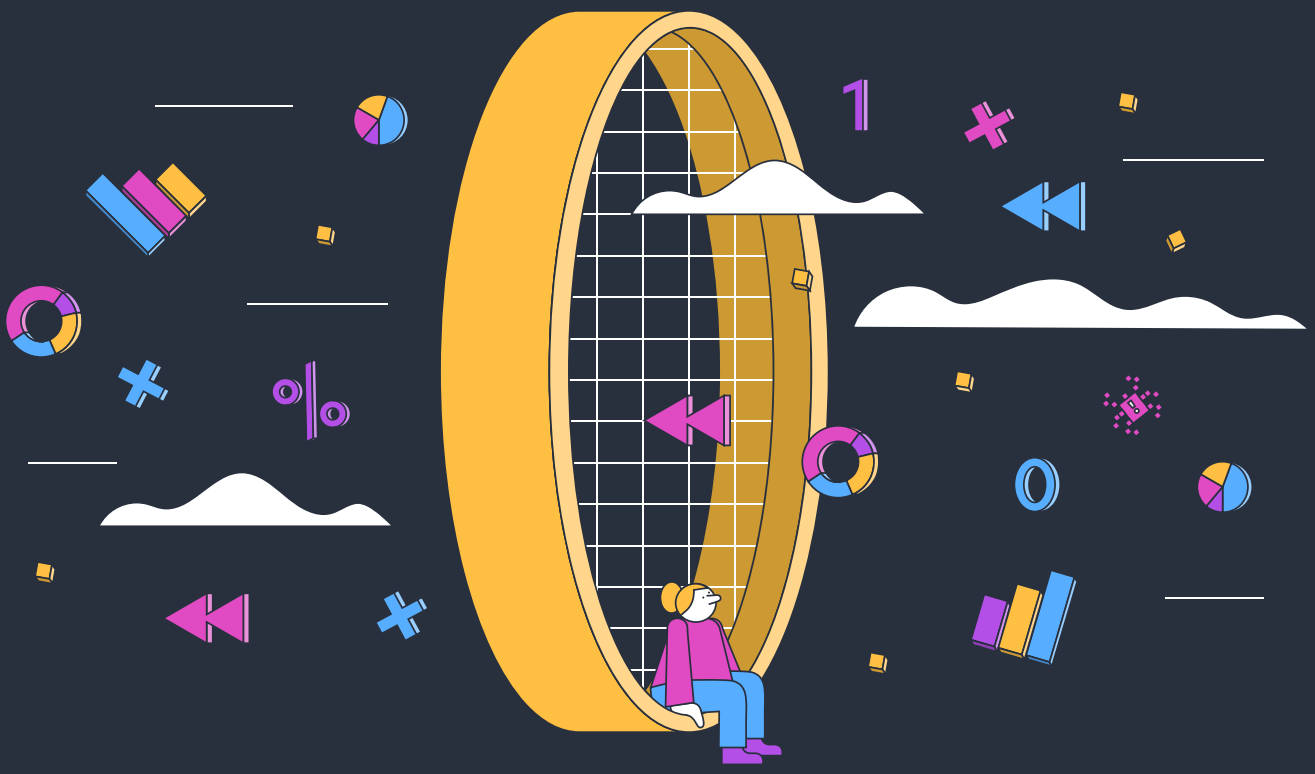
Raconteur

SaaS success: secure data strategies for 2024



salesforce | Own

Contents

How to make better use of SaaS data in 2024

If used strategically, data is one of the biggest competitive advantages an organisation has. So how can organisations up their data game?

Steve Hemsley

Data provides organisations with a massive competitive advantage if they maintain it effectively and are committed to data governance.

As the adoption of software as a service (SaaS) and cloud technologies accelerates, organisations should invest adequately in the most suitable tools for their specific needs. They must also ensure that everyone working across the organisation understands the value of the data collected stored in these platforms.

When everything is in place, a robust data strategy improves the customer experience and assists with new product development. This should fuel a growth in sales, boost profits and increase market share.

Modern data architecture is essential for ensuring efficiency and security, and delivering the service customers have come to expect. The business world has shifted quickly from simple personalisation to hyper-personalisation. Yet for this to work effectively, there needs to be a seamless integration of real-time data, AI, machine learning and analytics.

Companies are also being urged to implement what is known as a horizontal data strategy. This is where data from one part of a product or service is used to add value and intelligence to another.

There are some high-profile examples of well-thought-out data strategies. Companies such as Netflix and parcel delivery giant UPS guide strategic decision-making, create exceptional customer experiences and streamline their operations by using data to innovate and improve.

