High-Tech Content Writing Samples
Marissa Tejada, Freelance Writer and Journalist

Business and Technology Content Clips

The Challenge of Secure Web Application Development | Veracode Blog

Tablet Security: Keeping it Safe | Kaspersky.com

Protecting Your Data Online | Kaspersky.com

High-Tech PR Press Releases for IBM

Wildlife Sanctuary Receives Cisco and IBM Technology Donation to Improve Animal Care

The New Information Infrastructure

National Football League Gets Ready for Game Day With IBM

IBM Expands High Performance Computing Capabilities for Clusters

ADDITIONAL SAMPLES

*The following content is no longer published online.

Client: **IBM** - **The Midsize Insider**
The IBM MI blog engaged midsize business owners by providing a platform that related their technology issues of the day with tech industry news content and trends.

Healthcare IT Analytics

Published: IBM MI Blog/March 2015

Healthcare IT analytics are an important part of giving the best accountable care, according to a new research report. When analytics systems are simply not performing at their best, there's a drop in healthcare workplace standards.

Workable Analytics

A new report by the RAND Corporation and the American Medical Association (AMA) featured in Health IT Analytics discovered that a solid healthcare analytics infrastructure helps to achieve a better financial structure for health institutions. The study took into account how dozens of physician practices utilized analytics for a year-long transition from traditional fee-for-service models to accountable care

reimbursement structures. Those who had to deal with insufficient, inaccurate, or untimely healthcare analytics systems were more frustrated with system changes. The study concludes that it is key to make sure ease-of-use, accuracy and effectiveness are very important for health IT information infrastructures.

Increased Reliance

RAND and AMA's recent collaborative study is another proof point to an increased reliance firms have with data analytics. Due to the rise of mobile and other third platform technologies, the healthcare industry is becoming more complex and IT managers need to deal with it. Analytics is increasingly becoming an important part of breaking down a firm's performance measures. Additionally, in the healthcare sector it enables companies to better manage population health management and with interoperability between various health electronic records systems. Two big challenges IT leaders face.

The backbone to a sound analytics infrastructure can be expensive and time-consuming if it isn't approached properly. Health analytics partners can help midsize healthcare companies to craft an infrastructure that has the framework and flexibility they want in order to provide their specific level of healthcare. Meanwhile, if analytics and data capabilities are more developed, vendors can assist to ensure the right tools are being utilized to manage various payment programs, monitoring of performance measures and patient care. Flexibility is key for growing firms.

Innovative eHealth solutions aim to eliminate fragmentation so health firms can comply with regulatory and privacy policies. Other solutions create a smarter view of patients and consumers. Analytics combines relevant data from traditional, transactional and external sources. Finally, advanced analytics and predictive modeling can help encourage new and informed business decisions that can lead to new healthcare healthcare products and services.

The Right Data

New research shows health organizations that follow accountable care and seek alternative value-based payment models are more effective if health workers and healthcare analytics are in synch. Without appropriate and effective analytics backing up a healthcare system, productivity can drop and errors in patient safety can happen more frequently. With the help of healthcare IT analytics experts, midsize firms can truly leverage the most innovative patient care strategies to achieve a healthier bottom line and increase patient care quality. In today's age of more complex healthcare systems and new regulations, analytics is playing a key role in keeping data organized and meaningful for increased productivity.

Mobile Virtualization Technology and MSPs

Published: IBM MI Blog / December 2015

Mobile virtualization technology is becoming more in demand as the bring-your-own device (BYOD) market continues to grow at an impressive rate. MSPs prepared for the BYOD trend shift that demands

virtualization can be prepared to assist growing firms that must keep their IT in tune with their business growth.

Mobile Strategy

According to research by TechNavio, featured in Information Management, BYOD is expected to reach a compound annual growth rate of 25 percent until 2019. The research firm concluded that as a result of that growth, organizations will want to add a mobile virtualization component to their policies which would allow for easier use, synchronization, organization of devices and 24-7 access. These days, separating company and personal devices isn't realistic anymore. Now, two operating systems, one for the corporate server and one for personal data, can run smoothly on a smart phone thanks to mobile virtualization technology. The challenge is making the transition and that's where vendors come in.

The report also pointed out that the various platforms including tablets, smart phones and phabets have led to increased functionality but also an increased need for security.

Shift Up in BYOD

With a shift upwards in BYOD implementation comes the natural need for mobile virtualization. In order to keep up with the competition, firms need to synchronize their mobiles which leads to a smoother transfer of data to help boost overall productivity. Since midsize firms have little time or resources to manage upgrades, MSPs have ample opportunity to assist them in the virtualization deployments that require, at the minimum, multiple operating systems on a device.

