Promoting Information Technology Growth

September 2015 Edition

Cyber Insurance: Why You Should Require Certain Vendors to Have It

10 Reasons Why Your Organization Needs Data Loss Prevention
Big Data, Business Intelligence

By: Ann Gallaher, COO, Technology First

Big data is the future. According to experts, business intelligence allows decisions to be made faster and smarter. Once the art or science is mastered with the aid of technology tools, volumes of data can be consolidated from multiple sources and be easily searchable. Large and complex data sets storing treasure troves of business-transforming information—if only it is mined through business intelligence.

Abbreviated Wikipedia says that a special interest group (SIG) is a community within a larger organization with a shared interest in advancing a specific area of knowledge to produce solutions within their particular field.

Technology is rapidly changing and peer information sharing is more critical than ever. The ability to share information among peers can be timely and sometimes essential.

Through the appeal of the CIO Council, Technology First initiated and has hosted a Business Intelligence special interest group since the fall of 2012. Past sessions have included preparing your company to begin business intelligence, presenting metrics through dashboards, visualization, and reports as well as a demonstration of vendor-specific tools.

Under the volunteer leadership of Jim Bradley the group has recently reconvened and re-engaged. Future topics include selling the value of BI to the business, master data management, and how to choose a BI tool.

The business intelligence special interest group creates an environment where technologists can discuss issues important to their specialty and the industry. Professionals interested in learning more and possibly participating should stay tuned to Technology First’s website. Hope to see you there!
Reinforce Physical Access Control With Next-Gen Architecture

By: Mac Thompson

Physical access control systems (PACS) have unquestioningly aided with managing the security of assets such as people, materials, and critical processes of commercial organizations in the past few decades. While the most important aspect of access control, granting or denying access, has not changed, the underlying technology of these systems definitely has. Manufacturers today utilize a wide array of new technologies and processes, such as cloud-based database servers in lieu of physical ones, support for the strongest card/cardholder authentication, and the ability to take full advantage of the organization’s IT infrastructure. Despite this, much of the PACS architecture of the past—imposing specific/custom hardware and some technology limitations—still persists. Next generation architecture is needed to reinforce the security so it aligns with IT capabilities.

Before organizations had widespread networks in place, their security systems were completely self-contained, with their functional processing abilities distributed throughout control panel hardware throughout the facility, thanks to limited processing power and speed. While computer power has increased to a level that is thousands of times faster than it was 10-20 years ago, a disconnect still exists between the capabilities that today’s PACS can provide and what current Information technology can accomplish. For instance, traditional PACS architecture are piecemeal solutions that consist of costly third party devices and/or middleware rather than providing native support for software-oriented networked systems, strong mobile device authentication/interaction, standards-based role and attribute management, and IT management of endpoint device security.

The trend of “Bring your own device” (BYOD) in the workplace could be a useful resource to consider implementing—after all, if a smartphone can be used as a boarding pass at an airport, surely it could double as an electronic access card. There have been pilot programs established at corporations and universities with large campuses that enable users to securely store access credentials within the NFC (near field communication) chips in their smartphones in order to gain access to certain buildings, departments, and entryways, just like a standard contactless smart card. However, one of its drawbacks is that NFC is generally featured on the latest models of smartphones, requiring users with older technology to use NFC-enabled cases or purchase the latest flagship smartphone outright.

A potential solution takes advantage of a feature that is universal to all smartphones manufactured in the past 5 to 7 years: the camera. The smartphone is able to essentially become the reader rather than the credential; by scanning QR codes placed at each entryway—ideally those without heavy traffic—the smartphone is able to identify which door the user is attempting to enter and verify and authenticate access thanks to integration with network-based real-time presence technology, ultimately reducing much of the door hardware costs normally associated with traditional physical access control interfaces. Furthermore, for ultra-secure spaces, phone-based biometrics (such as a fingerprint reader) or a numeric PIN can provide additional two-factor authentication. Migrating to next generation PACS architecture achieves a much lower total cost of ownership than what the hardware-centric current architecture provides due to no limits in its interface capabilities or scope of near-time operations. A shift to this software-based approach that leverages existing network hardware technology will provide native support for integration with systems dealing with identity management, cloud computing, secure authentication, and other emerging access technologies that may develop.

