What Doesn't Kill You: Regulations | What does kill you: Rigidity - Gautam Dev

What Doesn't Kill You: Regulations | What does kill you: Rigidity

Published on September 13, 2017

Gautam Dev

The old cliché ***“What doesn’t kill you makes you stronger”*** seems to be the mantra of regulators everywhere these days.

Companies in verticals such as financial services, healthcare, and retail already reel under the pressure of meeting tough regulations designed to protect confidential customer data. When they fail and experience data breaches, there is blood in the street as Wells Fargo, Anthem, and now Equifax have learned to their peril.

Anthem’s serial challenges, with a new data leakage incident following hard on the heels of their $115M settlement to 80M victims of a 2015 data breach has likely helped elevate the issue of information risk management (IRM) to board attention at enterprises in all industries.

With Equifax we still have to know, if we will and can ever know, but rigidity is what they need to be done with and accept. (No it’s not an AA7 step sermon but then just maybe it may work with these some rigidly drunk execs playing third blind eye poker with public data. □ □).

They who think they have it Rigidly figured out need to first accept the flaw and then second the extent of insecurity for their clients because of that flaw.

Irma, Harvey have provided enough answers towards rigidity against uncertainty.

This "**third eye blind rigidity against uncertainty**" by the execs as in Equifax case is not going to get anyone to be safe.

Read Ken Pfeil's post on seven cyber risk questions that should be on every board agenda.

Read Case of The Cyber Embattled Level "C"!

However, regulators are tightening cybersecurity regulations for all companies as the bombardment of cyberattacks like ransomware and Trojans financed by state and other actors are causing more frequent data breaches. Since regulations vary with industry, national jurisdictions, and even states, enterprises often face a bewildering patchwork of requirements to meet.

Catching the "Runaway Train" of Regulations

Risk and compliance leaders should be realizing that regulatory complexity is outpacing their ability to manage. Simply adding compliance staff and performing rigid assessments doesn't scale, and playing the "waiting game" often creates fire drills when new regulations or updates are finally passed. As we have now seen and in all industries, companies need to "industrialize" risk management by creating a solid foundation with a scalable and predictive risk management framework.

This can be a hard sell. Compliance is often seen as the redheaded stepchild of enterprise: tackling a necessary, dirty job that no one else wants to do but grudgingly admits needs to be done. Line of business (LOB) leaders often view compliance requirements as a stumbling stone to innovating because so much staff time is spent meeting mandates or even worse, meeting with regulators. In financial services, there is nothing that send a chill down a risk or compliance leader's spine like receiving a Matter Requiring Attention (MRA) and knowing the scope of the effort it will take to address it.

Is that still rigidly enough?

If there is any good news about the increase in cyberattacks, it is that that senior leadership openness to investing the time, energy, and cost into creating a risk framework is probably higher than it has ever before. The C-Suite realizes that creating enterprise governance and process and embedding it into the system development life cycle is the only way they'll ever be able to create the visibility and control they need to manage risk for the digital era. Only then can the C-Suite obtain a risk score, which provides a real-time look at the organization's cyber security health.

Do you need help understanding what an actionable risk framework can do? Check out these infographics

Yours truly,

Your colleague in cyber risk assurance,

Gautam Dev.

@devZter