LogicMonitor

eBOOK

The Top 10 Mistakes Companies Make Handling Outages and How to Avoid Them All

No one likes to talk about outages. They're horrible to experience as an employee and they take a heavy toll on customer confidence and future revenue. But they do happen.

Even publicly traded tech powerhouses fall prey to outages.

Even publicly traded tech powerhouses, such as eBay and Microsoft, who have more technical resources than you'll ever have, fall prey to outages. And when they do, they are closed for business, much to the chagrin of their shareholders and executive teams. Aberdeen Group estimates that the average cost of downtime for businesses is $161,000 / hr.

Root causes of outages include:

- The infamous fat finger (human error)
- Gaps in knowledge about complex systems and their interdependencies
- Equipment failures, including out-of-date machines or those not configured correctly
- Hacking or other security breaches
- Poor or missing processes
- Any combination of the above

eBOOK

The Top 10 Mistakes Companies Make Handling Outages and How to Avoid Them All

Consequences of outages include:

- Irretrievably lost revenue, such as the estimated half a million dollars that Facebook reportedly lost in a half hour outage in June
- Lost productivity, like when Office 365 recently went down and stranded its customers without email
- Irate customers, such as the small businesses dependent on eBay and their reaction to recent “intermittent service issues”
- Outright failure of the business, like when Codespaces suffered a crippling DDOS attack from a hacker who was attempting extortion, and gained access to their Amazon EC2 Control Panel and deleted unrecoverable customer data

It’s not so much a question of whether an outage will occur in your company but when. The secret to surviving them is to get better at handling them and learning from the mistakes of others. Nobody is perfect all the time (LogicMonitor included), but we hope by talking about these mistakes we can all begin the hard work required to avoid them in the future.

Here Are the Top 10 Mistakes Companies Make Handling Outages and How to Avoid Them All:

1. Not having a tried-and-true outage response plan

Does this sound familiar?

An outage occurs. A barrage of emails is fired to the Tech Ops team from Customer Support. Executives begin demanding updates every five minutes. Tech team members all run to their separate monitoring tools to see what data they can dredge up, often only seeing a part of the problem. Mass confusion ensues as groups point their fingers at each other and Sys Admins are unsure whether to respond to the text from their boss demanding an update or to continue to troubleshoot and apply a possible fix. Marketing (“We’re getting trashed on social media! We need to send a mass email and do a blog post telling people what is happening!") and Legal (“Don’t admit liability!”) jump in to help craft a public-facing response. Cats begin mating with dogs and the world explodes.

OK, that last part may not happen. But if the rest sounds familiar, your company might be making Mistake #1.

eBOOK

The Top 10 Mistakes Companies Make Handling Outages and How to Avoid Them All

How to avoid: A well-formed process for handling outages must define who is accountable for resolving issues, who is in the escalation path and who is responsible for communicating about issues. It includes a post-mortem process for analyzing the root cause behind the outage and addressing any gaps, which can range from building redundancy into systems to changing monitoring settings so that issues can be caught and resolved before an outage might reoccur in the future.

2. Lack of communication about the outage with impacted customers

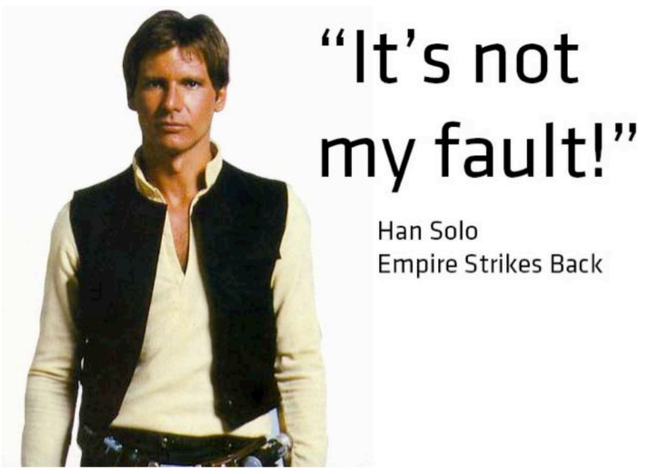
In the heat of trying to get your company back online, it's easy to "go dark." Unfortunately, not communicating with customers often causes a host of negative consequences, including a flood of support calls, longer hold times and poor customer experience, and it can produce a perception that your company is unresponsive, untrustworthy or not in control.

