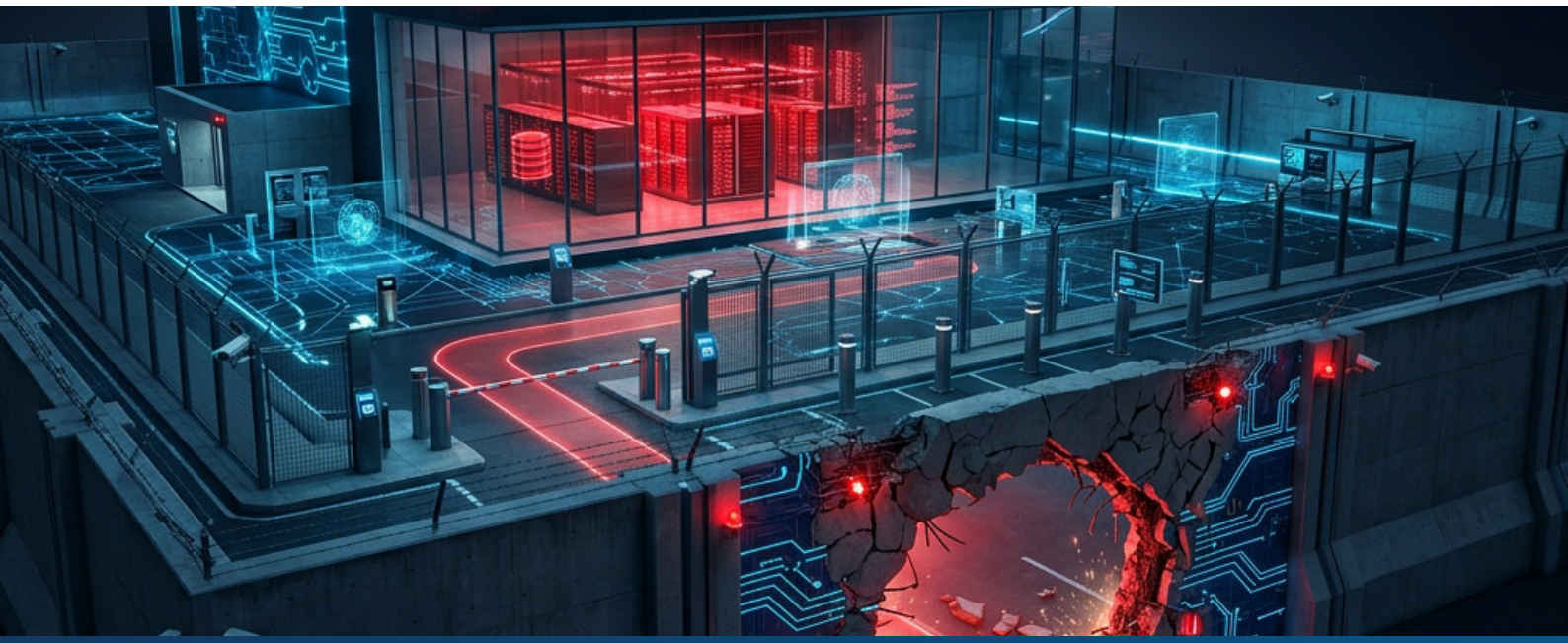
The reality facing executive leaders today is clear... While cyber security controls reduce the likelihood of a breach, they do not eliminate the possibility of one.

Recent breaches involving Medibank, Optus and Latitude Financial demonstrate an important lesson. While each breach involved different circumstances, public scrutiny ultimately focused on the same issue... What information was exposed?

These organisations were not judged solely on how attackers gained access. They were judged on the sensitivity of the information affected, the number of people impacted, and how effectively they responded once the breach was discovered.

This highlights a critical shift in cyber resilience.

The organisations best positioned to respond to modern cyber incidents are not simply those with strong security controls. They are the organisations that already understand their information landscape, know where sensitive information resides, and can rapidly determine the impact of a breach.



Cyber Security Investment Paradox

Government organisations have made significant progress in strengthening cyber security capabilities: Investments in identity management, endpoint protection, threat intelligence, security monitoring and employee awareness training have become standard practice across many agencies.

These controls play a critical role in reducing risk and strengthening resilience against an increasingly complex threat landscape. However, they all share a common objective: prevent attackers from gaining access.

