AITS Newsletter

Did you know that the acronym RAID used to stand for Redundant Array of Inexpensive Disks, although now the acronym spells out Redundant Array of Independent Disks?

How to Update Your Computer's Operating System [By Chris Stoermer]

One big advantage of enterprise computing on campus is the power of IT. Between the distributed support teams and our System peers who host many of our security solutions, the managed workstations and laptops on campus stay reasonably secure. In fact, on most campus computers, you only need to log out, or shut down at the end of the day, to keep current with the automated update processes.

Many of these automated procedures will work off campus, as well, for mobile University-owned machines. You just need to be connected to the campus VPN to ensure your machine can talk to all the right systems.

Check with your support department for more specific steps to keep these computers secure and updated.

*Unfortunately, in most cases, this support level is not available at home on your personal computer, so how do you keep **your** computer secure and up to date? It's actually not very complicated on most of the newer operating systems. Let's take a look:*

Windows 7
1. Open the Control Panel and select **System and Security**.
2. Click **Windows Update**.
3. From here, you can check for updates and also review, or change, the Update settings.

Windows 8 & 8.1
1. Open the Control Panel and select **Windows Update**.
2. From here, you can check for updates and also review, or change, the Update settings.

Windows 10
Microsoft moved Windows Update from the ***Control Panel*** to the ***Settings App*** in Windows 10.
1. Open Settings and select **Update & Security**.
2. From here, you can check for updates and also review, or change, the Update settings.

Note: You can get other Microsoft Product updates (like Microsoft Office) through Windows Update too. Check the Update settings.

Apple OSX
Updating Apple's OSX is even more direct.
1. Click on the Apple in the upper-left of the menu bar
2. Select **Software Update...**

Note on Mac OSX: Depending on how many user profiles you have, there may be additional login requirements to the Apple Store for any single-user licensed software.

Remembering to log out, or shut down, at the end of the day, or manually checking your home computer regularly for updates, are two simple steps that will help keep your machine safer in the wide world of web.

Happy and Safer Surfing!

Computing has always been about the division of labor in that there are chips that do processing and others that perform the role of memory storage. Researchers in Singapore and Germany are working on a way to make a single chip perform the task of both processor and memory!

How secure is your password? [By Troy Bacon]

If you are using your pet's name, your child's name, or an easy pattern on a keyboard, then your password may not be secure.

Some of the most common passwords in use today are very simple... these include "passw0rd" (with a zero), "123456", "qwerty", "baseball", and "football"...

And I can assure you, that if you're using these as your passwords, you are at a great risk of being hacked... In fact, in the past few months, there have been several hacks into the email of high-profile people, and these hacks were possible because their passwords were too simple...

If you want to keep your accounts from being hacked, then I suggest you change your "passwords" into "passphrases". Passphrases are long strings of words, perhaps a complete sentence, where certain letters are capitalized and numbers are inserted.

Here is an example...

Take this sentence: *I'm looking forward to going to the beach!*

Converted to a secure passphrase: *IMl00king4ward2going2thebeach!*

Notice that I capitalized various letters, replaced the "oo" in "looking" with "00" (zeroes), and replaced words with numbers where it made sense. Also, the length of the passphrase is longer than most typical passwords, so it would be almost impossible for a hacker to try to guess the passphrase.

Passphrases are also easier to remember when compared to some random word.

If you choose to use passphrases to secure your online accounts, you'll be able to rest easy knowing your accounts are safe from hackers.

If you were to write out the year UNT was founded (1890) in binary it would be – 11101100010.

Two-factor Authentication [By Abraham John]

We all have personal email accounts that have, over time, gone from simple communication mechanisms with family and friends to repositories that channel and house very important and confidential information. Our personal email accounts have also become tied to our identities i.e. people recognize us electronically via our email address. Our email addresses also provide us with storage and apps that we use to manage documents, spreadsheets, presentations, pictures and the security needs for these range from the mundane to highly confidential. As a result, the need to control access and keep "the bad elements" out of our secure locations important.

