Hacking Your Users: Toward a more human-centric IT

- Introduction
  - Most of us spend all of our time dealing with massive systems. We've built networks that span buildings or states, or continents. Our charges are servers by the dozen, virtual machines and their attendant requirements. We manage routers, switches, plists, databases, repositories and structures.
  -
  - In many cases, we act as the machine interface for management.
  -
  - But our role is dual. We also serve as the human interface for our Users. We sit in the middle. It's up to us to build great systems, but it's also up to us to build better Users.
  -
  - Much of what we do is about building systems of trust with our machines. We bind machines to our directory masters, we bind users to machines, we deploy software to Users and machines, we backup data from Users and machines. We spend much of our time in this space, acting on hardware and software to make sure that they work according to a complicated web of licensing, support agreements and any number of custom-crafted systems.
  -
  - But how much time do we spend working on a web of trust with our Users? Do we match the time that we spend on our Munki and Puppet installs with training and engagement?
  -
  - Let's talk about some of the problems that we have with perception.
  -
  - **Nick Burns**
    - This might be my least favorite stereotype of IT pros. It might also be the most frequently correct.
  -
  - **Roy Trenneman**
    - Have you tried turning it off and on again? Is it definitely plugged in?
    -
    - These are questions that we often have to ask - yes - but how we ask them is important.
  -

Hacking Your Users: Toward a more human-centric IT

- We know these stereotypes. We might even aspire to parts of them! But we do best with our users when we surprise them with flexibility, with understanding, and best of all with knowledge and education. They may have spilled another coffee in their laptop, or used the Trash as a filing system. But it's our job to make it so that doesn't matter.
-
- There's a problem, though, in these stereotypes. They make it harder for us to do our jobs. Whenever people take shortcuts in their impressions of us - whenever they avoid our department because they're afraid of MOVE or "Have you rebooted yet" they're routing around you, and that's a problem.
-
- The problem is: when they route around you, you're no longer part of the discussion and the process.
-
- So how do you show your users that you're not Nick or Roy? Let's talk about combating some stereotypes by using some. I can sense the irony flowing through the room, but let's take a look at some of the ways you help your users trust you more.
-
-
- **Hacking Your Users:**
-
- But first, a warning. No one likes to be manipulated. And that's what you could be construed as doing, so be cognizant of that fact before you go ham handing it around.
-
- No one likes being pigeonholed or singled out, so spend a little time thinking about tact and handling this with grace and dignity. This isn't an end to end guide, and every person is different. I'm going to repeat that because it bears repeating: every person is different.
-
- We're IT pros, the bunch of us, but there's no one path to IT success or knowledge. I'm a liberal arts graduate with a masters in science & technology studies. I know amazing IT people with PhDs in archaeology, high school diplomas, and every degree under the sun. Your staff have the same gamut, and they're no less distinguished.
-

Hacking Your Users: Toward a more human-centric IT

- **Enthusiast Users**
  - We all have them. They know about the latest software patches and releases and versions shortly after (or in some cases, before) you do, and they're always clambering to get the latest and the greatest.
  - These are users who believe in asking forgiveness, not permission, so why not engage their enthusiasm and work with them?
  - If you don't work with them, they will go around you, and you're going to be spending all your time hardening every possible access point, switch port, physical system, farm house, hen house and out house in a 3-mile radius instead of doing your job.
-
- **Knows Enough to Be Dangerous Users**
  - Teach them to be less dangerous. Yes, I said I teach. More on that in a second.
  - But protect them from themselves. Backups that users can restore on their own goes a long way to make the building of knowledge the hard way, well, a little bit less hard.
  - Rich gave me an excellent example that some of their 10.8 Users experienced - The new All My Files view can be pretty confusing if you don't know what you're looking at, and you could accidentally do a substantial amount of damage there. Why not roll out a Profile or payload-free package that switches the default Finder view to their home directory instead?
  - Your
-
- **Fears All Computers**
  - This is your hardest row to hoe. But the most rewarding. Start small by teaching them ways out of trouble. Capturing crash logs, which in turn can be read to diagnose a problem can help the user feel in control of small computer issues.
  - Chances are, you need to be as much their machine therapist as you do their IT guy. This can be exhausting.
  - Jargon is your enemy with these users, so think twice or three times about individual jargon words that are deeply ingrained into our social interactions with each other - especially at events like this - and step back. Break down big concepts into their component parts. Don't go too far, don't patronize, but find the metaphors that the user is going to accept and work from there.

Hacking Your Users: Toward a more human-centric IT

- Recognize what is frustration, what is fear, and what you can do to combat those fears.
- In some regards, you're their computer therapist, not just their IT guy. You will have to deal with ghosts of previous data losses, previous mansplaining IT bros, and any number of additional issues. You may not have asked for this, but here we are, and it's better to get busy living than getting busy dying.
- And, recognize that Macs are not devoid of crashes, don't get defensive when your users say things like, "I thought Macs never crash!"

