Digital Transformation: Beware the Legal Details

https://mbdev.aplussdv.com/2019/08/12/digital-transformation-beware-the-legal-details/

Erika Morphy

Digital transformation can be a prime opportunity for a company's growth and development, however, it can also be a prime opportunity for cybercriminals, according to Dan Hanson, SVP of management liability & client experience with Marsh & McLennan Agency. Cybercriminals have found that targeting companies when they are in a state of flux, such as a digital transformation project, can be very fruitful.

"As you are putting more and more things online internally to inform employees about what is happening, they are more apt to click on emails that appear to be from the company, and open links precisely because they've been getting so many emails and they need to stay on top of projects," Hanson said. Simply put, employees are more likely to fall to a bad actor during a digital transformation.

That will hold little sway with regulators that monitor privacy and cyber breaches. "A company not only can incur large costs to compensate damaged parties, but also some large — up to seven figures or more — government fines, particularly if HIPAA rules have been impacted," he says.

One of Many Legal Pitfalls

Data breaches, unfortunately, are just one of many possible legal pitfalls that can trip up a company during a digital transformation. Not treating digital assets according to the appropriate intellectual property (IP) laws is another potential pitfall and as with cybercrime, it is easier to get this wrong during a time of transformation.

> "Digital transformation is a broad term that covers a wide range of business activity," said Eric Ostroff, trade secrets and IP attorney and

partner at Meland Russin & Budwick. “But whenever a company is making a substantial change in the way it does business, including through a digital transformation, it is very important to make sure that IP protections do not go by the wayside.” Businesses going through a digital transformation can easily be distracted by business-side issues, he said. For that reason, Ostroff suggests the company gets its IP attorneys involved to ensure that the strategic changes are paired with appropriate IP protections.

Still, it must be noted that the general standard industry practice is that customers maintain ownership of their own data and the vendors maintain ownership of their technology, said Jeff Lazarto, practice leader at UpperEdge. The customer receives a license right to use the vendor’s technology to operate their own business as part of the subscription fee paid for the service, while vendors receive a right to use the customer data and the scope of these rights can vary. “Typically vendor rights to customer data are limited for the purpose of providing the services in the contract, but also include the right to use aggregated customer data to measure and report on service performance, usage volume, and to gain insights into customer trends, etc. The line is typically drawn at aggregated data and does not allow the vendor to extract and exploit identifiable customer-specific data.” But, Lazarto added, the devil is in the details of the contract, which is why it is so important to state and understand the IP rights in the contract.

Losing Rights to Your Data

In fact it is possible — albeit unlikely — that a company’s branding and IP rights may be compromised as part of any systematic changes, said Dana Simberkoff, chief risk, privacy and information security officer at AvePoint. “This might come in the form of a lift and shift-type data migration, vs. one that carefully and fully integrates compliance.” Indeed, data that was previously protected may inadvertently end up in the public domain, Simberkoff continued. “Security is often compromised when massive systems and data overhauls are implemented,” she said.

The contract therefore, for all the obvious reasons, must be examined carefully, said Dan Cleveland, an IP attorney at Fennemore Craig. “If you use an outside contractor to solve the problem they will own any inventions and copyrights in code unless a

contract says something different," he said.

Perhaps more alarmingly, he added that this can also be the case if you use an employee who was not hired to do the transformation as part of his or her job description. "We increasingly see negotiations over data rights and access to data where, for example, a community of users who are different legal entities might benefit from a software service providing data analysis of their combined data pool. In other instances, a web hosting service may wish to mine your data for marketing purposes that provide no direct benefit to you, or such a service may have concerns over liability issues if the data is misappropriated." Such activities can become very complicated and contentious if medical data is involved, due to HIPPA, Cleveland added.

Compliance and Digital Storage

Another area of concern with digital assets is storage and related compliance issues such as privacy, said Chris Goodnow, a partner at Goodnow McKay. "Every company has compliance issues whenever digital storage is involved," Goodnow, who was also the CTO at a former firm, said. For example, state bar laws differ on what types of storage methods are allowed, even if these methods are compliant with federal law. Using third-party cloud storage companies can be problematic because they often integrate with other tools that keep them very functional — however, these companies may not have high-end security, he said. "A company may choose function over privacy and that can lead to troubles.

And when troubles do arise it is the company that pays the price, Lazarto said. "The general standard industry practice has been that the customer assumes this risk. The vendor's general position has been that if they had to assume this risk, the cost of their services would be much higher."

That said, vendors are greatly incentivized to keep data safe, he continued. "If a vendor were to have a customer data breach, depending on the severity and extent of the breach, it could irreparably tarnish their reputation and trust in the market and potentially ruin their business." Unfortunately, however, that will not help you much when it comes time to face a regulator.