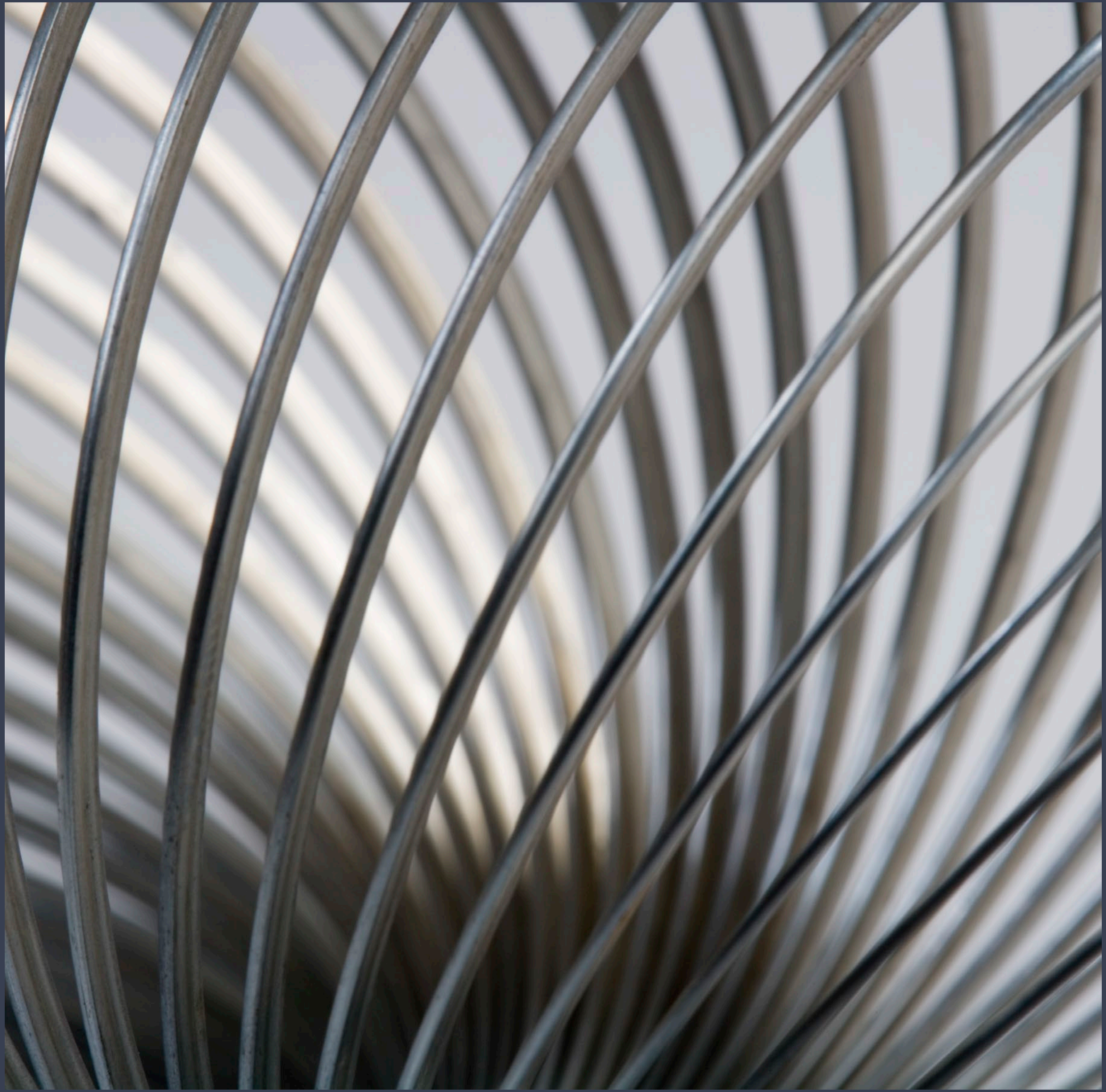
NUGM 2024

PAYING DOWN YOUR TECH DEBT

Marc Harbeson, NovoROI Systems LLC



WARNING

- This session is not meant to make you feel good
- If you are not compliant, it is our responsibility to inform you of your risks
- We are not going to beat around the bush here
- This is designed to be a candid conversation

FORMS OF TECH DEBT

- Not keeping your software up to date
  - You made a significant investment up front
  - You are also paying for upkeep benefits which include access to up-to-date technology
  - Don’t squander the benefits afforded to you
- By not keeping Manage-2000 up to date there is downstream tech debt
  - Your Windows / HPUX release is out dated
  - This causes security issues which are not under review by the platform
- You are running ancient hardware
  - Older hardware is prone to supply issues when (not if) it fails