The fault often lies in poor or missing lines of communication between customer-facing groups and your Tech Ops team. Not having systems (blogs, forums, mass email, RSS feeds, etc) with which to notify customers of issues can be a big problem. Or companies don't communicate about the outage based on the mistaken belief that customers might not notice the issue (customers will notice) and that damage will somehow be minimized (lack of communication only makes it worse.)

How to Avoid: Ensure you have a defined communication process in place with clearly assigned responsibilities for both internal and external communication during and after the outage. Make sure everyone involved is familiar with it. Don't just store it on your company's website, because that may not be accessible during the outage.

3. Playing the blame game

Blaming a partner or vendor is a tactic companies sometimes employ in responding to outages. It rarely proves successful, because customers see it as abdicating responsibility for a decision the company ultimately made. (Who chose to depend on that vendor or partner? You did.) By not accepting responsibility, the company is also not taking steps to prevent recurrence of the problem, which is unlikely to be a crowd pleaser.



The Top 10 Mistakes Companies Make Handling Outages and How to Avoid Them All

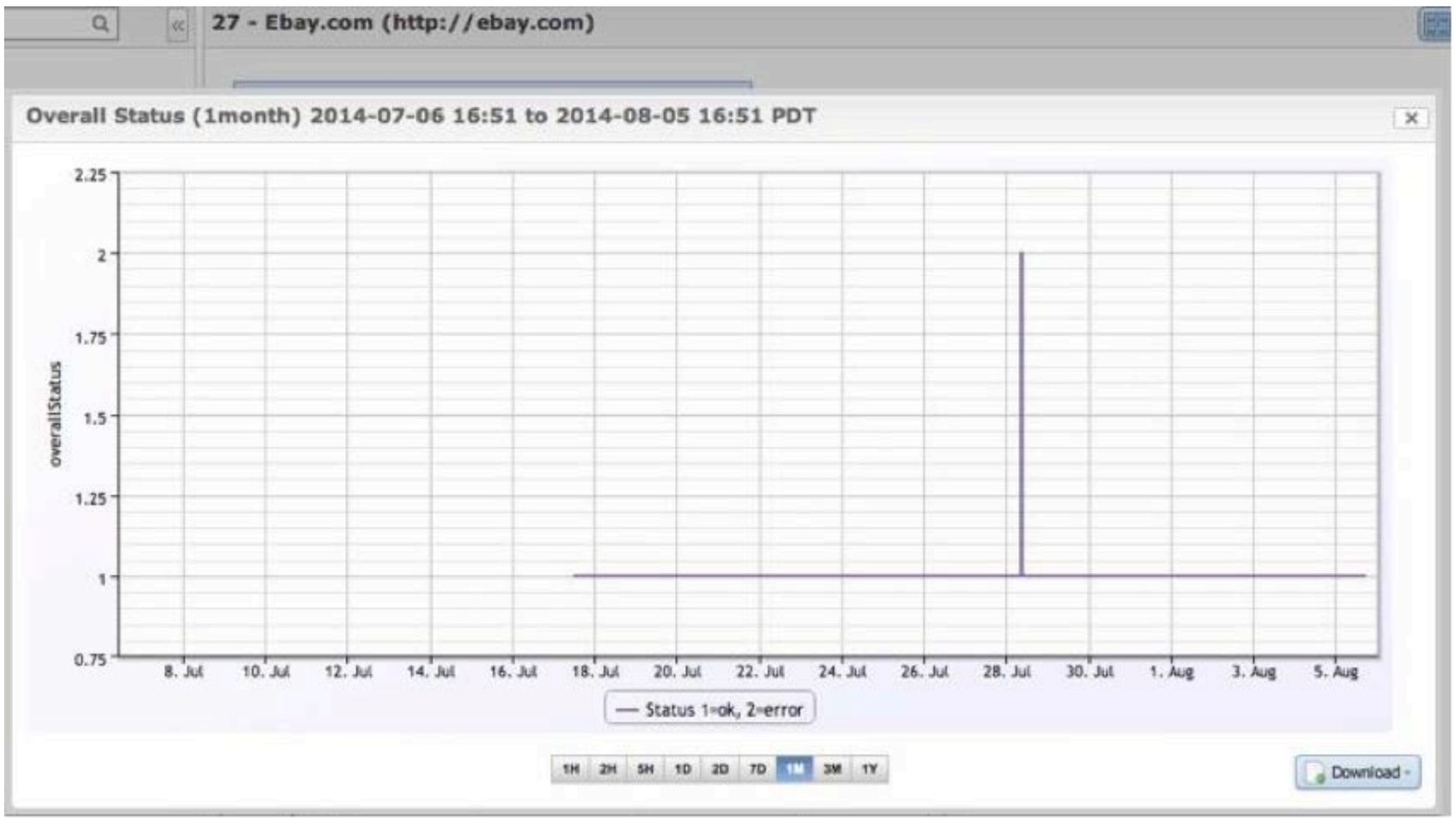
How to Avoid: Taking broader responsibility and instituting a review of vendors involved, setting up redundancy or reviewing processes that might have contributed to the issue are all better options than playing the blame game. Ensure post-mortems are blameless and get to the root cause of the failing process by using the 5 Whys method.

