Chad Ballay

Week 9-2

CYBR320-342

6/21/2020

**Week 9 Assignment 2 – Course Review**

*Describe what you think are three of the most important risks to a corporate environment and what types of mitigation or remediation could be put in place to prevent these risks.*

**Employee Job Mobility**

COVID-19 sped up the inevitable push to having a dynamically scaled workforce. The days of working for one company for 20+ years are gone. Now the 5 and 10 year tenure routes look to be endangered. With this comes a hefty amount of risk around all the onboarding and offboarding. We’ll have to deal with a workforce that probably hasn’t drunk the koolaid like previous years. Never mind the fact that interactions will be governed by a much shorter timeline. Don’t do the long-term relationship building since they’ll be gone in an year most of the time.

So getting new people up to speed and shutting down access correctly is going to be critical. Every company seems to do this differently and none of them do it well. To fix this we’ll need people to understand that if the process isn’t documented/automated then it isn’t sustainable. Previously the pain was only mildly bad, but it’ll get worse and this needs to be proactively dealt with. Time to first commit is a great token metric I see in developer teams. How soon from when someone finishes orientation to when they do their first commit. All the preconditions for work have to be met to commit code. Laptop, access, skillset, etc…. These types of stage gates need to be identified and monitored. Termination to account freeze should be near instantaneous. Account access auditing for dormant access.

**Acts of God & Other Resiliency Challenges**

Ohhhh the cloud. Everyone wants to talk about how great it is until some yokel with a backhoe cuts a major chunk of fiber and it triggers a cascading failure. In a dire view of things we have more money than sense being spent on the big three’s cloud offerings. We don’t have the tools developed or the standards in place to cope with bad designs. Sure the infrastructure analysis tools are getting better but what’s to stop someone from leaving port 80 open on some compute with no firewall. Sure the vendor will have mechanisms to keep it up but they aren’t going to own locking things down. Same goes with geolocation aware load balancing. Massive botnets targeting a region for an outage. In a really dire view of things, if all this climate change crisis stuff comes to pass, we’ll have a lot of turmoil impacting everything from supply chains to utilities. Resilient systems that are secure from day one are going to be an issue.

Not to buzzword drop too much from the discussion topic, but DevOps and more specifically DevSecOps needs to be a thing. Automation like inflation is a powerful thing if we do it early enough.

**Rise of the Machines**

When AI based stock trading caused a crash in 2010 it was a wake up call. Slapping a fancy term on some glorified chain of if/then/else statements is going to be a problem. More and more of the watching is being shifted from human eyes and brains to machine learning and AI. When, not if but when, those algorithms fail they will fail spectacularly. Common sense isn’t a function or library or linter that you can implement, and it shows. We’ll have crippling but short impacting events occur as weird corner cases come out. They will occur with more frequency as we put more and more work into this basket. We don’t have a solid theory and practice on appropriate baselining on expected behavior. Instead we are data rich and information poor. Important decisions will be made with incorrect assumptions and that mess will leave gaps in the system. Gaps that attackers will use to further their goals.

Industry best practices will have to emerge and to do that will require the STEM first personality types to let go of the steering wheel. Getting more technical writers is great but what about creative writers who can make engaging scenarios for tabletop games. Graphic designers are worth their weight in gold for making interfaces and branding a selling point for cohesiveness. All those soft and squishy type areas of expertise should be brought in closer even if it means killing a bit of the hacker machismo that is in place right now.