Axcient

The QBR Handbook for MSPs

The Four Rs of QBR Success

Introduction

Central to successful sales and marketing outcomes in the managed services channel is the relationship between MSPs and their SMB clients. Quarterly business reviews (QBRs) reinforce these crucial **relationships** that often fall victim to "out-of-sight, out-of-mind" neglect. SMBs can forget how critical IT service providers are to business continuity and disaster recovery (BCDR) without significant shifts in IT needs or data loss incidents. If there's no reason to contact their MSP, many SMBs won't. They're satisfied as long as the business continues to run.

QBRs provide a regular intersection point between you and your clients outside of a disaster, allowing you to show the value of your MSP.

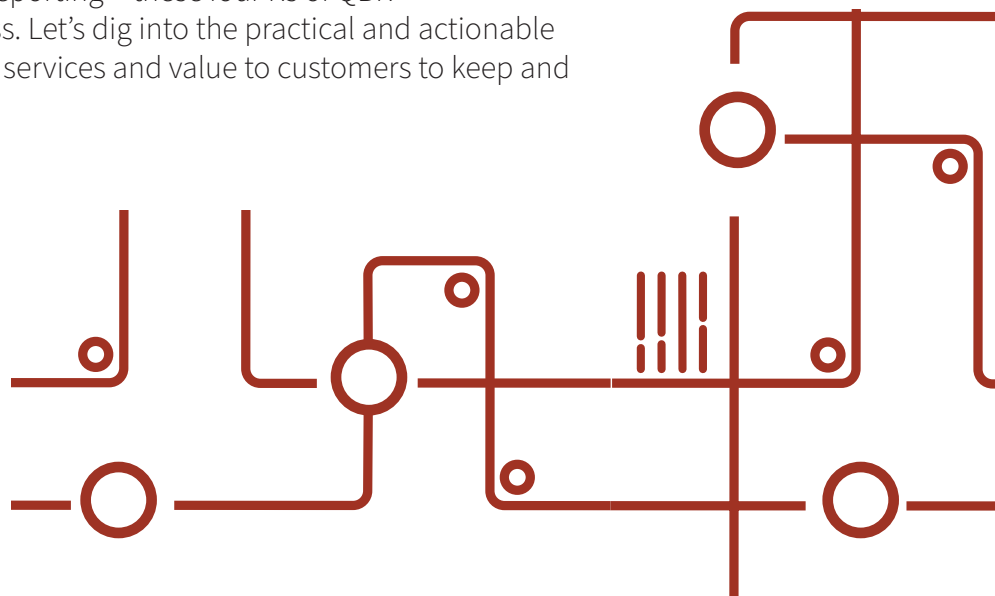
- Remind clients of the importance of your services and authority in SMB cybersecurity.
- Deliver updates on client backup health with reporting insights.
- Revisit proactive and post-disaster recovery features to reinforce preparedness.
- Complete disaster recovery testing to analyze the efficiency of disaster recovery plans.
- Participate in incident response planning to optimize disaster response.
- Introduce new and upcoming products, features, and upgrades.

Emphasizing your value contributes to client **retention**, which is vital for your MSP's bottom line. Increasing customer retention rates by just 5% can increase profits by 25% to 95%. Furthermore, retaining existing customers is less expensive and requires fewer resources than acquiring new clients. Therefore, fostering these relationships regularly and building rapport with clients is in MSP's best interest.

The face-to-face or screen-to-screen interaction during a QBR is a huge opportunity to generate new **revenue**. Put on your consultant hat and approach these meetings to retain and expand client connections, leveraging upsell and cross-sell opportunities and emerging trends like bundled services.

Existing customers are 50% more likely to try new products and spend 31% more, on average, than new customers. In-depth, timely, and accurate **reporting** is essential to back up service expansion and prove the benefits of your services over other MSPs.

Relationships, **R**etention, **R**evenue, and **R**eporting - these four Rs of QBR success are the cornerstone of QBR success. Let's dig into the practical and actionable ways MSPs can use them to highlight their services and value to customers to keep and then grow your customers.