MSPs that are knowledgeable in the integration of virtual machines and embedded hypervisors to keep data safe will also be valuable for potential partners. It is key, in these virtualized environments, to isolate data and protect it from any malicious threats. Mobile virtualization is often chosen over containers which aren't as effective. Containers require separate sensitive apps in but can end up sharing the same space with unprotected apps. Midsize firms want to avoid this type of complexity. MSPs with experience can accelerate and simplify the transition to a mobile virtualized environment starting out with the proper integration of hardware, software and services. Defining security and streamlining backup and data recovery is the next step.

Market Opportunities

The latest study shows that virtualization is even more necessary for firms to implement due to the rise of the BYOD movement. The BYOD market surge is an opportunity for MSPs specializing in solving the latest challenges with the latest mobile virtualization strategies. They are in the position to reach out to midsize firms that need to get their BYOD under control in an increasingly mobile business world.

Client: **Veracode**
This application security company is based in Burlington, Massachusetts. Founded in 2006, the company provides an automated cloud-based service for securing web, mobile and third-party enterprise applications.

www.veracode.com

Best Practices to Minimize Risks Across Multiple Devices Your Employees Carry

Published: Veracode Website/Blog/September 2014

In today's mobile world, solutions that can effectively protect data from growing security threats like mobile device management (MDM) are becoming necessary. Your staff is on the go, and you want them to be. The fact they can work from anywhere and at any time increases productivity and the mobiles that they carry all day long are just as important as the apps they log into. The issue is keeping those devices that house those very productive applications secure.

Mobile World

Bring your own device (BYOD) initiatives are here to stay and are proving to be a win-win for both employee and employer. Some firms stick to issuing their own corporate devices. Whatever fits the needs of your company the fact remains mobile is necessary for productivity and it must be secure .The challenge falls on the shoulders of IT professionals who need to make sure each device in their fleet is complying with data security and privacy regulations. The consequences? Data breaches are one. So are large fines and litigation. Let's not forget damage to a company's reputation.

Steps to Take

If you plan to keep data safe, mobile and application security is no longer an afterthought. With a security-focused strategy firms can reap all the benefits of the web and mobile as well as its useful applications while minimizing risks. Here are a few steps to consider:

1. Policies that Educate. Educate staff about your BYOD or mobile security policy which should outline the rules and protocols for everyone in the company when it comes to using mobile and using apps in the workplace. This increases awareness. Employees should be aware what effort is going into securing the code and design of their apps and how they can prevent breaches and mishaps. With a little effort to organize informative sessions, employees can also be accountable for security to a certain extent.

2. Launch MDM. Choose a MDM solution that is flexible and scalable enough to meet your firm's demands. It should not only protect data but be suitable for up and coming technologies. It can also offer a single solution for viewing and managing mobiles. Check out solutions that also protect data with remote password locks and data wipes.

3. Patch those Apps. Don't assume there's a safe place on your sever for your Web applications. Stay on top of patches and understand that there is always some vulnerability that will need to be addressed. When it comes to the mobile world, we all know that developers them fast to stay competitive. That's one reason why some may not have the right levels of security. Seek out solutions that ensure the data in-transit is secure including SSL or VPL tunnel.

4. **Pick a Good Security Partner**. The code on all types of mobile and web applications need to be checked upon regularly. Without in-house experts to establish a good security plan, vendors can step in to fill the knowledge gaps. Reliable vendors can also counsel you on MDM and perhaps cloud based application security solutions you may be overlooking.

Security Steps to Success

If your web app developers are outsourced, security should be part of the deal. Work together to figure out the security maintenance and check-up schedule. Security is one part of an organization that simply can't be skimped on. Choosing proven solutions and working with good security vendors also helps take the complexity out of managing the growing number of endpoints in your network.

Protecting corporate data effectively takes time, personnel and resources. It's the backbone of good service and customer satisfaction. Mobile device management helps to secure BYOD devices and the mobile and web applications that help your firm work at its best. Investing in the right measures means you can avoid unexpected costs that relate directly to today's growing IT security disasters.

Client: **Electric Cloud**
A DevOps optimization software company based in San Jose. The company provides DevOps Release Automation solutions that simplify and accelerate the delivery of software updates to end-users.

www.electric-cloud.com

The ROI of Continuous Delivery

Published: Electric Cloud blog/March 2014

Continuous Delivery (CD) delivers software a faster and in a more stable production environment. In the past, software release processes were once error prone and time consuming. When teams utilize CD, features are carefully designed, implemented, tested and automatically deployed to production.

CD is automated, reliable and fast. It reduces operational costs, improves quality and shortens the time to market. It also has a key advantage of increased ROI helping to increase the overall productivity of the team behind the software including engineers, QA managers, release managers and IT administrators. When they employ CD practices, they notice a change in their roles. Since developers are releasing at a quicker pace, development starts overrunning the other roles. As a result, there are adjustments to be made but in the end the CD takes the risk out of IT.

