DISASTER PLANNING FOR MSPS

DISASTER PLANNING FOR MSPS

In the past few months, the southern United States has experienced significant damage from the ravages of hurricanes Harvey and Irma. These natural disasters are freakish and unexpected but unfortunately they are not uncommon. Even at a lesser degree of intensity such as a tropical storm, the results can take the form of significant damages and IT outages.

The question then becomes how to prepare for the unexpected. What are the best practices and tools teams need in order to handle a catastrophe effectively? While it might seem like an oxymoron, effectively handling a catastrophe is just what your MSP might need to do.

To that end, we have created this whitepaper to highlight:

- Ways to convince your clients that they need a disaster recovery plan
- Steps that IT teams should follow to prepare for a serious outage or disastrous event

WHO NEEDS A DISASTER RECOVERY PLAN?

Small and medium-sized businesses (SMBs) are becoming increasingly vulnerable to security risks and data loss resulting from malware attacks, DDoS attacks, server failures, and natural disasters. The main reason for this vulnerability is that many believe they will not be a target for cybercriminals because they are too small. Similarly, SMBs also believe they will never experience a fire, flood, or other catastrophic incident.

The fact is SMBs can be even more vulnerable to cyber-attacks than larger enterprises. In fact, according to a recent survey, **70 percent of ransomware attacks target small businesses**.[1] Furthermore, disaster can strike at any time regardless of the size or location of a business, and all it takes is extreme weather, a fast-moving fire, or a major earthquake to shut down a business for an extended period of time — or even permanently.

So, what can SMBs do to protect themselves? A good first step is to create a disaster recovery plan, something **75 percent of SMBs don't currently have in place according to a Nationwide Insurance study**.[2] This represents a significant opportunity for MSPs to grow their businesses and create new revenue streams around disaster recovery planning. However, that same Nationwide study found **38 percent of small business owners do not believe it is important to have a disaster recovery plan in place**. This statistic indicates that MSPs have their work cut out for them.

HOW TO CONVINCE YOUR CUSTOMERS THAT THEY NEED DISASTER RECOVERY PLANNING

"DO WE NEED ONE?!" Customers who are skeptical about their vulnerability to cybercriminals or natural disaster might need some convincing. A good way to start this conversation would be to point to case studies that illustrate how such a disaster could affect their business, or to recent news stories or statistics that highlight the need for disaster recovery planning.

[1] https://resources.flexera.com/web/pdf/Research-SVM-Vulnerability-Review-2016.pdf
[2] https://www.nationwide.com/about-us/083115-small-biz-survey.jsp

"I DOUBT DOWNTIME COSTS WILL BE HIGH"

According to the Institute of Business Home and Safety, 25 percent of businesses that close due to a disaster never reopen[3]. Approach your customers with a few key questions that might make them think. Questions like:

- what would happen if they weren't able to open/operate e-mails
- what would happen if they couldn't open their app
- what would happen if they couldn't' open their website or e-store for an hour or a day

By highlighting the value of Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO), MSPs can help their SMB customers identify how much data they can lose without significantly impacting their business and how long they can go without this data before it hurts their bottom line. It is important to note that if the SMB operates in a highly regulated industry, it will typically need tighter RPOs and RTOs to maintain normal business functions.

"DISASTER RECOVERY PLANNING IS EXPENSIVE."

Demonstrating to customers the value of developing a disaster recovery plan can be difficult for MSPs. However, business who believe putting a disaster recovery plan in place will be too costly are failing to see how expensive a disaster could be without a plan in place. MSPs should ask their SMB customers whether or not they can live without recovering all of their on-premise data if something were to happen.

SMBs should never underestimate the power of a well-crafted disaster recovery plan, and it is always better for their data to be safe rather than be sorry when it is gone forever. For MSPs, disaster recovery planning can provide a way to add value for their SMB customers, and when they are able to leverage this tool to proactively protect their customers from experiencing a catastrophic loss following a cyber-attack, server failure, or natural disaster, everyone wins.

MAKE SURE YOU TOO ARE DISASTER READY

Now that you've convinced your clients they need you to come up with a disaster recovery plan, here are some steps for you and your team to follow to make sure you are disaster ready.

STEP ONE: CATEGORIZE ALERTS

Not all alerts are created equal. As such you need to determine which outages are high priority and which are low priority. This step is essential so that you can prioritize your efforts and make sure you focus on the most important issues first and leave non-critical issues to be handled at a less hectic time. Priorities will change based on the business model at hand so they won't necessarily be the same for any two businesses.

Determine which metrics you will use to define the significance of the issue.

- High priority issues are ones involving a critical situation that must be resolved immediately. These critical issues can be ones that impact the IT's overall availability as well as the end customer. These high priority issues might be ones such as downed servers, downed infrastructure or inability to access key information in the cloud.
- Low priority messages can typically be responded to with some delay without facing consequences. These low priority issues might be ones such as customers experiencing latency or a bug that has limited impact on usability.

[3] http://gazette.com/7-shocking-disaster-recovery-stats-for-small-business-owners/article/1590436

By having these available at your team's disposal, you can ensure that alerts are handled more appropriately and with the appropriate level of immediacy.

In the case of disasters like hurricanes, IT will be faced with high priority issues demanding an immediate response. The better issues are categorized, the faster teams can respond to these issues and the quicker the end customer can back to their business.

STEP TWO: ESTABLISH PROTOCOLS

Your IT team needs to have a practiced game plan around who on the team will get alerted and how they will respond.

CREATE AN ON-CALL SCHEDULE:

When disaster strikes, it shouldn't be a guessing game as to who is notified. There needs to be a pre-defined disaster team who knows that they are the first line of defense, no matter if the technology belongs to their company or to a client. The team and back-up responders need to have their names in a digital schedule so that when an alert comes in, it can be forwarded to the right IT engineer on call right away.

