Why isn't infosec working?

Did you turn it off and back on again?

By mubix "Rob" Fuller

root@localhost~#: kinit mubix@BruCon

- Internal Red Team for large companies (General Electric, IBM X-Force Red)
- US Government Contractor (Pentagon, Senate)
- US Military SOC Analyst (USMC)
- Small Startup (R5 Industries)
- Large Startup (Uber, Cruise)
- Pentest/Red Team Consultant (Rapid 7, Cisco)
- Bug Hunter (Syn Ack, H1, Bug Crowd)
- TV Show Consultant (HBO's Silicon Valley)
- Security Consultant (UN Initiatives in Ukraine and Syria)
- Security Meetup Founder (NoVA Hackers)
- Security Contest CTO (MACCDC)

root@localhost~#: kinit mubix@BruCon

- Internal Red Team for large companies (General Electric, IBM X-Force Red)
- US Government C
- US Military SOC A
- Small Startup (R5
- Large Startup (Ub
- Pentest/Red Team
- Bug Hunter (Syn A
- TV Show Consulta
- Security Consulta
- Security Meetup F
- Security Contest C

B.S in Cyber Security

Western Governors University

The Board of Trustees of Western Governors University,
upon the recommendation of the faculty, has conferred upon

Robert Fuller

the degree of

Bachelor of Science

Cybersecurity and Information Assurance

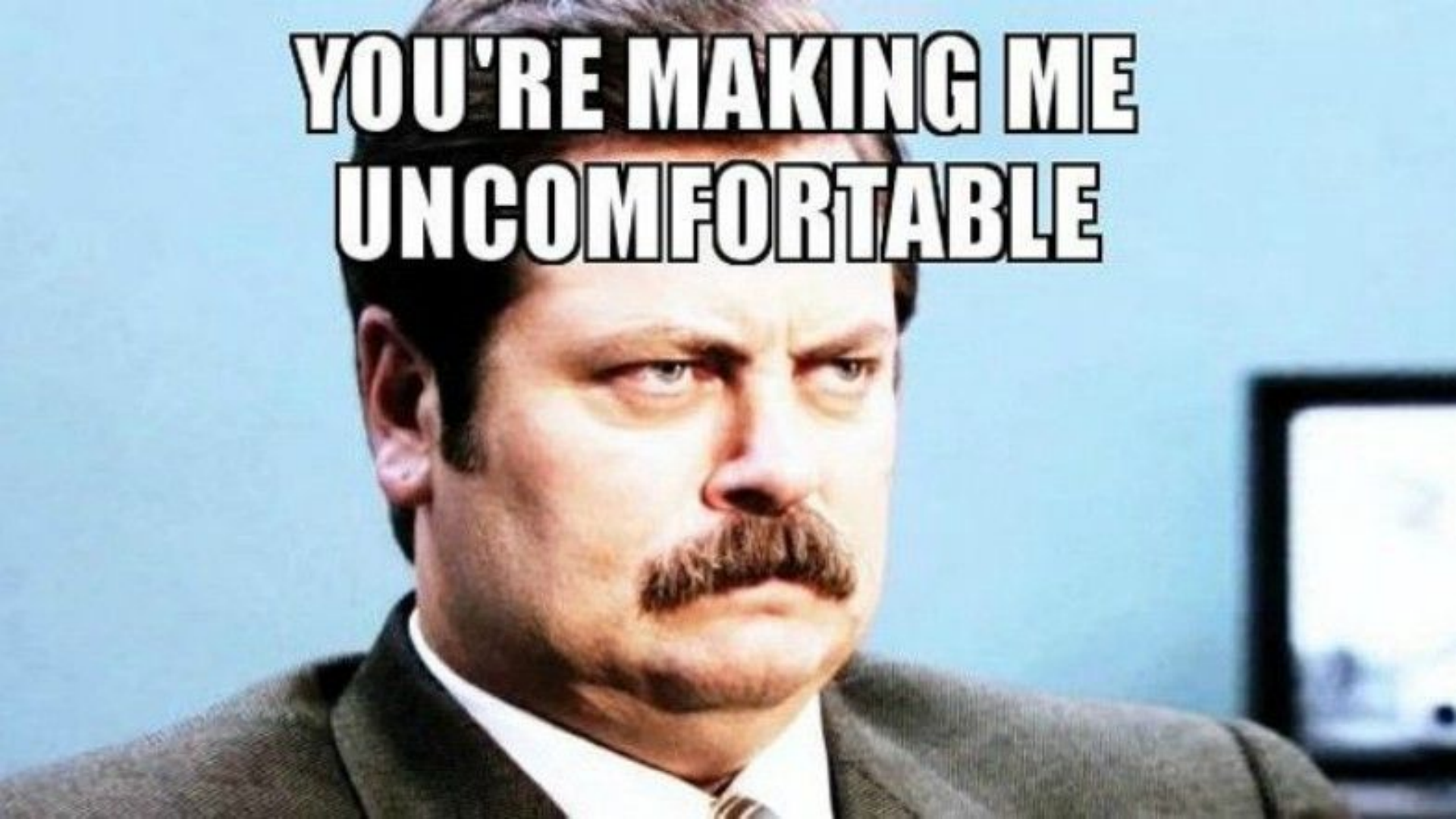
With all the rights, honors, and privileges thereunto appertaining.
In witness whereof, the seal of the University and the signatures as authorized by
the Board of Trustees, Western Governors University, are hereunto affixed,
this tenth day of January, in the year two thousand and nineteen.

