Running Distributed Projects in an Insecure Digital World

Extending tech development beyond a single office should not require a new layer of cybersecurity — it should be there in the first place.

February 23, 2016
By Alexei Miller

Hacks are often informed or initiated by information supplied from the inside. That such information is easily available is often caused by failure of corporate governance and compliance rather than IT. Business managers often turn a blind eye on employees, ignoring or corrupting security policies by, for example, storing confidential client data on local computers.

Normally, extending technology development beyond a single office wall should not necessitate creating a new layer of cyber defenses — they should be there in the first place. Security policies for employees should be extended to contractors. The chance of a disgruntled former employee planting an exploit or copying proprietary code before they leave is no smaller than external contractor doing the same. This is why operational measures, such as code reviews and static code analyzers, should be part of any development-team procedure.

Second, smart use of technology can significantly reduce the risk of unauthorized data access. The choices are endless, but three things are standard fare. Even for companies hesitant about running critical data systems in the cloud, PaaS are a very efficient, and very secure, place to set up development environments. Automated data obfuscation techniques ensure efficient development and testing without risking client data.

Last but not least, clever DevOps and deployment automation minimize the need for humans to access and manage real production environments. The fewer people who have access to critical databases,

the smaller the risk. And the only way to ensure it without losing productivity is smart automation.

Finally, the classic issue of "us vs. them" must be dealt with from the outset. Management will only buy in to the idea of relying on a vendor for a complex distributed project when the concept of "outsourcing" is replaced by "co-creating." By structuring the relationship so that the vendor is motivated by the system's long-term success, the company can significantly reduce its security exposure.

Long-term, build-and-operate contracts with significant clawback provisions are helpful in aligning interests, as are many other operational and legal techniques. Such methods have been used for years to reduce all kinds of risk. Now, with distributed teams becoming increasingly critical to project success, it is time to add cybersecurity risk to the list.

Original article – http://www.nearshoreamericas.com/cybersecurity-running-distributed-projects-digital/