IN THIS WEEK'S ISSUE: Reasons To Buy Whitebox, How To Bust Silos, & Edward Snowden. Please remember to enable the images; the magazine looks a lot better that way!

Table of Contents
(aka The Project Plan)

Issue Number 40

09/16/2016

The "Doing things differently" issue.

Thought For The Week:

Firewalls don't have to be secure to meet policy--they just have to be there.

1. Nine Reasons For Buying Whitebox Switches

by Greg Ferro

Someone asked me for reasons why they should buy whitebox switches. I came up with nine.

1. **3-year ROI.** A low-cost product can get ROI in less time and be replaced sooner. Faster hardware rotation equals more innovation/feature adoption. (Big shout out to Cisco Nexus 7000 customers on decade-long ownership cycles.)

2. **Software bugs.** Vendors take months to locate, accept, and fix bugs, which has enormous impact on your business (see here). With OCP-compliant whiteboxes, you can switch software and keep your business alive, or work around slow vendor support.

3. **Self-sparing.** For some/most use cases, self-sparing is better than relying on vendor inventory. When products are cheap, you can hold inventory in your data center and bring MTTR down to hours instead of days.

4. **Pre-inventory.** Low-cost switches held as internal stock reduce lead time for new project provisioning. Don't wait for approval/PO/delivery, just pull from stock. Also, stocks of SFP modules for whitebox switches can be held when they cost 1/10th of vendor units.

5. **Vendor management.** Using at least some whitebox can coax better discounts or engagement from incumbent vendors. Most companies will have a core/pod architecture and use a mix of branded/whitebrand/whitebox. Encourage your vendors to be better aligned to your needs by not buying their products.

6. **Supplier risk.** Using different whitebox vendors can reduce your risk from hardware bugs. A single switch model reduces operational costs, but also places an enormous bet on a single supplier product.

7. **SDN.** Move your operational focus from a vendor-specific CLI to an SDN solution. If you're concerned about having multiple vendors to operate, then buy a SDN solution that is device independent. Products such Anuta and Apstra remove the hassle.

8. **Core/pod architecture.** You can build a new network using modern design principles like ECMP without affecting your existing networks. Don't have one network, have many "network pods."

9. **Low port utilization.** If switches are cheap enough, you don't have to use every port to get an ROI. This avoids stretching cables between racks or rows, or paying for expensive SFPs to long-haul a couple of servers.

Final Advice

You'll note that I didn't explicitly cite the cheaper price of whitebox switches as a reason to buy them. That's because companies don't really care about cutting costs. Seriously. Companies are more than willing to spend big if they believe value is returned in some way. Companies waste time negotiating prices with vendors just to pretend they haven't overpaid for a particular brand, or over-provisioned the solution 'just in case.'

You might also notice that I have explained how cheaper products can change the way you design and operate a network. And that's how you should present this to management.

2. How To Bust Silos, Even If Your Job Won't Let You

by Ethan Banks

Here at Packet Pushers, especially on the Datanauts podcast, we espouse silo-busting. That is, we've been encouraging folks to step outside of their technological comfort zones and develop skills in other areas. The logic is simple: we see IT disciplines converging.

Some IT cross-over is happening now; just look at converged and hyperconverged products in which a bunch of tech has come together to form a unified system. Folks working on converged platforms will better serve their organizations if they have some idea of how all of this tech works together.

Some cross-over is on the horizon. For instance, enterprise IT seems headed toward private and hybrid cloud, but it's a slow shift. It's going to take a few more years to even get to the 50% mark, according to some data VMware gathered and shared in a keynote at VMworld US 2016.

But the shift toward cloud is inexorable as opposed to trendy. Cloud operations imply converged operations. The more you know, the better off you'll be.

However, busting into another silo is not always easy. Some of you have pointed out that what you do on the job is written in virtual stone. Some of you have contracts that stipulate exactly what your job is, and neither initiative nor ambition will break you out of that contractual cage. You can only do what you're allowed to do, and no more.

