SPONSORED

20 of the Most Painful Lessons IT Pros Had to Learn the Hard Way

By Dimension Data | Follow

Jul 23, 2014 12:17 PM

By David Spark

You can't become a great IT pro without breaking a few metaphoric networking eggs. It would be great if all these mistakes happened in a sandbox environment. Unfortunately, they often happen during business operations.

While learnings from these mistakes are invaluable, making too many of them does not bode well for the future of your job or business. Alternatively, if we could collect the knowledge gained from these costly mistakes, we'd all be wiser. The only cost to you would be the time it takes to read this article.

1: Complex systems are expensive to operate

"If systems don't have to be complex don't make them complex or you could risk not having the necessary staff to fix things," said Nestor Rincon (@RinconDynamic), Founder of Rincon Dynamic, who became the single point of failure for a custom network he designed.

Ian Rae (@ianrae), CEO for CloudOps, concurs, "Avoiding network complexity has a huge operational payoff."

"If you are the only one in the world to use a particular combination, it means that your headaches are also very unique," said Michael Bushong (@mbushong), blogger and VP of Marketing for Plexxi. "While it might seem expensive to modify your practices to suit an architecture, think about the risk of being a snowflake when everything is on fire."

"In order to meet the industry needs of today, enterprises need to move from traditional legacy networking that is manual, requires device-by-device configuration and complex, to a network that is more simple, agile and automated," advised Kash Shaikh (@KashShaikh), Global Marketing Leader for HP Networking.

2: Complex systems will be replaced

"The temptation for a lot of people is to tune infrastructure for very specific behaviors," said Plexxi's Bushong. "Every time you

add helpful but not quite necessary things into your network, you add complexity… At some point, the whole thing comes crashing down."

"Custom server hardware is eventually replaced by commoditized consumer hardware re-purposed as servers, which in turn is eventually replaced by virtual servers," said Dwight Koop (@dwightkoop), Cofounder and COO of CohesiveFT.

3: Lack of pre-planning and testing will bite you

"It is just so easy to skip the planning, testing, and architectural alignment work to make quick changes or upgrades particularly when you managed to get away with it maybe 75 percent of the time, or at least to get away with it," said Rich Schofield (@DidataInsights), Business Development Director, Networking for Dimension Data. "However, when things go bad, they go really bad."

Schofield realizes that most of us think the disciplines around change and release management are overdone, but when things go wrong, they go really wrong.

"A disciplined approach, followed with every change and release, is key to a well-run and cost-efficient network," said Schofield. "Next time you are planning for changes or releases and you find yourself thinking, 'this is such a pain,' remember the pain when things go wrong."

4: Don't underestimate the complexity of running a network remotely

For years, North Coast Security Group had managed networks remotely through secure UTM appliances. With little to no on-site visits to resolve issues, they felt they were ready to handle everything remotely, so they started bidding out-of-state contracts, explained Hassan Abdul-Zahir (@northcoast_sg), North Coast Security Group's Cofounder and CTO.

While Abdul-Zahir thought he could just ship UTM appliances and have his clients install them on site, the clients ended up moving equipment and changing ISPs without telling the North Coast team. Not being there resulted in far more reengineering, development, and partnerships to make the remote operations possible.

"We vastly underestimated the human component in the contingency plan and that was the hardest lesson we have learned thus far," said Abdul Zahir.

5: The current design isn't going to last

"My most painful lesson is succumbing to the temptation to believe that current design will suffice for a period of time longer than what is realistic," admitted Tom Fountain (@TomFountain9), CTO of Pneuron. "The quicker, cheaper path is to assume that current requirements will suffice rather than ensuring multiple years of support for what the business throws at IT via sound architecture, capacity planning, and built-in flexibility."

"Design needs to take into account redundancy, which will allow an upgrade to happen without taking the environment offline," said Isaac Conway (@Latisys), Director, Network Engineering for Latisys. "Actual usage on the new platform should be under 25 percent starting at day one. This will allow you to at least double in size before upgrade conversations need to happen."

"New paradigms like Big Data and cloud applications are forcing the entire IT industry to rethink the importance of infrastructure flexibility and scalability," said Tim McIntire (@StackIQ), CEO of StackIQ.