- If you've got individual concerns, I'm here after the talk and available by email, and I'm happy to help you through some difficult situations.
-
- What it all comes back to, though, is Building Trust.
-
- Here are some general tips for increasing IT's effectiveness with your staff through working through your Trust issues.
-
- **User Education > User Control**
  - Systems of Control create friction. The degree to which your imposed friction affects your staff's life will absolutely affect their opinion of your IT systems.
  - Every added measure of control, be that complicated user-installed 802.1x certificates for WiFi, 20 character login passwords that change every 60 days, and any enforced use of a specific application over in the place of alternatives will increase your friction, without sufficient understanding among your staff.
  - Once friction gets above a certain level, your Users may stop talking to you. They may just cut you out. I have a friend who works for a large office in DC, and it's gotten sufficiently bad with their IT department that they frequently just don't report problems until they have long since past what any of us would consider an emergency.
  - When they stop asking questions or asking for help, you've got either perfect users, or you've got a problem you don't know about yet. Which do you think is more likely?
  - Consider something when you implement it: Would I want this for myself?
  -
- **Not every human problem has a technical solution.**

Hacking Your Users: Toward a more human-centric IT

- That means that you may have to rely on your users to be good and benevolent people. Or maybe just protect them from themselves.
- If you allow your user a measure of control over their system, that control can extend to messing things up.
- But it can also extend to them feeling ownership over their environment and that empowerment - even if it's illusory - engender trust in your workers the same way soda in the office fridge and ping pong table might.
- Ownership means buy-in, which means you've got a partner out there, albeit one that doesn't necessarily share your goals and needs, and that's okay.
-

- **Fight For Your Users**
  - We all have that friend who has a restrictive firewall or application control
  - It should be your goal never to have to put one of those in without good reason. There *are* good reasons, especially for our education market friends,
  - This can mean managing upward, and they're your Users, too.
  - At the end of the day, you're not going to win every fight. You may not even win most of them. The point is: fight for your users every time it's possible to do so. That engenders trust and support, even in a losing fight.
  - Stay focused on the experience that your Users have, because that absolutely matters. If they can't get to Facebook on their desktop, they're going to spend more time on their phones, and that may not be what you want, either. Think about being results-oriented when it comes to IT restrictions. What's the outcome you're looking for? What are the unintended consequences?
    - My wife works in the Internet Services department of a large non-profit. When they re-built their firewall restrictions, suddenly all of the tools that my wife used for communicating with her members - Facebook, Twitter, LinkedIn, YouTube and others - were totally unavailable. So she filed a help desk ticket. For every web URL she couldn't get to.
    - While that's going to help your closure rate, maybe, it's sure going to make your life a bit frustrating in the meantime.
  -

Hacking Your Users: Toward a more human-centric IT

- We should have some goals for IT departments or IT agency when it comes to our users that are part of these systems of control. We should have a set of goals for how we build our Machine Systems of Trust, so they're part of our Human Systems of Trust
  - Give our Users a quality experience
    - Fighting technology shouldn't be part of the day to day.
  - Protect them from (self) harm
    - Backups are crucial. Anti-Virus (at least at the network/email level) is becoming a requirement. Teach people how to recognize phishing attempts - AND what to do if they think they've gotten caught up in a phishing scam. Security is only going to get more important in the next few years, and that means helping people get savvy. In addition, giving users tools to help diagnose their issues - and how the basics work - is a valuable thing to do.
  - Educate them where possible
    - Don't make them come to trainings unless you're going to make it worth their while. Instead, co-opt a few minutes of other meetings they're in to talk about what's coming down the pike, what's changing, or what's crucial
  - Fight for them against the unnecessary
  - Be their machine interface, too
- Jody talked about being happy on Thursday morning. Enjoying what you do is really important. Working with integrity - and building trust with your people is integral to the role -
- Charles talked about giving without expectation of return, and that should be an IT mantra, as well.
-
- I'm a musician. I'm a vocalist with years and years of training. My favorite single piece of music is Bach's B Minor Mass. You can probably find a recording of me doing the Baritone aria from the B Minor if you google enough. The first time I studied the piece of music, when it came down to the Dona Nobis Pacem, the final movement of the piece, I have a note from Gretchen, my conductor, and it's become my motto in IT.
-
- I don't have the original German that she spoke from the podium, reading it from Johann's own notes on the B Minor, but the English translation is pretty clear.
-

Hacking Your Users: Toward a more human-centric IT

- Send it forth, with deliberate intent.
-
- What an amazing time to be in IT. We live in the future, where we can reprovision whole machines in less than half an hour because of SSDs, where backup storage space in the cloud is effectively limitless, and where machine management, thanks to tools like Munki and Puppet and Casper, has never been easier.
- Monitoring, thanks to tools