What's a prospective silo-buster to do in this situation? I have a few thoughts.

1. **Don't let a job description inhibit your ability to learn.** You can still go after new skills, even if you won't be able to exercise those skills on the job. Not using new skills on the job might make it harder to retain specific mouse click and keyboard presses, but don't worry about that so much. Instead, work on comprehension of previously unfamiliar technology -- what the tech does and what problems are being solved with it.

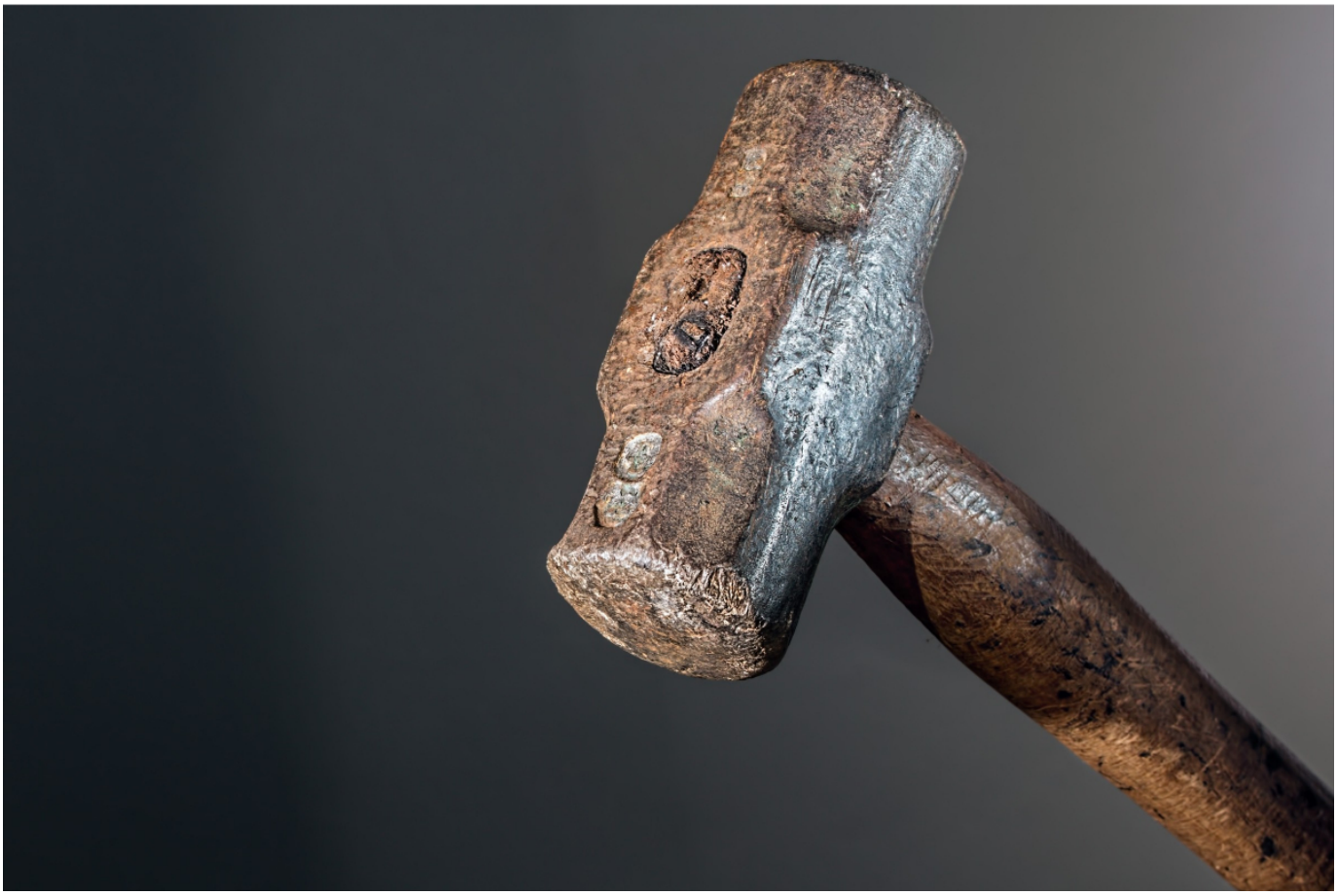
2. **Recognize that knowledge always helps.** Technology breaks. Having a technology perspective outside of your silo means that you'll have insights others might not when a complex IT system breaks. When the system is down and you're on that all-hands call, big-picture knowledge coupled