"Avoid network management systems that are so rigid that they restrict the enterprise from simple development, and fast time to market, for new applications and services," said Bob Rodio (@ciena), CTO for Network Transformation Solutions at Ciena. "You don't want to forsake available functionality because of management system limitations."

6: Don't assume

"Assuming can be the difference between success and failure," said Adam Haines (@Adam_Haines), Director, Systems for Federated Sample.

Early in Haines' career he encountered a networking issue that caused production servers to disconnect intermittently. The team went through a battery of tests, network traces, and wild theories as to what was going on, until Haines just looked at the switch and discovered a cable was creating a loop.

"I learned that day troubleshooting is a delicate art form and assumptions cannot be made," said Haines. "Each and every aspect of the problem has to be considered."

Rincon Dynamics' Rincon agrees, "Always try the basics first and see if it fixes it."

Rincon had a situation of a failed database that couldn't cross the network. After four hours of troubleshooting, he looked at the firewall. Sure enough it was blocking the database.

"That was a bruise to my ego but it definitely made me a better IT professional," admitted Rincon.

7: Backups are worthless if you don't test them

"I learned the painful lesson that the false peace of mind that comes from running regular backups is worthless without testing that the backups are actually working as expected," said David Reischer (@LegalAdvice), Information Systems Manager for LegalAdvice.com.

"It's never enough to trust anything critical to a process that has a single point of failure," warned Dean Wiech (@dwiech), Managing Director of Tools4ever.

Both Reischer and Wiech had to learn the hard way. After they had succumbed to data disasters that couldn't be restored, they started verifying backups.

This advice also holds true for verifying backup support from vendors.

"Just because something is written in a contract, doesn't always make it so," warned Mike Vitale (@TalkPointDotCom), CTO for TalkPoint. "If your network vendors promise N+1 or 2N redundancy, make sure it's being tested on a regular basis. Don't wait for a real emergency to find out your colocation facility or content delivery network has been cutting corners."

8: Vet consultants for interoperability and business alignment

"The wrong consultant can ruin your relationships and leave you with a smoking wreck to manage once they have completed their assignment," said Ben Trowbridge, Chairman for the Outsourcing Center. "Make sure the consultant understands you and your company and can navigate both the cost savings/transformation you seek and also improve your working relationship with your carrier."

"Despite vendors adhering to a standard, it's quite likely their products will not gracefully interoperate," said Bernard Golden (@BernardGolden), VP of Strategy for ActiveState. "There's really no way around this except by diligent testing. The alternative approach is to require the vendors to demonstrate interoperability and then write it into the contract."

"Look at the OEM vendor closely and directly before committing to an enterprise wide solution," said Eric Ingram Adjunct Instructor at APT College, LLC. "Don't rely solely on the information provided by the distributors."

Ingram admits to being burnt a couple of times due to OEM products losing support soon after purchase. If he had done just a little research into their background it would have shown they should not be relied upon for future networking needs.

9: Always be monitoring your performance efficiently

"You need to take pro-active steps to automate the alert processing. Or else you'll find that all your best resources get sucked in to do the day-to-day firefighting and noise control, and that is counter-productive for the organization," warned Raju Chekuri (@rajunetenrich), CEO of NetEnrich.

With the understanding that networking is a collection of various systems and network components that depend on one another, Bruno Scap (@MaseratiGTSport), President of Galeas Consulting, advises administrators to "configure your network monitoring in a way that follows these dependencies. This will decrease the number of alerts and increase their accuracy. For example, when a network device controlling a remote link fails, you will get notified that the remote network is unavailable, without getting additional alerts for all the other systems that are connected to that particular network device."

"Having information [about network performance] makes the conversation with your provider much different, and much more productive," said Matt Larson (@matthewhlarson), CTO of Dyn. "With the right tools in hand, it's harder for a provider to deflect responsibility or resist taking action in the face of hard data."

10: Just because you can't see it, doesn't mean it's not out there

"We deploy monitoring and management systems, and we put faith in the results they provide," noted Jay Botelho (@jaybotelho), Director, Product Management for WildPackets. "Because these systems are mostly accurate we are lulled into a false sense of security."

What happens when NetFlow data transitions to a sampling mode because the dependent router needs the processing power to route packets? Our monitoring system isn't collecting the necessary data and we have no idea it's missing.

