

## **Swine Flu**

Boy the media likes being wrong. It's H1N1 not swine, pork, pig or ham flu.

They think the swine... oops... H1N1 might come back in a few months or next season with a potential vengeance, mutated, resistant and more than a billion people could be caught up in the pandemic.

If this were a computer virus/worm like the Conficker or other hostile code that we know about in advance, we'd start reverse engineering the code and tell folks to behave themselves more than ever.

But H1N1 presents another security issue. Let's hypothesize that this is all real and that masses of people are going to get sick-sicker-sickest.

How does a company plan for its corporate execs, security experts and 15-30% of its staff being out with the flu? Some companies use temporal dispersion to avoid having all execs and mission critical folks sitting in one physical location every day. But will the same rules apply with a pandemic?

It's called Graceful Degradation. Technically this means, "how can a business conduct business with certain key portions of its infrastructure broken." When it comes to H1N1, Graceful Degradation needs to apply to the human Domain of the Integrated Security Triad.

Think about how this can be handled in two ways:

1. From the company viewpoint and maintaining operational readiness.
2. From the personal standpoint, developing a means to work in different manners than normal, such as telecommuting – potentially for extended periods of time.

## **SMBs, Botnets and (Sort of) What To Do**

Recent studies show that the SMB (Small Medium Business) sector is getting nailed by botnets and hostile code with greater severity than Big Business. They don't have the budgets, IT staff or security experts on staff and so, well, they get nailed.

In fact, a friend of ours runs a fairly large construction company in British Columbia, Canada. He is the epitome of the SMB market. He called me with 'Troubles'.

His network was at a standstill. His e-mail was down... and he was freaking out. His IT guy, who is not a security person, asked for advice. The advice was comparatively simple, inexpensive and workable:

1. Keep your internal data and applications server(s).
2. Keep your existing end-point applications.
3. Use the usual mess of A/V, spyware detectors and so on at the proper places in the internal network.

4. Get rid of your own mail server. Outsource it for like – what - \$10 month? Let them be responsible. If you want your QoS to be higher, pay \$100 month. Just admin the user accounts and use a decent client at the end points.
5. Get rid of your Sharepoint server, your internal collaboration servers ad nauseum. Write down a set of specifications and features you want. Search for the SaaS Cloud Based product that meets the majority of your needs. (Nothing is perfect.) Outsource it – SaaS – and let them have the headaches.

This example is only one possible variation on the endless myriad possibilities we face. This solution is not for everyone or for every business, but the approach is sound.

It is also exceedingly sound for the very small or startup company who wants to invest its time in revenue generation instead of infrastructure building.

The Cloud world of SaaS (Software as a Service) is growing capabilities so that any company – regardless of size – can have access to the same services.

### **It's Only Sensitive... So Let DHS Get Hacked**

The latest hack into a DHS coordination and planning network was really no surprise. If it wasn't them it was going to be... what some nation-state keep messing with the FAA systems (with 3,800+ holes)... and that's really bad.

Back in 1987, Congressmen Glickman and Valentine were the point men on the CSA, Computer Security Act of 1987. (This is the committee that told me cyberwar/terrorism/etc. was a figment of everyone's imagination. Quality folks, there.) One major goal of the Act was called "C2 by '92".

In the old security parlance of the Orange Book, C2 security was good enough for "sensitive but unclassified" information. Big push. Big initiatives. Big goose egg of security tongue wagging.

So, the DHS is downplaying this sensitive but unclassified hack as, "no information can be posted on HSIN that would cause anything more than minor damage to the homeland security mission."

I am sorry. No, they should be!

Any data leak is potentially monstrous. So, this data was C2. Fine. Then another C2-level hack here and another there... and you glue together all of the data from these hacks and suddenly the amalgamated data is secret.

Data in isolation may seem worthless, but a cut, a snip and a paste later you've got yourself a database worth boatloads to the bad guys.

What is even worse, that these days DHS can't practice Security 101 and avoid getting hacked.

<http://www.fcw.com/Articles/2009/05/13/Web-DHS-HSIN-intrusion-hack.aspx>