



A NEW CHAPTER IN BUSINESS UNIT-IT STRESS

The stress between the business units and the IT department is almost legendary. The two have different agendas and perspectives on the use of technology and the priorities and time frames for getting things up and running. The business wants everything as soon as possible to use to increase business revenue. IT wants to ensure the applications are supportable, scalable, conform to company standards, and don't create cyber risks, and that takes time. Both views are valid.

With each succeeding generation of computers and applications the prices came down and the technical skill required to use the applications also came down making business units became more self-sufficient and independent.

Cloud computing took this even further as all you needed now to bring up a new application was a check book or charge card.

All these changes didn't mean IT was less concerned about the need for security and standards to protect company and customer data as required by law.

The latest chapter is no code/low code development platforms. These make application development as simple as point and click at pre-built components. The platform takes care of everything else. Experienced developers and those with no development experience can use these applications to create working mobile or web applications. This is certainly advantageous for certain types of low risk uses.

Now for the bad news. Prior to no code/low code development platforms, even if IT wasn't aware of new development, the business unit leaders usually were. Now, this simplicity means anyone can do development and even the business unit leaders may be unaware of what is going on.

Cybersecurity has reached the point of being critical to every company's survival. Applications developed without proper oversight, especially those that access NPI from customers or are used by customers or third parties means they are not being validated for cyber security standards compliance.

Cyber regulations are applicable to almost every company, not just those in the regulated industries. Whether these applications will be deemed violations remains to be seen. But with all the unknowns and the accessing of potentially Non-Public Information, it certainly appears to be non-conformant or at least suspect.

While these capabilities are highly desired by many business units, their use should be restricted to simple functions such as form development, that do put the entire company at risk of cybercrime.

Want to learn more about cyber security and education, contact one brightly cyber at info@onebrightlycyber.com or call (888) 773-1920.