

IN THIS WEEK'S ISSUE: Technology Changes, But People Don't; Does Your Employer Have To Keep Your Information Secure? Please remember to enable the images; the magazine looks a lot better that way!



PACKETPUSHERS

Human Infrastructure Magazine

A Newsletter About a Life in Networking

Table of Contents (aka The Project Plan)

Issue Number 50

02/16/2017

- [1. Enterprise Tech Is Changing. People Aren't](#)
- [Sponsor: Interop ITX](#)
- [2. Court Says Employers Don't Have To Protect Employee Data](#)
- [Internets Of Interest](#)
- [Product News](#)
- [PacketPushers.net - The Last Five](#)
- [Watch This!](#)
- [Quick Survey: Tech Conferences](#)
- [Last Issue's Survey Results](#)

The "Time to step up" issue.

Thought For The Week:
Is it spring yet?

1. Enterprise Tech Is Changing. People Aren't

by Ethan Banks

Networking technology is moving quickly. Orchestration systems are trying to take over network provisioning. Automation tools are helping make the orchestration vision possible. Overlays are adding a manageable connectivity layer on top of that pesky, difficult-to-manage hardware underneath. Open networking has separated the NOS from the hardware, making it possible to mix and match switches and operating systems. NFV has made easier distributed networking architectures that eschew massive appliances, favoring many small software instances running on x86 instead.

The payoff is financial, with the ability to (arguably) spend less and get more. The payoff is also in efficiency, where routine tasks are automated, and applications are stood up faster. The payoff is in a reduced risk, where a well-designed, distributed network architecture (hard) has a reduced blast radius during inevitable failures.

And yet, most enterprise networks seem to be stuck in the past. Why is this? It's not the tech. I acknowledge the tech isn't mature yet, at least not all of it. I've bemoaned the immaturity issue multiple times. Even so, I don't think young tech is at the core of the new technology adoption issue, because an awful lot of it is good enough.

I believe the issue is people.

Now, I said "issue" and not "problem." I can't blame people for not getting into new networking tech. It's who we are.

People are slow to react to new information. This is especially true with new technology, where implementing new hardware or software is

far more involved than a casual decision to try something new.

People are resistant to change, and with good reason. Folks fear being displaced by change, where the value they once brought goes out the window due to something new beyond their influence. People will defend their turf, especially engineers with deep knowledge they acquired over years of experience.

Some people are too stressed to handle one more thing, when that one more thing arrives in the form of new technology that might or might not move the needle for them.

Some people are simply ignorant. If you're a Packet Pushers reader and listener, that's probably not you. Obviously, you have some intent to keep up with the industry. But some folks don't have that drive. They aren't trying, and thus they haven't even heard of new techniques they could use to improve how networking services are delivered in their shops.

Yet other people try to keep up, but can't contextualize the information. They don't know what to do after reading an article about a new networking technology. Is it useful? Is it applicable? Would it have a positive impact on operations? For some, those questions are too hard to answer, and so new technology gets filed away and forgotten about.

Other folks are kept in the dark against their will. Business leaders chronically underfund training budgets and conference attendance. I'm on record as having mixed feelings about most conferences, but I still believe there's value there. And training is a must! Businesses that don't invest in their tech staff don't invest in their future infrastructures. The two ideas go hand in hand.

Of course, business leaders are also risk-averse, and they tend to assign new technology a higher level of risk by default. Because "new" is scary and unproven, so the logic goes. This logic prevails despite the track record of incumbent vendors offering horrid technical support

and buggy code releases.

All technology has to be taken on its own merits at this point. The age of a vendor, whether startup or established, is no longer an indicator of the risk their product introduces to a computing environment. Don't presume that because it worked before, it will work again.

Business leaders are also unwilling to change if there is no clear indication that they need to. Some companies sail calmly along, cranking out steady revenue and a decent profit, with no great drive to change their IT practice, no matter what inefficiencies exist. Some leaders might acknowledge the need for an IT improvement here or there, but there's not enough pain to actively seek pain relief. What they have is good enough, and reactivity is easier than proactivity.

What About You?

In my experience, hard IT change is often driven by individuals. People who are willing to take a leadership role and grasp new technology, despite the odds against them, can affect change in an IT organization.

It's driven by people who stand up in a meeting and agree to take on the discovery, the research, the hard task, the complex role, the difficult integration, the questions. The blame. The sniping. The blame thrower aimed at the new switch with the new NOS every time some little thing goes wrong. Those are the people who make IT better, ultimately.

And those are the sorts of folks who are going to make networking better. They'll do the hard work. They'll get a handle on the new tech. They'll make a different recommendation than usual for the next refresh cycle. They'll take ownership. They'll take responsibility. They'll be willing to stand and deliver.

Is that you?



