The Big Book of Selling Data Protection
What the most successful MSPs are doing differently—and how you can do it too

eBook
# Table of Contents

When business is driven by data, protection is essential ......................................................... 3

  What’s the difference between backup and data protection? ................................................. 3

  How do I sell more data protection? ......................................................................................... 4

Understanding the client’s needs and perspective ................................................................. 5

  How can I tell if a client needs data protection? ..................................................................... 5

  Questions to ask during the discovery phase ......................................................................... 5

Educating the client on the value of their data ......................................................................... 7

  How do I convince a client data protection is needed? ...................................................... 7

  Uncovering the real cost of downtime ................................................................................. 8

Tailoring a solution to the client’s needs and budget ............................................................. 9

  Does one size fit all? .............................................................................................................. 9

  How do I meet the needs of all my clients? ......................................................................... 10

  What should I look for in a data protection solution? ...................................................... 10

Tips and tricks for completing the sale ................................................................................... 12

  When is the best time to discuss data protection? ........................................................... 12

  How do I deal with objections? .......................................................................................... 13

  What to do if they still say no .............................................................................................. 13

Want to sell even more data protection? We can help .......................................................... 14

About N-able ............................................................................................................................. 15
When business is driven by data, protection is essential

From colossal enterprises to the smallest home-based ventures, all businesses depend on data. That’s why backup and recovery solutions have become essential safeguards against data loss.

Companies large enough to tout their own dedicated IT teams tend to be fairly well-protected. But small- and medium-sized businesses (SMBs) are often lacking in this area.

Many SMBs have resorted to a hodgepodge of unreliable, cobbled-together backup systems. Because they are often cost-conscious, it can be hard to convince them to switch to a new solution. Even though they read the headlines, they don’t always appreciate how much risk they face—or what data loss could do to them.

So how do top MSPs overcome those obstacles and capitalize on the backup opportunity? By selling not just another backup product, but something much more valuable: comprehensive, full-service data protection.

WHAT’S THE DIFFERENCE BETWEEN BACKUP AND DATA PROTECTION?

Data protection refers to a broad range of capabilities that go far beyond just running a backup. Companies today now expect their MSPs to:

- Safeguard their data against compromise and loss from user error, malicious attacks, and service outages
- Make decisions with their data security, privacy, and governance requirements in mind
- Ensure their data is available when needed—and immediately recoverable if disaster strikes, with minimum downtime

Because data protection can encompass so many different service elements, it can play a key role in helping you build more recurring revenue:

<table>
<thead>
<tr>
<th>Reactive</th>
<th>À la carte</th>
<th>Proactive</th>
<th>Managed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Supporting whatever backup software the client already uses.</td>
<td>Selling either software or a basic service as a monthly line item to provide ongoing management of backups and reporting.</td>
<td>Sold as part of a package (per user, per device) to provide ongoing backup, reporting, and recovery testing—as well as recovery as needed.</td>
<td>Sold as part of a bundled package (per user, per device) to provide ongoing backup, reporting, and recovery testing—as well as recovery with defined SLA levels.</td>
</tr>
</tbody>
</table>

$ $ $ $ $ $$$

The closer you move toward the “managed” side of the spectrum, the greater your potential for profitability—and you’ll provide more value to your clients.
YOUR PURPOSE IS CLEAR

Many small business owners have spent 10, 20, or 30 years building up their companies—and they're counting on you to keep them from losing their livelihood and legacy.

That's one of the main reasons you need to provide them with more than just basic backup software.

HOW DO I SELL MORE DATA PROTECTION?

Despite the challenges inherent to the SMB market, building up your data protection business doesn’t have to be difficult. You just need the right approach—and the right solution.

The right approach can be broken down into three simple steps:

1. **Understand** the client’s needs and perspective
2. **Educate** the client on the value of their data
3. **Tailor** a solution that fits the client’s needs and budget

Read on for an in-depth look at each step.

Did you know?

Small businesses are the victims in nearly half (43%) of all data breaches¹.

---

Understanding the client’s needs and perspective

HOW CAN I TELL IF A CLIENT NEEDS DATA PROTECTION?

Many MSPs tend to jump right into pitching a solution the moment a potential client shows interest. What you really need to do is slow down.

Pause and ask questions to make sure you truly understand the client. You need to uncover their goals and assumptions to find out what really matters to their business, so you can provide them with the best possible solution.

In sales speak, this is called the discovery phase.

Beyond learning more about their business needs, you should also take this opportunity to better understand where their data lives. Many SMBs store data on laptops, phones, and other endpoint devices—meaning it’s not just their servers that need backing up.

Make sure you fully appreciate the impact a major data loss would have on their business and how long it would take them to reproduce that data. You’ll need to take into account any regulatory requirements around data privacy to which your client may be subject (such as HIPAA) and what the consequences might be if they aren’t compliant.