Apply Now for Fall 2015

Earn Your Master’s in 12 Months

Raj Soin College of Business
Wright State University

Master of Information Systems
Master of Logistics & Supply Chain Management

12 months, 9 courses
Hybrid Program with Residence + Online Learning Certificate Project in a Real-World Setting
(937) 775-2895
valerie.iostand@wright.edu
business.wright.edu/ISSCM

Technology First | September 2015
Cyber Insurance: Why You Should Require Certain Vendors to Have It

By: William C. Wagner, Taft Law

One way to protect your business from financial loss, reputational damage, and the expense of regulatory scrutiny in the event of a data breach is to require your vendors, with access to your customer and employee personally identifiable information, to carry cyber insurance.

Many businesses routinely require their vendors to promise to indemnify them from any loss or expense arising out of the vendor’s goods or services. They also routinely require their vendors to maintain certain types and amounts of insurance coverage, have their business named as an additional insured under the vendor’s insurance policies, and provide proof of the insurance coverage as conditions to their contracts.

But the types of losses, damages, and expenses that arise from a data breach are often not covered by the standard insurance policies listed in most vendor contracts. An instructive case to businesses on this issue is Recall Total Information Management, Inc. v. Federal Insurance Co., which was recently affirmed by the Connecticut Supreme Court.

In that case, IBM entered into a contract with Recall to transport and store various IBM electronic media. IBM also required Recall to indemnify it from any loss or expense arising out of Recall’s services. Later, Recall entered into a subcontract with Executive Logistics, Inc. for transportation services. Under the subcontract, Executive Logistics was required to maintain various insurance policies, including a $2 million commercial general liability policy and a $5 million umbrella liability policy, all naming Recall as an additional insured.

Unfortunately, during one of the transports, a cart containing 130 IBM computer tapes fell out of an Executive Logistics van as it was exiting a highway ramp. The tapes contained personally identifiable information, such as names, social security numbers, birth dates, and contact information, for some 500,000 past and present IBM employees. Some unknown person retrieved the tapes, but the tapes were never properly recovered. Luckily, the tapes were encrypted and required specialized equipment for access to read the data on the tapes.

As you may know from our other blog posts, there is a patchwork of various state laws governing the types of notice that must be given to affected individuals, state attorneys general, and others in the event of a data breach. While some states do not require notification of a data breach to affected individuals where the information was encrypted, the encryption key remains safe, and the risk of disclosure is miniscule, other states require notification if there is simply any disclosure of personally identifiable information regardless of whether it is encrypted.

IBM took a cautious approach following the data breach of its employees’ information. IBM spent $162 million in total to respond to the data breach. This included $25 million to notify the past and present employees of the breach, $600,000 to maintain a call center to answer their questions and concerns, and $3.1 million for credit monitoring services. IBM demanded that Recall indemnify it from these losses and expenses, which Recall paid. Recall then made a demand to Executive Logistics and the insurers for reimbursement.

To make a long story short, the insurers denied Recall’s claims on several grounds, including that there was no evidence that the personally identifiable information had been published, or was made known, to a third person. The Connecticut Court of Appeals and Supreme Court held that without evidence of a publication of private information, the policies’ coverage had not been triggered. In hindsight, Recall should have required its subcontractor (Executive Logistics) to maintain cyber insurance. Cyber insurance policies, among other things, typically cover the cost for computer and data loss restoration, notification costs, credit monitoring, and liability to third parties from your failure to handle, manage, store, and control personally identifiable information belonging to others. Recall and Executive Logistics could have also tried to limit their liability by capping their indemnity obligations to the amount of the contract, their existing insurance policy limits, or in other ways.

But the valuable lesson is that anytime a vendor has access to your customer or employee personally identifiable information, you need to have a discussion about sharing or transferring the risk of loss if there is a data breach, including through the use of cyber insurance.
The newly created Ambassador group was formed to enhance the membership experience. Technology First ambassadors will help members learn about upcoming events, how to get involved, and how to maximize marketing tools such as Tech Source, the website for job postings and the monthly news magazine. Ambassadors will have a teal “flag” on their name badges identifying them at each event.

