Greater Dayton Employer

Information Technology Workforce Forecast | 2016

A Career in Information Technology in the Dayton Region

9 Steps to Implementing a Successful Configuration Management System
Workforce Collaboration 2016

By: Ann Gallaher, COO, Technology First

McKenna Golf Tournament Scholarship
Each year Technology First and the Robert V. McKenna Golf Tournament Committee collaborate to award scholarships to deserving IT college students. We are pleased to announce this year’s winners!

The McKenna Memorial Golf Tournament that supports this scholarship is being held on August 12th at Yankee Trace Golf Club. For more information, visit www.mckennagolf.org.

Terence Lee
Sinclair Community College
CIS / Software Development
$1,000

Troy Kauffman
University of Dayton
MIS
$1,250

Adam Adkins
Sinclair Community College
Web Development
$1,000

Garrett O’Grady
University of Dayton
Computer Science
$1,250

Infrastructure Forum
The special interest group, Infrastructure Forum is open to all data storage, help desk, and network professionals working in an information technology department. On March 25, Heidelberg Distributing hosted the group as they discussed help desk software and tools.
A Career in Information Technology in the Dayton Region

There are 21,800 information technology (IT) professionals working in the 14 county Dayton region. Information systems and business technologies empower every industry today. Approximately two-thirds of these professionals work in non-IT industries such as healthcare, manufacturing, and construction. There are 1,307 information technology companies with an annual payroll of $1.7B and revenues of $3.5B.

IT professionals averaged an annual salary of $69,900 in 2014, which is 49% more than the average salary for other occupations at $46,900. Jobs in the information technology profession are supposed to grow 16.3% over the next ten years.

Critical Incumbent Skill Shortages | 2016

Top 25 Skills in Demand

<table>
<thead>
<tr>
<th>Skill Description</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMWare/Virtualization Skills</td>
<td>27%</td>
</tr>
<tr>
<td>.Net Development Skills</td>
<td>22%</td>
</tr>
<tr>
<td>Cisco Network Administration Skills</td>
<td>22%</td>
</tr>
<tr>
<td>SQL Server Database Skills</td>
<td>22%</td>
</tr>
<tr>
<td>Java/J2EE Development Skills</td>
<td>20%</td>
</tr>
<tr>
<td>Business Objects/Business Intelligence Skills</td>
<td>20%</td>
</tr>
<tr>
<td>Web Services/Service Oriented Application (SOA)</td>
<td>20%</td>
</tr>
<tr>
<td>iOS Mobile Application Developers</td>
<td>13%</td>
</tr>
<tr>
<td>Linux/Unix Administration Skills</td>
<td>13%</td>
</tr>
<tr>
<td>Android Mobile Application Developers</td>
<td>13%</td>
</tr>
<tr>
<td>C# Development Skills</td>
<td>13%</td>
</tr>
<tr>
<td>Oracle ERP/Development Skills</td>
<td>11%</td>
</tr>
<tr>
<td>SharePoint Skills</td>
<td>11%</td>
</tr>
<tr>
<td>Project Management (PMP)</td>
<td>11%</td>
</tr>
<tr>
<td>Voice-over IP Administration Skills</td>
<td>8%</td>
</tr>
<tr>
<td>Windows Server 2008 Skills</td>
<td>8%</td>
</tr>
<tr>
<td>PHP/Perl/Python Development Skills</td>
<td>8%</td>
</tr>
<tr>
<td>Oracle Database Skills</td>
<td>8%</td>
</tr>
<tr>
<td>QA Specialists</td>
<td>8%</td>
</tr>
<tr>
<td>MySQL Database Skills</td>
<td>5%</td>
</tr>
<tr>
<td>Info Security</td>
<td>5%</td>
</tr>
<tr>
<td>Microsoft Dynamics AX (ERP)</td>
<td>3%</td>
</tr>
<tr>
<td>Microsoft Business Intelligence</td>
<td>3%</td>
</tr>
<tr>
<td>IBM DB2 Database Skills</td>
<td>3%</td>
</tr>
<tr>
<td>Visual Basic Development Skills</td>
<td>3%</td>
</tr>
</tbody>
</table>