"Take the advice of a woodworker," said Botelho, "Measure twice, cut once. Or in other words, for critical functions, monitor the same data in multiple ways, reducing to the greatest extent possible assumptions, both known and unknown, that are built into our management systems, and ourselves."

11: Your redundant systems will be broken

"Continuity planning, including regular failover testing of all systems, is as vital to your business' health as knowing your fastest exit out of a building in a fire," said Jay Winters (@brinkmatdotcom), Director, Technology for delivery.com.

"Despite all your efforts to build in redundancy, a new situation will arise that is not handled by your redundant systems," said Jason Lamb (@jasonclamb), IT Systems Operations Manager for Eliassen Group, who points to situations of degradation that don't trigger redundant systems, yet weaken your office's ability to operate.

"Engineers need to account for many types of problems, capacity and bandwidth requirements need to be reviewed proactively, and the act of rerouting traffic must be operationalized as much as possible," explained Pat Harper (@OpenText), CIO for OpenText.

One common issue, an unexpected power outage, can wreak havoc on business operations given the amount of live data.

"Billable hour docketing and unsaved Microsoft Office documents instantly become corrupted files," said Steve Prentice (@steveprentice), Senior Writer for CloudTweaks. "It can easily turn into a nightmare of downtime and person-by-person recovery."

12: Crisis management training shouldn't just be about putting out fires

"An over worked technologist who is completely focused on fighting the day to day fires of desktop support ends up neglecting patches and security updates from pure lack of time," said Anthony Butler, CEO of Precision IT.

"The worst mistake for a technology executive is to build crisis management skills and to focus mostly on those to extinguish fires when best practices dictate that prevention and thoughtful planning go a longer way and justify pre-emptive investments," said Max Dufour (@maxdufour), Partner at Harmeda. "The cost of downtime and the cost of fire drills can be greatly diminished by efficient IT management and strategy."

13: Remember to think about the future

"The most painful lesson I've learned with managing a network is a failure to think towards the future. I've always felt that I was missing pieces of information when I had issues in the past," said Michael Spratt (@milkmanstl), Sr. Customer Operations Support Specialist IPS for MasterCard Worldwide.

"I now take time from my projects to be innovative and think towards the future. Discovering ways to make parts of my job automated helped me the most," said Spratt.

Network management | networks

SPONSORED

20 of the Most Painful Lessons IT Pros Had to Learn the Hard Way

By Dimension Data | Follow

Jul 23, 2014 12:17 PM

"The network – and our thinking about it – must evolve," said Eric Reed (@GECapital), CTO for GE Capital – Americas. "This includes not just the underlying technology, but how we manage and provision it (e.g., SDN), how far it reaches (e.g., WAN, LAN, VPN, mobile), and how we secure it. As we move away from traditional workforce ideas (e.g., employees sit in our offices using PCs connected to our physical network) and into a more mobile and connected workforce, how we architect and secure our networks has to be looked at constantly and we have to be willing to change."

14: You're only as good as your ISP

"As companies rely more heavily on a remote workforce, satellite offices and cloud-based services, it's essential to get every bit of bandwidth that is promised by your service provider," Dan Tully, EVP at Conduit Systems.

Tully had a biomedical client that was slowly growing its demand for bandwidth intensive resources. They needed more bandwidth for hosted video, web research, and their growing mobile workforce. All put a huge strain on the bonded T1 and the ISP's aging hardware.

"Pay attention to the gradual change in corporate focus and makeup as it can shift before your infrastructure is ready," said Tully.

15: Don't just look at the current choke point

"When you have an immediate bottleneck to deal with, the tendency is to purchase a bigger box to relieve the pressure but what you need to be thinking about is the next place your network is going to choke," Karthi Subramaniam (@ADARAnetworks), Chief Software Architect at ADARA Networks. "You also need to make sure that you trace bottlenecks from one end to other because simply adding more bandwidth or upgrading the network gear alone won't solve application performance or fidelity issues. This will make you less vulnerable to vendors who use these symptoms (bottlenecks) to upsell their gears and shift the problem to another vendor's box."

16: If the network has a problem, then the business has a problem

"The network is in the middle of virtually every service offered and is a core component to every person in the business ecosystem," said OpenText's Pat Harper. "That means that if the network has a problem, potentially everything that's built on top of it has a problem."