The challenge is that cyber security is not an absolute guarantee.

Attackers need only one successful entry point. That point may be a sophisticated technical exploit, but increasingly it is not. More often, it involves a compromised credential, a trusted third party, insider activity, or a successful phishing campaign.

Phishing and social engineering remain among the most common attack vectors because they exploit human behaviour rather than technology vulnerabilities.

For executive leaders, this presents an uncomfortable reality: even organisations with mature security controls, advanced monitoring capabilities and well-defined security policies remain vulnerable to a single successful phishing attempt.

A convincing email, a compromised credential, or a momentary lapse in judgement can provide attackers with the access they need to bypass multiple layers of defence.

The Medibank breach provides a powerful example of this: Compromised credentials ultimately enabled attackers to gain access to highly sensitive personal and health information affecting millions of individuals.

The lesson is not that security controls failed, the lesson is that no organisation can assume a breach is impossible.

Cyber resilience cannot be measured solely by an organisation's ability to prevent unauthorised access, it must also be measured by its ability to understand and manage the consequences when prevention fails.

Executive leaders must therefore move beyond a prevention-only mindset and ask different questions....

If an attacker gained access to our environment today, what information could they actually reach?

And how confident are we that we could answer that question within hours, rather than weeks?

The Visibility and Funding Gap

Cyber security investments are relatively easy to justify. Executive leaders can see the threat. Security teams can demonstrate attempted attacks, phishing campaigns, malicious activity, vulnerability assessments and compliance obligations.

As a result, budget is allocated to firewalls, endpoint protection, identity management, monitoring platforms and security operations. Information risk is different.

While most organisations recognise that information has value, few can quantify the risk associated with the information they already hold.

As a result, information risk management often struggles to attract the same level of funding and executive attention as traditional cyber security initiatives.

This creates a significant imbalance. Organisations invest heavily in preventing attackers from gaining access to their environment, yet comparatively little in understanding what information those attackers could access if they succeed.

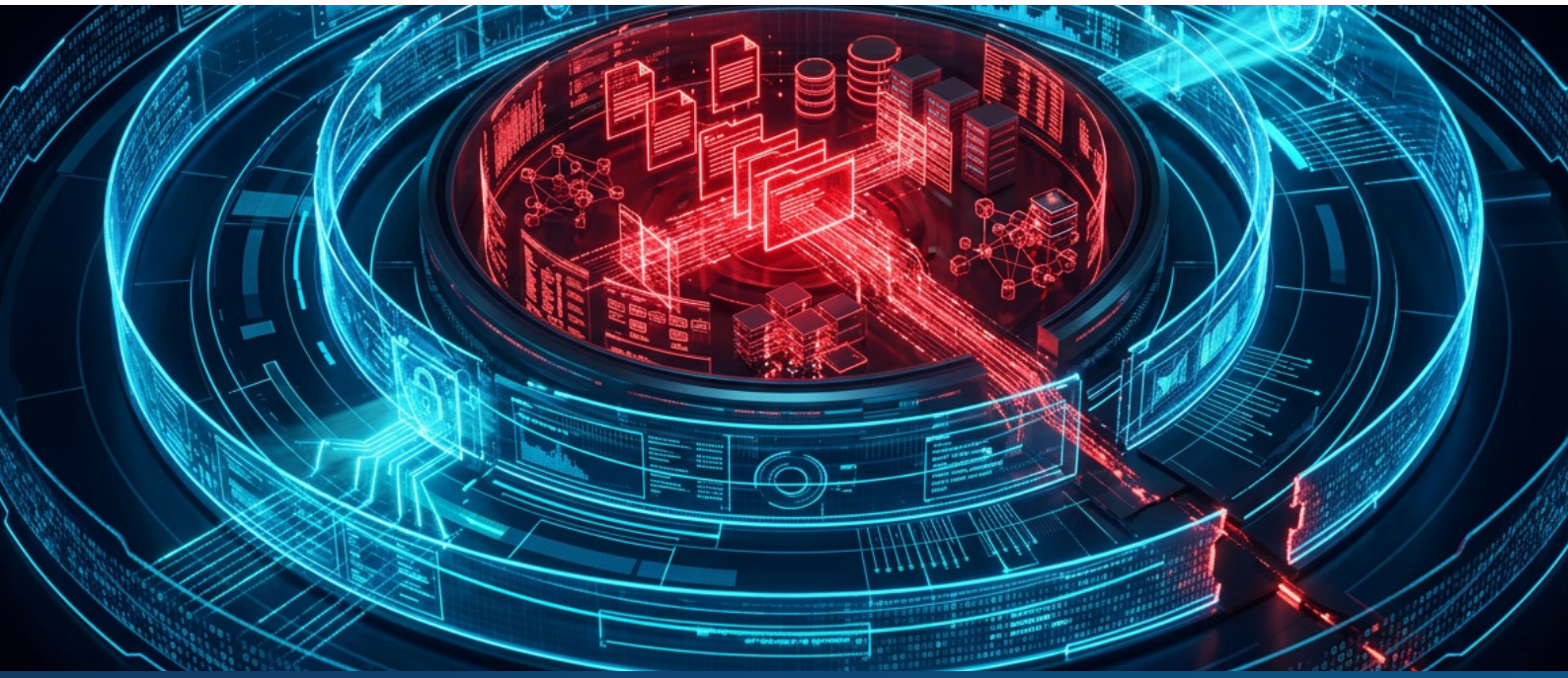
Ironically, when a breach occurs, it is rarely the security controls that determine the severity of the incident, it is the information exposed.