Sponsor: Interop ITX

Where Tech Pros Go For Objective Full Stack IT Education

[Interop ITX](#) takes place May 15-19 at the MGM in Las Vegas. Join Greg Ferro and Ethan Banks for The Future of Networking Summit – a two-day session where we'll take a deep dive into next-generation developments in wide area networks, data center networking, network operations, and software-defined security.

Register for Interop ITX and attend other hands-on workshops like The Future of Data, Container Crash Course, Dark Reading Cyber Security Summit and the Open Source IT Summit. The event's Conference tracks focus on Security, DevOps, Cloud, Infrastructure, Data & Analytics – all the technologies you need for a successful Full Stack IT strategy. If you're looking to accelerate your career, there are also plenty of sessions on leadership and professional development. Plus, check out over 100 vendors at Interop ITX's Business Hall where you'll

have an opportunity to meet with leading and emerging tech vendors.

Join us at Interop ITX this May. Use promo code: **PACKETPUSHERS** when you register, and you'll receive 20% off any pass.

We want to see you in Vegas, so visit interopitx.com and reserve your spot today.

2. Court Says Employers Don't Have To Protect Employee Data

by **Drew Conry-Murray**

A panel of judges in the Pennsylvania Superior Court [recently ruled](#) that UPMC, a large healthcare provider in Pittsburgh, had no obligation to secure its employees' personal information.

The ruling came about because of a class-action suit against UPMC after a breach in 2014 exposed the information of 62,000 employees. At least 817 employees have been victims of tax fraud related to the breach, which exposed Social Security numbers, bank account details, salary information, and home addresses.

The Superior Court decision upholds a previous trial court ruling in which the court stated that the employer "[did not owe a duty of reasonable care in collecting and storing employee information.](#)"

To its credit, UPMC did notify employees of what happened, and did provide identity theft monitoring services. But that seems like paltry compensation for the hundreds of people who were already victimized

by fraudsters.

This is a ruling that should make employees uncomfortable, given the prevalence of data breaches and the cost and burden that come with trying to undo the damage of identity theft.

One concern I see is that employees don't have the option of deciding whether to share such sensitive information with their employers; if you want the job, you have to give them what they ask.

I understand there are benefits that come with giving your employer sensitive information, like direct deposit of paychecks. And I also understand that companies don't want to be breached.

However, the suit leveled against UPMC alleged that the company failed to take reasonable security measures, such as the proper use of encryption, to protect employee information. We won't know if that's true because the judge's ruling has essentially shut down the lawsuit.

It's common knowledge that many organizations don't take security seriously. That's why we end up with things like breach notification laws, HIPAA compliance, and industry mandates such as PCI—it takes regulatory threats to get organizations to invest in security practices.

This ruling only affects Pennsylvania employers. I don't know if it can be used as a legal precedent elsewhere, but it feels like a step backward.



Exploring the latest data center innovations including storage, virtualization, networking, and convergence

Datanauts



Subscribe now to get automatic updates

 PACKETPUSHERS

Join the Datanauts on their mission to bust silos and explore the latest developments in cloud, convergence, data centers, and more. [Sign up free here.](#)

The Network Break



PACKETPUSHERS

Where Too Much Networking Would *NEVER* Be Enough

Network Break is a weekly podcast that delivers news & analysis on the networking industry in a fun, fast-paced style. [Subscribe here!](#)

Internets Of Interest

A collection of pre-loved links that might interest you. "Pre-loved" because I liked them enough to put into this newsletter. It's not *true* love.

By **Greg Ferro and Drew Conry-Murray**

Vendors Please Stop the Mud Slinging!

Blogger Daniel Dib is [taking vendor marketing departments to task](#) for taking cheap shots at their competitors. Aside from being childish, it doesn't actually serve potential customers either.

"It's 2017. People are well educated, smart and have access to a wealth of information at their fingertips. Slinging mud just isn't a good marketing strategy."

As he notes, a technical audience deserves better.

Intel's Ticking Atom Bomb

Tom Hollingsworth, aka The Networking Nerd, [has an excellent overview](#) of the problems occurring with Intel's Atom chipset clock signal failures, which are causing serious problems in networking gear from multiple vendors. In addition, he raises a good point about relying on commodity components. On the one hand, they help keep costs down and are widely available. On the other hand, a widely deployed component that goes bad could have a significant impact.

"Imagine a huge Internet of Things (IoT) deployment that relies on a weak link in the chain that can fail at any point and brick the device in question. The recall and replacement costs would be astronomical."

Money For IoT Bugs

Dark Reading [reports on a contest called GeekPwn](#) that awards cash prizes for security researchers who uncover vulnerabilities in IoT devices. The contest organizers report vulnerabilities to the affected companies. According to the story, participants have discovered more than 100 bugs in consumer and business IoT devices.

An Epic Rant

This is a few months old, but it's [an impassioned cry from a frustrated customer](#) about a product that's not performing the basic functions it was advertised as performing. We've all been there.