Barry Coatesworth is a director at Guidehouse, a global provider of consulting and managed services. He says the fusion of AI and machine learning is deepening the understanding of predictive capabilities.

"It offers insights that were previously beyond our reach," he says. "But the evolving landscape of data privacy and governance will continue to challenge us to be ever more vigilant and innovative in how we manage and protect data."

Coatesworth adds that a vigorous data strategy also means fostering a culture where data is managed ethically and legally to build trust. This means aligning with regulations such as GDPR and the CCPA (California consumer privacy act).

Industry collaboration initiatives, such as the Zero Copy network led by Salesforce, are addressing governance and security, as well as sustainability and other ethics considerations.

"Ensuring data quality, accuracy and reliability helps to build an effective strategy and reinforce the faith placed in organisations by those who share their data," says Coatesworth. "This enables informed, thoughtful decisions that affect real lives."

These informed decisions often come from historical data. In any highly competitive environment, organisations must be able to learn from their past. Historical data is a strategic advantage, and AI and machine learning can help by activating analytics and delivering business insights. AI can provide instant access to time-series data so sales teams can analyse pipeline trends.

At international accountancy and tax firm Mazars, director of data trust services Foyaz Uddin says AI is exciting but requires appropriate guardrails to protect everyone, especially with off-the-shelf products such as ChatGPT.

"AI has transformed the accessibility of datasets and this is shaping research," he says. "It can look for patterns and go through huge amounts of data which can be valuable in research and development."

In the payments sector, organisations are increasingly relying on SaaS solutions to manage and leverage their data.

Keren Ben Zvi, chief data officer at PayU, an online payment service provider operating in more than 50 countries, says being able to leverage SaaS data is vital to remaining innovative and focused on customers.

"It's important the data offers insights that can be used to guide overall business strategies and support regular decision making," she says. "But the data must be real-time and accessible to all relevant stakeholders. It should also be encrypted to ensure it is secure and adheres to compliance standards such as PCI DSS (payment card industry data security standard). I recommend regular audits to ensure data integrity and enhance the accuracy of the insights."

Orlando Ruiz is manager in technology, data security and infrastructure at global recruiter Robert Walters. He says the SaaS data industry is so fast-moving that some organisations will be left behind in their specific sectors if they cannot keep up.

"In the last three years, more organisations are investing in an embedded data strategy so stakeholders can make data-based decisions and compete in their market," he says. "Ultimately the most successful businesses have data at their core, make sure it is democratised and that people are encouraged to – and know how to – use it."

In the advertising industry, for example, brands are using data to make their media buying more efficient. Carlo De Matteo, co-founder of consultancy Mint, says data insights inform marketing teams about how campaigns are performing, while historical data enables comparisons to be made; and this informs future advertising activity.

Getting data to a point where the organisation can learn from it is still considered much harder than it really is. Companies will see results if they invest in the right people skills, tools and support so they can confidently delve into the data and reveal those actionable business insights.

AI has transformed the accessibility of datasets and this is shaping research

Protecting and activating SaaS data as the attack surface expands

Keeping up with the pace of technology and the inevitable evolution of cyber threats that come with that can seem like an impossible task. How can IT leaders get their priorities right in 2024?

Steve Hemsley

It is becoming harder for organisations to stay one step ahead of cybercriminals to protect SaaS data.

Consultant PwC's 2024 Global Digital Trust Insights Survey discovered that the proportion of businesses that have experienced a data breach of more than $1m had grown from 27% to 36% in a year.

A cyber attack is the most likely reason for an organisation to undertake a data security policy review, according to research commissioned by Own Company in the 'State of SaaS Data Security and Protection in Europe'. Yet despite acknowledging that cybercriminals are the biggest threat, only 44% of businesses have a comprehensive data backup strategy in place.

When it comes to SaaS data security, it is important to remember that there must be shared responsibility. Many organisations assume that the provider is taking care of the security of data in the cloud. However, while the security of the cloud platform itself is the responsibility of the provider, customers are responsible for the security of their data stored on the cloud platform.

Law firm Hunton Andrews Kurth advises some of the biggest tech companies in the world including Google, TikTok and Meta on data privacy and cybersecurity matters. Partner Sarah Pearce says every business must be better

prepared, regardless of the high investment made in security by the provider.

"There are risks wherever data is held or processed, so organisations do need to think about how they look after it from a privacy and security perspective," she says. "There are consequences of getting this wrong, not just financially, but reputationally too. Your own processes need to be robust."