Scott D. Pulsipher
President

Governor Jim Geringer
State of Wyoming, 1995-2003
Chairman, Board of Trustees

krbtgt


RAISE
YOUR
HANDS


YOU'RE MAKING ME
UNCOMFORTABLE

The InfoSec Echo Chamber

Top 10 ~~Complaints~~ Echos in InfoSec

1. Users are dumb.
2. Passwords will never get better, don't write them down, just use 2FA/PMs
3. No one ever listens to hackers/us/infosec/nerds/etc
4. Open Wifi == Bad
5. Antivirus is useless!
6. Roll your own crypto / software is stupid vs Blinky Boxes don't fix anything!
7. It's "Legacy"... ugh...
8. Just [Sanitize Input, Disable NTLM Auth, WPAD, LLMNR, NetBIOS, Macros]
9. You can't measure security!
10. I.T. sucks at Asset Management!

Users are dumb.

The Problem

- Computer Users, Employees, Non-security people don’t tend to follow security best practices
- One of the biggest targets for organizations is it’s users
- Phishing is the #1 cause of breach for that last X years.

The Simple Truths

- Users will continue to click links, use random / sketchy software, open documents with macros in them
- User awareness training can help decrease these numbers but is like taking Vitamin C for a cold.
- User awareness training just another corporate training that ***EVERYONE*** tries to get through as quickly as possible with the least amount of effort.
- Incentivizing security is a far better answer

Vitamin C

For the average person, taking vitamin C does not reduce the number of colds you get, or the severity of your cold.

In terms of how long your cold lasts, some studies have looked at people taking vitamin C every day, while others have focused on participants taking it once they develop a cold. In 30 studies comparing the length of colds in people regularly taking at least 200 milligrams of vitamin C daily, there was a consistent reduction in the duration of common cold symptoms. However, the effect was small and equates to about half a day less in adults, and half to one day less in children. These types of studies also found a very minor reduction in the amount of time needed off work or school.