Aaron Flatter, Design and Sales Consultant with Garber Connect for 12 years, has lived in the northern Dayton area his entire life. Believing it’s important to build strong relationships, you may find him on the golf course or in a coffee house educating and promoting the needs of quality surveillance and structured cabling to safety and IT directors. His hobbies include spending time working on restoration of antiques, golfing and sailing with his beautiful wife!

Announcing New Annual Partners!

Technology First is proud to announce the addition of new annual partners. RoundTower Technologies and CommitDBA have become major supporters of the organization. We look forward to working with them and our other annual partners as we begin our 2015–16 year!

IO utilizes the latest modular data center technology with pre-integrated DCIM capabilities to deliver the highest performance and security for any Ohio colocation requirement.

Call to schedule a tour of IO Ohio 1.866.628.3439
IO.com
10 Reasons Why Your Organization Needs Data Loss Prevention

By: David Poarch, Anne Grahn, Forsythe

Security breaches rocked 2014. Sensitive data from high-profile organizations ranging from Fortune 500 retailers and multinational conglomerates to sandwich restaurant chains fell into the hands of hackers, affecting millions of customers and employees. It was a terrible year for data privacy and security, and a wake-up call for chief technology officers and corporate legal departments everywhere.

Data volume has been growing exponentially, dramatically increasing opportunities for theft and accidental disclosure of sensitive information. In the past, the amount of data doubled every four years. According to technology research firm IDC, it now doubles every two years, and by 2020 the digital universe—the data we create and copy annually—will reach 44 zettabytes, or 44 trillion gigabytes. These facts, along with increases in the portability of data, employee mobility and penalties for failing to comply with strict data protection regulations, raise the question: “What more can organizations do to protect themselves and their stakeholders?” An integral part of the answer may be data loss prevention (DLP).

DLP identifies, monitors and protects data in use, data in motion on your network, and data at rest in your data storage area or on desktops, laptops, mobile phones or tablets. Through deep content inspection and a contextual security analysis of transactions, DLP systems act as enforcers of data security policies. They provide a centralized management framework designed to detect and prevent the unauthorized use and transmission of your confidential information. DLP protects against mistakes that lead to data leaks and intentional misuse by insiders, as well as external attacks on your information infrastructure.

In the wake of recent security events, interest in the technology has exploded. In its “Forecast Overview: Information Security, Worldwide, 3Q14 Update” report, Gartner predicted that DLP will be the fastest-growing security segment through 2018, with a combined annual growth rate of 18.9 percent.

The loss of sensitive data and other forms of enterprise information can lead to significant financial losses and reputational damage. While companies are now well-aware of these dangers and data protection has become a hot topic, many organizations aren’t very familiar with content-aware technologies, and don’t fully understand the business case for DLP initiatives. With this context in mind, we have outlined 10 reasons your organization needs data loss prevention.

1. You aren’t sure where your company’s confidential data is being stored, where it’s being sent and who is accessing it.

DLP technology provides IT and security staff with a 360-degree view of the location, flow and usage of data across the enterprise. It checks network actions against your organization’s security policies, and allows you to protect and control sensitive data, including customer information, personally identifiable information (PII), financial data and intellectual property. With a thorough understanding of this data, your organization can set the appropriate policies to protect it, and make risk-prioritized decisions about what assets need to be protected and at what cost.

2. Your company has a plan for protecting data from external intruders, but does not protect against theft and accidental disclosure of sensitive information by employees and partners.

Not all data loss is the result of external, malicious attacks. The inadvertent disclosure or mishandling of confidential data by
internal employees is a significant factor. DLP can detect files that contain confidential information and prevent them from leaving via the network. It can block sensitive data transfers to Universal Serial Bus (USB) drives and other removable media. DLP also offers the ability to apply policies that safeguard data on a case-by-case basis. For example, if a security event is detected, access to a specific workstation can be blocked instantly. Policies can also quarantine or encrypt data in real-time response to events.

