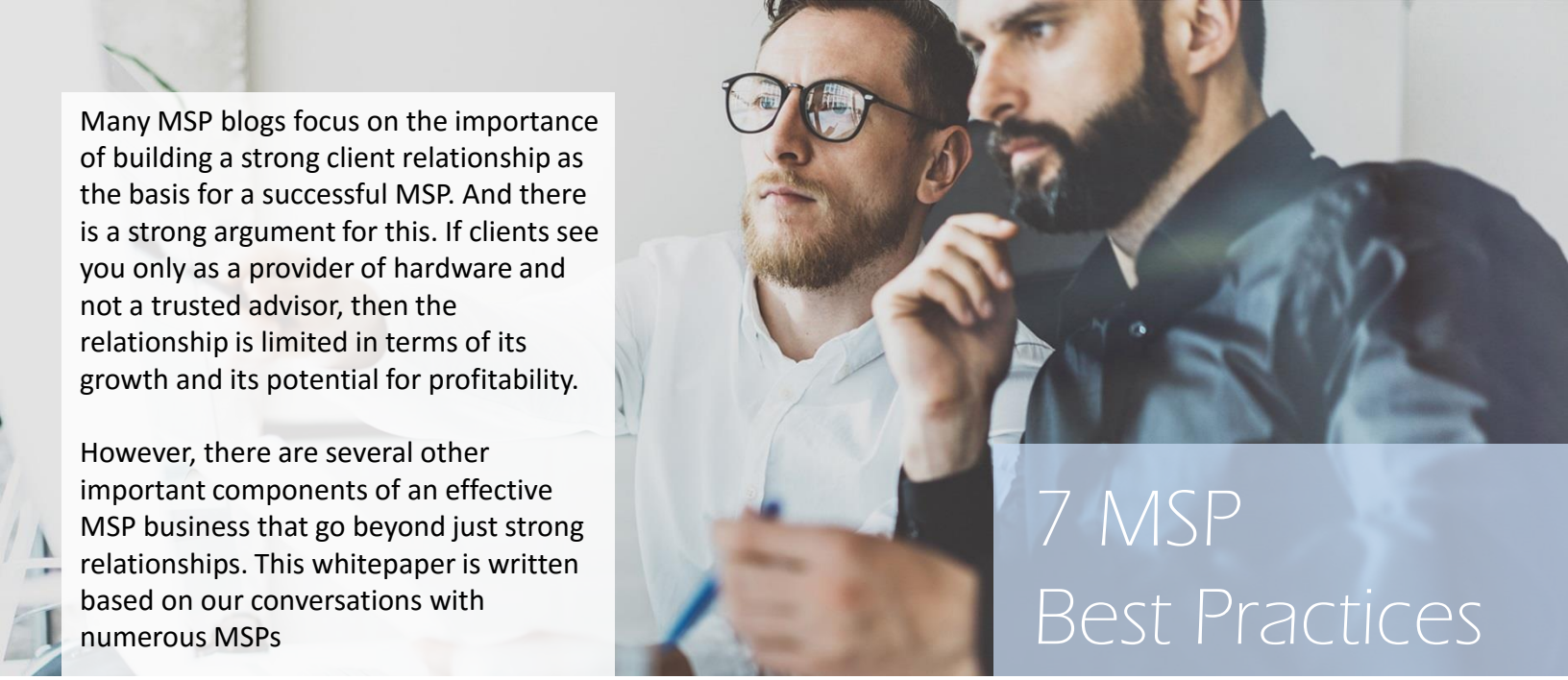
WHITEPAPER

7 MSP Best Practices



7 MSP Best Practices

Many MSP blogs focus on the importance of building a strong client relationship as the basis for a successful MSP. And there is a strong argument for this. If clients see you only as a provider of hardware and not a trusted advisor, then the relationship is limited in terms of its growth and its potential for profitability.