Developers and QA Managers

CD improvements are delivered on a feature by feature basis which means the entire team is working together and focused on getting the feature right the very first time. CD empowers developers to decide what is ready for release, when a feature is ready and when scripts can be run. This means everything moves at a faster pace. The developer is responsible for the release and therefore has the incentive to fix solutions. The last thing they want is to release buggy code. In the end, developers understand the importance of their role to write and run automated tests.

Through CD, QA managers shouldn't receive bugged up code from developers. That means they can have more time to focus on quality. QA managers are more poised to build good scripts for testing and deployment. The roles of QA managers then become more valuable to developers who appreciate their expertise.

IT Administrators

CD also requires an IT administrator who can write scripts to automate testing, deployment, and measurement. IT administrators aren't responsible for builds and releases but can offer developers the automated tools they need. Through these IT administrator tools which are packaged as Software as Service (SaaS), the process can move forward quickly and with accuracy.

Product Managers and Senior Managers

Features are important and what they look like remains in the hands of product managers and product owners. They are experts in usability and their goals are often driven by metrics. Through CD, product managers and owners can work in harmony with developers to ensure every feature is of value.

Senior Managers are also interested in delivering value. They can pinpoint bottlenecks that stop that value from being delivered. With CD in place they can ask for measurements during the development process and be responsible for a few high priority requests. The opportunities for development are great once the process begins. Managers can move ahead quicker with their launch and marketing responsibilities.

The ROI

CD builds a competitive advantage that comes about as a result of faster and more accurate collaboration between the team members behind the product. CD's automated delivery pipeline creates an efficient delivery cycle. Overall, small portions are tested and isolated. Risk can be managed. CD ensures that when features are fully deployed the system is in a stable status.

By following CD, software can go to production in days rather than months. The entire team from developers to managers is empowered to work together. They understand that their collaboration can achieve rapid, reliable releases. The combination of a motivated team and a scalable methodology such as CD results in the best ROI possible – one that delivers the best and most innovative software to market.

Continuous Delivery and the Internet of Things

Published: Electric Cloud blog/December 2015

Smarter devices and appliances are creating a world known as the Internet of Things (IoT). Objects, animals and people are becoming increasingly connected to the internet, with the ability to transfer data over the networks. The growth of the IoT creates a whole new set of opportunities and threats.

Smart phones, home thermostats, security cameras, refrigerators, microwaves, home entertainment devices, car dashboards and more are being released with new features, offering a new level of convenience and improving the quality of daily living. At the same time, the need for better security is

becoming apparent. Cyber criminals see IoT devices as easy opportunities to steal personal data and breach systems to cause havoc.

IoT Security

The threat of cybercrime is a top concern for consumers and producers alike. Hackers who can target a device's firmware that's out of date or not patched. Meanwhile, the firms behind the latest devices can face liability, PR and financial losses should their products fall victim to a malicious hack. According to Security as a Service provider, Proofpoint, a global hacking campaign that took place between December 2013 and January 2014 hijacked 100,000 consumer gadgets. More than 750,000 malware filled emails were sent from the devices including home-networking routers, connected multi-media centers, televisions and even a refrigerator. Turns out poorly protected devices can be easier to infect than traditional cybercrime targets such as PCs, laptops, and tablets.

Security can begin at development. Software that is built within the processes of continuous delivery (CD) will prove to have the most promise. That's because developers that employ the discipline of CD put their build through automated testing. The design practice results in a product developed to the highest standards. Developer teams can fix bugs, push out enhancements and develop features. Continuous delivery maximizes reliability and efficiency all through automation.

CD Enables

Continuous delivery creates a more secure product due to frequent software deployments. As features are bundled together, naturally there will be more opportunities to experience configuration problems. With CD, developers can roll out many deployments in very small increments. Errors are reduced and if they do pop up, they are easier to deal with. Furthermore, CD is a process that enables developers to identify problems sooner, an approach that finds bugs immediately. It's an environment in which improvements can be implemented quickly. In the end, the live product's quality is raised to a new level.

In the entire scheme of the IoT, CD offers a precise and calculated way to keep web applications updated. Products can improve even after they are bought to market. Updates can automatically upload new code to fix any bugs or even add new features to the product. It is possible for firms to use CD to change product specifications based on consumer complaints or even their suggestions.

Amazing Opportunities

The number of IoT devices is growing at an amazing rate. Cybercrooks also see an amazing opportunity to hack them. As time goes on, firms will pay more attention to securing IoT devices as the existing security models may continue to be too weak to defend against the latest threats. By employing CD practices, software developers can add a strategic level of security, as the IoT device is created. A safer experience for the consumer is possible if software is built to the highest quality. That safety reaches another level if the software is available to update and refine as threats change. Furthermore, implementing CD processes offer peace of mind for the innovating firms that aim to release the smartest and safest IoT products possible.

##