2. You are concerned about the liability, negative exposure, fines and lost revenue associated with data breaches.

Data breaches have been making headlines with alarming frequency. They can wreak havoc on an organization’s bottom line through fines, bad publicity, loss of strategic customers and legal action. The Ponemon Institute’s Second Annual Study on Data Breach Preparedness reported that sixty percent of nearly 600 executives surveyed said their company had experienced more than one data breach in the past two years—an increase of nearly 10 percent over 2013.

3. You are concerned about your next audit and want to maintain compliance with complex regulations.

More than 50 countries have enacted data protection laws that require organizations in both the public and private sectors to safeguard sensitive information. Penalties for noncompliance with strict privacy regulations and breach notification laws continue to grow. Requirements exceed the simple provision of written policies to prove compliance. Technology controls are becoming necessary to achieve compliance in certain areas. DLP provides these controls, as well as policy templates and maps that address specific requirements, automate compliance, and enable the collection and reporting of metrics.

4. You need to protect proprietary information against security threats caused by enhanced employee mobility and new communication channels.

Many employees are turning to social networking, instant messaging and other Web 2.0 applications to keep up with consumer trends. DLP helps to prevent the accidental exposure of confidential information across these unsecure lines of communication while at the same time keeping them open for appropriate use. With the proliferation of mobile devices and employees working remotely, corporate data is increasingly resides both in and outside of the organization. Whenever data travels in transit on the network, at rest in storage, or in use on a laptop or smartphone, DLP can monitor it and significantly reduce the risk of data loss.

5. You would like to monitor your organization for inappropriate employee conduct and maintain forensic data of security events as evidence.

Insiders represent a significant risk to data security. An employee who emails a work-related document to his personal account in order to work over the weekend may have good intentions. However, he or she poses a tremendous threat when there is confidential data involved. DLP technology offers 360-degree monitoring that includes email (both corporate accounts and webmail), instant messages, keystrokes, typed, documents accessed and software applications used. It also allows you to capture and archive evidence of incidents for forensic analysis. With DLP, you can limit and filter web browsing, and control which applications employees can access. It can invaluable tool in the effort to stop dangerous or time-wasting activities, and helps to detect problems before they can damage your business.

6. You are uncertain of your organization’s level of protection for confidential data in cloud applications and storage.

Large amounts of data are being moved to applications in the cloud—an environment in which it is not apparent where data will be physically stored and processed. Protecting sensitive information in virtual and cloud models is critical. DLP recognizes confidential data and automates its encryption at rest, in motion and in use, preventing its transmission to third-party infrastructures.

7. Your organization would like to proactively prevent the misuse of data at endpoints, both on and off the corporate network.

DLP technology monitors all endpoint activity—whether on smartphones, tablets, laptops or desktops, on the corporate network or off. It can block emails or attachments containing confidential data, enforce policies on the transfer of data to removable media devices such as USB thumb drives, and even prevent activities such as printing, copying and pasting. DLP offers complete data visibility and control, ensuring that employees, third-party vendors, contractors and partners are prevented from leaking your data—intentionally or inadvertently.

8. You would like to automate corporate governance as a means of improving compliance while saving time and resources.

DLP capabilities for the enforcement and automation of corporate policies and processes can help improve technical and organizational efficiencies, promote compliance, and provide methods for more comprehensive information governance. DLP provides up-to-date policy templates and...
maps that address specific requirements, automate compliance, and enable the collection and reporting of metrics. When a policy need is identified, DLP can make the change as simple as enabling an appropriate policy template on your system.

**You would like to gain a competitive advantage, in both brand value and reputation.**

When organizations fail to take the necessary steps to identify sensitive data and protect it from loss or misuse, they are risking their ability to compete. Whether it's a targeted attack or an inadvertent mistake, confidential data loss can diminish a company's brand, reduce shareholder value, and irrevocably damage the company's reputation. DLP enables the protection of valuable trade secrets and other vital intelligence, and helps to prevent the negative publicity and loss of customers that inevitably follow data breaches.

**Data Loss Prevention Should Not Be An Afterthought**

If you are surprised by how many of these 10 reasons apply to your business, you are not alone. Many organizations don't fully understand the benefits DLP offers. Developing a comprehensive data loss prevention strategy shouldn't be an afterthought. DLP transforms sensitive data into an operational asset, and can prevent your organization from making the wrong kind of headlines.