However, there are several other important components of an effective MSP business that go beyond just strong relationships. This whitepaper is written based on our conversations with numerous MSPs

1

Practice 1: Identifying and responding to incidents on a 24/7 schedule

Our world is no longer *increasingly* 24/7. *It is 24/7*. So, when your client's backups fail afterhours or servers are down at 2 am, there is an expectation that the MSP will be there to provide a solution. MSPs are supposed to understand how to provide the best solutions to their customers both during and after business hours.

Effective MSPs need to understand how to best identify and respond to their customers' incidents. And while this doesn't mean constant nightly after-hour calls, there are often several times during the calendar year when a client needs after-hours help.

2

Practice 2: Incident and service management

In addition to enabling alerting on a 24/7 schedule, MSPs need to provide a full life-cycle approach to tickets and events. When an incident occurs, the MSP wants to make sure that:

- The incident is ticketed through a robust tool.
- The incident comes with specific information as to which device is having trouble and the nature of the incident.
- A persistent alert is sent to the on-call engineer apprising them of the event. The alert needs to continue until it is responded to.
- If the alert is not responded to within a given time span, it needs to escalate to the next engineer on call.
- When the incident is responded to, this action is updated in the ticketing database

- Both MSP and client need real-time updates on an incident's status.
- Management should be able to monitor and audits response times by its engineers to ensure your MSP meets SLAs

Practice 3: Cybersecurity intrusions

3

Adding security to an MSP practice is a difficult proposition. In addition to providing the proper software, MSPs must encourage a security based culture that has proper security hygiene, security workflows and alerting. In addition to offering firewall and endpoint protection software, MSPs need to consider how they will be alerted when an incident occurs.

Your job as MSP is to act as a trusted advisor. Knowing that small businesses are the most likely to be compromised by a cybersecurity intrusion, it is the MSP's job to ensure that strong alerting is also in place to ensure the MSP can remedy any intrusion as quickly as possible.

Practice 4: SLAs

4

SLAs are the foundation of any good MSP business. SLAs allow an MSP to build strong client relationships. Strong SLAs also help establish standards in case something goes wrong. A well-crafted SLA is a great way to demonstrate the value of your MSP business. It is particularly important that your MSP clarify its SLAs around response time to any incident.

Practice 5: KPIs

5

Your MSP needs to identify key areas of the business which you wish to improve and grow. These are your Key Performance Indicators (KPIs). While different businesses will choose to monitor different aspects of their business as KPIs, one that is almost universal is service delivery.

Clients expect that your SLAs will clarify a mean time until response for incidents. That is, how long should clients expect it will take your MSP to respond to their incident? If you are not tracking response time, then not only is your client losing money due to downed IT but you are failing your client.

Practice 6: Automate processes

6

One MSP we spoke with discussed the importance of automating those processes that can be automated rather than leaving them to an antiquated, manual process. MSPs should, of course, look to the cloud for back-ups of their client's information. However, they should also think about automating those processes that are less obvious.

For example, integration with a ticketing tool that allows clients and MSPs to monitor alerting, response times and ticket updates is a huge asset for the MSP and client relationship. The MSP is able to respond to, monitor and update the status of any incident. At the same time, the client can see that their incident is being taken care of. Throughout this virtuous process, all updates are automated.

Practice 7: Better workflow

7

Being an effective MSP requires people, process and technology. An important part of this process is a good workflow. Good workflow extends to how hardware is installed, how backups take place and how incidents are responded to. Is the first sign that a client has of a downed server an inability to make successful back-ups? Let's hope not.

Instead, a good MSP will be proactive rather than reactive and know, even before the client, that there is a problem. As part of being proactive, the MSP will have a workflow that encompasses strong alerting, strong notifications and SLAs.

The MSP, for its part, will ensure that even if one of their engineers is unable to respond to the alert, there will always be an escalation so that an issue is never left to rot.

Conclusion

We hope you are able to take these insights and use them to improve your MSP offerings.

Learn more about what critical alerting and incident management can do for your MSP by calling BVoIP at +1-215-402-7200 or reach out to us at www.bvoip.com