Percentage of employers surveyed (N = 38)

Professionals in Most Demand

- Developer/Programmer Analyst: 23%
- Desktop Support Analyst: 15%
- QA Associate/Analyst: 13%
- Project Manager: 10%
- Server Administrator: 8%
- Business Systems Analyst: 6%
- Network Engineer: 6%
- Information Security Administrator: 5%
- Business Intelligence Analyst: 5%
- Data/Database Administrator: 4%

Percentage of all professional openings (N = 123)

Highest Demand by Experience

Entry Level or Intern (0–3 years experience)

- Developer/Programmer Analyst
- QA Associate/Analyst
- Desktop Support Analyst
- Network Engineer

Advanced Position (4+ years experience)

- Developer/Programmer
- Desk Support Analyst
- Project Manager
- Business Systems Analyst

Programming Skills in Highest Demand

- .Net: 22%
- Java: 20%
- iOS Mobile: 13%
- Android Mobile: 13%
- C#: 13%

23% of all planned openings are for programmers

Application skill in highest demand: SharePoint
There is no doubt that the information technology infrastructure library (ITIL) has grown to become a widely accepted reference for information technology (IT) best practices. But to think that after reading any of the books in the ITIL library, a practitioner would be in a place to take what they read and make it actionable, is at most very optimistic.

With this limited guidance, organizations should not jump right into implementing a configuration management system (CMS) without establishing a clear vision of their objectives. This nine-step plan can help you create an actionable strategy and plan for successfully implementing a CMS and place you in a better position to add value and enhance your organization’s management capabilities.

Step 1: Establish a governance framework and policy
Start by assigning a configuration management process owner who will be responsible for owning the configuration management strategy, structure and process. One of the first tasks that the process owner should undertake is creating and ratifying a Service Asset and Configuration Management (SACM) policy. In general, a SACM policy should define scope, roles and responsibilities, policy statements, guiding principles, and references to other related policies, and standard operating procedures.

Step 2: Define roles and responsibilities
All participants in the SACM process should understand their roles and responsibilities. Common roles and related responsibilities include:

• Configuration owner: Responsible for the overall CMS strategy and process maturation.

• Configuration manager: Oversees the process and is the highest ranking manager involved in the day-to-day CMS activities. Responsible for the day-to-day maintenance of the CMS.

• Configuration database administrator(s): Responsible for the day-to-day maintenance and updates to the configuration management data bases (CMDBs).

• Configuration item (CI) owners: Responsible for the status and attributes of the CI.

• Configuration database developers: Design solutions and provide technical knowledge.

Step 3: Determine the CMS primary usage
With the process owner and roles identified and positioned, this team should then consider how the CMS will facilitate all IT disciplines throughout the entire service lifecycle. Will its primary use be to facilitate incident management by identifying the caller information or identifying CI owners and support groups? Or maybe support change management by making it easier to assess impact and risk?

Other usages can include visualizing and displaying service representations, and identifying application and infrastructure component dependencies to support problem management triage.

Ensure you recognize the key benefits and value propositions for each usage identified so you can develop a business case and provide the necessary details to properly prioritize each usage. An implementation roadmap should be developed that can introduce these capabilities in an orderly fashion.

Common CMS usages include incident management, event management, problem management, change and release deployment management, measurement and reporting, service continuity and disaster recovery, and processes external to IT (vendor, contracts and organizational).

Step 4: Determine what types of records it will hold
By definition, a CMS provides the representation of all of the information for configuration items within scope of your organization’s configuration management effort. Based upon the outcomes of step three, determine what types of records and data can enable these capabilities.

