The Data Security and Governance Sales Guide for MSPs

This guide helps you have the conversations with SMBs that lets them know you understand their concerns while clarifying their risks to position your MSP as the trusted partner to secure their data estate.

pax8.com

What Are Data Security and Data Governance?

Data security and data governance are closely connected and both essential to effective information protection.

- **Data security** means protecting your client's most valuable information from unauthorized access, loss or misuse, whether by cybercriminals, employees or AI-powered threats.
- **Data governance** is the set of policies, roles and procedures that ensure data is managed responsibly, stays compliant with regulations and is trustworthy. Without proper governance, security efforts can miss hidden risks, leaving your clients vulnerable. Strong data security and governance work together to safe-guard the entire data estate.

Together, they create a comprehensive defence that not only shields data but also ensures it is handled responsibly, compliant with regulations and trustworthy for business use.

Making Data Security Real for Your Customers

74% of organizations recently surveyed experienced at least one data security incident in the last year.[1] But when you talk to your customers about data security, it's not just about facts and features. It's about helping them truly understand the risks their business faces every day.

Try opening the conversation with something like:

"Imagine leaving a safe open without any security around it. No cameras or tracking to see who enters and leaves, just asking every employee not to go in the safe. Feels risky, right? Yet that's exactly what happens with sensitive business data when the right protections, controls and monitoring aren't in place."

Attacks grow more sophisticated every year with AI tools being responsible for 40% of data security incidents in 2024, nearly double the figure from 2023, and the average cost of a cyberattack is over $250K and up to $7M.[1]

Why Data Security Can't Wait

Every day, organizations suffer data breaches that cost them millions, damage their reputations and put their customers and employees at risk. Insiders account for 20% of data breaches, adding to costs. The total average cost of activities to resolve insider threats over a 12-month period is $15.4 million.[1] Data security isn't just about compliance or ticking a box, it's about protecting the business you've worked so hard to build.

Here's what can happen without strong data security:

Scenario	What Happens	Risk Type
Employee clicks a phishing email and gives up their login	Outsider gains access to sensitive systems and data	Data compromise by external threat
Staff member copies files onto a USB and uploads to their own cloud	Critical company information ends up in a competitor's hands	Data theft by malicious insider
Someone accidentally pastes sensitive data into a generative AI tool	Proprietary data leaks outside the company	Data leak by negligent insider
Disgruntled employee deletes or alters key data before leaving	Company loses essential information, projects or IP	Data sabotage by disgruntled insider

If you wouldn't trust every employee with an open safe, don't trust them with your most valuable digital information without safeguards.

Understanding the Risks

External Risks

- Phishing attacks, malware and hackers constantly looking for ways in.
- Cybercriminals exploiting weak points in your cyber defences.

81% of SMBs believe AI increases the need for additional security controls.[2]

Internal Risks

- Well-meaning employees making mistakes with sensitive data.
- Malicious insiders seeking profit or retaliation.
- Departing staff taking valuable data with them.

68% of SMBs consider secure data access a challenge for remote workers.[2]

Many risks come not only from direct attacks or insider actions but also from gaps in data governance. Poorly classified data, unclear ownership and weak access policies leave SMBs exposed to breaches, compliance fines and loss of customer trust. MSPs that help clients implement effective governance will better manage these risks and deliver stronger, sustainable data security.

New and Amplified Risks: Generative AI

It's no longer just traditional threats you have to worry about. Generative AI brings a whole new set of data risks that can't be ignored. As it introduces new attack surfaces and data leak risks, clients must govern how AI tools access and use sensitive data. Strong governance policies, such as data classification, controlled AI access and monitoring, help ensure that adopting AI enhances productivity without putting data security or compliance at risk. Here are the data risks associated with generative AI:

Scenario	What Happens	Risk Type
Sensitive data leaks	Employees accidentally or negligently share proprietary or regulated data with AI tools	Data leak
Insider threats	Insiders overshare or intentionally leak confidential data using generative AI, by accident or design	Data theft/data leak
New attack surfaces	Generative AI systems vulnerable to attacks (jailbreaks, prompt injections, hallucinations)	Data exfiltration/manipulation
Expanded attack surfaces	AI orchestration, plug-ins, model flaws or unprotected training data introduce new gaps	Emerging AI vulnerabilities

If you wouldn't leave a safe open without any oversight, is it really any safer to leave your company's data wide open to AI-driven leaks, accidental exposures or insider misuse?

