

Human Infrastructure 82: Who Benefits From Vendor Best Practices?



Issue 82 Table Of Contents

- Who Benefits From Vendor Best Practices?
- Would You Like To Update Now?
- Making The Most Of Post-Mortems
- Thanks, Internet
- Internets Of Interest
- Packet Pushers On YouTube
- Product News

Who Benefits From Vendor Best Practices?

By Greg Ferro

Many so-called network professionals rely on 'vendor best practices' as a reference for projects. For vendors, this ensures that customers deploy the same solution, design and operational process. It also reduces the vendor's sales costs and provides the customer some assistance.

But there are other ways to see the impact.

For customers, best practices are a low-cost method of consulting and advisory services. No need to have good staff with training and expertise--just use 'best practices.'

For resellers? Avoid long delays by referring to your design as 'best practice' to stop the customer from asking difficult questions. No need to find the pre-sales engineer or get technical signoff. Simply point to the best practice or reference design and make grandiose claims about 'validation' and 'vendor approved'.

No need to start from the baseline, analyze requirements, establish needs, select the right products, and go through a review process!! Avoid the hassle by pointing to the 'reference design' and hoping that it works out after the purchase order has been processed.

How Good Is The Best Practice?

Will it work better? The reality is that vendors expect their solutions to fail in the field.

Bugs are a fact of life and vendors appear to do little to prevent bugs, much preferring to clean them up after customers pay their staff to find and report bugs.

After all, explaining the right way to use a product means that you haven't done a good job making the product fit for use. You can always charge professional services once the PO has been booked.

The production and publishing of these design and deployment guides is enormously expensive for vendors. It's common for three to five senior engineers to spend up to six months preparing the document. Lab testing and validation is likely a key component. Pricey. But don't worry, the customer is paying for it anyway.

There is little value in building knowledge and expertise if you take a non-specific, generalised design and apply it. Don't worry your head about the technical details and whether your company has the ability to operate a 'best practice' infrastructure because, let's face it, we are all headed to the cloud so that infrastructure becomes someone else's problem.

And money? Design guides prepared by vendors take their preferred view that 'dream customers' exist and want to spend large amounts of money. Therefore, vendor designs are oversized, overspecified and generously larded up with expensive features.

Result? Sales can extract maximum money from the client with little effort.

And that's what everyone wants.

Would You Like To Update Now?

By Drew Conry-Murray

Your smartphone chirps: there's a fresh build of the OS and you'll need to restart. You put the phone aside as the software downloads and the device reboots.

You turn to your laptop. You open an application to catch up on some work, but a notification slides in from the right side of the screen: a new version of the application is available that contains critical updates. You've already clicked "install later" a half-dozen times; the thing won't work until you run the latest software.

Fine. You give in and download the new version. Rather than sit and wait as the little wheel spins, you sort through the mail on your desk.

There's a letter from your car dealer. The manufacturer has issued a recall notice due to recently discovered [firmware vulnerabilities](#) that could affect the vehicle's functions. You won't be charged for the updates, but they have to be done at the dealer. That means you have to make an appointment, drive across town, and drop off the vehicle.

Feeling your irritation level begin to rise, you check the phone. Update's done. You head to the living room. It's dark. You open your home lighting app, thinking you'll try the new "Quiet Contemplation" setting to help you relax.

But there's a notification on the app: something about [GDPR and the service being disabled](#). What the hell? The lights don't work.

You aren't in the mood to sort it out right now, so you go check on your laptop. Still spinning.

OK then. You head to the den and turn on the TV. You twiddle with the remote as a new software package gets downloaded. You click through the EULA without reading it and then flip to the news.

The lead story is about a new hack that [exploits a home smart lock system](#)—the same smart lock system you just installed on your front door last week.

You utter a few choice curses. This is getting out of hand.

And then from your darkened living room comes a sound. You listen closely, the hairs on the back of your neck standing up. It's [a sinister laugh](#). But you're the only one home.

Making The Most Of Post-Mortems

By Ethan Banks

A post-mortem is where an operations team gets together to review a major outage. I believe there are two major things that should come out of post-mortems.

1. A clear, detailed understanding of what went wrong.
2. Options to prevent the outage from recurring.

What Went Wrong

From an IT operations perspective, you should understand what went wrong on a couple of levels.

First is the business. The business was impacted because something with the the organization's information technology went awry.

For instance, a post-mortem might state that during the time that the SQL server was offline, the main online ordering tool was not working. Because the online ordering tool wasn't working, potential customers went to competitors to place their order. As a result, a certain amount of topline revenue was estimated to be lost.