For more information visit www.forsythe.com

---

**7 practices, 1 partner: Sogeti**

With experts in Advisory Services, Application Development, BPM, Infrastructure, Mobile, Product Engineering and Testing, our Local Touch—Global Reach approach to consulting means you have access to local experts and a global team.

**Uptime Solutions Associates, Inc.**

Call us to discuss your plans. (937) 237-3400

www.uptime-inc.com
When Should You Rewrite an Application?

By: Sogeti

According to the book, Software Craftsmanship, an application should last longer than ten years. Joel Spolsky goes even further to say that “the single worst strategic mistake... rewrite the code from scratch.” Developers, on the other hand, are quick to bring up to their management, the need for a rewrite when they feel that the code is a mess. Should you ever throw the old application into the fire and write a new one?

What drives business is revenue and agility. Here are some business reasons to re-write an application:

1. Rewrite when the code base causes a high turnover in resources. I once worked for a company where the code base was so awful to work with that there was a 70% turnover in the IT Department every year. The turnover significantly impacted the company's bottom line. I have also seen an entire IT department leave, because no time was being allowed by the business for refactoring. It took the replacement developers twenty times longer to find and change the code.

2. Rewrite when a technology is deprecated by the language vendor. If there is no clear upgrade path to the latest version, this will cause a development resource shortage. I talked to a manager recently where their core business application was written in VBA. They were unable to find any developer resources that desired to maintain it.

3. Rewrite when the maintenance costs are causing a negative net operating profit. There was an application, which had such a high maintenance cost that it caused the company to abandon the product.

4. Rewrite when it affects your customers. If the performance or user experience is causing your business to lose customers to your competitors, rewrite those pieces.

5. Rewrite when it affects the agility of your business. If the maintainability of the application prohibits frequent releases, look into what is causing the delays. Keep track of your competitors. How often do they release? What new features did they add?

6. Rewrite the application when the refactoring cost is higher than a rewrite. Estimate how long it will take to refactor the application versus how long it will take to rewrite it. Long term cost savings will be gained by increasing the maintainability of the application.

Experience the power of being understood.

When you trust the advice you're getting, you know your next move is the right one. For a tailored approach that aligns your technology, processes and people to help improve productivity, turn to McGladrey.

We help you plan, select and implement new software solutions, address your technology risk and design your technology infrastructure.

Experience the power. Go to www.mcgladrey.com/technology or contact us at 800.274.3978.

McGladrey © 2015 McGladrey & Puller, LLP. All Rights Reserved. McGladrey® is a registered trademark of McGladrey & Puller, LLP.
In my last blog post, we covered the current state of backup and recovery plans as presented in a recent FEMA report. The report indicated that more than 30 percent of surveyed companies report major fails when it comes to data and systems recovery.

To that end, below is a list of the information you’ll need to identify and understand to create and implement a smart backup and recovery plan for all your organization’s data and systems.

### The Back End of Your Smart Data and Systems Backup and Recovery Planning

1. **Identify systems.** Identifying and understanding your business’ systems types, operating systems, physical and virtual servers, and hypervisors will frame the recovery devices needed.

2. **Identify important information.** Know what and where your business’ most important information is. It’s critical to take the time to meet with leadership and key team members to identify what data and systems keep your business running every minute of every day.

3. **Schedule.** After you’ve identified your systems, figure out how often data needs to be backed up. Remember that FEMA report in the last blog post? It said 58% of companies said they could not sustain any amount of data loss. Can your company afford data loss or downtime?

4. **Cost pyramid.** Clearly, data is an essential part of your infrastructure. When creating a backup and disaster recovery plan, determine how much budget to invest in this. Prioritize what must get done. As you can see from the diagram below, you have the recovery point objective and the recovery time objective, and as you increase and go toward the center with seconds or even zero downtime, costs rise.

5. **Backup vs. replication.** Review your goals to decide between backup and replication—and there are cases when a business requires both. Backup systems generally have a retention policy, which supports compliance requirements and granular data restoration. Backup involves making a copy or copies of your data, and your business can choose to do as many backups as it likes. Replication copies and moves data between a company’s sites so in the event of a disaster you can quickly restore your systems and data.

