Five Risk Treatment Strategies to Apply Now

Greetings!

Welcome to Framework and our little corner of the GRC world.

Before we dive too deep into the meat of this delicious diatribe, I want to set the stage and tell you who this is for, and who it's not. This particularly juicy morsel is aimed at the small to mid market company on a tight budget, with even tighter resources, and the ever growing need to do more with less. While these items are certainly applicable to you in the enterprise, I'm here to help the little guy.

So the title of this article is a lot fancier than its content. These are simply the five things that I've run into over the course of my career that could have easily been implemented and saved a whole lot of pain, misery, and jobs. We're not talking about single occurrence instances either, over and over and over again. These are so simple that most of you will write me off as a simpleton, I'll bet though that most of you aren't doing them regularly.

Testing your backups

Not reading a log and verifying that they completed, a no kidding restoration of your backups. Yes, I realize that these come in all shapes and sizes and that you have the newest fanciest block-level replication, yadda, yadda, yadda. I get it.

Have you tested it?

A test of your restoration process will help uncover a myriad of little nagging issues lurking about. The most notable of which is something that has yet to become commoditized (like bandwidth, storage, and processing), the time it takes to complete. This is the most expensive and most often overlooked factor in the equation.

Sure, you may have the most effective backup strategy in human history that can absolutely become useless if it's going to take three days to bring your data online. But I use the newest Cumuo-Nimbulus could provider that has all of these fancy dashboardy pretties that blink and tell me what's going on and such. AWESOME! HI FIVE! Have they tested their backups? Yes.

Ok good, make them prove it.

You should have a provision in your contract that will allow for third party audits and disclosure of the controls and processes surrounding your data. Don't have that provision in your contract? You should have had a CISA look at it beforehand. That's unfortunate, try to renegotiate immediately if at all possible. Also, look for our upcoming whitepaper on Cloud Provider: Risk Transfer or Shift or.. Shift.....Fer.....

Verify that your AV and Malware updates are completing successfully

Ok this one will take you 20 minutes, 30 if Janet in Accounting wants to tell you about her cats. Go test this, today. It's simple. Take a sample of machines and just go put your eyeballs on the signature files and make sure that they're up to date. Listen, I'm all for automated solutions that eliminate these manual processes, but they have to be verified. Just do it. Now... No seriously, go do it... I'll wait.

Ok now that you're back, and Janet told you all about FiFi and Pringles, let's jump into a few more things that will make you sleep better at night knowing that they're done.

Make a backup of your network device configurations

Most notably, your firewall (if you manage it).

Look, most modern appliances are going to implicitly deny traffic out of the box and when something goes wrong and you need to back up and punt, you're not going to be worried about keeping the bad guys out as much as you will be trying to get the good guys back to the world of connected goodness.

This is especially critical if you have 3rd party connections, VPNs, or a really crabby boss with a Facespace addiction. This will take you 30 minutes (you have to find the privileged password that you wrote down last April, first). Look, I get it. Your network devices are all backed up in the Turtle (all Clouds in my Utopia are shaped like turtles) and all I have to do is wiggle my nose and viola!! Awesome!! Finger Guns!!! Goto 1. End

Create an Incident Response Plan

This can be the most rudimentary of documents but make an effort to script out what's going to happen, who gets called, who gets woken up, etc., etc. before Janet is surfing some Russian website looking for a soul mate for Pringles and infects the whole network with a crypto-virus.

At the very least, this will be a correct contact list (include all third party providers and individuals), and a process that says who's doing what. (Send Janet home).

Give this to everyone that needs it.

Classify your data

If you have no idea what's critical and what isn't, you're playing a game of chance bringing the most critical items back online in a timely fashion in the event of an incident.

A Data Classification Policy also gives you the added benefit of uncovering the awesome little nugget of who the data owner or custodian is. It's really handy to know. I'm not saying that you inventory every document, but start with putting items in buckets and finding out who cares about what's in that bucket.

Framework
FRAMEWORK.JUVOTEC.COM
(601) 746-2900
info@framework.juvotec.com

Protect from within

Ok, this is a bonus item.

We spend SOOOO much time talking about security, keeping the bad guys out, yadda yadda yadda. The real threat is already sitting inside your perimeter.

It's Bill, he sits next to Janet.

In all seriousness, that battle is lost, your biggest threat is internal human error. Always has been, always will be. In an auditor's nirvana, everyone has a comprehensive security policy that every employee has committed to memory and keeps a hardbound copy ready at their fingertips at all times. The training is monumental and everything is reported in a timely, organized, and complete fashion.

The reality is that Bill gets cold easily,

and he's going to bring his heater that was manufactured sometime during the Carter administration (because it's warmer).

It sets his pants on fire.

It triggers the sprinkler system.

All hell breaks loose.

Bill is fine because he remembered to stop, drop, and roll, but now the second floor is soggy and Janet needs the financials that were on her machine the CEO's meeting with some potential investors.

Oh, and it's month end.

Framework
FRAMEWORK.JUVOTEC.COM
(601) 746-2900
info@framework.juvotec.com