Generally speaking, a CMS integrates information from many sources including:

• Incident, problem, change and release records

• Known error and knowledge management records

• Application and infrastructure records

• IT support groups, service level agreements (SLAs), operating level agreements (OLAs) and underpinning contracts

• Corporate data about employees, suppliers, business units and services

• Measurement and reporting detail

• The CMS can represent data from several different CMDBs or management data repositories (MDRs), constituting a federated CMDB.
Step 5: Determine existing data repositories

Begin by taking an inventory of your organization’s existing data repositories that are internal and external to IT, in accordance with your organization’s data requirements identified in step four. This will facilitate establishing priorities for each usage. This information may appear in the form of a list or spreadsheet, or reside in formal databases.

Once these data repositories are identified, it is equally important to discover the following information for each:

- Primary purpose of the data
- Location
- Owner
- Users of the data
- Accuracy of the data
- Completeness of the data
- Level of data detail (too little or too much)
- How is the data supported and maintained?
- Is the data integrated with change management?
- What is the single trusted source for the data?
- Is the data federated or is it replicated?

Next assess and plan the level of work associated with scrubbing the data and gathering new data in support of the requirements. In some instances, you may even find it more effective and efficient to discard existing data and start anew.

Step 6: Understand what tools are available to support the process

Investigate what current tools are available within your organization for collecting, storing, managing and updating the CMS data. Identify which tools meet the defined requirements, and which requirements have yet to be met by existing tools. Knowing your tool inventory will have a huge effect on the creation of your organization’s eventual data model and CMS structure.

Use tools to automate data collection and help mitigate the risk of errors that can be introduced by manual data entry and maintenance. An effort should be made to identify any additional tools that could help in the automation process and determine if a business case can be made to support their purchase. While developing a business case may be difficult, aligning it back to the planning activities conducted in steps three and five will help justify their purchase.

Step 7: Decide on a configuration item (CI) categorization and naming scheme

Start by determining how the CIs will be categorized. Many organizations find using type, family and class to be an acceptable starting point. Then, decide on a naming convention. A naming convention is essential for organizations where data should be integrated into the CMS, but is stored in multiple CMDBs across the enterprise. Utilizing a standard naming convention helps to ensure the integrity of other IT service management processes, including incident management, measurement and reporting.

Step 8: Decide on CMS structure

After categorization and naming conventions are in place, design your CMS structure. Your CMS structure should be aligned with the primary usages established in step three and designed with the goal of satisfying their priorities. Many organizations design their CMS structure in a manner where there is a balance between:

1. Breadth: the number of families and categories of CIs that will be tracked.
2. Depth: the extent to which component CIs will be tracked. For example, the disk drives or cards within a server can be tracked as CIs.
3. Detail: the number of attributes and types of relationships for each class of CI that will be tracked.

A good rule of thumb when designing a CMS structure is to lean on the side of collecting less. Not all available data provides value and collecting excessive data can lead to a CMS system that is expensive, difficult to build and challenging to maintain.

Once the CMS structure is defined, you should determine your organization’s CI population approach (this can include using a phased or wave approach) and the order of execution. It is also important to identify ownership and support group structure for all CIs.

Step 9: Establish an improvement process

It is extremely important to plan for improvements and their implementation. Usually, the most successful improvement programs are the ones that are designed to bring gradual but continual improvement. One of the most widely used improvement processes is the Deming Cycle (plan, do, check and act).

To ensure your CMS is providing the expected value, review each of the CMS usages defined in step three and then validate how well the CMS is meeting those needs. This may require a measurement and reporting strategy combined with a continual improvement process. The ITIL library has dedicated a whole book to the subject of continual improvement and includes a detailed seven-step improvement process that provides a circular set of activities designed to help organizations improve. ITIL’s continual service improvement book is a great starting point to address this need.

