DISCOVERY FOR DISASTER RECOVERY: CMDB NEED NOT APPLY

One of the best parts of my job is meeting with customers. I get to talk to people in departments across the organization about their challenges and obstacles and try to figure out how we can help. These conversations are meaningful at the personal level but also allow me to see bigger trends happening in enterprises around the world. When I hear the same thing over and over, I know something is going on that needs to be discussed in a broader venue.

Right now, that "something" relates to disaster recovery (DR). Whether companies call it disaster recovery, resiliency, continuity, etc., they are focused on how to prepare for and recover from unplanned events that impact business continuity. Today's businesses have to be ready - but for the leaders in charge of DR, that's not easy.

Disaster recovery leaders (and their security counterparts) are frustrated. To do their jobs effectively, they need accurate, always up-to-date IT inventory data. They need a complete, correct "corporate source of truth", usually a CMDB. They can't build a continuity plan without a trustworthy source of information... but they don't have it, and they can't sit around and wait for it to get built when their careers and their company's data (and reputation, and market value, and...) are on the line.

There's a good reason they don't have it: a large majority of CMDB projects fail to develop an inventory that its data consumers can trust. Why? Not because the people in charge don't value the CMDB – Service Management has been trying to get it done for years (thanks ITIL). The traditional approach to building the CMDB just did not work.

This is not Service Management's fault. Many have been advocating that Service Management own

the CMDB as part of an overall ITIL-based approach to collecting and harvesting information to build an IT inventory. The CMDB was the field of dreams: if you build it, they will come. Problem is, the approach typically used to build it was flawed because it involved consuming and munging multiple disparate data sources, usually from existing in-house tools.

All too often, a result of this approach was a massive data store that nobody really used or trusted. Even worse, the data only told half of the inventory story. While the various sources often captured configuration information, they rarely if ever discovered important relationships between IT devices and the business services "applications" they supported.

Ideally the consumers of IT inventory data can quickly and easily visualize and report on inventory data from a business service perspective and make informed decisions based on the inventory. But Excel isn't built for that. It takes far too long (often 3-4 years) and even then, it's incomplete. Hence the frustration from Disaster Recovery folks.

This situation is frustrating for Service Management, too. This approach was supposed to work, but it hasn't. Many of the advanced use cases they bought their ITSM platform to do simply can't function without this data, leaving them with a tracking system rather than a proactive management platform. They've been trying to get adoption. They've been working incredibly hard to create a reliable source of truth. They understand that their stakeholders are dissatisfied. But you can't throw the baby out with the bathwater, so to speak. So now what?

The fact of the matter is that an accurate CMDB is great, but many of the data consumers like DR don't need a CMDB to have an accurate IT inventory. The efforts are and should remain connected, but they don't have to be synonymous. Stakeholders don't need to be dependent on the CMDB team to get data - fast - that anyone can use. Tools like BMC Helix Discovery can automate the scanning, collection, and recovery of configuration AND relationship data across the entire IT stack very quickly, bring that information back into one format, visualize and report on it, and extract that data into other tools to remediate/take informed action.

These capabilities can be tremendously beneficial to DR and security teams. For example, a large bank suspected they had blind spots in their IT Inventory. Using BMC Helix Discovery, they found and confirmed thousands of CIs that were missing in the CMDB. We created an extract report of the CIs, pushed that into a patch management solution, and remediated a potential security threat.

The Disaster Recovery team needs to know what current state looks like to plan for continuity. BMC Helix Discovery enables DR and Security to see current state, identify where the vulnerabilities are and which business services they're connected to so you can prioritize your approach, then take action and remediate the risks. You can't do that in Excel.

If you're a DR or security professional, you need accurate, up-to-date information so you can make informed plans and decisions. If you're on the CMDB team, you need a way to give your stakeholders what they need AND improve adoption and the effectiveness of your CMDB initiative. BMC Helix Discovery accomplishes both of these objectives quickly and powerfully, no matter which ITSM platform you're using - it can populate them all.

For more information on BMC Helix Discovery, watch the demo or read the IDC report, *BMC Helix Discovery Helps Organizations Optimize ITSM Operations and Asset Management*.