ACT Tech Summit - Cyber Spotlights

*VETTING CYBER VENDORS

What is my biggest agency hurdle in getting started on a solid cyber plan? Where do I start? Step 1: Risk Assessment.

I come from an MSP background and have been a part of cyber / rasome cleanups. Do you have any data on price points and how much it should / can cost and what you should be gettng for that?

How much should be spent on these services? What is a range to spend per user?

Looking for standards on requirements for PEN testing and standards on what should be performed for this?

*AGENCY STAFF, TRAINING

The best defense you have is a disaster recovery plan, proactively practice recovery when it is not an emergency, train agency staff and discuss scenarios on how people get fooled.

Need help on convincing my staff/owners that cyber needs to be a top focus.

Training Training training!!!

*CYBER CLAIMS PRACTICES

Agency rep shared they had an insured with a cyber claim and it was roughly $45,000 for forensics. No breach or loss of date was found, so most of that amount was forensics.

Should businesses be concealing that they have cyber insurance in place and those policy limits? Seems like a massive honey pot just waiting to blow up - Ex: An insurer getting breached and leaking all those policyholders..

Needs validation: Comment that the FBI actually recommends to not pay a ransom because 2/3 of the outcome can go against you.

guarded about who asks for what information and for what purpose. Good cybersecurity awareness training can make this clear. As more people demand a snapshot of a company's security posture and resilience, stronger