With that information, you’ll be in a prime position to pinpoint exactly where data protection is needed. You’ll also be better able to assess their existing backup and recovery system and draw attention to any areas for improvement.

**Remember, you’re the expert**

Your clients hire you for your expertise and expect you to be their trusted IT advisor. At the end of the day, they probably don’t care what data protection solution you’re using. Like spark plugs in their car, the brand doesn’t matter; they just want it to work.

By going through this discovery phase, you can confidently deliver a solution that will meet their needs—and keep their trust long-term.

**QUESTIONS TO ASK DURING THE DISCOVERY PHASE**

**To get started:**

- What are you doing today to protect your business?
- Have you experienced any downtime in your business? What was the impact?
- Do you have any concerns about how downtime would affect your business?
• Do you have a plan in case your systems or data are not available?
• How has your reliance on computer systems changed in the last five years?
• Could your business operate if it had to go back to pen and paper temporarily? For how long?
• Does your current situation keep you up at night?
• What are your goals for the next two years? How do you plan to modernize and grow your business?

To dig deeper:
• How many transactions do you typically process in an hour? What would downtime cost you per hour?
• What legal liabilities might you face if your services were suddenly unavailable?
• How long could you realistically go without access to your data?
• What would be the impact on your reputation if you were unable to serve customers for a day? For a week?
• Which business processes and applications are most essential and therefore must be working again first?
• Which underlying systems and data are required to get those critical applications up and running again? Which servers or devices do those systems and data live on?

Finally, look at their other business applications and data types:
• Which could safely be unavailable for a longer period with minimal business impact?
• What would it cost (in terms of employee time and wages) to recreate this less important data if it were lost completely?

Speak plainly

Depending on how technical your client is, it’s probably best not to use terms like RTO (recovery time objective) or RPO (recovery point objective). Just know you’re essentially defining these qualities through the questions you ask.
Educating the client on the value of their data

HOW DO I CONVINCE A CLIENT DATA PROTECTION IS NEEDED?

Don’t start by trying to sell a specific product or solution to your prospective clients. To convince them they need data protection, begin by educating them about the value of the data located on the servers and devices—and how the loss of that data could do serious harm to their business.

This is basically a two-part argument:

Data loss happens

The ways businesses can lose presentations, financial reports, and other important files are numerous. Whether it’s file corruption, hardware failure, malware attack, accidental deletion, or a natural disaster, every business is at risk. While your clients might wave away the idea they could unknowingly scrap an important file, accidental deletion is in fact one of the most common forms of data loss. And they’ve definitely seen the headlines about businesses crippled by ransomware—and need to be aware the same thing most certainly can happen to them.

Productivity suffers

The loss of an essential file means it has to be rebuilt, which will eat up hours of time that could be spent on other critical tasks. Every business has important data that would be difficult or, in some cases, impossible to recreate. Months or years of financial information would be impossible to replace, yet many businesses store their accounting or other critical data on a single workstation with no duplicates.

Did you know?

As a consequence of major data loss:

- 19% of SMBs experienced less than one hour of system downtime
- 41% experienced one to eight hours of downtime
- 40% experienced more than eight hours of downtime

UNCOVERING THE REAL COST OF DOWNTIME

When making the case for data protection, put it in terms any business owner will understand: money.

Two things that will quickly justify purchasing data protection are data losses that lead to major financial losses, or data that would take hours or even days to recover or replace (which costs employee time and effort).

To make this more concrete, ask your client to envision a scenario where their systems are completely down, with zero access to any data—and then do the math on what that will cost. In comparison, data protection will look like quite a bargain.

You can use the following example to guide your conversation:

**25-employee design firm**

$100,000 revenue per employee per year

25 employees X $100,000 per year = $2.5 million in total revenue per year

250 working days per year = $400 in revenue per day

$400 X 25 employees = $10,000 in revenue per day

**TOTAL IMPACT:**

**Lost productivity:** $10,000 per day

**Remediation:** $800 per day

**Reputational cost:** unknowable

• What if a project is not delivered?
• What if they lose a customer?
• What is the word-of-mouth impact?

Other types of risk

In addition to financial risks, such as lost productivity, remediation costs and reputational damage, there are other types of risks your small business customers are expecting you to address.

For example, does your client have to comply with strict regulations on data privacy, security, and archiving? What might the consequences be if personal, financial, or medical data were lost or stolen?
Tailoring a solution to the client’s needs and budget

DOES ONE SIZE FIT ALL?

In short, no. Not all your clients need (or can afford) the same level of protection. That’s why it’s important to align your services with your clients’ expectations and requirements around downtime and availability.