First Things First: Starting Where the Client Is

Ideally, QBRs are completed frequently to provide evidence of growth over time. Of course, these interactions can also highlight inefficiencies and additional IT needs to avoid downstream interruptions and catastrophes. Regardless of where the client sits and what the intentions of the meetings are – for both MSPs and SMBs – you have to initiate QBRs based on the client's current state of IT.

Don't assume that SMBs know the ins and outs of their cybersecurity infrastructure or the current IT landscape. After all, they hired you to understand and combat these threat vectors with robust BCDR solutions and IT services. Therefore, it's your job to provide evidence of where clients are today, what warrants additional protections, and why updates to a client's environment are necessary.

Performance Metrics

MSP360™ recommends the following performance metrics to educate clients, measure progress over time, and gauge outcome success with context. Present these findings at each QBR to standardize meetings with familiar information that clients understand.

- **Proof of ongoing backup status:** Help clients sleep soundly with evidence of backup health, protection feature performance, and recovery readiness.

- **Open projects review and planning:** Show clients what cybersecurity projects are being executed on their behalf, review milestones achieved, and establish goals for the future that reflect the business needs.

- **Ticket metrics insights:** Utilize the following performance indicators to highlight current best practices and opportunities for improvement.
    - Endpoint and infrastructure management.
    - Patch management.
    - Endpoint, data, and network security.
    - Warranty reporting.
    - Server patch status.
    - Comprehensive network uptime.

Tracking the right metrics in your QBRs quantifies the tangible impact of your services on supporting your client's business goals.

01

Relationship Building for Client Loyalty

Quarterly business reviews provide a regular platform for strategic discussions between MSPs and your clients. These meetings go beyond transactional topics like equipment purchases or staff training. Instead, QBRs focus on the client's overall business goals and how your IT services can contribute to their achievement. Traditionally, QBRs are lengthy, report-heavy sessions that don't contribute much value to a client's overall business goals. However, a shift towards conversation and collaboration is taking hold, promoting a more effective team-oriented approach.

By prioritizing a strategic perspective in QBRs, MSPs transition from simply being another vendor to a trusted advisor. Focusing on long-term goals demonstrates a genuine interest in your client's success and your commitment to supporting and safeguarding their business. As an extension of your client's internal teams, conversations beyond traditional backup and disaster recovery (BDR) reaffirm your dedication to the client every quarter.

Reinforce Client Connections To…

Shape stronger partnerships: QBRs provide the framework for new MSPs and new representatives to forge lasting relationships with clients that foster their business growth. For established MSPs, QBRs offer a chance to solidify one-on-one connections even with a rapidly expanding client base.

- **Enhance customer retention:** By showcasing the return on investment (ROI) of your client's experience, services, and support, QBRs reinforce your MSP's value while solidifying your position as a trusted partner with a proven track record.
- **Strategically align through collaboration:** Open and honest discussions during QBRs enable a deeper understanding of your client's overall business health, future aspirations, and past achievements. With this knowledge, MSPs can tailor strategies and services to each client's desired outcomes.
- **Demonstrate outstanding service:** Regular QBRs remind clients of above and beyond service capacity and signal a genuine focus on the client's business success. This demonstration strengthens a client's perception of your MSP and categorizes you as an essential partner for the future, boosting the likelihood of contract renewals and long-term loyalty.
- **Proactively solve problems:** In-depth QBRs can uncover potential discrepancies within the service level agreement (SLA) or identify situations where clients may not be a perfect fit for your services. This proactive approach allows you to address concerns, make informed decisions, and potentially adjust or choose the right client relationships for a mutually beneficial outcome.

02

Retention with a Forward-Thinking Focus

Technology roadmaps must be fluid and adaptable to accommodate the ever-evolving cybersecurity threats and risks challenging SMBs. MSPs must continuously develop, assess, and adapt their roadmap to align with changing client business models. Equipping clients with the technology to propel them to the next level strengthens the MSP-client partnership and fosters long-term success.

Once clients experience wins with your MSP – through recovery success, consistent support, free marketing resources, significant cost-savings, or gaining the ability to scale and consolidate efficiently – it reinforces the positive impact of your MSP. As wins accumulate, clients feel more secure with their MSP and your capacity to keep up with their business.