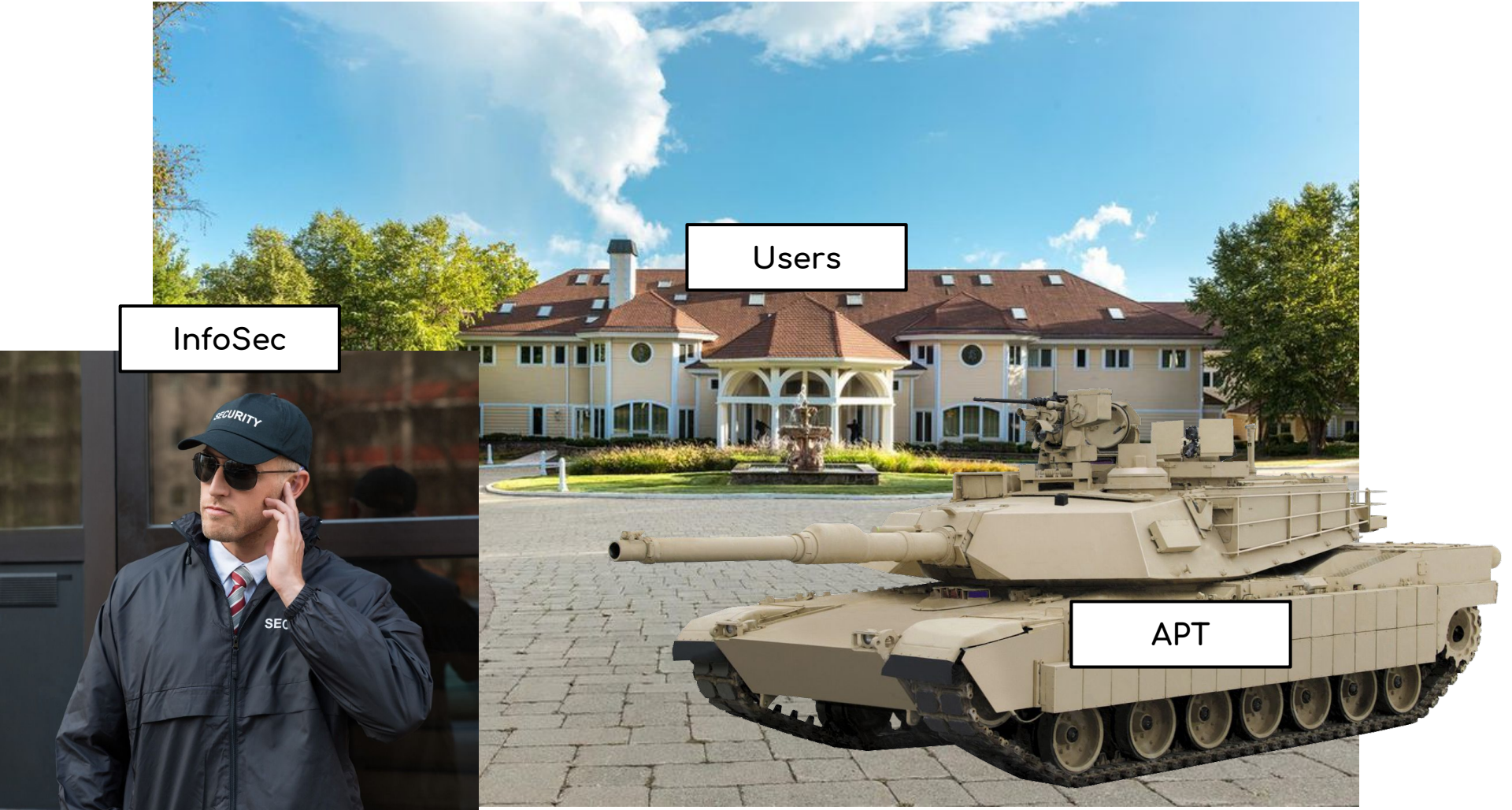
Source: https://medicalxpress.com/news/2018-08-vitamin-supplements-cold.html

Steve, can you believe that the idiots that live here don’t know the first thing about self defense?

I know, right? They asked me to quit bothering them with teaching them knife awareness drills. Don’t they know they could get mugged just walking down the street?

Amateurs...
I’ve been doing this for 10 years. Of course they need knife fighting skills.


SECURITY


Users
InfoSec
APT

The Hard Truth

It’s not their job.

It’s ours!