Organizations are concerned about data leakage in generative AI, with over 80% of leaders citing leakage of sensitive data as their main concern around adopting generative AI.[5] But 75% of global knowledge workers are already using AI and the number keeps rising.[4] So the threat is quite real and protecting them and your business is vital. Because generative AI doesn't just multiply your risk. It gives every employee and every attacker new tools to steal from your business, whether by accident or on purpose.

Building a Data Security and Governance Plan with Your SMB Clients

When you discuss data security with your SMB clients, it's important to position this not just as a technical checklist but as a strategic approach to protect their business now and as they grow, especially considering risks from generative AI.

Discover and classify data:

Know what data exists, where it lives, who owns it and categorize it by sensitivity. This clarity drives better protection and reduces exposure risks.

Manage access and enforce policies:

Use role-based access controls, multi-factor authentication and clear governance policies to control who can access data and AI models.

Apply key security controls:

Implement email security, endpoint detection, segregated backups and continuous threat monitoring to defend against breaches and AI-powered attacks.

Train employees:

Educate staff regularly on phishing, data handling and AI risks. Informed employees are a vital defence layer.

Govern AI usage and compliance:

Set policies to manage AI tool data inputs and outputs, ensuring privacy, ethical use and regulatory adherence.

Control data lifecycle:

Manage data from creation to secure deletion to minimize risk and maintain compliance.

This flexible framework helps MSPs guide SMBs in building scalable, effective security and governance programs that protect data, ensure compliance and prepare for AI-driven challenges.

The Cost of Fragmented Security

Fragmented security efforts are often accompanied by fragmented governance—multiple inconsistent policies, unclear roles and uncoordinated compliance efforts. MSPs that help clients establish unified governance alongside integrated security tools unlock stronger visibility, faster response and easier AI risk management. The typical organization uses more than 12 different solutions to secure their data estate. This leads to:

Exposed infrastructure gaps

Disparate systems often can't 'see' or defend against threats that move between silos, leaving blind spots that attackers can exploit.

Operational complexity

Juggling multiple tools means more overhead, higher costs and greater chance for misconfigurations or gaps in policy enforcement.

Lack of unified visibility

Without a centralized view, it's nearly impossible to spot, investigate and respond to threats, especially the fast-moving ones enabled by generative AI.

Unified, integrated security closes these gaps—so you're not just securing against today's threats, but also tomorrow's.

Positioning Microsoft Purview as a Strategic Compliance Solution

To wrap up your data security strategy, we recommend introducing Microsoft Purview through Microsoft 365 E5, Microsoft 365 E5 Compliance add-on or Purview Suite for Business Premium. This comprehensive solution is purpose-built to:

- Break down data silos and enable unified protection across your environment.
- Enhance regulatory compliance with intelligent, automated tooling.
- Safeguard Microsoft 365 Copilot data with advanced, AI-ready security features.

The Microsoft 365 E5 Compliance Bundle delivers end-to-end data security and compliance readiness. This is ideal for organizations preparing for generative AI and evolving regulatory requirements.

Connect with a Pax8 expert to learn more about pricing for Microsoft Purview or take advantage of our Pax8 Professional Services.

Secure Your Clients' Data and Grow with Pax8

Strengthen your clients' data security. Partner with Pax8 to deliver comprehensive, unified solutions that safeguard sensitive information from external attacks, insider threats and emerging risks like generative AI.

For more support in driving customer conversations, access our Data Security Sales Talk Track and download the comprehensive Data Security Fact Sheet packed with insights and messaging tailored to help you confidently sell data security solutions to SMB clients.

With Pax8, you're empowered to build trust, lower risk and drive personalized business growth through smarter, stronger data security strategies tailored for SMBs.

pax8.com

1. Microsoft Data Security Index, 2024 https://marketingassets.microsoft.com/gdc/gdcqTplAT/original
2. Woodgate, Scott. "7 cybersecurity trends and tips for small and medium businesses to stay protected." Microsoft, October 31, 2004.

   https://www.microsoft.com/en-us/security/blog/2024/10/31/7-cybersecurity-trends-and-tips-for-small-and-medium-businesses-to-stay-protected/
3. First Annual Generative AI Study: Business Rewards vs. Security Risks, Q3 2023, ISMG, N=400