LET'S START AT THE LITE END OF THE ISSUE

- Software maintenance is designed to deliver benefits to you:
  - Enhanced functionality as developed over the years
    - New functionality that addresses new technology evolution
  - Bug fixes
    - This can also be read as security enhancement at times
    - Erratic software is not something anyone should be comfortable supporting
  - Enhances support
    - None of us can support 20 versions of Manage-2000
    - We quite frankly don't remember everything about your ancient release
    - We are trained on the current releases, not the ones from 20 years ago
  - Older releases of the software run on versions of Windows which are out of support with Microsoft
    - If Microsoft is not comfortable – why are you?
    - What do you know that Microsoft does not?

WHAT IS THE DUMBEST THING I CAN DO?

- Discontinue your software support
  - You lose access to the ability to add users, modules
  - Reinstallation is complicated on ancient versions of software (If it can even be done)
  - Rocket Software considers you a pariah
    - Terminating your M2K agreement invalidates your Rocket agreement as well
    - UniData is embedded into M2K, so you will not be able to call Rocket
    - Let me be clear: You are nothing to them now
- The excuse: “We are upgrading to Fantastic New ERP. We don’t need it.” – BS!!
  - Until it happens – it is not happening
  - It will not happen until AFTER you are live (which may never happen)
  - FALSE – you are still going to be looking things up LONG after you go live
    - You will not convert all data – it adds cost
    - You will have tax reporting requirements

BACKUPS

- It does not matter how loud we scream this, someone in this room will find out this year.
- Every year, sometimes multiple times per year, we have clients experience a loss event that was preventable:
  - Back up minimum DAILY
  - Backing up with no verification is pointless
  - “I thought I had daily backups” – that’s nice
  - That and $1 buys you $1 worth of candy at the candy store
  - Trust (actually don’t) but verify
  - Monthly copies should be retained off site, and/or immutable by policy
  - Do not consider the hardware failure as your only risk (Hint 2 slides forward)
  - If you have a failure as a system admin and are not following these minimums – **you may be fired**
- How much should you spend on backup recovery for your critical systems?
  - How much will downtime cost you?

TECH DEBIT COSTS

- “Failure is not an option”
- If you are down, what is the loss of productivity for your company?
  - Per minute, hour, day, week, month? It is not zero! Want to find out? Unplug it!
  - What customers will you lose due to inability to deliver. Can you ever get them back?
  - Will your competitor take advantage of this situation? (Answer: Absolutely yes)
- If your insurance carrier finds out, how will they react?
  - Some of you will have answered various levels of questions when obtaining the policy. Are you telling the truth?
  - Your coverage could be invalidated. Know your policy.
  - Do what you say and say what you do.
  - Your enhanced risk equates to higher premiums.
- We have clients who have never fully recovered from this kind of event.

SECURITY SUCKS – WE AGREE

- But laziness is no excuse for leaving the door wide open
- **Security is the biggest threat you do not see**
    - Using weak access strategies to your systems (Opening ports instead of forcing VPN)
    - Having weak access policies (grant only access to required resources)
    - Not using MFA. Full stop here: Stop doing this. You're asking for it. Really.
- Let’s tell you how the event will go down:
    - Hackers gain access via a social engineering or physical security weakness
    - They install malware – then take their sweet ol’ time watching your network, evaluating what goes where
    - They steal any intellectual property of value (Contacts, Financial Records, Designs, etc.)
    - Once they take what they want, they issue a command to lock everything up and encrypt it all
        - They will take extra effort to make sure your backups are inaccessible
    - The End – You are screwed. They know how much to ~~ask~~ demand because they know your financial health.

MINOR RISKS WHICH WE NEVER HEAR OF

- Tornado took out our datacenter
- Fire took out our datacenter
- Our datacenter flooded
- The theme here: The risks redundant expensive data center co-location addresses
- The true risk to you is virtual and/or data loss through hackers and hardware failure