Pearce adds that companies also need the best people to help tackle the potential risks internally.

"There needs to be investment in talent, bringing in people with the right skill sets who can guide a business through security in an appropriate manner."

With this in mind, it is important industries work together to share experiences when it comes to cybersecurity to improve knowledge.

The Ladies of London Hacking Society is a pioneering social enterprise providing offensive and defensive cybersecurity skills to women. The community has members who meet regularly to discuss current trends and threats.

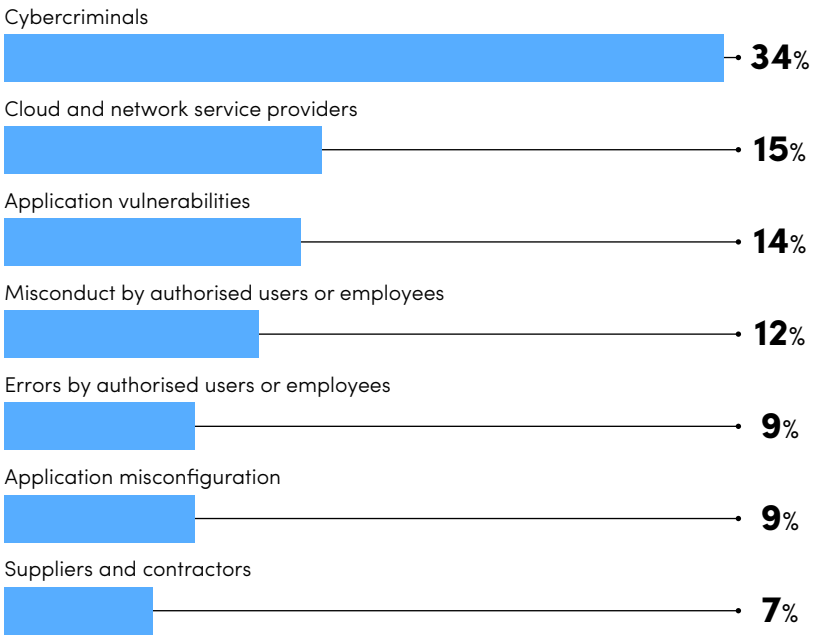
Chapter lead Didar Gelici works as head of risk, compliance and data security at a leading food delivery brand, and she says organisations need to be on top of the latest cyber dangers.

One of these is shadow IT, where employees use software or hardware within an enterprise network that has not been approved by the IT department. This is a challenge that is being fuelled by hybrid working.

"We are seeing clear difficulties when it comes to balancing user experience and business productivity, while establishing more control over where data goes," says Gelici. "CTOs need an understanding of the data security gaps in their business. They must then examine and clearly define roles between IT, security and users to guide policy decisions and raise awareness of risks and best practice."

Del Heppenstall is head of UK cyber at KPMG UK and says that because good businesses are built on good data, an organisation can tumble like a house of cards when there is a cyber attack.

Greatest threat to SaaS data security in next 12 months



Own Company, 2023

He suggests scenario planning to help identify the potential costs and using cyber risk quantification (CRQ). The latter is a process of measuring cyber risks in monetary terms. If leaders are aware of the possible financial impact, they can be clearer in their decision-making and know where to prioritise their cybersecurity budget.

"CRQ enables the analysis and critical thinking necessary to understand the true likelihood of something bad happening, and the business impact if it does," says Heppenstall. "A critical part of the approach to CRQ involves thinking through potential cyber scenarios, such as ransomware or a data breach, and estimating the most likely and worst-case impact should they occur."

Organisations are also being urged to invest more in upskilling their workforce so individuals have a better understanding of how cyber threats could ultimately close down a business.

Barry Coatesworth, director at Guidehouse, a global provider of consulting and managed services, says investing in SaaS data security is an investment in trust and integrity.

"A proactive stance against cyber threats is a testament to the commitment to your customers and the ethical stewardship of their information," he says. "This goes beyond technical measures; it involves nurturing a culture of data privacy awareness so there is best practice among your teams."