5 Ways to Fuel Client Continuity:

Embrace the journey ahead.

While reviewing past success at a QBR is important, always looking ahead is just as essential. As you transition from reports proving MSP service successes to proactive discussions about expanding client growth, recommend new and upcoming solutions to client-specific problems like migrations and upgrades that align with their goals. Provide reasoning for your recommendations, clear timelines, and potential impacts to get on the same page as clients for informed decision-making about their IT future.

Align your roadmap with client goals.

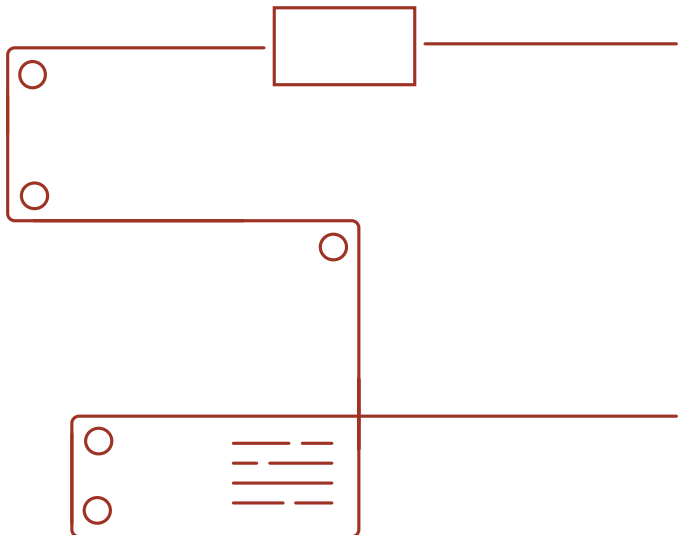
MSP QBRs present the perfect opportunity to revisit your technology roadmap and ensure it remains relevant to the client. Coordinating upcoming MSP enhancements with client goals requires a deep understanding of your client's business objectives, key initiatives, and future growth projections – all things you should revisit at each QBR. Proactively evaluate the impact of your MSP on a client's growth and expansion plans by continually removing pain points and introducing new and upgraded SMB capabilities.

Proactively plan for IT refreshes.
During your QBRs, assess the lifespans of remaining servers, storage capacity, and network equipment to proactively discuss infrastructure pivots such as embracing cloud technologies and consolidating IT stacks. Reviewing aging hardware regularly and replacing appliances on a staggered schedule helps avoid unexpected cost spikes. MSPs should recommend replacements that align with client growth plans, prevent disruptions, and ensure smooth IT operations. Additionally, MSPs should review endpoint systems and software for updates to keep clients competitive.

Give clients a reason to stick to you.
While every interaction between an MSP and its clients should build on a solid foundation and foster rapport, raising awareness of the conscientious work you perform on their behalf keeps clients "sticky." It's your chance to leverage reporting insights and analytics for transparency and trust between your MSP and the client. This requires robust reporting capabilities coupled with easy-to-digest and understandable outcomes.

Executive summaries provide a comprehensive overview of a client's environment, outlining why and how MSPs protect their client's infrastructure, data, and business continuity. Non-technical business leaders aren't typically aware of the intricacies of their protected systems. This is why executive summaries should be designed to illustrate what the client is paying your MSP for and how their data and infrastructure are being protected. As clients gain a deeper understanding of your services, SMB threats, and benefits to the business, they become more sticky, introducing opportunities for upsells and cross-sells as environments evolve.

Take a TL;DR approach.
While many in-depth reports excite MSPs, QBRs should be tailored to the client's priorities – keeping their business moving. Come to the table armed with easy-to-interpret insights that highlight the benefits of your particular MSP services. If you've embraced data security automation, rely on proprietary and patented technology, or reduce costs with things like pooled storage at a flat fee and hardware-free BCDR, don't relish details but focus on client takeaways. TLDR means too long, didn't read – but when QBRs are simple, clear, and understandable, even a layperson should see the obvious benefits. Take advantage of straightforward reporting structures with unobstructed insights that can easily be tailored to a client's environment.