The key benefits

Using this nine-step approach can help you develop your own configuration management plan and reduce many of the frustrations experienced by your IT staff that read the ITIL library and still feel like they don’t know where or even how to begin. This approach also reduces the risk associated with attempting to implement a CMS/CMDB without adequate analysis and design, namely the risk of an outcome that is not required or of a tool set that provides little value or management capability.
What allows elite teams in football to be great while other teams struggle for decades? Why do some companies grow and flourish, while others die off? How do you go about readying yourself for your career? How do you afford vacations or to retire one day? In one word: strategy. But what exactly is a strategy? You might say a strategy is what one team uses to beat another team in a sport. Or that strategy is what a commanding general uses in war to outmaneuver and defeat his enemy. Let’s look at the definition of strategy as defined by Google before we travel any further.

Strategy—“A plan of action or policy designed to achieve a major or overall aim.”

Now, let’s take a look at each part of this definition to see how it applies to business, projects, and more.

“A Plan of Action…”

This seems pretty straightforward, right? You process a set of actions ahead of time and do them. Simple. Easy. Everyone can do it. Unfortunately, this is not always the case.

Multiple Perspectives

A good plan is developed by a diverse group of people with multiple perspectives. Allowing one person or a group of similar minded people to take control of a plan can make it one sided. Also, consider involving end users in your planning sessions. Create a platform where you encourage employee feedback. Often, direct input from the employees can help avoid major operational issues.

Forest and Trees

A good plan accounts for the details but does not get lost in them. For example, it does not make sense to spend time detailing the process of a key change that will occur much later in your project timeline. You want to consider that process during the meeting but ensure it does not become a time trap. Details such as this should be accounted for by the right people at the right time.

A Plan without Action is Just a Dream

All the planning in the world is nothing without action. Creating the right plan is the first step, but executing the plan is what makes the project a success. The project managers should have the ability to plan and take action. Learning ways to communicate a message to a diverse group of people is vital. How would you approach asking a contractor to proceed with a minor task? What about asking an executive to approve a budget? While both move your project forward, they need a different style, tempo, and tone. You should adjust your communication based on the target audience.

“…Or Policy Designed”

When I think of a policy, my mind goes to big box retail stores. Sometimes, the word policy evokes negative experiences. “No, you can’t return that sir. It’s against our return policy.” While policies like this are seen in a negative light, a well-designed policy can be helpful when creating a strategy. The best way to design a policy is to leverage standard practices as a baseline.

Standard practices allow you to use predetermined processes to create a path for your project. Much like planning, these standards allow you to keep your team focused and on track. When an employee has a question about a process, standard practices can be the perfect guide. When you communicate the standard practices to your team in advance, your standards can lead to a successful outcome.

“…To Achieve a Major or Overall Aim”

To achieve a major aim, you have a goal in mind.

Off Target

One of the biggest mistakes made by project managers is losing sight of what they showed up for. If you begin a company that makes pizza boxes, and you end up making pizza, you have lost sight of what you came here to do. The logistics of going from a cardboard box manufacturer to a restaurant are complicated and costly.

Scope Creep

Scope creep, as it is often called, is the natural enemy of your original goal. Your project can get derailed by adding new tasks that might seem helpful or productive at the time. In reality, those new tasks can delay progress or be counterproductive to your end goal. To prevent losing focus, you should incorporate regular discussions around direction and goals.

A well-prepared plan leveraging standard practices will allow you to focus on your end goals. Using strategy as your guide you can excel where others might fail.
The Technology First Leadership award recognizes the contribution of information technology students and professionals ensuring a vibrant Dayton community. Recognizing Individuals and Teams exemplifying Technology First Values: creating a community to share knowledge, grow business, and explore the future.

**Categories:**

1. **Emerging Technology Leader**
   - An IT college student or student team that exhibited excellence while delivering a capstone project.

   **Nominees:**
   - University of Dayton MIS / Mikesell’s Intranet Project
   - Wright State University / Speedway 3-D Printing Project
   - Sinclair Community College / Teradata Application Programming Project
   - Wright State University / WinSupply Business Intelligence Project
   - University of Dayton / Imagery Solutions Business Automation Project

   **Past Winners:**
   - Clark State Community College – 2015
   - Hanen Alkhafaji, PQ Systems – 2014

2. **Innovative Technology Team**
   - An IT company or IT department that has designed and implemented an innovative use of technology.