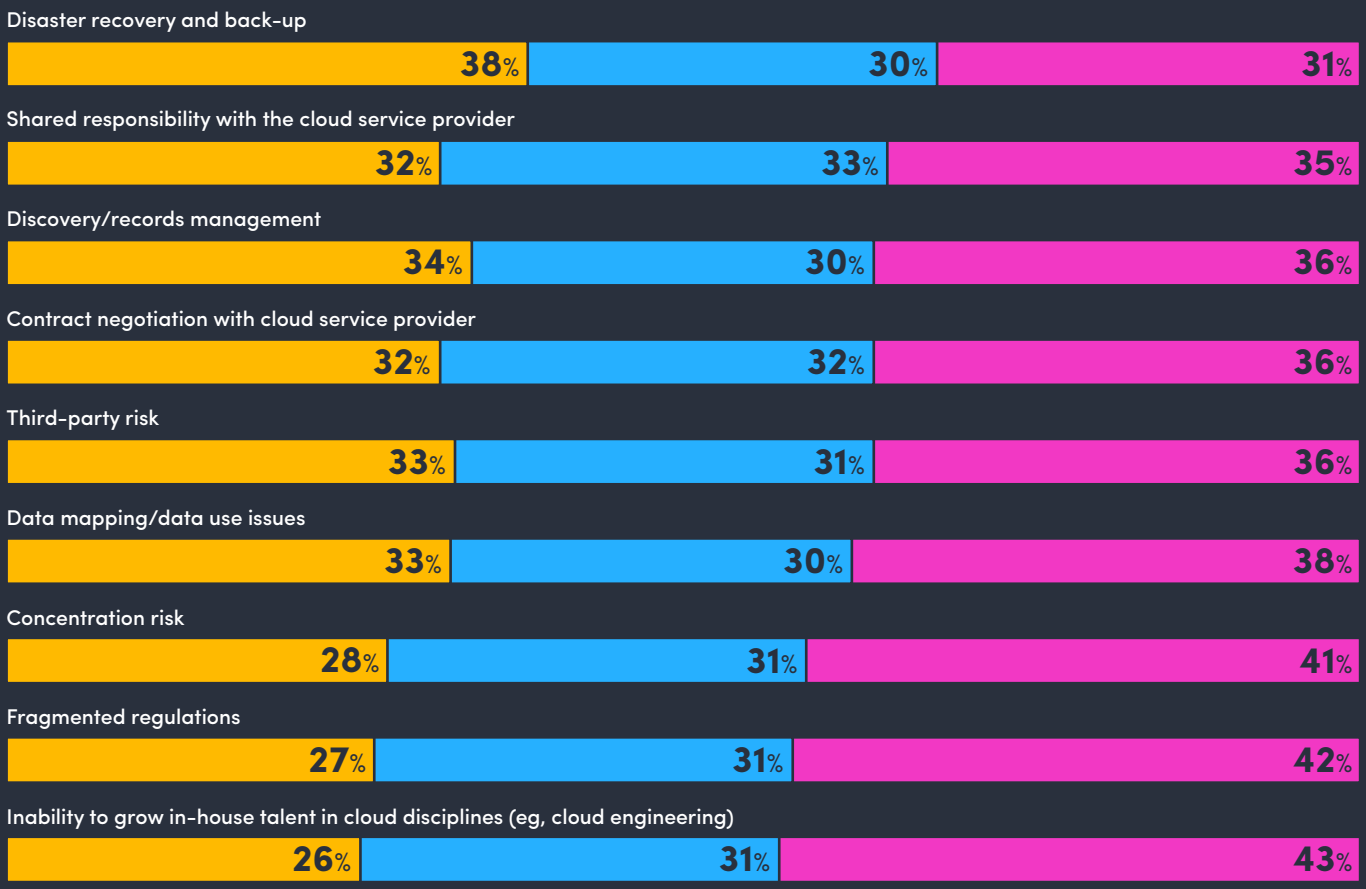
> **A proactive stance against cyber threats is a testament to the commitment to your customers and the ethical stewardship of their information**

Cloud cover: securing SaaS data

How well-protected is data in the cloud currently and what do organisations need to focus on next?

There is still a way to go to ensure data security in the cloud, with 97% of organisations globally having gaps in their cloud risk management plan

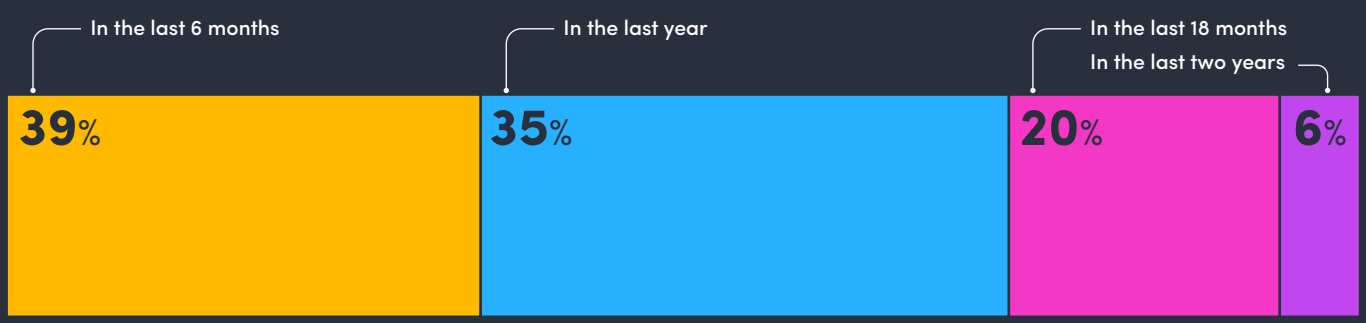
To what extent has your organisation addressed the following challenges with your cloud service provider(s)?