03 

Revenue Growth Leveraging QBR Sales Opportunities

Like most SMBs, many MSPs lack the extensive resources for a dedicated sales and marketing team. QBRs provide the perfect segue to initiate cross-selling and upselling, but à la carte cybersecurity is being replaced with all-in-one simplicity. Yes, these sales strategies can increase sales, but MSPs aren't just selling—you're protecting, and that's the priority.

A Client Who Wants to Risk Its Data Is Also Risking Your MSP

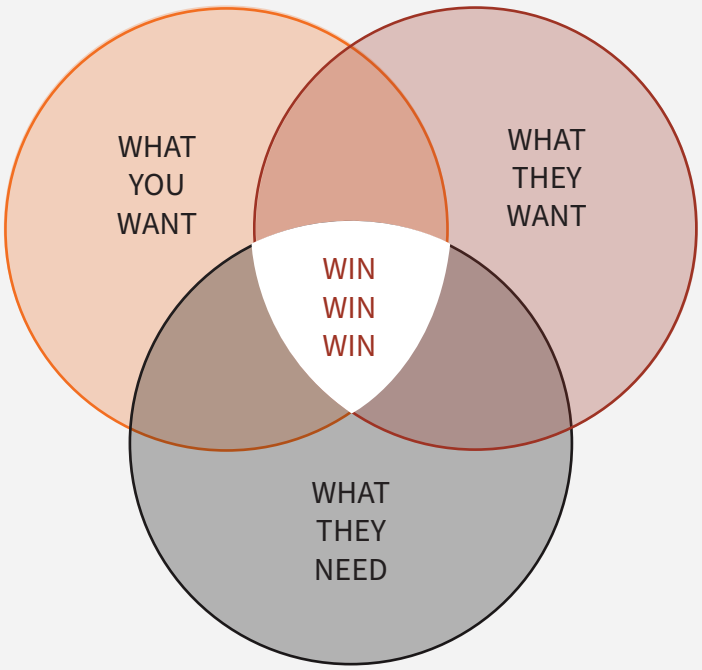
In today's cybersecurity landscape, MSPs are up against sophisticated, calculated, and frequent attacks on your clients and your MSP. Despite these realities, well-intentioned MSPs wanting to satisfy various client budgets end up offering some essential security measures as "optional." While tiered features can attract budget-conscious clients and introduce opportunities for cross-sales and upsells, they also allow customers to forgo business-critical data protections.

Clients without comprehensive business continuity and disaster recovery solutions jeopardize their business, end-users, and your MSP. Growing state regulations and the court of public opinion hold service providers responsible for data breaches. As an authority on cybersecurity resilience, it's your job to provide the appropriate layered security approach required to thwart attacks, prevent data loss, and ensure recovery.

When a client suffers a data loss incident, service providers face more than just recovery and restoration. Fines and penalties can be steep, but a public record of a breach under your watch quickly breaks trust and deters clients from resigning contracts. Avoid damage to your reputation and ability to compete in the market with a security-first approach to all client interactions – even in sales and marketing – especially at QBRs.

The Win-Win-Win Approach to Built-In Upselling and Cross-Selling

Bundling the essential protections your clients need is an efficient design to make BCDR solutions your MSP's most profitable offering. All-in-one data protection is a no-brainer for clients who understand the seriousness of a compromised IT infrastructure and the increasing dangers and costs of breaches and data loss.



Acknowledge That the Client Isn't Always Right…

Education is essential for clients with budget concerns or people who may think you're just trying to make more money. Many MSPs refuse to take on clients who are unwilling to accept their standard bundled services. Others may allow clients to pick and choose but require those clients to sign an acknowledgment of the education and guidance provided by the MSP and a waiver of liability in case of a data loss incident. Physically signing on to take responsibility in a disaster will often jolt clients into seeing the benefits of your bundled services for protection against the most probable – data loss due to human error.

…But Bundled Services Are.