Passwords will never get better, don’t write them down, use MFA / Password Managers

The Problem

- Most people pick **bad passwords** for things.. You do too. Don’t deny it. I’ve seen security professional’s passwords.
- Password managers **aren’t supported** in many places (either you can’t copy/paste or install software/sync)
- **We** keep feeding the media stories about how 2FA via SMS is horrible, but the nuance that not all 2FA is SMS is lost on non-tech people.

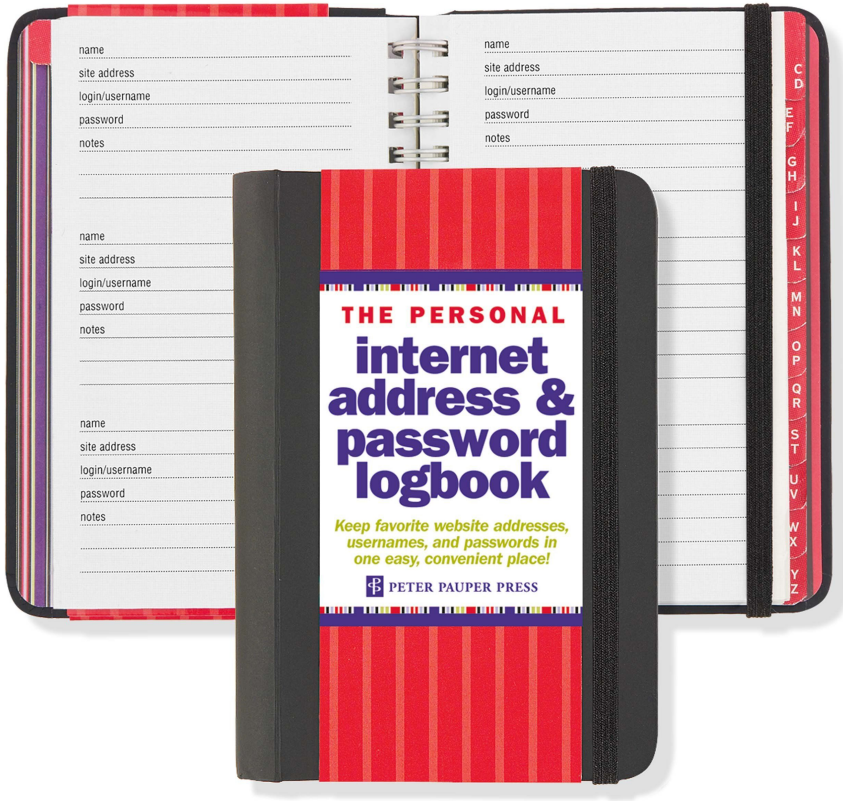
The Simple Truths

- Password managers are **difficult to use**. Apple is actually starting to fix with with their iCloud keychain (as scary as that sounds)
- 2FA/MFA is also **difficult to use** and near impossible to migrate between devices.
- We tell people not to **write down their passwords** even though 99.9% of the threats are digital.

The Hard Truth

Stop making fun of this:

Making security tools user friendly is the key to adoption.



