On the Patch Treadmill

Ongoing Support and Maintenance of ICS Platforms

Eric Byres, P.Eng, ISA Fellow
eric.byres@aDolus.com

∧adolus

The Conflict: Stability vs. Agility

- **Industrial processes demand:**
  - Thoughtful design
  - Change control
  - Careful testing
- **Security demands**:
  - Agility and rapid response
  - The bad guys aren't waiting for you to be "ready"

Λadolus

A Small Political Problem?

Dr. Anton Chuvakin liked

Dr. Anton Chuvakin ✔ @anton_chuvakin · Jan 18
"Our IT refuses to patch because **WHAT IF THAT PATCH INTRODUCES A NEW VULNERABILITY**" #overheard
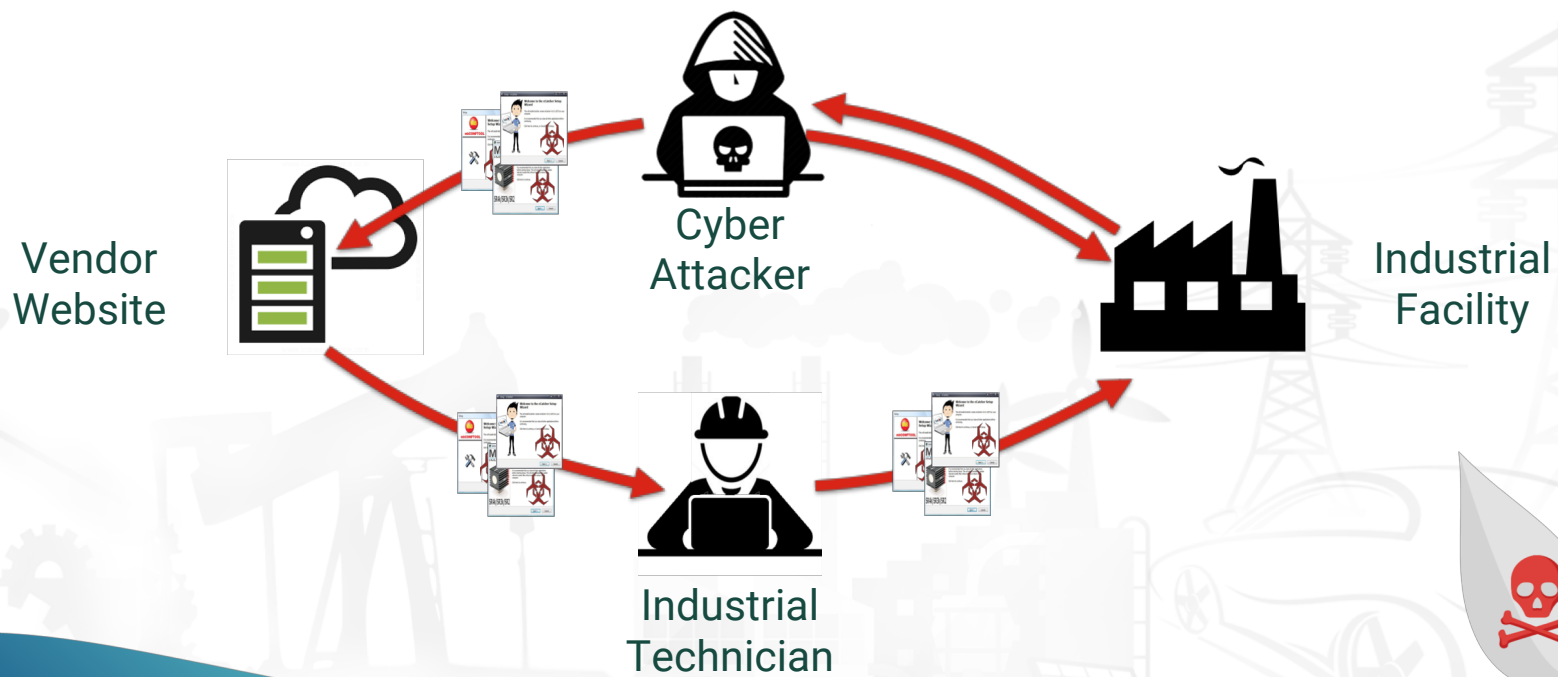
💬 22   ⟲ 34   ♡ 145   ✉

adolus

Walking into a Trap
Are those patches counterfeit?

What am I Patching?

- **What equipment actually needs patching?**
  (Asset Management)

- **Do I really know what software need?**
  (Software Inventory)

- **Do I really know where the software came from?**
  (Software Supply Chain)

adolus

An Organized Panic?

- **Which patches matter, which patches don't?**
  (Prioritization)

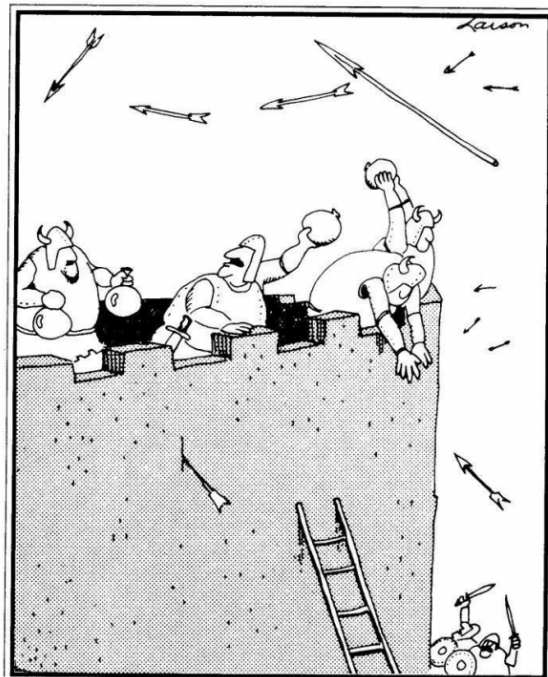- **Where do I start patching first?**
  (Patch roll-out strategies)

Mitigating Controls

What to do while you are waiting to patch?

- Waiting for the manufacturer to approve the patch
- Waiting for a maintenance window to install the patch
- The patch breaks the process
- Waiting for Godot… will there ever be a patch?

adolus

Can We Win the Battle?

"Hot Oil! We need hot oil... Forget the water balloons!"

Final thoughts…

"The picture is pretty bleak gentlemen… The world's climates are changing, the mammals are taking over, and we all have a brain the size of a walnut"