with your silo-specific expertise can help rule out suspected problems quickly.

3. **Understand that what you know about other silos will impact how you behave in yours.** For example, if I'm deep in my silo and never pop my head out, I might simply set sub-second network failover timers to accommodate a specific application requirement that's been handed down to me from on high. However, if I've studied to understand the details of the application architecture and how the underlying protocols work, I might have enough knowledge to suggest an alternate application architecture that accomplishes the same resiliency goals. Yes, there are architecture teams dedicated to this sort of thinking in large organizations, but that shouldn't stop you from acquiring that knowledge yourself.

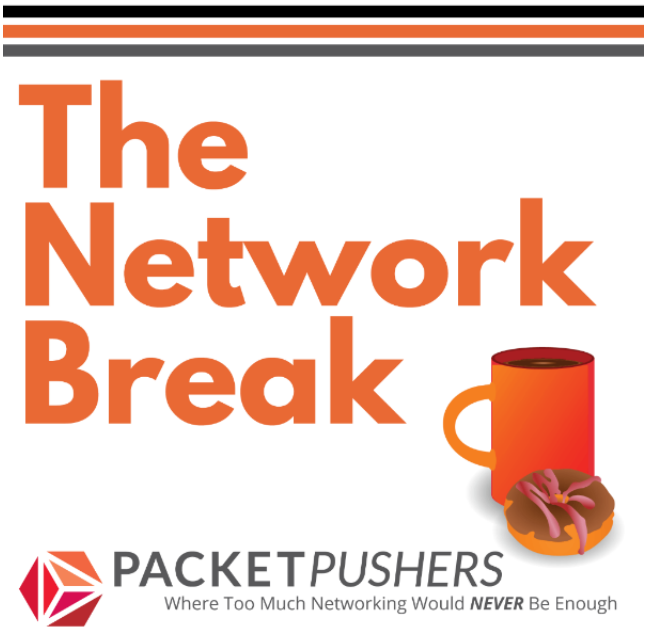
4. **Think of your future.** Career opportunities in technology are often based on what you know. Deep knowledge of a specific silo is powerful, and perhaps exactly what your current job description calls for. But what about that next opportunity? Don't limit your options because you chose to look at your job description, shrug, and take the path of least resistance.

Future-proofing your career requires that you know more about more. Even if your job description prevents you from crossing silo boundaries, you need to enhance your skillset to keep up with changes coming in IT.



Get to work--that silo's not gonna bust itself.

Join the Datanauts on their mission to bust silos and explore the latest



Network Break is a weekly podcast that delivers news &

developments in cloud, convergence, data centers, and more. Sign up free here.

analysis on the networking industry in a fun, fast-paced style. Subscribe here!

3. A Pardon For Edward Snowden?

by Drew Conry-Murray

Recently a New York Times editorial called for Barack Obama to pardon Edward Snowden. The editorial argues that by exposing the U.S. government's far-reaching surveillance of its citizens, Snowden served the public interest and deserves to be forgiven for illegally revealing classified documents.

I agree with the first part: Snowden's revelations are a public service. Unbridled data collection with little to no oversight imperils our privacy. It lays the infrastructure for a surveillance state, and opens the door to any number of abuses by government individuals and institutions.

Our day-to-day lives are now essentially digital windows, into which anyone with the requisite technology can peer. This makes it all the more imperative that we have robust controls over who gets to see what, and how much.

