Data security: Your greatest risk management challenge [Part 3 of 3]

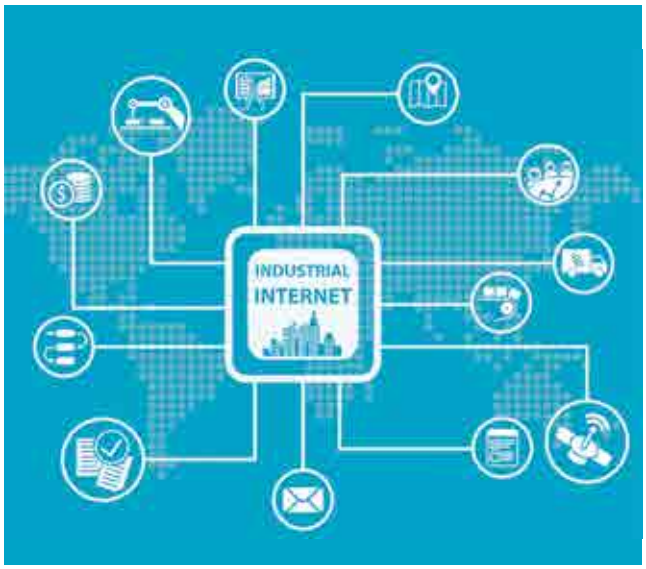
Increased liability is the last thing your company needs, but that's exactly what the data explosion is delivering to your doorstep. Most experts are convinced that the manufacturing sector is facing an imminent uptick in risk management concerns due to an exponential growth of data. The pump industry is no exception.
A single online search for the term Big Data (also known as the Internet of Things or Internet 4.0) pulls up 300,000,000 Internet references in just two-thirds of a second. The sheer volume of accessible information illustrates the double-edged sword of data: its scope is overwhelming, both in terms of business potential and business risk.

By Jeff Eiben, Principal Owner, River Point Technology

To harness the potential, you must manage the risk

Data risk is battering businesses on every side. By 2020, more than fifty billion Internet-connected devices will be feeding data into cyberspace; that number translates into a 4300 percent increase in annual data production.

While it's easy to conjure up images of iPhones, iPads and laptops, the devices that are creating data are at work in every aspect of consumer and business operations: health records, audio, video, images, transaction and web logs, thermostats, security systems, automobile telematics, machinery, medical devices – the list goes on. The term Internet 4.0 was coined to convey the prediction that virtually everything would one day be connected to the Internet. This result is a mind-boggling flow of data that is forcing companies to strike a balance between business risk and business potential.



The range of data breaches continues to broaden: employee misconduct, loose internal security protocol, malware and the growing criminal enterprise of hacking. Add to that the fact that cyberattacks continue to become more sophisticated. Hackers already know how to maximize the potential of big data; in fact, they are very adept at targeting breaches at will, by industry, geographic location, company size or any other factor. The bad guys leave little to chance, and therein lies a recipe for disaster.

Data risk is already a reality for your business

Now that the data risks have ratcheted up more than a notch, companies are beginning to realize that the old way of doing things no longer suffices. A 2016 Ponemon Study reveals the alarming fact that 89 percent of

healthcare organizations experienced data breaches within the past two years, at a cost of USD $6.2 billion. In no way is the healthcare sector suffering alone. In 2016, up to 75 percent of all large businesses had to deal with the same type of data security breaches.

Surprisingly, the incidence of data breaches has shown no decline since 2010, despite increased awareness and the IT industry's thundering call to action. The majority of companies continue to subject themselves to an overwhelming amount of risk, including the loss of confidential information, negative press, lawsuits, financial loss and shareholder discontent. Unfortunately, for some businesses, a data breach is equivalent to a death warrant.

A sound IT architecture is the first layer of protection against data breaches

To mitigate risk, IT Infrastructures must be scalable rather than one step from obsolete. From a functional perspective, an IT infrastructure should be able to: integrate massive amounts of data; breakdown internal silos; deliver accurate analytics to the right recipients in a timely fashion; and have the inherent ability to identify and isolate potential data security breaches.

It is possible for a company to balance the risk and potential of big data, but it takes a concerted effort. Given today's business environment, executives and internal IT professionals are concerned about the threat of data breaches, yet only 10 percent say that they have confidence in the security of their connected devices. The reason? Many companies don't have the internal IT resources to keep up with ever-changing trends without interrupting responsibilities crucial to daily operations.

More and more companies are turning to external IT architects to help mitigate the threat of data breaches.

Steps to begin reducing risk

The following steps are in no way sufficient to ward off data security breaches, but they are components of a risk mitigation plan that you can implement today:

- **Develop and document internal security protocol:** Be sure to detail acceptable Internet and email activity, including the use of Wi-Fi for non-business activity, opening email attachments and clicking on links within the body of an email.
- **Encrypt your data:** Hackers are keen on information such as bank routing digits, credit card accounts and employee social security numbers. That data, whether actively transmitted or sitting at risk, should be encrypted.
- **Secure your hardware**: Good old-fashioned breaking and entering still works for thieves who want your hardware. Even if they don't access your files, you have still lost control and run the risk of jeopardizing confidential information.
- **Lock your network**: It's hard for some of us to imagine Wi-Fi hacking, but it happens all the time. Some call it "wardriving." Hackers stay on the move, driving around with high-power antennas that identify unlocked or poorly secured networks. In actuality, the result is no different than if you had invited them in to take their pick of your information.
- **Install anti-malware and anti-virus protection:** Malicious software or viruses can be introduced in a variety of manners, including spam emails and unsafe websites. Once malware has taken up residence, it can collect user names, passwords and other sensitive information. Hackers don't have to take a break when you do; they can log in as you and harvest information at will.
- **Educate your employees:** This is a big one. Once you have a compromised device, your entire operation can be at risk. Provide guidelines, educate your employees and allow for regular reinforcement of data security policies.
- **Invest in data security:** Spending dollars on a data security partner might seem prohibitive, but limiting exposure to data breaches is not only worthwhile, but indispensable. Failure to plan will likely lead to a much greater drain on resources at a most inconvenient time.

These industry experts have the capacity and bandwidth to deliver an infrastructure that is affordable, responsive, scalable and secure.

The time has passed to make data risk mitigation a discussion "for another day"

According to a recent Ernst & Young study[1], 72 percent of respondents understand the importance of big data technologies as a barrier against fraud, yet only 2 percent have implemented any such technology. Times have changed, though, and data risk mitigation can no longer be delayed.

Companies that take the data breach epidemic seriously will hurry to implement technology that has the capacity to collect, store, analyze and secure both historic and real-time data. These companies are preparing to absorb the imminent explosion of data, therefore positioning themselves for a competitive edge. On the other hand, companies that continue to hold to a "let's wait and see" attitude will eventually find themselves in the "we wish we would have" heap.

References:

1 EY's Global Forensic Data Analytics Survey 2014.

To read Part 1 and Part 2 of Jeff Eiben's article series, check out the February and April issues of *Pump Engineer* magazine.

About the Author

Jeff Eiben is principal owner of River Point Technology, a Pittsburgh, PA-based company. River Point prides itself on "taking the complexity out of data" by helping companies visualize the benefits of data-driven solutions. Eiben can be reached directly at jeiben@riverpointtechnology.com. More information is available at www.riverpointtechnology.com.