BigDataRevealed for the past year has posted our contention that it's not if you will be hacked, it's just when and what will they walk away with.

Now most major Cyber Security and Data Related websites, and even the NSA are reflecting our thoughts and even taking them to new levels.

- At the October 2, 2017 conference on Cyber Security held by The GW Center for Cyber and Homeland Security, speaker Rob Joyce, coordinator at the National Security Agency, stated "You can't assume that offense won't get through the defenses we put up. So you have to have capabilities to find and cover intrusions as fast as you can, minimize and localize the impact of those intrusions and then," he said, "recover and recover quickly

- A recent article in the Guardian has the following quote. "A "category one" cyber-attack, the most serious tier possible, will happen "sometime in the next few years", a director of the National Cybersecurity Centre has warned." A category one cyber-attack is described as being so severe that governments are forced to take action to stabilize the situation. Cyber-attacks are occurring more frequently and hitting with an unusual vengeance, we are getting closer to that Category One attack.

When will your company be the most vulnerable? As a result of the new General Data Protection Regulations being enforced by the European Union this coming **May of 2018**, BigDataRevealed feels that Hackers will shortly increase their attempts to penetrate corporate cyber security systems. These regulations require that huge fines be levied against any company that exposes the Personally Identifiable Information of European Union citizens. Hackers will have even more incentive to attempt intrusions, including personal, political and even the desire to assist your competitors. Hackers might want to make a point, pick on those companies they dislike or even influence political events in some countries. They can prove to those claiming they are protected, that they are not, putting financial pressures on the major 100 and 1000 companies around the world as well as the 3 million Companies that must comply with the EU GDPR.

Successful major hacks, designed by individuals or sponsored by hostile governments, could create a rush of EU Citizens exercising their right of Erasure (Right to be Forgotten). This will add an enormous burden on companies already fighting the PR nightmare, resignations, firings, Government Investigations, Audits and disgruntled shareholders, **and even from class action law suits from anyone wishing to profit from your non-compliance with protecting Personal Information.**

Studies have been published indicating only 2-5% of companies in the EU, UK and USA are even claiming they are close to being prepared for EU GDPR. Based on our conversations with Industry experts, organizations such as the GDPR Institute, response to our blog and other related research, companies are fearful of the future and are desperately searching for a technological solution to solve their dilemma. BigDataRevealed is aware that governments realize companies will never be safe from hacking but governments absolutely mandate that companies take responsibility for protecting consumers' personal information entrusted to them. **The US has created regulations known as Privacy Shield, China has passed Cyber Security and Canada has passed PIPEDA.**

If you are hacked, how can Personal Information still be protected? BigDataRevealed believes the only logical solution is to **Encrypt** that data wherever it resides. Certainly the first task is to discover where in your environment that data resides. It could be buried in comment fields, mixed together with non-personal information, in Word documents, PDFs or emails. It could be streaming into your company from any number of Social Media feeds or third parties. **You need a product**, like BigDataRevealed, specifically designed and tested to easily discover the existence of PII or Personally Identifiable Information in all its forms by using pattern recognition algorithms. Then you need to encrypt or remove that data and have a product that manages the complete process.

When developing your approach to meet the needs of the fast approaching World of Data Regulation do not underestimate the difficulty of discovering what is known as Indirect Identifiers. These are fields that when combined together will positively identify an individual. All regulations require these fields to be protected even when they are scattered across multiple files originating from various systems anywhere in your entire data ecosystem.

For over a year we at BigDataRevealed have anticipated the expanding threat that intrusions represent to your businesses and have rigorously and meticulously developed our product to meet the requirements identified above.

BigDataRevealed has created the means to allow customers to enter consent granting you permission to use some or all of their personal information, as well as to capture their request requiring total erasure of PII found anywhere in your data environment. The 'Right of Erasure' is not a single processing event. Daily business transactions, new purchases of third party data, and streaming social media feeds are just examples of ongoing business operations subject to the 'Right of Erasure'. BigDataRevealed uses our Consent/Erasure system to continually validates that Customers data is in accordance to their wishes / Demands and is not overridden by new processes or data.

Protocols over who's responsible for gathering consent, in what format the consent should be captured, how to verify the Consumer knew they were giving the consent and is it valid to take consent from a third party is a debate that may take some time to resolve. We believe our Consent/Erasure system gives you the most flexibility to adjust in a manner most advantageous to you as resolutions become clear.

When you have implemented a plan to discover and encrypt PII, hackers will still attempt to attack your installation but will find little of true value. You will still need to disclose a successful intrusion but you will have confidence that regulating agencies will find you had no damaging information exposed.