6. **Retention.** If your business involves healthcare or the law, retention is needed to adhere to compliance rules. Determine how long data needs be stored and what the legal requirements are.

7. **Infrastructure.** Evaluate these items in your business’ infrastructure to ensure your objectives are met: type of backup hardware; hard drive space; bandwidth charges; data deletion or segmentation to different locations to overcome space limitations; and data location.

8. **Geographic diversity.** In case of natural disaster, you’ll want to have a site replicated somewhere other than onsite to ensure diversity in backup.

### The Front End of Your Smart Data and Systems Backup and Recovery Planning

1. **Communicate.** Communicating your plan is vitally important. If needed, schedule an all-company meeting to devise or revise a plan together. Keeping everyone on the same page is essential to ensure data and systems aren’t lost during a recovery.

2. **Define and implement roles and responsibilities.** Determine the person or team managing backup and recovery. Also decide what processes need to be in place and who needs to be kept informed throughout the process. Communicate your goals to your entire company so they understand how backup and recovery will be handled.

3. **Bandwidth.** Know bandwidth requirements needed to effectively back up systems and data. If midday backups use all your bandwidth, then productivity is lost because employees can’t work. Also, learn how your bandwidth goes from one facility to another. If your office facility has 500 Internet or lacks bandwidth to accommodate backups, you’ll experience slowdowns, and eventually miss recovery point and recovery time objectives because of it.

4. **Test and evaluate.** How will you know if your plan works if you don’t test it? Test at least twice a year, evaluate ruthlessly, adjust as needed.

### Backup, Recovery and Disaster Recovery Services

WEDNESDAY, NOVEMBER 18, 2015
SINCLAIR COMMUNITY COLLEGE PONITZ CENTER
7:30 AM UNTIL 5:00 PM

Presentation opportunities (member pricing) are going fast… call to reserve your spot!
Contact Michelle Marek at 937.229.0054 or mmarek@technologyfirst.org for more information
What's Real and What's a Misconception About the Cloud?

By: Peak 10

When it comes to business media predictions regarding the cloud, do phrases like “CapEx savings,” “elasticity” and “ability to compete against much larger companies” have a physical effect on your CEO? Do these words currently force your CEO to flag you down, demanding to know your company’s cloud strategy? If so, your CEO is not alone. And if you are still cautious about the cloud, you’re not alone, either.

It’s true. Forbes, The Wall Street Journal and Bloomberg have foretold the riches to be gained by switching to the cloud, especially for mid-sized companies, in the coming year. But these publications are not in IT. You are. And your job is on the line if you move your company’s applications and data to a cloud environment, and the results turn out to be different than what was predicted. If you’re still considering the cloud and the thought of resources and elasticity of the cloud sound enticing, you’d prefer to address your concerns before you make a move.

Vulnerability to Hackers

You’re worried about hacking. It’s a legitimate concern. No one is exempt from hackers anymore. But Gartner debunked the claim that the cloud is less secure than an on-premises data center as a misconception.

“Cloud computing is perceived as less secure. This is more of a trust issue than based on any reasonable analysis of actual security capabilities. To date, there have been very few security breaches in the public cloud — most breaches continue to involve on-premises data center environments. The majority of cloud providers invests significantly in security technology and personnel and realizes that their business would be at risk without doing so. However, assuming they are secure is not advised.”

“While security at cloud vendors varies widely, the good ones typically employ the latest security technologies and processes, enabling them to offer an environment that is safer than what your organization could create. Among the attributes to seek out:

- Monitoring by onsite staff 24/7/365
- The availability and uptime of a Tier II or higher data center
- The ability to meet compliance requirements regarding safety and security along with many industry standards

In terms of a cloud services provider, Gartner recommends the following: “Don’t assume that cloud providers are not secure, but also don’t assume they are. Cloud providers should have to demonstrate their capabilities, but once they have done so there is no reason to believe their offerings cannot be secure. There are enterprises whose security capabilities are formidable, but so are the capabilities of most cloud providers. However, the security levels of cloud providers will vary. Assess your actual capabilities and your potential provider’s capabilities and hold both to reasonable standards. Assuming on-premises capabilities are more secure can lead to a false sense of security.”