Consider the “maturity model” below:

Data backup
- Mostly onsite
- No DR plan
- Recovery is best effort
- High risk to business

Disaster recovery
- Full system backup
- Onsite and offsite
- Periodic recovery testing
- Medium risk to business

Business continuity
- Full system backup
- Onsite and offsite and fallback location
- Continuous recovery testing
- Low risk to business
- Minimal downtime
- Part of business continuity plan

Right now, where are you in terms of the backup, recovery, or data protection solutions offered to your clients? Can you effectively meet the needs of customers across all parts of this model? If so, you’ll likely see higher margins and more profit.

Practical tip

Once you’ve come up with a successful approach to selling data protection to a certain type of business, like a law firm or retailer, you can often apply similar methods to other clients in the same space.
HOW DO I MEET THE NEEDS OF ALL MY CLIENTS?

Offering a single solution would make things easier for your technicians but lead to a pretty lousy customer experience. But if you were to create completely custom solutions for every client, things would get quite difficult to manage on your end.

By offering **two or three standard packages**, however, you can effectively meet the recovery requirements and budget parameters of the vast majority of your clients.

Providing consistent data protection packaging and pricing at various service levels (e.g., low-cost, mid-range, high-end) will help you offer “just right” protection for many different customers and data types. Here’s how it could look:

<table>
<thead>
<tr>
<th>BRONZE</th>
<th>SILVER</th>
<th>GOLD</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Data backup</strong></td>
<td><strong>Disaster recovery</strong></td>
<td><strong>Business continuity</strong></td>
</tr>
<tr>
<td>$75 per server</td>
<td>$100 per server</td>
<td>$150 per server</td>
</tr>
<tr>
<td>• Full system backup</td>
<td>• Full system backup</td>
<td>• Full system backup</td>
</tr>
<tr>
<td>• One backup per day</td>
<td>• Two backups per day</td>
<td>• 12 backups per day</td>
</tr>
<tr>
<td>• 28 days retention</td>
<td>• 60 days retention</td>
<td>• 90 days retention</td>
</tr>
<tr>
<td>• Offsite storage</td>
<td>• Offsite storage</td>
<td>• Offsite storage</td>
</tr>
<tr>
<td></td>
<td>• Hybrid backups for faster restores</td>
<td>• Hybrid backups for faster restores</td>
</tr>
<tr>
<td></td>
<td>• Monthly archiving</td>
<td>• Monthly archiving</td>
</tr>
<tr>
<td></td>
<td>• Quarterly restore testing</td>
<td>• Monthly restore testing</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Standby VM with daily screenshot</td>
</tr>
</tbody>
</table>

For the least critical data (or most limited budgets) you can provide a basic level of recovery with a 24-hour SLA and varying recovery locations.

At this level, you can offer recovery in the cloud, with an SLA of resuming operations within a four-to-12-hour window.

A full, warm standby server is available for immediate recovery of your clients’ most critical applications and data.

With these options on your services menu, your clients could even choose to protect different types of data at various levels.

WHAT SHOULD I LOOK FOR IN A DATA PROTECTION SOLUTION?

Your success ultimately hinges on offering the right data protection solution—one that meets SMBs’ needs in terms of cost and features.

The ideal data protection tool should be flexible and configurable enough to be offered across multiple service-level tiers and packages. It should also be:
Easy to deploy and use

You need to be able to manage your customers as efficiently as possible. Look for a web-based, multitenant dashboard that allows your technicians to view all customer data types across multiple environments from a single screen—checking the backup status of every managed server and device and then drilling down into issues with a single click.

Versatile

Your solution should be able to back up and restore data from any location; on physical and virtual servers and workstations and in the cloud as part of software-as-a-service applications, like Microsoft 365™. It needs to protect data across the full range of operating systems and hypervisors. And it must be capable of all forms of restoration, including file/folder-level recoveries, bare-metal restores, and virtual or continuous recoveries.

Cloud-first

An onsite backup is good for fast recovery, but local storage is susceptible to the same vulnerabilities as your client’s other on-premises IT systems. A solution that includes offsite, remote cloud storage will put you in a better position to protect against all-out disasters. The ideal solution will offer both options—and we call this “cloud first” because while it’s not cloud-only, it also doesn’t rely on local-only protection.

If you can use a single solution that boasts all these features, it will be easier for you to provide the service levels to meet your SMB customers’ varying needs. You’ll also decrease your own cost of service delivery through improved efficiency and automation.

Make your techs more productive

Switching between multiple backup products can add hours to a technician’s week. Reducing the number of backup products and dashboards to be supported can bring real productivity benefits—and free up technicians to focus on more valuable, interesting, and engaging work.
Tips and tricks for completing the sale

WHEN IS THE BEST TIME TO DISCUSS DATA PROTECTION?