   **Nominees:**
   - AfidenceIT SYNC Methodology
   - Teradata Customer Services IT Knowledge Centered Support Project
   - Midmark Customer Tracking System Project
   - Red Hawk Technologies Development Team Web-based Telephony Application Project
   - Boost Technologies LLC dba Shumsky Promotional Core System Project

   **Past Winners:**
   - University of Dayton Information Technologies – 2015 Academic
   - Midmark – 2015 Enterprise

3. **IT Executive of the Year**
   - A senior level professional responsible for influencing progress and developing teams through leadership excellence.

   **Nominees:**
   - Jill Campbell, Director of IT, Heidelberg Distributing
   - Brian Clayton, Chief Information Officer, Taft Law
   - John Huelsman, Director of Information Technology, Hobart Service
   - Srujal Sheth, President, Vana Solutions

   **Past Winners:**
   - Mark Human – 2015
   - Steve Hangen – 2014
   - Tim Hull – 2014 Community Advocate

4. **Outstanding Technology Team**
   - An IT department that has impacted the efficiency, productivity, and performance of their company.

   **Nominees:**
   - City of Fairborn—Infrastructure Project
   - Midmark—Point To Point Encryption Solution
   - Speedway—Speedy Rewards Agile Project
   - Net Gain—Connectivity Project
   - Taylor Communications—Consolidation Project

   **Past Winners:**
   - Hobart Service – 2015
   - Lion – 2014

---

May 5, 2016
University of Dayton
Arena Flight Deck
4:00 – 6:00 pm

Title Sponsor: AVATAR
Business Continuity and Disaster Recovery Planning: Can the Cloud Help?

By: Scott German, RSM

It is not pleasant to think about, but disasters happen, and no business is immune. They can manifest themselves in many different ways, potentially bringing your business to a halt and causing significant financial, operational and reputational harm. Every organization must maintain a thorough business continuity and disaster recovery plan, and cloud technology is emerging as an effective tool to help companies protect their environments.

Disasters are typically thought of as natural events such as a flood or tornado, but they are actually categorized as anything that can disrupt your business for a period of time. Power outages and server failures are also considered disasters in many instances, as well as an Internet disruption or a key IT person leaving the business. While you can’t predict when disasters will happen, you can be prepared for when they occur.

Before you know where your disaster recovery plan needs to be, you need to know what your technology capabilities currently are. To evaluate your current posture, you should first go through a discovery phase, connecting business units, and their needs, to technology.

The initial step is to understand your current IT environment, including hardware and software such as network infrastructure (servers, routers, switches, operating systems, wireless access points, etc.) and all business applications. The discovery phase also includes assessing the recoverability of your current systems. Determine if anything needs improvement before looking at the disaster recovery plan, including the usability and accessibility of systems, remote accessibility, performance, and planned and unplanned downtime.

It helps to have someone from IT involved in the discovery process to provide input from a high level about how systems are related to the business. Often, organizations will bring in a third party for this step, including it in an overall technology assessment. The third party can help evaluate what is being done well, what needs to improve and how to leverage technology in the future.

Connectivity is a key element of discovery that is often overlooked; you must understand your current bandwidth, as well as alternative options for access. This can dictate the design of your disaster recovery plan, and whether the cloud can be leveraged in your strategy.

The final phase of discovery is business continuity planning. Begin with the high-level strategy of the business and determine what applications, systems and data are most critical to those goals. Having that organizational plan front and center during the process helps ensure that an effective plan is implemented.

The key part of business continuity is a financial impact analysis; you need to know what the impact to your business is if a system or data set is not available. This discussion should include people that use specific applications to understand dependencies and how applications are used to perform tasks. This process includes questionnaires and focus groups to understand the financial and operational impact that could occur following a disaster.