PwC, 2024

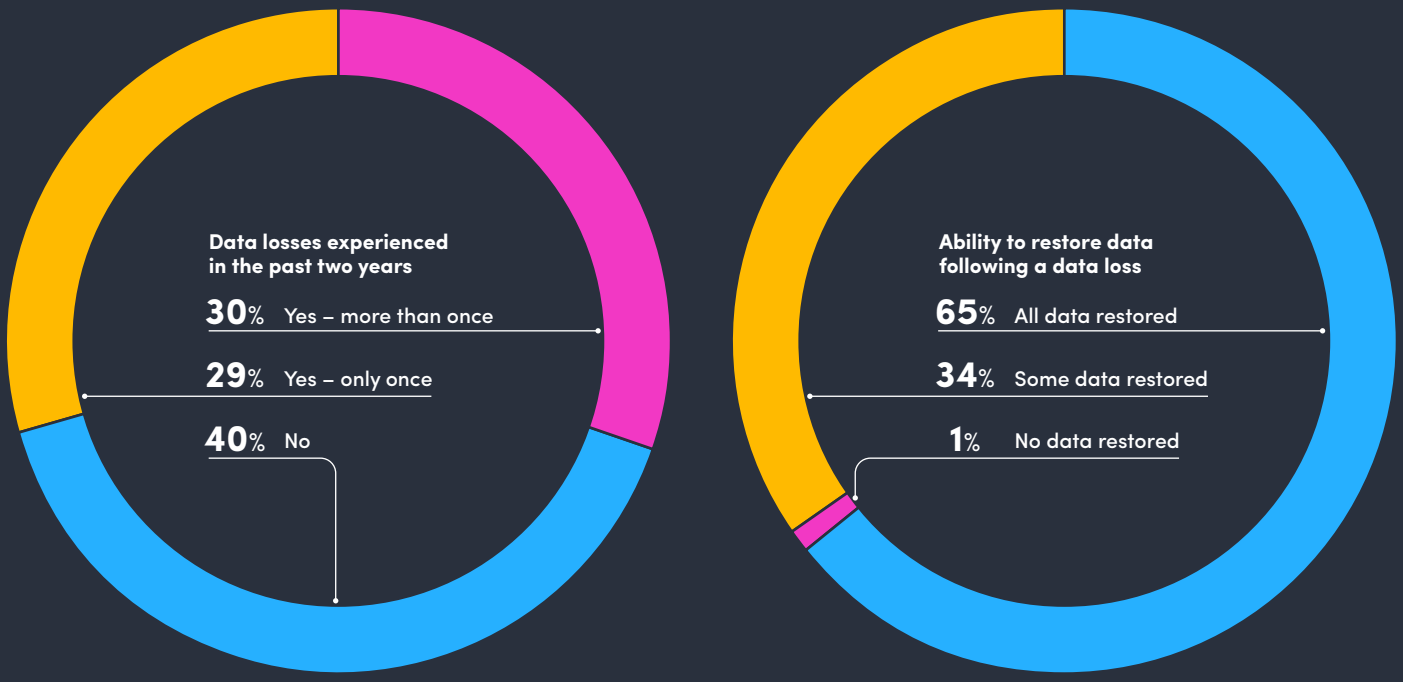
In Europe, most organisations have reviewed their data security policy in the last year

When did organisations last review their data policies?