4. Not knowing they are having an outage in the first place.

The worst way to hear about an outage is to have your customers tell you (or possibly having your boss tell you). Having your monitoring infrastructure in the datacenter that's being monitored is an excellent way to have outages and not get alerted – because monitoring is off-line too. Even if your datacenter is Amazon, you may suffer the embarrassment of not knowing your service is down, which is what happened to Loggly during an extended outage a few years ago.

The best way: get an alert from a unified SaaS-based platform like LogicMonitor that tells you if your whole datacenter is down. Your monitoring platform should provide a complete view of websites (including performing synthetic transaction checks), applications, databases, network, servers, virtualization and the Cloud (wherever your IT infrastructure is housed), so that you can proactively fix issues before customer experience is impacted.

Below is an example of what an outage looks like in LogicMonitor graphs using SiteMonitor™, which is free with every LogicMonitor account. (Note: eBay is not currently a LogicMonitor customer.)



The Top 10 Mistakes Companies Make Handling Outages and How to Avoid Them All

5. Inappropriate communication about the outage.

When Dreamhost customers experienced an issue with their billing system, they responded with what they thought was a humorous explanation, prompting a legendary furor on the part of customers who focused on Homer Simpson cartoons and jokes rather than apologies and responsible explanations. They savagely attacked Dreamhost in online comments and in social media.

How to Avoid: If the impact of an outage affects your customers and their ability to conduct business, take it seriously. Someone at your customer's company selected you as a vendor and their judgment could be called into question because of your outage.

6. Missing any of the 5 elements to a successful outage communication/apology

"I'm so sorry that this happening, but I cannot help you. Yes, I realize that not providing you with any useful information about ***why this is happening*** *and* ***what is being done to solve it****, giving you an* ***ETA for*** **resolution** *and telling you how we* ***plan to prevent it from happening again*** *and* ***what we intend to do to*** **compensate** ***you for the trouble*** *must be incredibly frustrating, and you have my deepest and heartfelt* apologies for any *inconvenience this is causing you. I know you depend on us, we value you as a customer* and we take this very *seriously, etc."*

Don't do this. This mistake can be a symptom of not having a direct and open line of communication between your customer support and technical operations teams or from softening apologies at the urging of Legal or Finance departments.

How to Avoid: The 5 elements (bolded above in case you missed them) are core to any well-formed apology. They will cost you far less, in the long run, than the loss of revenue you'll experience if your customers leave in large numbers because you mishandled the outage.