No one ever listens to hackers / us / infosec/ nerds / etc

The Problem

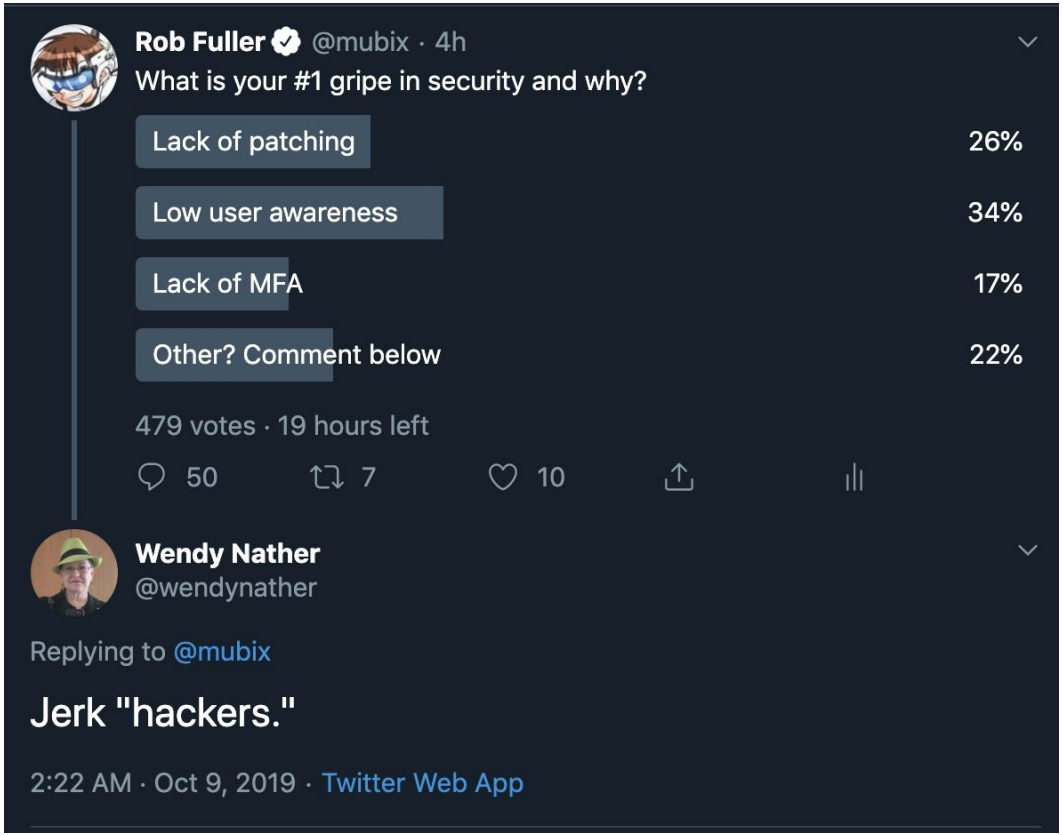
- Management buy-in on security projects / budget is hard
- Security programs are sometimes undervalued
- We regularly deliver advice in condescending, expensive, full of friction and hard to follow ways.

The Simple Truths

- Companies survive and pay salaries based on revenue
- Security doesn’t have direct return on investment
- Security keeps getting more expensive.

The Hard Truth

- We **complain** constantly when we don't get our way.
- We **extort** companies who don't do things we want them to do
- We lord our "**power**" over others and flaunt it regularly at conferences.
- We have to be **forced** to talk in business terms instead of hacker terms



We are a bunch of jerks...

Open Wifi == Bad

The Problem

- Open Wireless is pervasive, from hotels and airlines, to ISPs (xfinitywifi for example)
- Evil Twin / Wifi MTIM is easy to perform

Let’s play a game..


RAISE
YOUR
HANDS

The Simple Truths

- Most websites use SSL/TLS now (Thanks **LetsEncrypt**!)
- Chrome changes so often it's actually harder to exploit just due to code change speed.
- Host based firewalls have been on by default since Windows Vista (especially for "Public" networks)

The Hard Truth

It’s just not that big of a deal anymore. Time to fix the problem (insecure transports and websites) and not the symptom (Open WIFI == bad).

Antivirus is useless!

The Problem

- Signatures are **horrible** at detecting new attacks
- Signature based security is **easily bypassed**
- Very few companies **EVER** look at the AV logs

The Simple Truths

- **Low hanging fruit** is the bread and butter of AV
- These signatures are sometimes the **best indicators** of compromise you could hope for. Like finding PWDUMP on a Domain Controller
- Getting every piece of tooling past AV is **actually** pretty hard.

The Hard Truth

Stop bagging on AV. It's actually much more valuable than you might think.

If it does happen to be junk, remove it.

Roll your own crypto / software is stupid

vs

Blinky Boxes don't fix anything!

The Problem

- Blinky Boxes from **$Vendor** rarely do any good
- Building your own software to do what the Blinky Boxes do **rarely** results in a finished product
- Building your own authentication and cryptography is **hard to do well**, and usually best left to frameworks

The Simple Truths

- **We** are telling companies that they can’t really do either, buy the solution, or build it. This results in miscommunications of capabilities and project timelines.