Own Company, 2023

But many organisations have experienced data losses and only two-thirds of organisations could restore all data after such a loss



Own Company, 2023

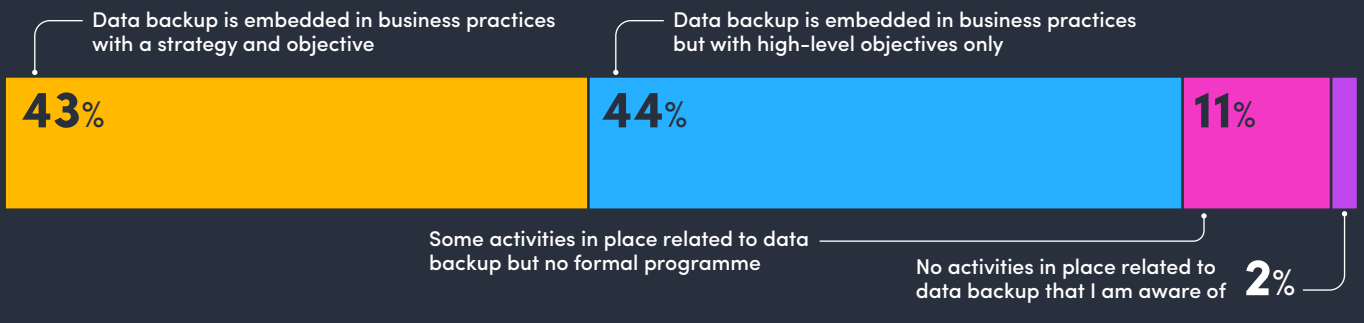
As a result of data loss, many organisations are investing further in cybersecurity

Actions taken as a result of a data loss

Own Company, 2023

Do organisations now realise the importance of having a robust data backup strategy? The majority of organisations say that data backup is embedded in their business practices but there is still room for improvement

Approach to securely backing up data



Own Company, 2023

Why data backup is just the first piece of the puzzle

In the event of data loss, what do organisations need to have in place to ensure they can get their business back up and running without major disruptions?

Steve Hemsley

Most organisations will face a data loss incident at some point. The question businesses should be asking is: what contingency plans are in place to get the operation back to where it was before?

Security professionals and C-suite executives are beginning to appreciate the negative impact that data loss can have on their business. In response, they are investing in robust data governance platforms that not only secure their data but also extract value from it.

Having effective backup procedures is only part of the puzzle when it comes to quickly recovering data.

Own Company, a SaaS data protection provider, helps organisations recover important data quickly in the event of data loss.

"Not all backup providers are equal, so you have to look at data governance as a whole," says Own Company's vice president of cybersecurity strategy and product development

Eoghan Casey. "When it comes to data history, an organisation can learn from the past to improve the future. The key is how fast can they do that, especially when there has been data loss."

Own Company helps clients understand the data they have and how it flows throughout their business. For example, is it classified, archived and anonymised correctly?

Casey says it is essential to have a strong security model both around and within the organisational environment. He advises adopting zero-trust principles of data-centric security, which means assuming that every connection, device and user is a potential threat.

It is also crucial to monitor how data is being used. This means checking who, based on their role, has access to specific data and when they retrieve it. For example, is someone working in a bank or hospital environment changing or using data in a way that might negatively impact financial services or patient care?

"You need to keep monitoring the deletion, alteration, creation and utilisation of certain data over time to detect activities that might be creating a risk in your environment. Without monitoring, you might not even realise you have had a data loss," says Casey. "The shift to more hybrid working means it is more important than ever to know where the risks might come from, especially if people are connecting to the cloud from all over the world."

Own Company's vice president of services, Andrew Hart, says robust authentication and authentication processes will control who can log in to particular data sets.

"It is not sensible to either lock down all your data or go to the other extreme and have all data open to everyone just because there is value in it. You need something in the middle," he says.

Ultimately, companies need to educate their employees at all levels about data governance, especially if the worst happens and a recovery plan needs to be implemented smoothly.

> **Not all backup providers are equal, so you have to look at data governance as a whole**

"There is an increasing number of problems, not only from external cyberattacks but also from within organisations where we see accidental data deletions, file corruptions or data being taken when it shouldn't," says Hart. "We help clients to be more resilient when it comes to data recovery, readiness and response. A backup is fine, but do individuals know their roles and responsibilities to get things up and running again? Are they aware of regulatory concerns and who must report data loss? Training and regular drills are essential."

He also points out that SaaS data does not exist in isolation. With an integrated system, there can be different impacts on data recovery and loss because data is being fed in and going out of the enterprise all the time.