"That is another ugly example of not doing anything right. Response time, reaction time is slow and I mean slow. Why put this into the ASA, if the CPU cannot handle the load?"



**WEEKLY
SHOW**

Where Too Much Networking
Would **NEVER** Be Enough

The Weekly Show channel is our one-hour deep dive on networking technology. [Subscribe today!](#)



**Priority
Queue**

Where Too Much Networking
Would **NEVER** Be Enough

Priority Queue tackles niche and nerdy tech topics and cutting-edge research projects. [Subscribe here!](#)

Product News

We don't often get new products worth talking about, so that makes it nice to have something to say.

Corsa Touts 100Gbps DDoS Protection

Corsa Networks is launching new appliances to mitigate massive DDoS attacks. The company's Red Armor boxes combine an internal switch fabric and a dedicated FPGA for what the company claims is line-rate packet processing at up to 100Gbps. It relies on third-party detection software to identify an attack, and has a programmatic interface to get mitigation instructions.

[LINK](#)

A 'Self-Driving' Private Cloud? ZeroStack Says It Has One

Startup ZeroStack offers private cloud software based on OpenStack. It will also sell you pre-bundled hardware, or provide a menu of validated infrastructure options from Dell, HPE, and others. Recently, the company announced that it had added a "learning capability" to its software to automate routine tasks. Does it work? We don't know. But if you're interested in private cloud, it may be worth a look.

[LINK](#)

Recent Podcasts

The last five podcasts published on Packet Pushers

PacketPushers.net - The Last Five

[PQ Show 104: Design & Build 12: Certificate-Based DMVPN Design](#)

[Datanauts 071: Everything As Code With Mitchell Hashimoto](#)

[Network Break 122: Snap's Big Cloud Spend; Atom's Clock Shock](#)

[Show 326: Big Switch & The Next Chapter Of SDN \(Sponsored\)](#)

[Datanauts 070: How Media & Entertainment Handle Extreme Scaling Challenges](#)



Watch This!

Where we collect some videos that make us reflect, think about our inner lives, or just entertain us.





Whatever your politics might be, this is a good spoof of campaign ads.



PACKET
PUSHERS

Link Propagation Newsletter

Our weekly newsletter delivering essential headlines, announcements, and useful news to your inbox

Can't get enough newsletters? Check out [Link Propagation](#), our newest publication. We send you a free weekly digest with tech news, interesting blogs, and industry announcements, all curated by the Packet Pushers. It's an easy way to keep up and stay informed. Subscribe at packetpushers.net/link-propagation.

Quick Survey: Tech Conferences

What's the most valuable part of attending a tech conference for you?

[A. Learning about new technologies/products](#)

[B. Talking to vendors](#)

[C. Interacting with peers](#)

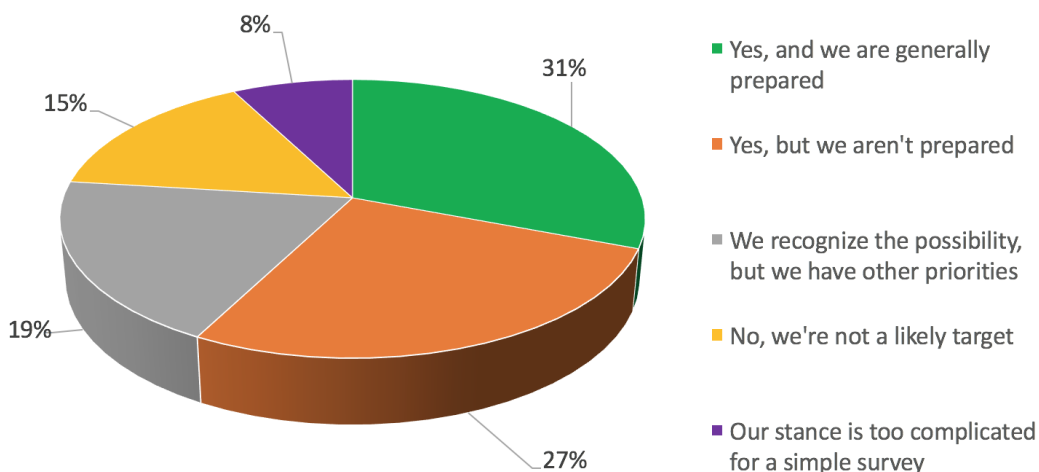
[D. Presentations from experts](#)

[E. Hands-on training](#)

[F. Other](#)

Last Issue's Survey Results

Are you concerned about DDoS attacks against your company?



Source: Packet Pushers Human Infrastructure Survey, February 3, 2017. 26 respondents



Did We Miss Something?

Got an link or an article to share? Email it to

The End Bit

Sponsorship and Advertising - Send an email to humaninfrastructure@packetpushers.net for more information. You could reach 5,013 people.

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 © 2017 Packet Pushers Interactive LLC, All rights reserved.

[unsubscribe from this list](#) [update subscription preferences](#)