The less visibility an organisation has into its information landscape, the harder it becomes to assess risk, prioritise remediation activities and justify investment before an incident occurs.

This disparity is not driven by the relative importance of the risks, it is driven by visibility.

Cyber security programs can demonstrate attempted attacks, security incidents and compliance obligations, making investment decisions easier to justify. Information risk often remains hidden.

Without visibility into the volume, location and sensitivity of information assets, organisations struggle to quantify exposure and secure funding for remediation initiatives. As a result, information risk is frequently underfunded, despite having the potential to determine the ultimate impact of a cyber incident.



The Question That Matters Most

When a breach occurs, security teams naturally focus on understanding how attackers entered the environment. This is important. However, it is rarely the question that executives, regulators, citizens or media organisations ask first.

History shows that attention quickly shifts away from the attack itself and toward the impact of the attack.

The questions that inevitably follow are:

- What information was exposed?
- How many individuals were affected?
- How sensitive was the information?
- What are the consequences?

Recent breaches provide clear examples:

Following the Medibank incident, public concern centred on the exposure of personal and health information.

Following the Optus breach, attention focused on the scale of customer information affected, including identity-related information.

During the Latitude Financial breach, attention centred on the volume of customer information impacted and the growing scope of the incident as investigations progressed.

In every case, the story quickly became about the information. Not the attack method. Not the vulnerability. Not the technology.

This represents a fundamental shift in how organisations should think about cyber resilience.

Cyber security has traditionally focused on preventing attackers from getting in but modern cyber resilience requires organisations to think about what happens if they do.

Breach Impact Is Determined by Information Exposure

Attackers are not targeting government agencies because they want access to servers, applications or infrastructure, they are targeting information.

Government organisations hold some of the nation's most valuable information assets.

Citizen records, health information, financial data, legal documentation, operational records and personally identifiable information represent significant value to both the organisation and potential attackers.

The true value of a successful breach is determined by access to these assets.