The lost sales will cause the company to miss its targets for the quarter, and the stock price will potentially be damaged. Depending on how financial analysts react, staff might be laid off to reduce expenses and attempt to bolster profit margins in the following quarter.

Not all IT professionals care about business operations, but they should. IT exists to serve the business, and therefore IT should have a clear idea of the criticality of the various applications and infrastructure in their system. Not all technology deserves equal attention in a business context.

Second is IT operations. You need to understand in detail what went wrong. It's not enough to say that the SQL server was offline. Drawn a a more detailed analysis, including questions asked and answered. Let's put some nuance around the scenario of the SQL server being offline.

1. Q: Why was the SQL server offline?

A: The DBA reports that technically, the database was online, but no transactions were committed. The SQL server was up and the SQL instance running for the

duration of the outage.

2. Q: Why were no transactions going to the database?

A: The lead network engineer says that the network was good for the entire duration of the outage. The SQL server was up and responding to pings from the NMS.

3. Q: Do we monitor the SQL database service itself, or just ping the server?

A: We just ping. We don't monitor SQL from the NMS because it's a Windows box, and APM licenses for our NMS are pricey. We got SCOM for the Windows stuff.

4. Q: <Head turns to the Windows folks.> So...what did SCOM tell us?

A: We didn't get an alert, so, we don't really know.

5. Q: Are we monitoring the SQL server with SCOM?

A: We'll find out.

6. <Someone from the SecOps team bursts through the door.> Just found out about this meeting. Thought everyone knew what happened already. Because of that new malware, we pushed a new Windows firewall security policy that filtered additional ports. The new policy shouldn't have hit the SQL box, but it's an old server in the wrong OU. Never got moved when we redesigned AD. Once we

reverted to the old firewall policy on that server, the SQL instance started receiving transactions again.

The Prevention Plan

In the scenario above, we ended up with enough information to consider several possible prevention plans. This is the most critical part of the post-mortem.

Understanding what happens matters, but sorting out how to keep it from happening again is what's critical for the business.

In this scenario, there are many directions that could be taken to prevent the issue from happening in the future.

1. A new microsegmentation solution could be used to manage firewall policies.
2. An audit could be performed to enforce that AD design intent.
3. An update to the change control process might increase the chance that someone would have caught that issue.
4. The SQL server could be identified as mission-critical and re-architected for redundancy.
5. Since the SQL process seems like a SPOF, perhaps the entire online ordering system should be re-designed.

There isn't a right or wrong answer in my list, because a decision like this can only be made by the business.

Why? All of these possible solutions cost time, money, and human resources to implement. To make the decision about how to fix the problem, IT must be the trusted

advisor to the business to explain, in simple terms, what happened, and what the options are to prevent a recurrence.

What's that you say? IT is not trusted by business stakeholders? Hmm. Sounds like a topic for a future issue of HIM.

Thanks, Internet

Sometimes interesting or amusing things show up in our social feeds. Here's one.

7 THINGS EVERY KID NEEDS TO HEAR

1. I Love You
2. I'm Proud of You
3. I'm Sorry
4. I Forgive You
5. I'm Listening
6. **RAID storage is not a reliable form of backup - use offsite**
7. You've Got What It Takes

Internets Of Interest

Links to articles and blogs you might find worth reading.

Ready Player Productive: On Virtual Reality and Cognitively Demanding Work - Cal Newport

Cal Newport, who writes the Study Hacks blog, has an [interesting piece](#) about "location-boosted cognition;" that is, work spaces that have some quality or qualities that enhance deep cognitive work such as writing, programming, lawyering, and so on. As an example, he cites a refurbished barn, filled with books and natural light, where author Simon Winchester works.

However, as Newport also notes, not everyone has the money or space to build an ideal location. Enter virtual reality. Is it possible that VR spaces might be used to create ideal, customized work environments? If a programmer, say, or a network engineer, needed to concentrate for a few hours, would it be helpful to slip on a helmet and map out a data center design from a beach-side cabana or the craggy cliffs of the Irish coast? For me personally, until we achieve holodeck-level VR, I'd rather make do with a workspace in actual reality, however bland it might be.