Loss of Control of Your Environment

You’re worried a cloud services provider will start moving things around or changing things without your consent or knowledge. Reality? An ideal cloud provider enables and expands your control of the environment: you have control over your internal servers and if you opt for a hybrid cloud, you’re now also the broker of what is available to it.

Loss of IT Value to the Company

You’re privately concerned if you go to the cloud, you’re done and out of a job. That’s a scary thought. Virtualization created the same concern, but the truth was it created more IT jobs, not less. The same is turning out to be true regarding cloud implementation. In 2013, Deloitte consulted with three organizations: Enterasys Networks, Aviont Group and the University of California San Francisco (UCSF). They published their results in the Wall Street Journal’s COO Journal four years later, stating that despite the vast IT departments at all three organizations, only two employees had been let go — arguably a lower rate than natural attrition.

A good cloud services provider enables you to do what you likely get into IT to do: exercise your knowledge, creativity, and abilities. You can finally build the applications you always wanted to build, tweak, and customize existing applications, make everything inside your company run the way only you knew it could run, because you have:

- Uptime. Going to the cloud offers unprecedented uptime.
- Growth and Elasticity. The cloud offers you agility. You’re not slowed down by weeks or months launching a new initiative because you had to physically make hardware purchases, install new servers and train. With the cloud, you make a call when you get the green light and say “I need more virtual machines stood up.” It’s fairly inexpensive and done quickly, all with a technical assistance center that can help.
- Cost Savings. You’ve known all along that by going to the cloud, CapEx savings will be mitigated by new subscription model costs. The reality is while many see hard cost savings with the cloud, the real value is in soft cost savings such as efficiencies and new capabilities. The biggest savings your company will likely make is getting YOU back as a resource. You will be able to help your company become quicker to market with new products and services. With that, your company grows, and your stature within the company grows with it. You’ll be doing what you’ve always envisioned, rather than spending the majority of your time fixing what is broken.
- Peace of Mind. Finally, therein the peace of mind that comes with going to the cloud: the servers are up, in a secure environment, and those who want to work overtime can.

Going to the cloud can not only enrich your company’s business strategies, it can help you lead the career you’ve always envisioned there. In the same Wall Street Journal article cited earlier, the IT spokesperson for Enterasys Networks reported that cloud adoption had allowed its IT department, previously bogged down 60 percent of the time on operations, to enjoy as much as 60 to 70 percent of its time on new application development.

The other two organizations studied reported similar results. Just think what the cloud could do for you.
Five Questions to Consider Before Choosing A GPS Tracking System for Your Vehicles:

By: RACO Industries

What Tracking Data is Relevant to Your Business?
Most GPS tracking systems available in the market today provide detailed information concerning your fleet of vehicles such as driver & vehicle data, alerts, and reporting. Some systems can even exchange information with the drivers. Depending on your business, some or all of this information may be relevant.

It is important for you to determine what specific information is best suited for your business and more importantly how you will apply it to your processes. Otherwise, you can get lost in all of the information and spend more time tracking your vehicles than utilizing the information for the purpose of improving your business processes.

How Will Your Employees React?
This is an area of concern because there will be employees who may view a fleet tracking system as a lack of trust from the employer. Some may even be apprehensive by viewing the system as an invasion of their privacy. However, the reality is most employees will accept this investment openly because the benefits will allow the drivers to perform their jobs better by increasing productivity, improving safety and providing documented proof of job performance. For those apprehensive employees, they are probably the ones who are most likely abusing your company vehicles and usage policies.

Prior to implementing a system, you may want to involve your drivers with helping to determine how best to apply a system for your business. You will help gain acceptance by involving them on the decision-making process and improve on the probability of utilizing the information to its fullest potential. Most employees want to help their employers increase revenue, reduce costs and improve safety. A proper, well thought out implementation of a fleet tracking system will help a company recognize the key benefits and yield a very quick return on their investment.