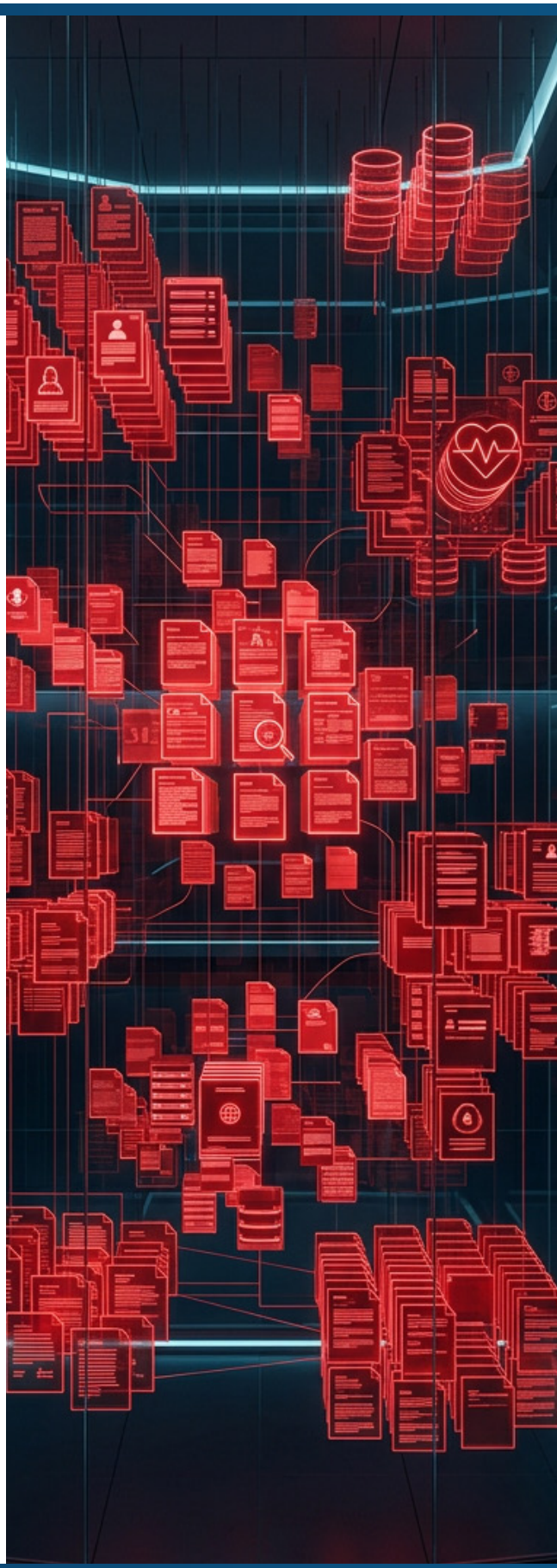
> **The Medibank breach reinforced the sensitivity of health information, the Optus breach highlighted the significance of identity-related information and the Latitude breach demonstrated the risks associated with large volumes of historical customer data.**

While each incident was different, all three reveal the same reality: the true impact of a cyber incident is determined by the information attackers can access once they are inside.

This means cyber resilience is no longer solely about securing systems, it is equally about understanding information. Because when a breach occurs, the challenge is not simply determining that an attacker gained access.

The challenge is understanding what information they were able to access and how quickly the organisation can assess the impact.

Increasingly, these are not IT questions. They are governance, risk and accountability questions that executive leaders and boards must be prepared to answer.



The Visibility Challenge

Understanding that information determines the impact of a cyber incident raises a critical question for executive leaders: how quickly could your organisation determine the scope of exposure if a breach occurred today?

Many organisations express confidence in their ability to respond to a cyber incident. They have incident response plans, containment procedures, recovery strategies and security teams prepared to act when an incident occurs.

These capabilities are essential, however once a threat has been contained, a different challenge emerges.

Leaders need answers. They need to understand what information was potentially exposed, which individuals may be affected, what regulatory obligations apply, and what remediation actions may be required. For many organisations, obtaining these answers is far more difficult than containing the initial incident.

The challenge is not necessarily a cyber security problem, it is an information visibility problem. Sensitive information is often distributed across shared drives, SharePoint, Microsoft Teams, email systems, cloud repositories, business applications and legacy platforms.

Years of information accumulation, duplication and inconsistent governance can make it difficult to maintain a clear understanding of what information exists and where it resides.

As a result, organisations may know that a system was compromised yet have limited visibility into the information contained within that system.

Without a clear understanding of sensitive information holdings, uncertainty quickly becomes one of the most significant risks an organisation faces. Investigations take longer, costs increase, regulatory reporting becomes more complex, and executives are forced to make critical decisions before all relevant facts are available.

Visibility into information does not begin during a breach investigation. It begins long before the breach takes place. Organisations cannot effectively manage what they cannot see.

Executive leaders routinely receive dashboards showing phishing activity, vulnerability scores, patch compliance and security incidents. Few receive equivalent visibility into their information risk exposure.

Without measurable visibility into sensitive information, organisations struggle to prioritise remediation efforts, demonstrate risk reduction outcomes, or build compelling business cases for investment.

Information discovery changes this dynamic by transforming unknown information risk into measurable and actionable intelligence.

Information Discovery: Building Visibility Before a Breach

If organisations are expected to quickly determine the scope and impact of a cyber incident, they must first understand the information they hold. This is where information discovery becomes a critical component of cyber resilience.

Many government organisations do not have complete visibility of their information landscape.