By exposing the NSA's rapacious collection habits, Snowden brought the debate about digital privacy into mainstream political and public discourse, which is exactly where it needs to be.

As for the second part, I don't agree that Snowden should get a full pardon. While I believe his actions were just, they were also illegal, and he should face the consequences.

And frankly, I think his cause would be better served if he came back to the United States and went to prison. The sacrifice of his own liberty would demonstrate the strength of his convictions. And it would remind us of the value

of our own freedom, and how much we have to lose if we don't push back against unchecked surveillance.

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

Excess Management Is Costing The U.S. $3 Trillion Per Year

I've been highlighting that the fact the IT management is in a poor state. IT engineering professionals have changed their practice and business skills over the last decade to become useful. Business professionals have done little to upgrade their skills or learn technology.

According to an article in the Harvard Business Review, managers are creating layers of excessive bureaucracy.

> *That works out to one manager and administrator for every 4.7 employees. Overall, managers and administrators made up 17.6% of the U.S. workforce and received nearly 30% of total compensation.*

It also highlights that over-employment of managers is a productivity burden.

> *Three trillion dollars represents 17% of U.S. GDP. If this burden was reduced by half over the next 10 years, productivity growth would increase by a compounded rate of 1.3% annually, essentially doubling the post-2007 productivity growth rate.*

Email this to your boss.

Did Hackers Tilt An Oil Rig? Getting The Story Straight

Cris Thomas (aka Space Rouge) tries to track down a rumor that hackers were responsible for causing an offshore oil rig to tilt by infiltrating the rig's ballast control system. It's a story that sounds plausible because we know industrial controls and SCADA systems represent juicy targets--malicious actors can cause physical damage and disruption from the cyber-shadows.

It turns out the claim is really hard to prove, even though it's been repeated in the media and by infosec companies.

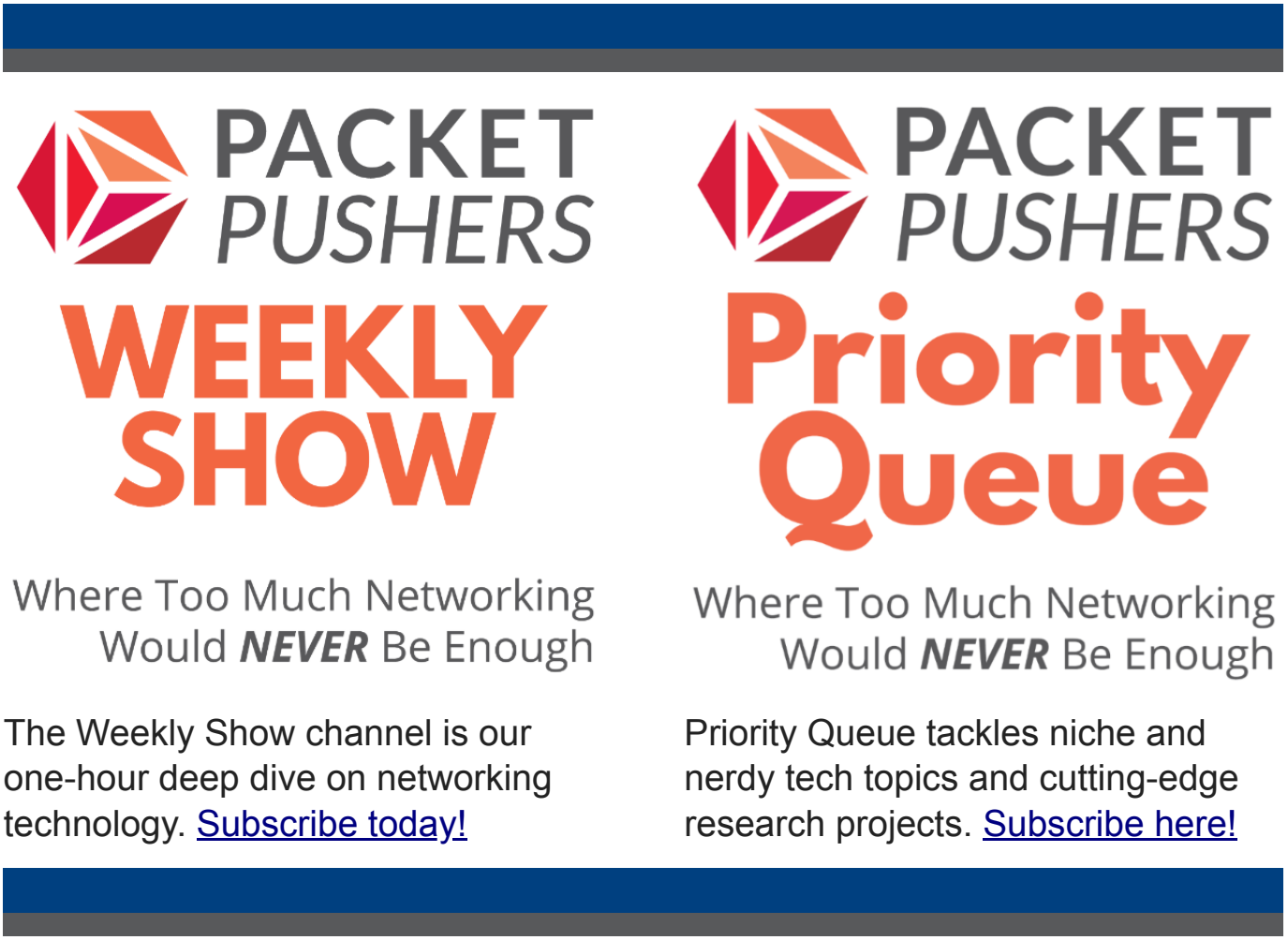
> *"I can easily see how someone could make a jump from...'problems with software' all the way to 'hackers did it'. Someone then half remembers the story and starts repeating it a few times and it spreads from there."*