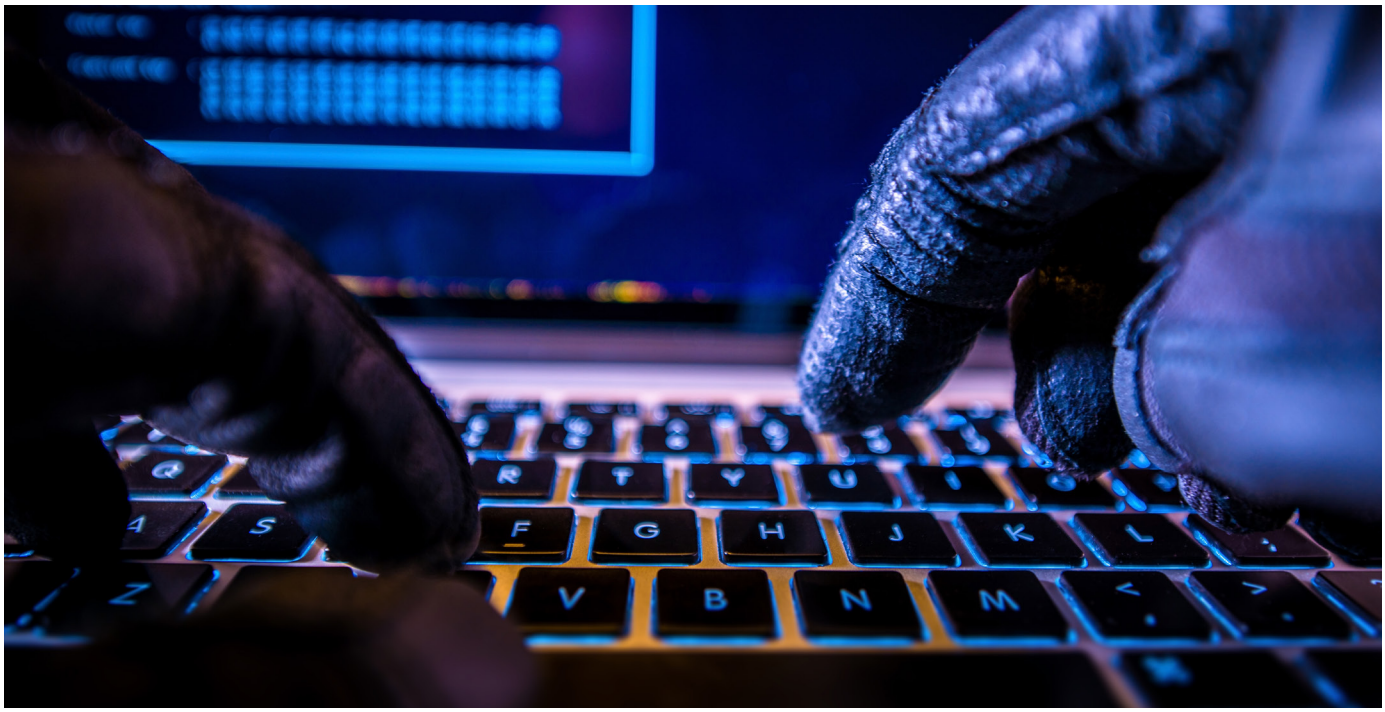
"You need to know if the data loss was isolated to the customer software such as Salesforce or if it has permeated elsewhere. Also, if you are putting data back into Salesforce, what impact does this have downstream in an integrated system? Maybe you need to stop users accessing the system," he says. "Backup is the easy part; it is in the recovery process where investment needs to be made."

So how quickly can data be recovered? Own Company says most clients are quite relaxed about this because they know their data is backed up. They tend to have a more strategic approach and, when problems do occur, take their time to discuss what should happen next with different stakeholders.

"If an organisation is working with an expert third-party provider and there is trust in that relationship around the backup of the data, there will be a conversation about what data is the priority to be repaired and restored," says Casey. "Data is incredibly valuable and a data loss is not always immediately obvious. We provide training and assessments to help organisations become more mature around data recovery, readiness and response so their data governance remains robust."

For more information please visit owndata.com

> **Backup is the easy part; it is in the recovery process where investment needs to be made**



Three considerations when assessing data risk

What approaches should leaders use to identify threats and weaknesses and determine the business impact of risks?

Steve Hemsley

Research by Own Company reveals that 60% of businesses have experienced a data loss in the past two years and one-third have experienced more than one. Only two-thirds could restore all the data lost.

These findings come at a time when critical data is increasingly being stored in SaaS systems and 81% of organisations believe cloud applications are more important than ever. So, what strategies should leaders use to identify data risk?

1 Understanding the potential business impacts of risks

Determining how a risk might impact the business must be a priority. "Risk is anything that results in some form of loss for the business," says the former chief analytics officer at Lloyd's of London, Waseem Ali. "That loss could be material, financial, brand reputational or impact on customer acquisition."