Once the business continuity plan is approved, IT can use that information as the basis for disaster recovery system development. In many cases, companies upgrade production systems and relocate older systems to the disaster recovery location. This lowers costs at the disaster recovery site, and ensures the best equipment is used at the production site.

The explosion of third-party cloud services and an increase in bandwidth has given businesses more options for implementing better disaster recovery systems in a more cost-effective manner. Some organizations take their first step into the cloud with a co-location strategy. It involves housing storage and servers to run the disaster recovery site in a third-party data center. The monthly costs for co-location are typically more manageable than major upgrades to an on-premises facility. A third-party data center also includes redundant power, connectivity and additional protections that middle-market companies cannot provide on their own at a reasonable cost. Most cloud service providers also have recovery or backup-as-a-service options to back up an organization’s environment to their cloud data center.

These solutions can be very cost-effective and a valuable solution because organizations do not have to purchase additional hardware or software to protect their environment from the effects of a disaster. They can also provide an entire backup and recovery solution, not only managing disaster recovery, but also everyday situations when files must be restored.

(continued on page 9)
Some companies are concerned about potential risks when transitioning their production environment to the cloud. However, a business typically achieves better uptime and availability in the cloud, as it takes many of the risks of physical servers out of the equation. The design of a cloud services data center is built for high availability and disaster recovery. Although, as with any application, you must perform due diligence to ensure the environment that you move your information to meet the requirements for your business.

The two main cloud platforms that can help improve disaster recovery and business continuity for an organization are software-as-a-service (SaaS) and infrastructure-as-a-service (IaaS). SaaS is the typical cloud services platform where data is stored in the cloud, and users access that application through a Web browser or application. For example, many companies are moving to Microsoft’s Office 365 cloud platform to provide enhanced disaster recovery capabilities for communications. Email is critical for today’s businesses, and you need to make sure it is always functional and available.

Vendors are introducing cloud options for other key business applications to keep up with demand. Anything that is moved from an on-premises environment to the cloud makes disaster recovery easier to plan and account for. When considering your disaster recovery strategy, it is a good idea to look at your vendors and see what cloud options are available and how they can benefit your business.

With IaaS, the cloud provider takes responsibility for virtualization, servers, storage and networking, but your IT department still has the flexibility to activate servers when needed, upgrade applications and move data. IT still performs its typical tasks, without worrying about the availability of hardware.

Regardless of your disaster recovery strategy, testing must be a critical component. Documentation is essential for future testing; any issues can help develop a stronger foundation for your business continuity plan. In addition, proper documentation provides the steps that must be followed to get applications back up and running if a disaster occurs.

An annual tabletop test is also a valuable exercise. The test involves discussing specific disaster scenarios as a group and walking through the process should those situations occur. Your users should evaluate necessary communication, what coordination is required with third parties or other organizations, and other items needed to run the business.

Technology changes at a rapid pace, and as it evolves, you must ensure you are utilizing it to make your disaster recovery plan more effective. Understanding how your technology investments align with business needs and determining which of your applications can be moved to the cloud can immediately improve your environment. By leveraging the cloud, you can simplify and enhance your disaster recovery strategy, and cost-effectively scale without making significant capital investments.
The value of human capital is crucial to the successful implementation of solutions. By understanding what human capital is, you will understand a context to understand how we develop as professionals. You will be able to identify the many strengths that you have, as well as the weaknesses you have and where you need to focus your time, attention, and learning.

When we are faced with challenges, dilemmas, and conflicts in life and work, we need to have the right toolset in order to provide the right solution. Capital is traditionally understood as wealth, assets, or an investment; human capital is the value an individual brings to a situation. In order to increase our human capital, the value that we bring to a problem, we need to increase our intellectual capital, technical capital, and relational capital.

Intellectual capital is the formal education and knowledge of theory and abstract solutions. Typically, intellectual capital is learned through University degrees, industry certifications, and training programs. Intellectual capital equips us with an understanding of frameworks, tools, and alternative solutions. Intellectual capital can be summed up with knowing the right answer. Even so, this does not imply that we know how to implement that answer, though. When we put our intellectual capital to work, we turn this head-knowledge into experience by using our technical capital.

