212° DATA BOILER
TECHNOLOGIES, LLC

Contact Us: (617) 237-6111 / info@databoiler.com
PO Box 181, Weymouth, MA 02191, USA

BIG DATA | BIG PICTURE | BIG OPPORTUNITIES

Support sustainable growth of the financial service industry

Big Data privacy and security control??

Photo by anonymous at Facebook, article by Kelvin To, Founder and President of Data Boiler Technologies, LLC

Does that look like your Big Data privacy and security control ... i.e. a big maze, but not very effective?

It is understandable to have privacy and security concerns with Big Data. However a complete lock down from extracting any Big Data intelligence would affect your competitiveness in the market. On the other hand, continuous building of data controls and governance procedures may unintentionally create big bureaucracy overtime. It affects operations efficiency while your privacy and security controls aren't necessarily any more effective than a little chain.

Think about who presents the biggest threat to your company's security controls. Are the little guys (junior staffs) able to break the chain of controls? Probably not, the moral hazard to them is high (losing their job is like losing everything to them). Most of them lack the technical sophistications to hack into systems. They probably cannot turn those trade secrets into profit as easily as some of the seniors who are friends with competitors behind door. To break a simple maker/ checker control, think about those who are able to organize a collusion to orchestrate an attack. No one will tell you the middle and senior management can be the biggest day-to-day threat to your company's privacy and security control.

"All staffs are 100% trained on company's security policy" may appear nice on the paper, but it is common for many seniors to designate their secretaries to attend the training on their behalf. Training is a minor control; you want to major in the major, not major in the minor. Therefore, take a step back and consider your organization as a chain of capabilities. Who has the knowledge across most of these capabilities? Who are in control over most of the resources? Who can easily steal using their authorities, knowledge, and controlled resources? Help these middle and senior management resist the temptations of wrong doing with three effective methods.

First - segregation of duties. This is the major control to prevent fraud and error. Maker/checker control is a low level type of segregation of duties. In Big Data, crowd computing separate systems containing sensitive data. It uses micro-tasking to farm out and distribute the work to various crowd workers (functional units) so no one particular unit would have the full big picture. Then combine the crowd computing with data obfuscation. As a result, only authorized users can access the necessary unscrambled data. This automated way in enforcing privacy and security is effective but not invasive to your operations efficiency if the distributed workflow is properly designed (as opposed to "everybody owns nobody owns").

Second - keep clean with high incentives. One may argue that ensuring privacy and security controls are everyone's responsibilities and that no incentive will ever be sufficient enough to overcome the greed. The reality is, most employees adopt the "not my problem" mentality and the threat from the crooked stealing data for a profit is real. Therefore, reward those who report vulnerability generously. You need them to point out where system nuisances can cause a security breach. Don't be cheap because certain threats are hard to detect, even for security professionals chasing down every process. Also, you need reliable information to prosecute the crooked. You want the whistleblower to consider the incentive rather than taking bribes from the crooked.

Third - precognitive fraud prevention. The movie, Minority Report, is an inspiring illustration of this method. It uses Big Data to anticipate attacks and look for symptoms of potential control breaches. How one keeps his/her self-discipline while no-one else is watching can be a good indication of their likelihood to commit wrong doings. This method does come with the false-positive and false-negative limitations. Greediness does not necessarily mean a person will commit theft. Still, prevention is better than curing and no single method can completely mitigate all risks.

In conclusion, don't create bureaucratic rules that hinder operations efficiency. To effectively mitigate privacy and security risks, it all boils down to three management fundamentals: (1) segregation of duties, (2) keep clean with high incentives, (3) precognitive fraud prevention. You may need to seek help when juggling these three methods because the key is to strike the optimal balance between the right controls and fulfilling customer needs.

This article is originally appeared on www.DataBoiler.com website