7. Disaster recovery that's a disaster

Companies make a number of mistakes in the area of architecting a Disaster Recovery solution. The first and most obvious is to not have DR in place. The second is to architect a solution but to not factor in the increased load on the secondary system that will occur when failover occurs. Most computer loads do not scale linearly. If two sites are each running with a database at 40% load – that does not mean that one site can handle the workload of both at 80% load. It is more likely to be 120% – which means that in a DR the failover of one site will bring both sites down.

The Top 10 Mistakes Companies Make Handling Outages and How to Avoid Them All

How to Avoid: Run capacity tests on your systems, so you know your headroom and the pattern of how your performance scales with workload. Another approach is to have the DR site not active at all, but be an idle replica of a production site. Of course, this almost certainly means that it will be slightly misconfigured in a DR event – unless you take to heart the next mistake.

8. Expecting perfection without practice

When Chelsey "Sully" Sullenberger landed a US Air jet in the Hudson River with no fatalities, he'd logged more than 20,000 hours of flight time and completed countless simulated emergency exercises. He put in the time in advance so that he knew exactly what needed to be done at each critical juncture.

Yet many companies fail to test their plans or test them often enough to develop an expertise at making them work. And when trouble starts, they're not ready.

How to Avoid: Form a Business Continuity Plan and test it multiple times. It's far better for something to go wrong during a test than during an actual outage.

9. Diffusion of responsibility

Researchers have shown in studies that people are less likely to take action or feel a sense of responsibility to handle emergencies when in the presence of a large group of people. Diffusion of responsibility is often used to explain why individuals in distress are less likely to receive assistance if a large group is present. In essence, individuals in that group collectively decide that, if others aren't acting, it must not be that serious. This happens far less frequently when individuals are confronted by the same situation.

Companies often have issues with diffuse responsibility during outages. Issues are not clearly assigned to individuals to resolve and groups point fingers at each other or fail to be able to identify who is responsible. This can often be the result of too many monitoring solutions or unclear escalation paths.

How to Avoid: Assign clear responsibility in your outage response plan and include timelines for escalation. And try and get all teams using a single monitoring platform, like LogicMonitor, which can automatically notify the correct person based on the type of issue being reported and which can have escalation chains set up so that, after pre-defined periods of time, escalation is automatic if the issue is not resolved and notifications go out to the next person in the chain.

eBOOK

The Top 10 Mistakes Companies Make Handling Outages and How to Avoid Them All

10. Suffering from the "Tyranny of the Urgent"

"Our dilemma goes deeper than shortage of time; it is basically a problem of priorities." – Charles E. Hummel, "Tyranny of the Urgent"

When I was writing this content, I reached out to a number of CEOs of rapidly-growing SaaS companies. I was surprised when one told me: "I'm interested in the topic, but I wouldn't be able to make the time to attend the live Web Seminar."

"Why?" I asked.
"Well… we aren't having outages right now," he responded.

Wrong answer.

It's easy to get caught up in the tyranny of urgent priorities and spend all of your time firefighting. The glory! The heroics!

But often, it's mismanagement of priorities that are important and not yet urgent that turns situations into 5-alarm fires that massively drain your organization's resources. Ignoring the little things that you can do in advance to prevent outages is equivalent to not spending a few minutes putting fresh batteries into your smoke detectors and having some fire extinguishers on hand. Being prepared and proactive is not as glorious, but so much smarter.

How to Avoid: Make preventing outages a priority by requiring teams to spend a portion of their time taking proactive steps to prevent them ever occurring. Your shareholders and customers will thank you for it. Improving management of outage incidents can produce better outcomes for your company's employees, customers and shareholders. It won't be easy. But it will be worth it. And it all starts with avoiding some basic mistakes that others have made before you. As Otto von Bismark once said, "Fools say that they learn by experience. I prefer to profit by other's experience."

LogicMonitor, Inc., 12 E. Carrillo St., Santa Barbara, CA 93101 Email: info@logicmonitor.com Contact Us: 1-805-617-3884