Technical capital consists of skills, tools, and the ability to turn theory into practice in order to provide a solution. For example, intellectual capital is having the know-how to develop HTML and CSS code, while technical capital is actually developing the code into a working product. Technical capital can be summed up with the principle of putting theory into practice. Having people on your team who know the right answer is valuable, but having people on your team who know the right answer and how to apply that answer is even more valuable. Still, we need to be able to use our head-knowledge and know-how with the context of other individuals in order to create a valuable solution. Therefore, we need to work with others by tapping into our relational capital.

Relational capital is the capacity and ability to work effectively with others. The ability to mentor others, work alongside others, and be mentored, is crucial to developing the relational capital required to work successfully in a team. Relational capital is the relationships of people in our lives whom we make better, and whom make us better. There should always be three types of people in your life to increase your relational capital—those whom you are mentoring, those whom you are being mentored alongside, and those who are mentoring you. When we put our technical capital to work, we turn know-how into shared experiences by using our relational capital.

Human Capital is the value that we bring to a problem. We can increase our human capital by adding intellectual capital, technical capital, and relational capital. Ask yourself the following questions in order to identify your current level of human capital:

- What aspect is my strongest human capital?
- What piece is my weakest human capital?
- What do I need to improve the most about my human capital?

The process of improving our human capital is accomplished through formal education, real life experience, and relationships with others. By growing our human capital, we add value, increase the effectiveness of solutions, and become accelerators in our teams and solutions.
The Web hosts a vast array of applications, many of them critical for business operations, from office suites such as Google Docs, to email, calculators, spreadsheets and data storage.

Nearly all mobile applications connect to the cloud, storing private business information, user names, passwords and other sensitive content. Employees tie into the Web with mobile device apps such as Google Maps, LinkedIn and Wink, which allows users to see from afar who is ringing the home doorbell or lets them dim the living room lights.

Along with functions that a decade ago would have boggled most minds, apps also have ushered in pervasive security risks from malware, phishing attacks and human missteps.

These risks top the list for organizations, according to the nonprofit Open Web Application Security Project:

- **Web application vulnerabilities.** Many apps don’t properly protect sensitive data such as credit card numbers, tax IDs and authentication credentials. Attackers may steal weakly protected information.

- **Operator-side data leakage.** This includes unnecessary copies of personal data in the workplace, and the pirating of loosely guarded location data, browsing behavior and device configuration to identify people.

- **Insufficient data breach response.** The average time to detect a data breach is 208 days, according to the Verizon 2015 Data Breach report. The lag only underscores the risk to organizations that don’t react nimbly to an incident. What constitutes a smart and thorough response? Continuous monitoring for anomalous activity to make sure the intruder is ejected, and a post-incident review of weaknesses in defenses, including updating and revising policies and controls.

- **Insufficient deletion of personal data.** PIN codes, passwords and answers to security questions often remain lodged in a computer if users don’t close out browsers or take other security steps. Vulnerabilities also crop up when personal data is on a disk or cached on line on a social network site. “Human frailty is the path into every targeted network,” said James Penrose, executive vice president of cybersecurity firm Darktrace.

- **Non-transparent policies, terms and conditions.** An organization’s polices may be outdated, inaccurate or incomplete; data processing may be insufficiently explained; and conditions may be so long and dense that users don’t read them.

---

**Top 5 Privacy Risks in Web Applications**

By: Taft Law

---

**Success Depends on Unique Ideas**

Taft’s attorneys focus on providing individualized, comprehensive legal strategies to meet our clients’ business goals.