Sensitive information is often dispersed across multiple repositories, accumulated over many years, and duplicated across systems with varying levels of governance and oversight.

As a result, organisations frequently struggle to answer fundamental questions:

- What sensitive information do we hold?
- Where is it located?
- How much exists?
- Who has access to it?
- Does it still need to be retained?

Without this visibility, assessing exposure during a cyber incident becomes significantly more difficult.

Data Risk Assessments and automated information discovery provide organisations with a clearer understanding of their information environment.

Rather than relying on assumptions, organisations can identify personally identifiable information (PII), payment card information (PCI), health information, financial records, sensitive operational information and other regulated content wherever it exists.

This visibility enables organisations to understand both the volume and location of sensitive information across their environment.

More importantly, it establishes a baseline for understanding potential exposure before an incident occurs.

Organisations can use information discovery tools such as EzeScan to scan shared drives, network folders, email systems and supported backend systems to identify documents containing personally identifiable information (PII) and other sensitive content.

Once identified, this information can be categorised and tagged, providing organisations with a clear view of where sensitive information resides, the types of information being retained and the volume of information at risk.

This visibility is presented through dashboards and reporting tools that help organisations understand their information landscape and prioritise areas of concern.

The value of this visibility becomes particularly apparent during a cyber incident.

Rather than manually reviewing thousands of documents across a compromised repository to determine what sensitive information may have been exposed, organisations can quickly identify repositories containing PII and understand the nature and scale of the information involved.

This enables faster investigations, more informed decision-making, improved regulatory reporting and greater confidence when communicating with stakeholders about the potential impact of a breach.

The Scale of this Challenge Should Not be Underestimated

Large government agencies often manage millions of documents containing personal, financial, operational and regulatory information spread across numerous repositories.

Identifying sensitive information manually is not simply inefficient; it is economically impractical.

Even organisations willing to dedicate significant resources would struggle to maintain an accurate understanding of information risk through manual processes alone. By the time an assessment is completed, the information landscape has already changed.

Effective information risk management therefore depends on automation. Discovery, classification, assessment and remediation must operate at a scale and speed that human review cannot realistically achieve.

Solutions such as EzeScan enable organisations to:

- Assess millions of documents,
- Identify concentrations of sensitive information,
- Prioritise risk
- Execute remediation activities consistently across the enterprise.

This level of visibility and control would be virtually impossible to achieve manually.

Discovery Is Good. Remediation Is Better

Before organisations can reduce information risk, they must first understand where that risk exists. Discovery provides visibility. Remediation turns that visibility into risk reduction.

Information discovery provides organisations with visibility into where sensitive information resides, how much exists, and which repositories present the greatest risk.

However, visibility alone does not reduce exposure. Once sensitive information has been identified, organisations must determine whether it still needs to be retained.

Over time, organisations accumulate large volumes of information, including historical customer records, duplicate files, archived reports and outdated personal information. While much of this information may no longer provide operational value, it continues to create risk. Every piece of sensitive information represents a potential target.

The Latitude Financial breach highlighted the risks associated with large volumes of historical customer information. The greater the volume of sensitive information retained, the greater the potential impact if an attacker gains access.

This is where remediation becomes critical.

Using tools such as EzeScan, organisations can automate the reduction of information risk by identifying records that should be disposed of, removing duplicate information, redacting personal information where it is no longer required, and applying stronger controls to high-risk content.