Attracting new clients is more costly and resource-intensive than retaining and expanding existing relationships. Therefore, it's best to build on the interest of new clients during the initial stages of your partnership. If you do not require that clients accept your MSP's bundled services, highlight this option first as the MSP's most highly recommended service offering. Walk them through critical capabilities tied to SMB outcomes, explain what could happen without total protection, and inform them of the cybersecurity risks and the frequency of data loss due to accidental deletions.

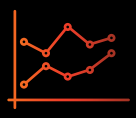
By expanding coverage and bundling one-stop-shop protection, MSP owners and sales teams get built-in sales opportunities every quarter with every client. Not only does that support your bottom line and competitive SLAs, but it generates a mutually beneficial win-win-win scenario:

Clients win uninterrupted business continuity and data availability that can withstand any data loss event—human error, cyberattack, or natural disaster.

MSPs win knowing they can recover client data if lost, breached, destroyed, or otherwise compromised.

MSPs win AGAIN, generating higher monthly recurring revenue (MRR) per client, contributing to margins, income, and profit growth.

Resource: An MSP's Blueprint for Profitably Selling Bundled Services

04 

Reporting Made Easy to Demonstrate Value

For a productive and efficient QBR, MSPs need a robust client executive summary that outlines what the MSP does to protect your client's infrastructure, data, and business continuity.

Tips for Turning Reports into Engaging Client Stories

- **Make it your own:** White-label digital and physical QBR materials with your MSP's logo and your client's logo to emphasize the collaborative nature of your relationship. Utilize their jargon and yours within a modern reporting structure that visually calls out the "need-to-knows" for further discussion and prioritization.

- **Summarize your services:** Craft a thorough and easy-to-understand presentation of the services and innovations in the client's contract as additional support for uninterrupted business continuity. You don't want customers to forget about all the behind-the-scenes systems and resources that go into protecting their data. MSP owners and non-tech leadership often overlook these built-in benefits, so remind them at QBRs alongside your roadmap for future improvements.

- **Provide proof of automation performance:** Automated BCDR features need tangible evidence to satisfy most cyber insurance requirements, cybersecurity compliance demands, and industry standards. These authorities must verify that automation is used according to best practices to mitigate human error. While you're emphasizing the high level of protection your MSP provides, you're also tying the value of these capabilities to helping clients remain in good standing with critical third-party regulations.

How MSPs Are Generating High-Value Reports for QBRs (and more)

Reporting, especially automated reporting, has long been a pain point for most MSPs. Data can be hard to uncover, needs additional information, or needs to be more thorough for actionable insights and analytics. At the same time, data-driven decision-making is necessary for client confidence, peace of mind, and MSP guidance toward the next best action.

Automation, Automation, Automation!

Thankfully, the same innovations used to automate disaster recovery planning and testing, backup integrity checks, and protection from ransomware are now available for generating client-specific analytics. Harnessing the power of automation is crucial for MSP productivity, cost-efficiency, technician happiness, and QBR success.

- **Eliminate error-prone manual reporting** in siloed workbooks, which can compromise your guidance and authority with clients and damage relationships by putting essential business functions—like BCDR preparedness, cyber insurability, standing with regulators, and SLA terms—in question.
- **Simplify to "easy button" reporting** to reduce tech debt while increasing reporting frequency for a better, broader, and more in-depth perspective of your protected systems, vulnerabilities, and client needs.
- **Streamline client-facing reporting** by removing the time-consuming manual interventions and stress of snapping screenshots, analyzing outcomes, and creating straightforward client reports. Instead, give customers visibility into their systems through self-service dashboards that do the reporting for you.

Many MSP vendors and solution providers have neglected optimizations for reporting functionality and efficiency, prohibiting MSPs from modernizing alongside their channel peers. It's never a wrong time to explore the market, and it's always a good time to break up with an insufficient provider who's compromising your competitive edge.

Utilize this BCDR Buyer's Guide for MSPs to weigh the strengths and weaknesses of solutions and vendors to find the right fit for your MSP and SMB clients today, tomorrow, and in the future.

Done-for-You Client Executive Summary Reports

As an MSP-only solutions provider, Axcient is dedicated to launching new backup insights and reporting to advance automation and usability for MSPs and your clients. Through regular product upgrades, new feature launches, and robust reporting capabilities, Axcient is constantly easing evolving MSP pain points.