---

**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.**

- $0 MRC Cross Connects
- Free Remote Hands
- SSAE 16 Compliant
- Carrier Neutral
- 2.5 MW Core Power

Call to schedule a tour of IO Ohio 1.866.628.3439 IO.com

---

Technology First | May 2016
Top 5 Reasons Why Backup is Not Disaster Recovery

By: US Signal

Today’s post was written by Jennifer Gill, Zerto’s Director of Product Marketing at Zerto.

Many organizations have a backup strategy but not a disaster recovery strategy, why? Because they think that if they have backup then they have a disaster recovery plan. Not quite. Here are 5 reasons why backup is not disaster recovery.

1. Service Levels – Low Recovery Point Objectives and Recovery Time Objectives

Backup products do not deliver recovery point objectives of seconds and recovery time objectives of minutes. Backups typically happen once per day and at night, so your recovery point objective could be 23 hours. If you are protecting a mission critical application, 23 hour data loss is not acceptable. Rebuilding a virtual machine, and everything that goes along with it, from tape can take days. If you are rebuilding from disk, it might be a little faster — a few hours. Again, this is not a service level that a mission critical application can tolerate.

2. Application Impact: Performance and Backup Window

There is a reason why backups occur at night — making a copy of an application and its data drains the CPU on the server. If you need more aggressive RPOs than 23 hours as stated above, that means you have to create copies more frequently. This is possible, but at the expense of CPU. This significantly impacts end-user productivity. Additionally, the backup window is a fixed period of time. As stated, this occurs overnight so most organizations assign 8 hours for a backup to complete. The application must be quiesced and then copied. As the applications grow and grow, quiescing the application and backing it up cannot be completed in the backup window.

(continued on page 13)
3. Retention
Backups are typically stored for a very long time for compliance and audit purposes. Disaster recovery information is stored for hours or days. Additionally, for a backup, you will have just one snapshot of the application and data. For an enterprise-class disaster recovery solution, you will have several points in time to failover to, just in case the last point in time is corrupted.

4. Automated Recovery
Building the environment from a backup, especially a tape backup, is extremely time consuming. This is why the recovery time objectives are so long. With an enterprise-class disaster recovery solution, the entire recovery process can be automated. The VMs on the protected site will automatically be shut down, and then the replicated VMs on the replication site will be started. Any re-IPing will happen to ensure end-users have fast access to the application and data. For mission critical applications, this entire process should take just a few minutes. This is a very different service level from a backup solution. Additionally, an automated process is a foolproof process, since every manual step that is introduced is an opportunity for an error. A disaster recovery strategy must eliminate as many opportunities for error as possible — automation accomplishes this and even verifies it through non-disruptive testing. It is critical that testing can be done without impacting the applications and data so that end-user productivity is not affected in anyway. Once the testing is complete, customers know that failover, recovery and failback will perform as the business requires.

5. Reverse Replication
Once an application is available on the replication site, end-users are using it, which is great. However, you must make sure that this application continues to be protected. A backup solution will not start taking backups and ship them back to the production site. A disaster recovery solution will ensure the replicated application is protected by replicating back to the source site.
Technology First would like to thank and recognize its Board of Directors. They provide input into the strategic direction of the organization and actively lead working committees that drive our programs and services.
Every year, cyber crimes cost companies more than $500 billion.

Applied Cybersecurity Training at Austin Landing

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

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

Train in Cyber Self-Defense! May 17

workforce.sinclair.edu • 937.512.2428

Sinclair Cyber Technology Center
Austin Landing
10100 Innovation Dr., Suite 310, Dayton

Scan with your smart phone to see a list of our upcoming classes.

SINCLAIR COLLEGE

workforce.sinclair.edu
Website Neglect

The Leading Cause of Missed Business Opportunities

Take advantage of the economical Managed Web Maintenance Programs from Bitstorm Web.

- Reduce your load times
- Improve security
- Maintain site upgrades
- Boost your content management
- Optimize search marketing
- Enhance ROI

Why go it alone when time is so limited? Partner with Bitstorm Web for effective web management services.

www.bitstormweb.com 937-438-3434 ext. 212 info@bitstormweb.com