How Will You Monitor the Application?
Making time to perform any additional tasks like monitoring a fleet tracking system for most employers is a very difficult proposition, especially in difficult economic conditions. But just monitoring the application from your computer really would not be a good use of your time. Instead of monitoring, the better systems available in the market help you manage your fleet by providing only the data that you need and when you need it to help your business processes.

The systems alerting and reporting functions should enable users to receive information based on events that trigger the alerts. These alerts can be speeding or other unsafe driver behavior, geofence ingress/egress or even vehicle preventative maintenance schedule. Management of the application can be performed via your web browser or remotely via a mobile phone application.

What Type of GPS Device is Best?
Due to the explosive growth of GPS tracking over the last several years, there are hundreds of devices available in the marketplace. As with other electronic devices, there are very good products available based on your needs but there are also products on the low end of the quality and performance spectrum. Most GPS fleet tracking companies have tested and qualified various devices and can recommend options. This service will help take the risk out of purchasing an inferior product.

Other considerations include warranty, data storage, power sources, and reliability. Additionally, the location of the device in your vehicle should be determined before opting for a particular device. The type of vehicle data weighs heavily on this decision. For example, if you want to collect engine diagnostic data, you should choose a GPS device that plugs into the OBDII port that is available in most vehicles. The device will stay powered while the vehicle is running and many of these devices gather engine diagnostic data that can be captured in many fleet tracking applications. Lastly, GPS data cannot reliably be received if the vehicle is inside a building or other structure. Be sure to select a device that has a store & forward feature so information can be transmitted once your vehicle moves outside.

What Kind of Costs Can I Expect?
All fleet tracking systems charge an ongoing fee, usually monthly, for usage of the application. The components of this cost are a data plan from a cellular carrier to provide real-time tracking, the software application and service/support. When choosing a fleet tracking provider, select one that offers the best combination of ongoing cost, the features of the software application that best helps your business, and support services including user training. The tracking data that your company will rely on is provided by the GPS satellite data, a cellular network to transmit this information, a dependable GPS device and a software application to help disseminate this information. It is important that you have reliable support from your provider for any issues that may arise due to potential outages.

There could also be the cost of the tracking hardware, as well as an installation fee.

RACO Industries is a leading national integrator of GPS, handheld, and wireless mobility solutions.
BLOGS

Set An Alarm Android Only:

You can set an alarm on your smartphone while at the comfort of your Google search bar, like this one reminding me to go home after a long day’s work.


Find That Exact Color

One of the handy Google Chrome web browser extensions I use is ColorPick Eyedropper. Find the exact RGB (Red-Green-Blue) numbers for a color by simply hovering the mouse pointer over the right spot. It’s useful if you’re looking to make a presentation a little more compelling by using a customer’s exact color scheme.

https://chrome.google.com/webstore/detail/colorpick-eyedropper/ohcpnigalezhgmcgclinkefpuffdolg

RACO Industries is a leading national integrator of GPS, handheld, and wireless mobility solutions.

More of Paul’s blogs can be found at http://paulsdailyposts.blogspot.com/
Every year, cyber crimes cost companies more than $500 billion.

Applied Cyber Security Training

Focusing on the need for training in cyber security, intelligent systems and data analytics, Sinclair Corporate College’s new Cyber Training Facility at Austin Landing is designed to help prepare businesses to mitigate the threat of cyber crimes.

For more information, call 937.512.3230

Sinclair Corporate College
Austin Landing
10100 Innovation Dr., Suite 310, Dayton

SINCLAIR CORPORATE COLLEGE
workforce.sinclair.edu

Business Intelligence • Analytics • Cloud
Cyber Physical Systems • Robotics
Health and Medical • Data Analytics
Smart Systems • Computer Forensics

Scan with your smartphone to learn more
It’s Time
To Go Mobile
Responsive

Bitstorm Web builds brand awareness and generates new business leads through:
- Responsive Web HTML5 and CSS3 Development
- Custom Apps Development
- Ecommerce Solutions
- Search Marketing
- Social Media Marketing
- Content Management Solutions
- 3D Modeling and Animation
- Video Production

www.bitstormweb.com  937-438-3434  info@bitstormweb.com