Be Ye Batman, not Superman

KANSAS CITY NSC National Security Campus

The Department of Energy's Kansas City National Security Campus is managed and operated by Honeywell Federal Manufacturing & Technologies, LLC under contract number DE-NA0002839

Or, why planning beats superhuman effort

KANSAS CITY NSC National Security Campus

The Department of Energy's Kansas City National Security Campus is managed and operated by Honeywell Federal Manufacturing & Technologies, LLC under contract number DE-NA0002839

John Welch

Sr. Systems Administrator at Honeywell in Kansas City

KANSAS CITY NSC National Security Campus

The U.S. Department of Energy's Kansas City National Security Campus is managed and operated by Honeywell Federal Manufacturing & Technologies, LLC under contract number DE-NA0002839

John Welch

I’ve been a part of the Mac IT world since the late 1990s

KANSAS CITY NSC National Security Campus

The U.S. Department of Energy’s Kansas City National Security Campus is managed and operated by Honeywell Federal Manufacturing & Technologies, LLC under contract number DE-NA0002839

John Welch

I've been known to be opinionated on installers, automation, UX/UI, documentation, best practice...

KANSAS CITY NSC National Security Campus

This document of Energy's Kansas City National Security Campus is managed and operated by Honeywell Federal Manufacturing & Technologies, LLC under contract number DE-NA0002839

occasionally

KANSAS CITY NSC National Security Campus

The Department of Energy's Kansas City National Security Campus is managed and operated by Honeywell Federal Manufacturing & Technologies, LLC under contract number DE-NA0002839

Today we are here to talk about Batman vs. Superman

KANSAS CITY NSC National Security Campus

Or, why dull boring preparation and planning beats superhuman effort every time

KANSAS CITY NSC National Security Campus

by preventing the need for it

KANSAS CITY NSC National Security Campus

The 2017 Maersk Attack

KANSAS CITY NSC National Security Campus

In June of 2017, Maersk was almost obliterated by NotPetya

KANSAS CITY NSC National Security Campus

Desktops, Servers, phones, nothing was safe

KANSAS CITY NSC National Security Campus

Their Global AD forest too

KANSAS CITY NSC National Security Campus

It literally shut down their business

KANSAS CITY NSC National Security Campus

The only thing that saved their AD was a single server in Ghana

KANSAS CITY NSC National Security Campus

Network Recovery took two weeks

KANSAS CITY NSC National Security Campus

Endpoint recovery took another ten days

KANSAS CITY NSC National Security Campus

$300,000,000

KANSAS CITY NSC National Security Campus

They absolutely Superman’d it

KANSAS CITY NSC National Security Campus

Which was a failure condition

KANSAS CITY NSC National Security Campus

How did they fail?

KANSAS CITY NSC National Security Campus

How did they fail?

- No one could find backups for the domain controllers that went back far enough

KANSAS CITY NSC National Security Campus

How did they fail?

- They *still* had Windows 2000 servers running

KANSAS CITY NSC National Security Campus

How did they fail?

- A 2016 call to fix lack of patching, outdated OS’s, lack of network segmentation was greenlit and budgeted, but because it wasn't a KPI for Maersk senior level execs, it never happened

The fact it took until 2016 to even *plan* was a failure

KANSAS CITY NSC National Security Campus

Even their 2016 plan was a Superman

KANSAS CITY NSC National Security Campus

Things should never get Superman-level bad

KANSAS CITY NSC National Security Campus

Once you get there, it’s too late. You’re not preventing, you’re cleaning up

KANSAS CITY NSC National Security Campus

Who you really need is:

KANSAS CITY NSC National Security Campus

“We don’t implement patches until they're tested”

KANSAS CITY NSC National Security Campus

WHY??

KANSAS CITY NSC National Security Campus

The false confidence of phishing training

KANSAS CITY NSC National Security Campus

The false confidence of relying on perfect performance from humans

KANSAS CITY NSC National Security Campus

Plan to fail

KANSAS CITY NSC National Security Campus

Plan to fail

- What happens after phishing training fails?

KANSAS CITY NSC National Security Campus

Plan to fail

- What happens after phishing training fails?
- What happens after someone cryptos your main auth server?

KANSAS CITY NSC National Security Campus

Plan to fail

- What happens after phishing training fails?
- What happens after someone cryptos your main auth server?
- What happens when the perimeter fails?

KANSAS CITY NSC National Security Campus

This includes facilities too

KANSAS CITY NSC National Security Campus

What do you think happens to a generator that's just sat for years when you try to run it at load for a week?

KANSAS CITY NSC National Security Campus

This is also about people

KANSAS CITY NSC National Security Campus

What’s your documentation like?

KANSAS CITY NSC National Security Campus

How many processes are documented at all?

KANSAS CITY NSC National Security Campus

How much of your onboarding ends at “you have a computer and access”?

KANSAS CITY NSC National Security Campus

What about offboarding?

KANSAS CITY NSC National Security Campus

Do you have proper staffing?

KANSAS CITY NSC National Security Campus

How many people can be out?

KANSAS CITY NSC National Security Campus

How long are vacations?

KANSAS CITY NSC National Security Campus

Batman has Robin/Batgirl/etc.

KANSAS CITY NSC National Security Campus

Batman has

KANSAS CITY NSC National Security Campus

Batman has *resiliency*

KANSAS CITY NSC National Security Campus

Planning, prep, all of it is about resiliency

KANSAS CITY NSC National Security Campus

When things go wrong, what do you do?

KANSAS CITY NSC National Security Campus

Before things go wrong, what have you done?

KANSAS CITY NSC National Security Campus

Case in point: VMware Fails

KANSAS CITY NSC National Security Campus

vMotion doesn’t work if the host fails faster than vMotion can handle

KANSAS CITY NSC National Security Campus

What’s your DR plan like?

KANSAS CITY NSC National Security Campus

How much of your system works sans power or network access?

KANSAS CITY NSC National Security Campus

Speaking of “Grand Plans”…

KANSAS CITY NSC National Security Campus

Grand plans:

KANSAS CITY NSC National Security Campus

And just as unreal

Grand Plans are a failure

KANSAS CITY NSC National Security Campus

Grand Plans are not resilient

KANSAS CITY NSC National Security Campus

Another Failure Condition:

KANSAS CITY NSC National Security Campus

“If it ain’t broke, don’t fix it”

KANSAS CITY NSC National Security Campus

“This <magical tool> will fix it!”

KANSAS CITY NSC National Security Campus

Those are all:

KANSAS CITY NSC National Security Campus

They are all failures

Batman is small

KANSAS CITY NSC National Security Campus

Batman is tedious

Batman is *boring*

KANSAS CITY NSC National Security Campus

But, Batman has better resiliency

KANSAS CITY NSC National Security Campus

Unfortunately, the PTB love them some Superman

KANSAS CITY NSC National Security Campus

Q&A

KANSAS CITY NSC National Security Campus

Thanks!

KANSAS CITY NSC National Security Campus