We need to beware of the FUD and stick to the facts. At present, Cris notes that Stuxnet and a Ukraine power outage are the only provable cases of a cyber attack causing physical damage.

Serverless architectures: game-changer or recycled fad?

Gojko Adzic has an interesting take on the 'serverless' phenomenon. Jokes and buzzwords aside, he asserts that what makes serverless so unique isn't the technology per se, but the financial incentives it creates.

"It's the first time, at least in twenty years I've been making software for money, that a deployment architecture actually creates strong financial incentives for good design practices, and clear financial penalties for bad design. And that, for me, is the thing that's really revolutionary about serverless."



The Weekly Show channel is our one-hour deep dive on networking technology. Subscribe today!

Priority Queue tackles niche and nerdy tech topics and cutting-edge research projects. Subscribe here!

Recent Articles

The last five articles published on EtherealMind and Packet Pushers

EtherealMind.com Latest

Enterprise IT Doesn't Care About The Price. Really.

Unregenerate 20160827 – The Week Gone By or To Come

Intel IDF: Convergence Is Everything

Why Google Slows Fibre Rollout

Response: Arista Market Share

PacketPushers.net - The Last Five

Show 306: Debating Network Complexity & Capability With VMware (Sponsored)

PQ Show 92: Network Or Endpoint: Where To Put Security?