The latest and greatest reporting tool for Axcient x360Recover, the most flexible and comprehensive BCDR solution for MSPs, is Axcient's Client Executive Summary Report. Now, MSPs can demonstrate their value to clients and security practices to third parties while introducing sales opportunities at QBRs and beyond.

What is Axcient's Client Executive Summary Report?

This is an in-depth, weekly report for MSPs to showcase their BCDR services, execution performance, and client outcomes. It's customizable and white-labelable, so MSPs can include specific information and branding when presented to clients, insurance providers, and regulators.

- **Deliver essential statistics** like the total number of backups completed and the estimated recovery time objective (RTO).
- **Add personalized comments** about backup performance within the report.
- **Get a detailed view of each client's protected systems**, complete with SLA history and vautomated backup integrity testing or Boot VM results.

How Do MSPs Leverage the Client Executive Summary Report?

Consistent and reliable reporting provides MSPs more opportunities beyond time and labor savings. Unlike other solution providers, Axcient's Client Executive Summary Report is reliable—there is no more missing or questionable data using limited "out-of-the-box" reporting. Instead, you can use unobstructed, accurate, and reliable data to make informed cybersecurity decisions for your MSP and customers.

Using…

- ☑ **Proof of backup test frequency and health** with Boot VM screenshots to verify backup integrity every night.

And

- ☑ AutoVerify automatic backup verification to demonstrate when and how backup integrity tests are performed.

MSPs Can…

- ☑ **Show the value of your MSP** to clients with evidence of best-in-class BCDR services, automation, and support they may not realize contributes to protecting their infrastructure, data, and business continuity.
- ☑ **Simplify the process of preparing for QBRs** leveraging automatic, client, and protected system-specific reporting that is easily understood for meaningful discussions with clients.
- ☑ **Initiate** upsell and cross-sell opportunities based on infrastructure vulnerabilities, cybersecurity reinforcements, and attack vectors while covering your a$$ when clients don't follow your guidance and something terrible happens.
- ☑ **Create** marketing and sales strategies highlighting advanced reporting as a differentiator from other MSP competitors: secure BCDR, transparency, and state regulation and breach notification support features.
- ☑ **Quickly meet cyber insurance policy requirements** that demand proof of regular, automatic backup testing to maintain insurance at the lowest premiums possible.

See Axcient's Client Executive Summary Report

How Do Axcient Partners Access Reporting Capabilities?

Lucky for existing x360Recover partners, the Client Executive Summary Report is available through the x360 Platform.

- Log in to the management portal.
- Click the “Reports” tab.
- Select “Executive Summary” at the top of the page.

For quality assurance, as you generate your first couple of reports, manually send them to your team to review before scheduling them to go out to clients. This review process removes any chance of sending something you want to keep private from clients or isn’t ready for external distribution.

Use the Axcient Knowledgebase for step-by-step guidance to generate a Client Executive Summary Report.

See Axcient’s Client Executive Summary Report

It’s Time to Schedule QBRs with the 4 Rs

Now that you have specific strategies designed for MSPs, you can start developing a quarterly business review process that incorporates and enhances the 4 Rs: Relationships, Retention, Revenue, and Reporting. With these four components driving business reviews, new client onboarding, and client communications, MSPs are poised to present their BCDR services and value to customers at every intersection.

If you’re not an x360Recover partner, choose one of our contact options to learn more about comprehensive BCDR with flexibility, profitability, and ease of use. Our team can demo the Client Executive Summary Report for you, or you can access it yourself with a free x360Recover trial.

Schedule a 1-on-1 Demo

Start Your 14-day Trial

Additional Resources

Disaster Recovery (DR) Planning and Testing Best Practices – Make Automated DR Planning and Testing a Routine at Your MSP

MSP Blueprint for Profitably Selling Bundled Services - An MSP Guide to Bundling Your BCDR Offering

Cybersecurity Insurance eBook for MSPs - Using Automation for Cyber-Insurability. Are you doing the right things to protect your MSP business?

MSP Sales and Marketing Playbook Bundle - Strategies for MSP Growth: What to do and how to do it