The Hard Truth

Blinky Boxes actually can have solid results

IF

infosec people actually invest the time in configuring and using them as intended

It’s “Legacy”… ugh…

The Problem

- Legacy devices, IoT, all seem to get a “**pass**” when it comes to security policy and regulations.
- Legacy devices and software are the results of the natural churn of a company and should be **planned for** and if possible, **mitigated**.

The Simple Truths

- Legacy systems and software **should not** be given security exceptions, they should be mitigated in other ways.
- Infosec professionals need to be **advocates** for this change and not lay responsibilities elsewhere.

The Hard Truth

Legacy systems or software have security solutions, we need to work with the maintainers and developers to find them and stop screaming and whining that it’s not a 100% solution.

Just [Sanitize Input, Disable NTLM Auth, WPAD, LLMNR, NetBIOS, Macros]

The Problem

- InfoSec Professionals love to say “just” do this, or “just” do that. Lack of experience in performing (and/or scaling) the fix is usually the cause.

The Simple Truths

- Disabling NetBIOS, WPAD, or LLMNR is difficult because the settings are **per-user, per-device** on Windows.
- Sanitizing input isn't always easy to do, depending on the framework used. Especially if the original developer no longer maintains the code.
- Office Macros are widely used for legitimate purposes, and are regularly tied to finance.

The Hard Truth

Swallowing our own medicine is hard. “**Just**” because you can implement a fix on your test lab or last job, doesn’t mean it scales or even works at a company level for this one.

You can’t measure security!

The Problem

- “Security is a Feeling” -- Chris Nickerson
- It’s very hard to measure feelings as they are arbitrary and change constantly.
- It’s hard to derive how many breaches were prevented (proving a negative isn’t easy)

The Simple Truths

- We need to start **performing actions** in a measurable way
- No, you can't measure a lack of "breach", but you can measure:
  - How many new rules were created
  - Asset coverage (% servers forwarding logs)
  - What coverage of the ATT&CK framework you have
  - Time to detection (with sophistication modifiers)
  - Time to eradication (with sophistication modifiers)
  - A phishing domain that was found **BEFORE** the attack
  - Weird behavior on a workstation before the attackers made it to prod
  - Malicious insiders detected before they stole something

The Hard Truth

We need to start measuring **failures** as well as successes.

Oh and hey Red Teams/Pentest Teams..
Please remember that getting caught is **SUCCESS**.

I.T. sucks at Asset Management!

The Problem

- Asset management has been **I.T.'s domain** for ages
- Usually it's focused around the procurement and de-commissioning **processes**.
- Cloud based assets can appear and then disappear from networks **in minutes**.
- Wireless networks can make **tracking of new assets** difficult.

The Simple Truths

- Tracking assets outside of **physical hardware** is not a priority for I.T.
- The security teams usually **have all the logs** needed to track down assets in multiple ways once an incident occurs

The Hard Truth

Why isn’t it InfoSec’s job to perform asset management? Why do we keep passing the blame to those who our priorities aren’t shared with?

“Other”

Things that didn't make the list but are just as in need of introspection...

1. There aren't enough infosec people (because we only want senior people)
2. We don't have enough time (because we can't hire / afford enough people)
3. No one else cares about security (yup, that's our job)
4. Infosec Sales people are charlatans (nope, they are sales, not security)
5. Infosec has so much drama (drama only works with an audience)
6. Laser focus on edge cases when the basics is what every sucks at (the basics are actually pretty hard because they are so general)
7. AI / ML is the end of the world (yup, i'm with you, F#$% fighting Terminator)
8. General apathy (ya.. not sure how to fix this one)
9. Perfection required vs Good enough (Perfectionists are just wasting time)

The End.
THANK YOU!

Rob Fuller

@mubix on Twitter

mubix@hak5.org

THANK YOU BRUCON!!!