When disaster strikes, your customers will inevitably call you—and expect you to save them in their time of need. By that point, it’s already too late to have the conversation about data protection. If they don’t yet have an adequate solution in place, your options to help will be extremely limited.

The best way to avoid this scenario? Don’t wait. On your next client visit, start talking about data protection. If you can, do this in a face-to-face meeting rather than by phone or email. Take the lead and walk the client step-by-step toward the right level of protection for their specific business needs.

Upselling to clients still using basic backup

If your client recently lost data and had a poor experience recovering it with their existing system, that gives you the perfect opening to explain how a more robust data protection solution could have prevented their headaches.

Do you perform a regular “health check” assessment, where you sit down with the client and review their IT environment? Do you provide regular reports on their backups—and can you pinpoint how their current system may not be delivering what they need in terms of storage or recovery? Have they adopted new services or platforms, or moved some of their critical business applications to the cloud, since your last assessment?

Any of these represents an opportunity to upsell them on a more robust and comprehensive data protection solution.

When upselling, it’s best to start by pitching your mid-tier option first. If the client balks at the price, you can always offer your lower-cost option instead. And if they decide they want a greater degree of protection, that’s good for them—and for your bottom line!

Use the headlines to your advantage

News stories about data breaches, ransomware, and other cyberattacks can serve as a good point of reference during conversations with your clients.

Don’t be afraid to point out what happened to the business across town that lost all its data—and how you want to do everything you can to make sure the same thing doesn’t happen to your clients.
HOW DO I DEAL WITH OBJECTIONS?

Some cost-conscious clients may hesitate to make the investment. Often, they’ll try to compare apples to oranges. That is, they might have done a quick online search and found a really cheap backup product (an apple) and can’t understand why your full-service data protection solution (an orange) can’t match that price.

Your task is to educate them on the difference between apples and oranges—and how the data protection service that you’re offering is much more than just backup software.

Clearly explain that, in addition to the software and storage, they’ll get full-service protection that includes backup monitoring and testing, business continuity, and one-call data recovery if something goes wrong.

You might also position your solution as a kind of insurance policy—something they pay for each month that provides peace of mind knowing they’re covered in case disaster strikes. After all, your client wouldn’t go without insurance on their storefront. So why wouldn’t they also have protection for their data?

Price is never an objection

Even if someone starts by citing price as their objection, when you start asking questions, you’ll almost always find that it’s not really about price. If you focus on the value your services offer, you should have no trouble allaying their concerns.

WHAT TO DO IF THEY STILL SAY NO

If the conversation doesn’t go as hoped and the client still refuses to invest in even the most basic level of protection, you’re left with three options:

• Prepare a release of liability letter explicitly stating you can’t be held responsible if data is lost and no backup is in place. The very act of being asked to sign this letter will make many clients think twice and reconsider their decision.

• Set up your own backup product in the background, then roll the cost of document-level protection into your managed services offering. This prepares you to be the hero if something goes wrong while offering the possibility of upselling to higher-tier data protection services as needed. In this model, you’re not charging specifically for the service, but rather including its cost in your basic services agreement.

• Make paid data protection a standard part of every managed services contract. Don’t allow something this important to be optional. As a condition of doing business with your firm, require all your clients to have at least a basic data protection service in place. Include it as a line item in every contract. If they question it, you can have a conversation about protection levels and price options.
Want to sell even more data protection? We can help.

To make the most of the advice in this guide, you'll need to offer your clients a great data protection solution.

**N-able™ Backup** is a modern, cloud-first data protection solution that is robust enough to handle data of all types and sizes—and to support all recovery types—from single deleted files to entire systems. With one product, you get the backup software, cloud storage, and a web-based dashboard to manage all your clients, as well as the flexibility to offer multiple service tiers to better meet their needs.

For more information, visit [https://www.n-able.com/products/backup](https://www.n-able.com/products/backup)

We also provide business and technical support to help you sell and deliver a comprehensive data protection offering.

If you want to learn more about sales and marketing, visit the SolarWinds MSP Institute. There, you'll find a wide range of resources and practical advice from industry leaders to help you grow your business.

You can also check out the **MSP Advice Project**, which offers real-world tips from other MSPs on how to overcome common business challenges.
About N-able

N-able empowers managed services providers (MSPs) to help small and medium enterprises navigate the digital evolution. With a flexible technology platform and powerful integrations, we make it easy for MSPs to monitor, manage, and protect their end customer systems, data, and networks. Our growing portfolio of security, automation, and backup and recovery solutions is built for IT services management professionals. N-able simplifies complex ecosystems and enables customers to solve their most pressing challenges. We provide extensive, proactive support—through enriching partner programs, hands-on training, and growth resources—to help MSPs deliver exceptional value and achieve success at scale.

n-able.com