[LINK](#)

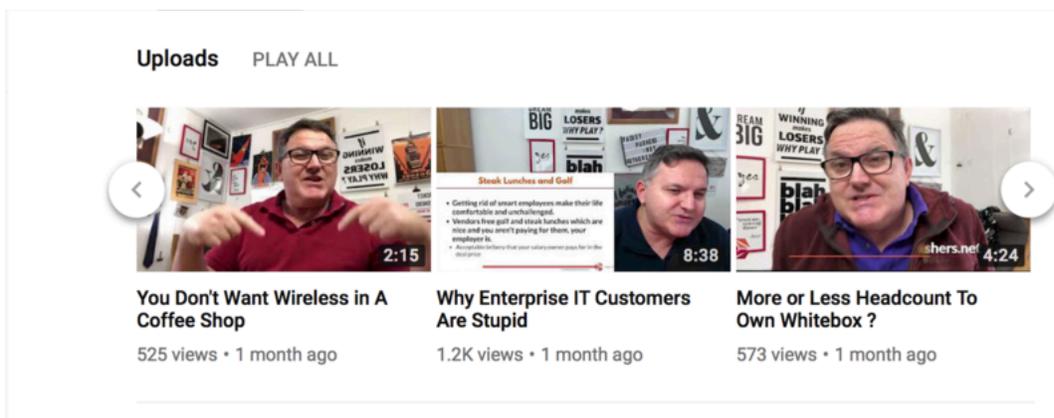
Packet Pushers On YouTube

What could be better than listening to the Packet Pushers? How about looking at them? Now you can, with our brand new [YouTube channel](#).

We (OK, mostly Greg) are producing short videos about networking, technology, the business of IT, and other topics. The format is generally commentary and opinion, along with a few more in-depth pieces, plus Greg's popular "Two-Beer Networking" series.

Why YouTube? In the short term, we're curious to see if there's an appetite and audience for video. You never know where you might find a new audience or future Packet Pushers members, so it makes sense to cover as many media bases as we can. In the long term, a visual medium gives us different ways to deliver information and analysis, and may be better suited to certain kinds of content.

For now we're in the experimental phase. If you're interested, [check out the library of material](#) that's already there. You can also subscribe to be alerted when new videos arrive.



The screenshot shows a YouTube channel page with the following content:

- Uploads** PLAY ALL
- Three video thumbnails are displayed in a row, each with a play button icon on the left and a right arrow icon on the right. The thumbnails contain the following information:
 - Video 1:** "You Don't Want Wireless in A Coffee Shop" (2:15), 525 views • 1 month ago.
 - Video 2:** "Why Enterprise IT Customers Are Stupid" (8:38), 1.2K views • 1 month ago. The thumbnail includes a list of bullet points:
 - Getting rid of smart employees make their life comfortable and unchallenged.
 - Vendors free golf and steak lunches which are nice and you aren't paying for them, your employer is.
 - How would you believe that your salesperson pays for his/her airplane?
 - Video 3:** "More or Less Headcount To Own Whitebox ?" (4:24), 573 views • 1 month ago.

Product News

We get briefed on new products and vendor moves. Sometimes we write them up.

Aerohive Challenges Cisco, Aruba With New A3 Network Access Software

Aerohive has [launched A3](#) access control software for wired and wireless networks. A3 competes against Aruba ClearPass and Cisco ISE, among other access control and policy enforcement platforms.

A3 offers capabilities for device onboarding, provisioning, and access control. The software can manage wired and wireless access for corporate and BYOD devices, as well as IoT devices. It also supports guest access for visitors, contractors, and so on.

[LINK](#)

Cato Networks Adds Threat Hunting Capability To Its SD-WAN Service

Cato Networks, which sells an SD-WAN service, has added a new threat-hunting capability to detect compromised devices on customer networks that may be communicating with command-and-control systems or exfiltrating data.

The capability, which is currently included as part of Cato's advanced services in its SD-WAN offering, takes advantage of Cato's view of key network metadata from its customers' traffic.

[LINK](#)

HPE Acquires Plexxi For HCI, Composable Infrastructure

Remember Plexxi? The company was founded in 2010, during the early, heady days of SDN when the industry was all aquiver with new concepts and architectures for building and operating networks.

[LINK](#)

The End Bit

Sponsorship and Advertising - Send an email to humaninfrastructure@packetpushers.net for more information. You could reach more than 5,000 subscribers.

Human Infrastructure is bi-weekly newsletter with view, perspectives, and opinions. It is edited and published by Greg Ferro and Drew Conry-Murray from PacketPushers.net. If you'd like to contribute, email Drew at drew.conrymurray@packetpushers.net.

We don't give away your email address or personal details because that would suck.

Copyright © 2018 Packet Pushers Interactive LLC, All rights reserved BUT feel free to share this email with ALL YOUR FRIENDS. They would love it, right? Just don't change it. Send it because it's beautiful.

[Unsubscribe From This List](#) | 95 Hidden Lane, Northfield, NH 03276