360 – THE FULL CIRCLE OF LIFE

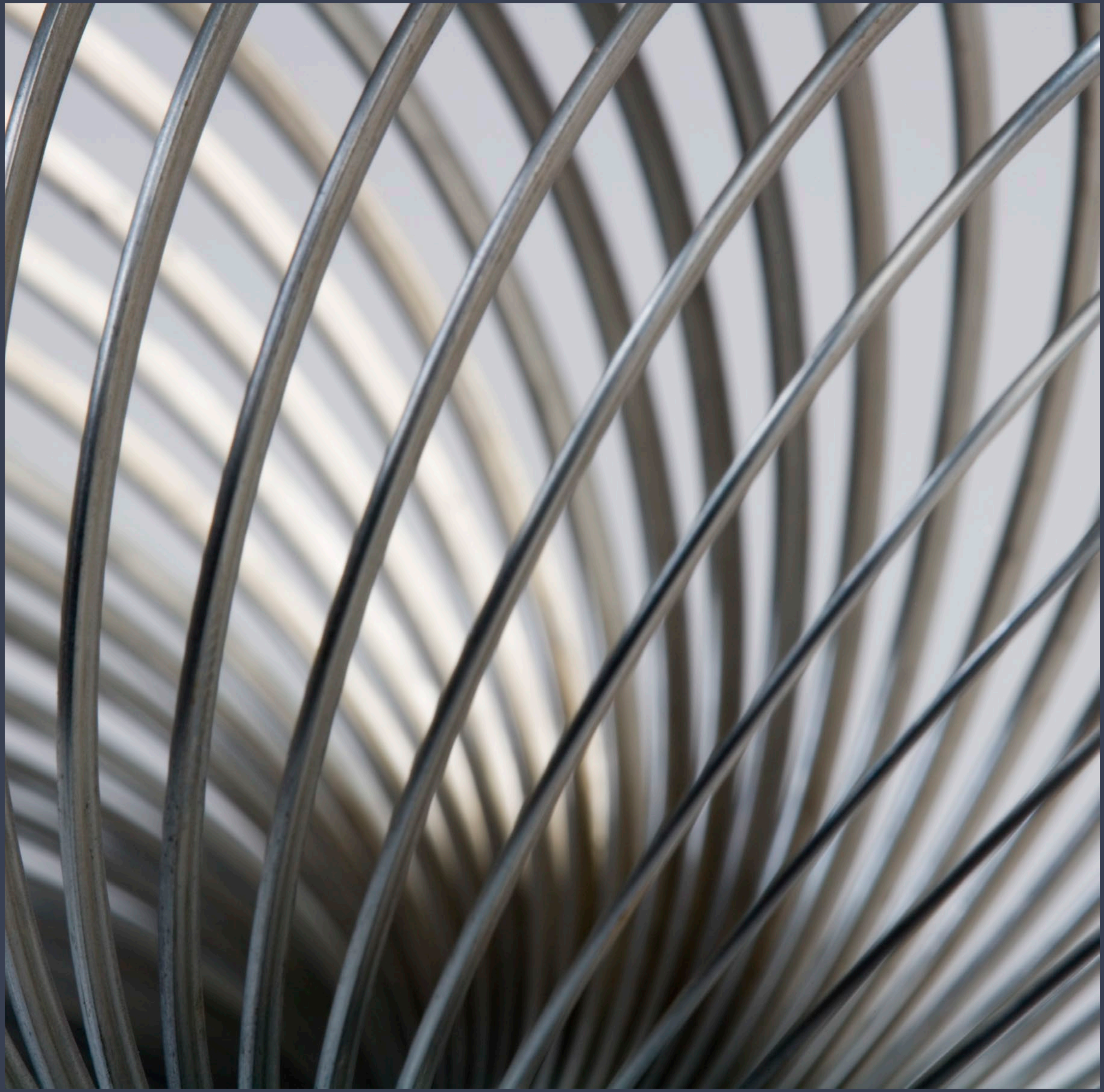
- How do I protect from this evil event?
  - Keep ALL of your software up to date within a support level covered by each supplier. If your supplier is not comfortable, why the heck are you?
    - Manage-2000
    - Windows (or HPUX / LINUX)
    - Your firewalls
    - Your desktops
    - Your infrastructure (switches, routers)
    - Your phones
    - You do not know what hole the evil doers are going to use to gain access
    - Treat them all as threats
  - Keep your backups off site. Full stop here. No exceptions.
    - Physical copies
    - Virtual copies (cloud storage)
    - BOTH!

SUMMARY

- This is preventable.
- In today's age, if accessing your systems remotely is not annoying, you are doing it wrong.
- Backups, Backups, Backups, Backups, Backups, Backups, Backups, Backups, Backups, Backups, Backups.
- Document your recovery:
  - Your restore procedure (which you should be testing monthly for verification)
  - Your re-installation kit:
    - Software media
    - Software keys
    - YOUR BACKUPS
    - Everything you need to re-create the environment
    - List of vendors you are going to need to call (AKA, your systems are unavailable – all of them)

NUGM 2024

THANK YOU



Marc Harbeson

NovoROI Systems LLC