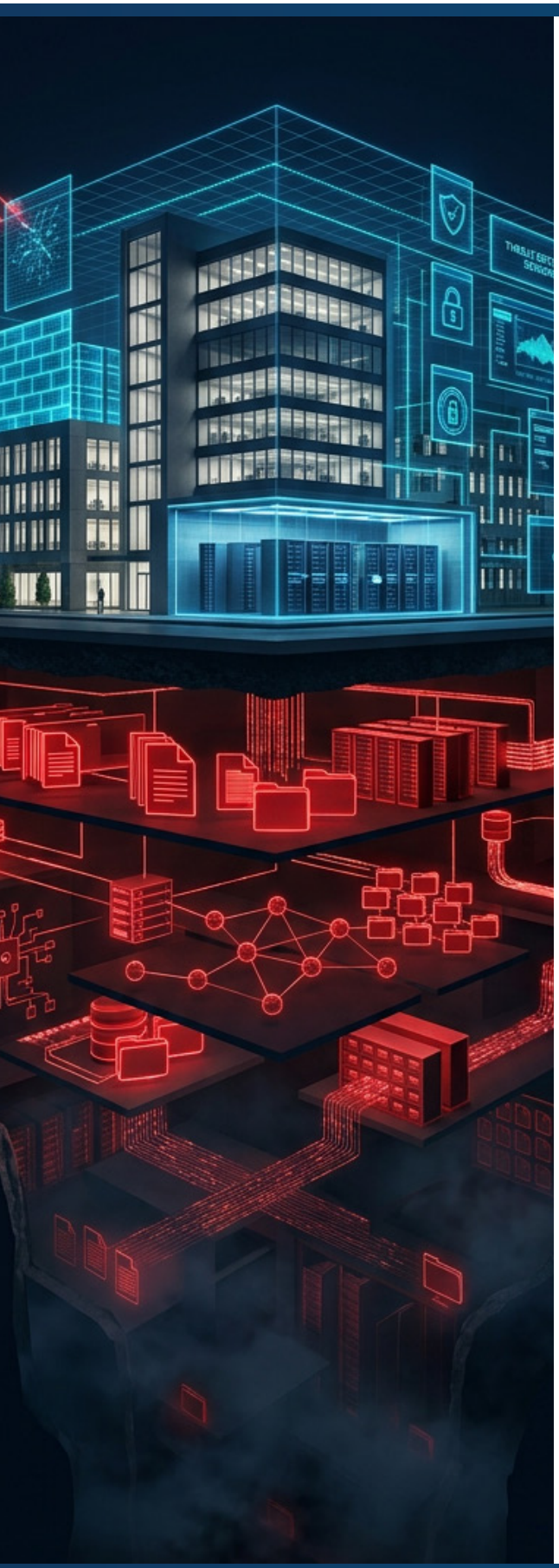
The result is a smaller information footprint and reduced exposure.

Information that has been appropriately disposed of cannot be exposed.Information that has been redacted cannot be misused. Information that has been removed from the environment cannot become part of a future breach.

Information discovery provides the visibility needed to understand risk whilst remediation reduces that risk.

Together, they help organisations reduce both the likelihood and potential impact of future cyber incidents.

Beyond Discovery: Continuous Information Risk Monitoring



Traditional information discovery exercises often provide a snapshot of risk at a particular point in time. While valuable, information risk is not static.

Every day new documents are created, emails are received, records are uploaded, files are shared and information moves across the organisation. The information landscape continually evolves.

EzeScan addresses this challenge through a combination of retrospective analysis, automated remediation and ongoing information risk assessment.

While organisations can use Data Risk Assessments to understand historical information holdings, EzeScan extends this capability by continuously assessing information as it is created, captured, received or modified. This ensures information risk visibility becomes an ongoing operational capability rather than a point-in-time project.

Organisations can conduct comprehensive Data Risk Assessments across existing repositories to establish an initial understanding of sensitive information holdings.

Once visibility is established, EzeScan can continuously monitor information as it enters the organisation or is created within business processes.

This approach enables organisations to identify, classify and assess sensitive information at the point of capture, enabling governance controls and remediation actions to be applied before information risk accumulates.

Rather than periodically discovering information risk after it has accumulated, organisations can continuously identify, assess and remediate information risk before it escalates into a cyber resilience issue.

Conclusion

For years, cyber security strategies have focused on preventing unauthorised access. That focus remains essential. However, no organisation can assume prevention alone will be enough.

Whether a breach occurs through compromised credentials, phishing, insider activity or third-party access, organisations must be prepared for the possibility that attackers may gain access to their environment.

What separates resilient organisations from vulnerable ones is not simply the strength of their security controls. It is their understanding of the information those controls are designed to protect.

Security investments reduce the likelihood of a breach but information risk management reduces the scale, cost and impact of a breach when prevention fails.

Organisations that can identify, measure, remediate and continuously monitor information risk gain a decisive advantage. They can assess incidents faster, minimise uncertainty, meet regulatory obligations with greater confidence and significantly reduce the volume of sensitive information exposed to future threats.

In a world where breaches are increasingly viewed as a matter of when rather than if, information visibility is no longer an operational concern.

It is a board-level capability, a critical component of cyber resilience, and the foundation for understanding, governing and reducing information risk before the next breach occurs.