Today Ali is CEO of Rockborne, a talent company supplying data consultants to businesses that need to strengthen their data and AI teams. He says companies must ask themselves: what could someone do if they hacked into the biggest asset in our organisation?

"If someone hacked into the model behind an ecommerce website, the recommendation engine could break," says Ali. "Let's say 30% of additional sales come through that recommendation engine, this could represent a 30% earnings loss to the business."

One tip for communicating such a technical message internally regarding the potential business impact of any data leak is to use real-life case studies to convey a story to stakeholders of what could happen to the business – and people's jobs – if valuable data is lost.

Running an annual exercise of how the organisation would respond to a ransom attack helps ensure that their people, processes and platform are prepared. This is required by updated security and resilience regulations.

2 Identifying exploitable vulnerabilities

Data often leaks when there is a lack of knowledge of how much an organisation has, where it is stored and how sensitive it is. Do businesses really know who has access to their data and how secure it is?

Richard Seiersen is a cybersecurity expert who co-wrote the book How to Measure Anything in Cybersecurity Risk (Wiley). He says identifying vulnerable areas starts with asking what a company stands to lose and mapping different risks at various levels of the business.

Today Seiersen is chief risk technology officer at Qualys and says the first 'highest level' would be your crown jewel assets.

"These are the assets most clearly associated with the largest magnitude of probable losses," he says. "These must get the most attention – with particular care given to the operational impact of any proposed remediation."

An organisation's data can become vulnerable when a third-party provider holds it.

Experts advise that during the onboarding of suppliers, contracts should insist on compliance with various regulations, for instance, GDPR. It should also be clear where exactly liability lies if there are any data breaches. This may depend on what the data controller can recover from the processor if there is a security incident.

There are also process-related vulnerabilities that organisations might not have considered. For example, do too many people have access to some data or is data being replicated in other places? Collaboration between departments should be encouraged to reduce the risks and plug vulnerabilities.

3 Performing a security risk assessment

It is impossible to eliminate data security risks completely but a security risk assessment can reveal vulnerabilities. Often a third party will review a business's platforms, tools and current risk levels. Considered risks include availability of data as well as confidentiality and integrity. This is particularly important when a data loss or ransom attack disrupts the business.

Any assessment should clarify how data flows into the business and from where. It should also analyse how data travels around the organisation and how and when it leaves. For example, the first data point for a retailer could be a customer coming into a store and buying a product. The data would then be stored and translated into an email receipt.

Top strategies organisations are taking to identify and assess risk

Own Company, 2023

"The input and output points can be easily accounted for, but for many businesses, it is the period in between which hasn't been comprehensively mapped out," says Ali. "This is where an organisation's data maturity and attitude to understanding risk can influence whether enough resource is being funnelled into breaking down every leg of that data's journey to reduce risks."

Del Heppenstall, head of UK cyber at KPMG UK, says many heads of security have relied on a basic risk assessment matrix that considers how likely the risk is and how damaging the risk would be to the organisation.

"This is an immature and subjective approach," says Heppenstall. "Organisations should have a more scenario-driven method underpinned by threat models. Any assessments must be performed on an ongoing basis to ensure the effectiveness of the controls, and address potential risks to the data."

Lauren Wills-Dixon, a data protection expert at law firm Gordons, says organisations should also run a data protection impact assessment (DPIA). This internal document identifies how data is processed and whether it is being used in the intended way so the risk to personal data is minimised.

"A DPIA is required for 'high risk' processing activities which could impact an individual's rights and freedoms," says Wills-Dixon. "It's good practice to implement at the start of a new project or technology, but certainly before any processing activity takes place."

She believes too many organisations still consider privacy as an afterthought and take action once the damage is done. "In a world where AI processing is growing and risks are somewhat unquantifiable, impact assessments are of ultimate importance."

Own is the leading data platform trusted by thousands of organizations to protect and activate SaaS data to transform their businesses. Own empowers customers to ensure the availability, security, and compliance of mission-critical data, while unlocking new ways to gain deeper insights faster. By partnering with some of the world's largest SaaS ecosystems such as Salesforce, ServiceNow, and Microsoft Dynamics 365, Own enables customers around the world to truly own the data that powers their business. It's their platform. It's your data. Own it.

Raconteur

Publication sponsored by

Although this publication is funded through advertising and sponsorship,all editorial is without bias and sponsored features are clearly labelled. For an upcoming schedule, partnership inquiries or feedback, please call +44 (0)20 3428 5230 or e-mail info@raconteur.net