ESCALATION:

Make sure your alerting policy uses escalations. By implementing escalations, you ensure that if an alert cannot be handled by a particular member of your IT team because they are busy, the alert will be forwarded to the next person in the on-call schedule. In the case of emergencies, this is particularly important.

RUN BOOKS:

When facing significant infrastructure failures, IT teams might not always know the correct protocols for resolving the issue. By having predefined run books with instructions for how to handle typical eventualities, much of the stress can be relieved from trying to resolve important outages.

PRACTICE:

At Netflix, IT teams are trained to handle chaos with ease. Netflix's Simian Army is known for randomly producing chaos in the network or code so that the IT teams are practiced in handling issues that pop up at a moment's notice. With this level of practice, teams learn to manage issues with aplomb.

STEP THREE: TOOLS FOR YOUR TEAM

With any disaster, it is important that your teams have the proper tools to receive alerts and respond appropriately. Your team needs to get alerted immediately when a critical event occurs so that they can spring into action.

THRESHOLDS & MONITORING

For proper alerting to occur, you need to make sure you have the proper monitoring in place. For monitoring, your team can use tools like Datadog, Solar Winds or one of many other monitoring tools. The goal is to also have confidence in the thresholds you have created. You want to make sure that your monitoring tool does not create false positives or create a high priority alert for an event that could be handled tomorrow morning at 9 am

ALERTING & COMMUNICATIONS

INTEGRATIONS.

Make sure your monitoring tool is integrated with an effective alerting tool that sends the critical notification as a persistent alert to a smartphone rather than as an SMS or email.

PERSISTENT ALERTS.

Ensure that there are persistent alerting capabilities attached to your alerting mechanism. Know that if the alert is not heard when it is first delivered to the person on-call that it will persist until it is responded to. Ideally, you will want your alerts tied to a digital on-call schedule so that the proper engineer is alerted in case of a disaster.

COMMUNICATIONS.

Communications are perhaps the most important element during a critical outage. If you are unable to communicate with your colleagues or your customers are unable to communicate with you, then the serious outage has just been magnified. Phone lines are easily downed during storms so communications need to occur over smartphones. By using the proper smartphone applications, your team can receive alerts from technologies, customers and colleagues. More importantly, they can use texting capabilities found on smartphone apps like OnPage that mark if a message has been received and read. With this knowledge of a message being read, team members know when their colleagues have received a message or if they need to escalate a request for help.

STEP FOUR: POST-MORTEMS

At the end, it is important to review the alerting process to see what went right and what could be improved. An effective post-mortem should be blameless and look at what actions were taken and what effects were observed. Also, what assumptions were made and what expectations did the engineer have?

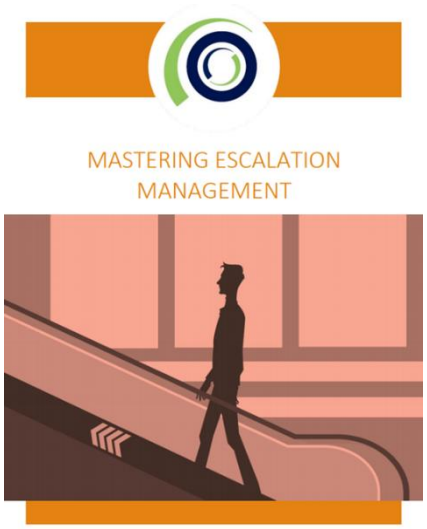
ENABLE POST MORTEMS AS SOON AFTER THE EVENT AS POSSIBLE: Memories are shaky. So it is best to enable the post mortem as soon after the event as possible. Team leaders need to be rigorous about recording details and sharing information

BRING IN INSIGHTS OF TEAM: Make sure the relevant stakeholders and participants are at the post mortem meeting. These stakeholders are people who might have contributed to the problem. In addition, you will want to include any people who responded to the problem as well as people who diagnosed the problem. Don't forget to include an invitation to a representative of the group affected by the problem. By bringing in this robust group, you will insure that you have the relevant parties at the table who can identify the relevant issues and help bring resolution to the issues.

CREATE A TIMELINE: If you don't have things written down, it can be hard to follow up on action items. The first point of action of the post mortem meeting should be to look at the timeline of events. As you were smart and invested in an incident alert management system that records the audit trail, you will have much of the relevant data you need to view the order in which the events unfolded.

CREATE A FINAL DIGITAL RECORD: It is important to create and share the final digital record. You need to publish post-mortems as widely as possible. Google drive is a good place to post this information. You need to educate other members of the team as to why the event occurred and commit to changes that will prevent the event from happening again in the future.

MASTERING ESCALATION MANAGEMENT



For IT teams to effectively manage a critical incident, the team members need to know when to escalate the issue to someone more skilled then they are or when to delegate the matter to a colleague because the alert's recipient is bogged down with other matters. Either way, it's important to know the communications and procedures to follow to make this hand off effective.

Download the white paper

HOW ONPAGE CAN HELP

These insights highlight the points you need to ensure your team is ready when serious outages or significant events arise and compromise IT's availability. You need to make sure you have the proper forethought, the right tools and the right procedures in place that can help your team grow.

OnPage can play a significant role in providing the scheduling and alerting your IT team needs to make sure it is prepared to help answer the call of duty no matter what time of the day or night the call comes in.

CONTACT ONPAGE TO LEARN MORE ABOUT HOW WE CAN HELP YOU WITH YOUR IT NEEDS.

TO LEARN MORE, VISIT OUR WEBSITE OR CALL: ONPAGE.COM

CONTACT- US 781-916-0040 OR DOWNLOAD THE APP

Available on the App Store

Get it on Google play