"From an operational perspective, every issue that affects application or site performance, availability, or user experience starts as a network issue until the network can be ruled out," said GE Capital's Eric Reed.

17: When upgrading equipment, don't make network changes

"When making major changes, such as upgrading computers, application changes, security changes or moving equipment

between data centers, don't make any network changes, said Abdul Jaludi CEO of TAG-MC. "Regardless of where the problem is, networking will always be blamed first when major equipment, system or data center changes are done in conjunction with network changes."

Repeatedly, Jaludi has seen network finger pointing when application and security changes are also made.

"Nine out of ten times the incident was caused by one of the other changes, but those types of issues are usually associated with networking and precious time is lost backing out the network changes only to find that didn't resolve the problem. Eventually the cause is identified as coming from the changes implemented by one of the other teams, but by then the damage is done, and the network team has to schedule another change package to re-implement the change that was just backed out. "

18: Watch out for those sneaky users and their nasty traffic patterns

"Stay on top of the types of traffic crossing the network. There's no telling what users will try to get away with," Matt Sarrel (@msarrel), Executive Director for Sarrel Group.

Sarrel has had clients with no traffic monitoring tools at all. By simply setting up his laptop to monitor packets for 24 hours he quickly discovered that an employee at one company was running a web server on his workstation that was serving up millions of JPGs a day. Another company had an active BitTorrent server chewing up company bandwidth.

"Many people try to connect all kinds of personal devices to their work Internet, from game consoles, like Xbox, to personal printers and wireless home routers," Rick Bylina, Senior Product Marketing Manager, Infoblox. "These devices, as harmless as they may seem, leave the network vulnerable to outside security attacks."

One Infoblox customer connected a wireless home router to the office network, which allowed over 200 million customer credit cards and other private information to be stolen, said Bylina.

19: Protect your network by managing your SLAs

"As organizations are increasingly delegating control of their network – including carrier services and service management – to third-party providers," said Sanchit Gogia (@s_v_g), Chief Analyst and CEO, Greyhound Research, "Defining your SLAs (Service License Agreements) is the most important lesson I've learned. in the starting years of my company."

The first major mistake Gogia made was not defining SLAs to the specifics. For example, one SLA he signed up for only indicated network availability to 99.99 percent. Later he realized that network latency and packet delivery would matter before bandwidth started failing. Today, Gogia has SLAs that define guarantees for network availability, notifications, latency, and packet delivery.

"It's important that SLAs are specific to help reduce cost of ownership," said Gogia.

20: Everyone has different expectations from IT

"Each user has a preconceived notion of what IT should and should not be doing based on their previous work environment," said Evan McCutchen (@emac_TA), CIO for TechnologyAdvice. "Our team members coming from small organizations, they expect hands on, step by step instruction which completely contrasts with our team members coming from corporate environments who look for resources which enable them to be somewhat autonomous."

"Whereas previously, we were able to dictate application utilization, security and corporate IT policies to create the confines with which we protected our organization's intellectual property, now we must be visionaries," said Ozzy Macias, Manager of IT for the Miami Marlins. "We must plan far into the future and predict solutions that are coming at us based on what is trending in the market."

"Reconfiguring business logic to suit the network costs an incredible amount of management bandwidth and time," noted Salim Ismail (@salimismail), Global Ambassador for Singularity University and author of "Exponential Organizations."

CONCLUSION: Moving beyond issues of network availability

"Knowing when a network node is down is easy, but determining why critical applications are not operating properly is the challenge," said John Isch, Practice Director for Network and Voice for North America, Orange Business Services. "We advise moving more applications to the edge of the network to give a solid handle on application performance."

"Network managers can no longer be satisfied with just ensuring network availability and uptime," said Bill Talbot (@btalbotjr), Senior Director of Product Marketing, Infrastructure Management for CA Technologies. "They need to recognize and eliminate application performance issues in real time or before they even occur. This requires an application-driven network performance management perspective that puts the health and operation of the network in context with the services being delivered to end users."

Network management | networks

PREVIOUS POST
20 Ways to Reduce the Operational Costs of Your Network Before it's too Late

PREVIOUS 1 | 2