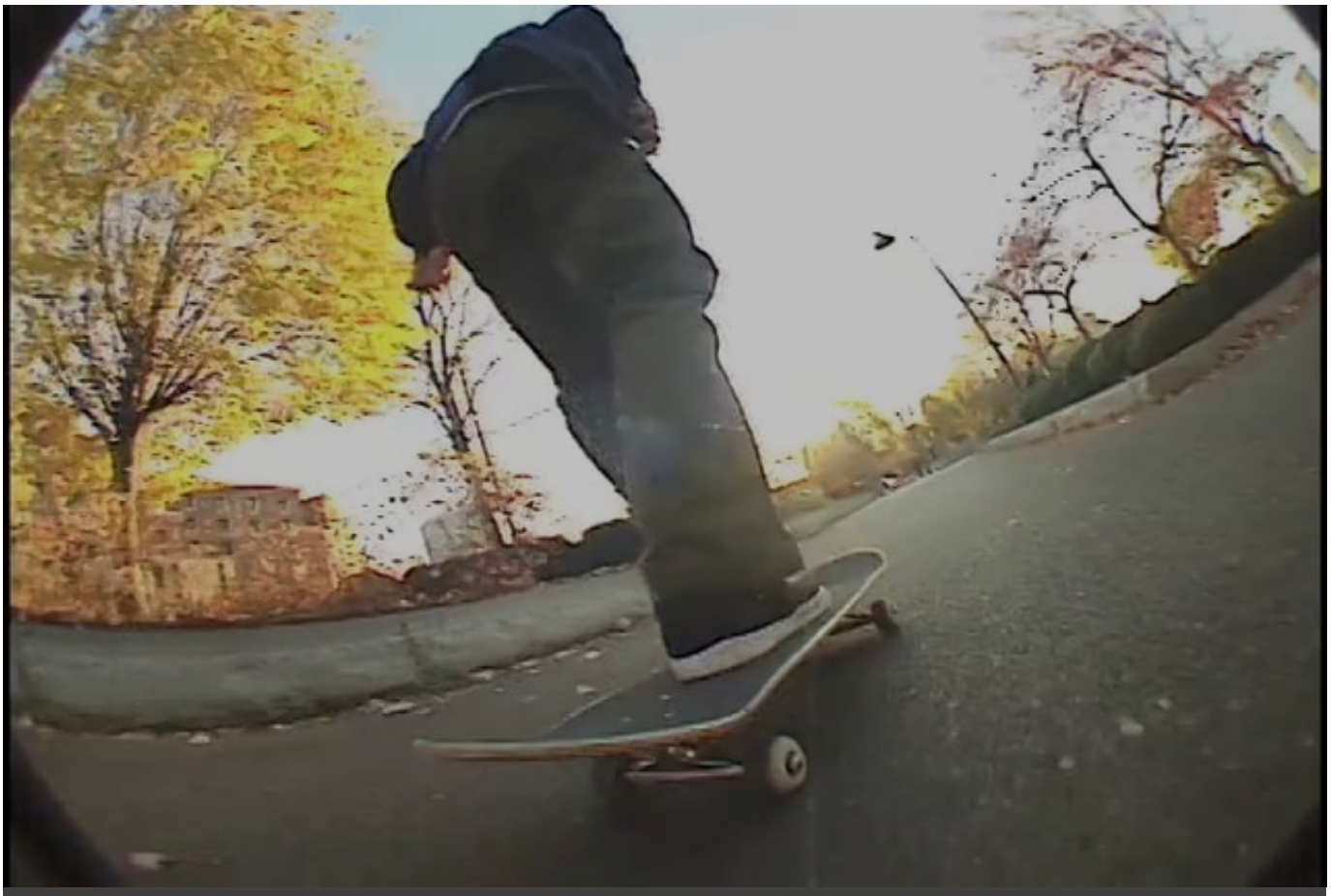
Datanauts 051: Intel & The State Of Software Defined Infrastructure (Sponsored)

Network Break 103: Dell, EMC Unite; HPE, Intel Sell Parts

Show 305: A Eulogy For TRILL?

Watch This!

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



I can't skateboard, but this video makes me wish I could. Here's a board-level view from various spots in Boston.

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: Filling Your Stack

Aside from your primary technical discipline (i.e., networking) in how many other disciplines (i.e., storage, security, applications, etc.) would you say you are competent?

A. None
B. One or two
C. Three or four
D. I'm full stack, baby!

Did We Miss Something?

Got an link or an article to share? Email it to humaninfrastructure@packetpushers.net

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.