When it comes to personal accounts, it falls on the **__individual__** to make choices and manage their personal accounts in a way that minimizes the risk of compromise. The traditional and standard way that we access out accounts is through the use of a user name (email address) and password. Passwords can range in complexity from the simple to complex. We have an article on passphrases vs. passwords in the release of the AITS newsletter that you may find illuminating.
Relying just on passwords leaves you open to compromise since most passwords tend to be relatively easy to guess or are open to brute force attacks.
This is where **two-factor authentication or 2FA** can be another tool that can be used to thwart the elements that want to compromise your accounts. So what is 2FA or two-factor authentication?

Two factor authentication adds a second layer before you can access your account. In other words the password is no longer sufficient. Two-factor authentication relies on something you know (password), something you have or something you are. Two-factor uses two of these and typically it will be something you know and something you have (phone where you can receive a call or text message with a code). If authentication uses something you are then it adds biometrics like fingerprint, voice, palm print, etc. into the mix as well.

While not strictly 2-FA, some accounts and services also provide a mechanism whereby you get a notification via email or other means when an account is accessed. This can be utilized as an early warning system if one of your accounts has been accessed without your knowledge or participation. Consider this another mechanism available to you in actively managing and securing your personal resources.

Given the extremely busy lives that we all have, you may be wondering why in the world you would want to add to the login steps and notifications which has the effect of adding to an already busy life. Unfortunately given the faceless, virtual world we currently inhabit, important and sometimes critical information ends up in locations that are in the "cloud" i.e. data centers and locations to which you have no physical access and to resources that can be "reached out and touched" at any time, by anyone and from anywhere. Since your specific resources are your responsibility, placing roadblocks and making it hard on the "bad elements" also is your responsibility.

Whether it is with your Google, Outlook (personal), Facebook and others, most consumer level systems offer two-factor authentication. I'll provide some breadcrumbs that'll lead you to the right locations for 3 of the common applications. Specific screen shots will be useless since interfaces change and it is better to know what 2-FA is and find it within your respective personal email and other accounts.

Google Mail
For Gmail two-factor authentication is referred to as **2-step verification** and once you login to your Gmail account you can find 2-step verification under "**Sign-in &**

security". Here you can turn-on 2-step verification and follow the wizard which will, at some point, ask you for a phone number where a code can be provided as a text message or via a call.

Outlook Mail (Personal – not work)

With Outlook (personal – not work) two-factor authentication can be found under **"View Account", "Security & privacy" and "More security settings"**. Follow the wizards and keep in mind, interfaces change but what you are looking for a secondary method of verification via text, call or email to a backup email account.

Facebook

Facebook calls their two-factor authentication "**Login Approvals**". You can find this under your security setting and look for Login Approvals. In addition to the standard code sent via text message to your cell phone, with Facebook you also have a few other options. Select the one that works best for you.
As with all security mechanisms, this does add a layer and step to your login process but it is well worth the trouble since it also makes it harder for the hackers to compromise your personal accounts.

Enjoy the added security feature of two-factor authentication (2-FA) and other features made available by these vendors and stay vigilant!

Did you know that the most prevalent networking standard in use today, TCPIP IPv4, has a maximum addresses space of 4,294,967,296 addresses?

Bionics - Not just for TV anymore [By Jason McMullen]

While conjuring up a very specific set of images, bionics are very broad and far reaching in their application. We might think of The Six Million Dollar Man (with shades of Dr. Evil for thinking that $6mil could buy all that tech) or some other science fiction.

The truth is, we've come much closer to those realities than one might think. But Bionics and it's close relative, Biomimetics, encompass a much wider scope.

Biomimetics is defined as any technology that mimics nature (biomimicry). Sonar and the like were developed through the observation of animals. And Velcro was designed from observation of plants (in this case, burs). The list of our uses for this technology is amazingly extensive.

Biomimicry can lead to better and more efficient ways of using energy, communicating, developing medicine, and many other discoveries. Nature has already performed the trials for us and developed incredible efficiencies.

To quote Ralph Waldo Emerson, 'When nature has work to be done, she creates a genius to do it."

But enough of that science stuff. What about super-human strength, seeing vast distances, or running 100 miles per hour?

Well, we are getting there. While we've seen many recent examples, I'd like to focus on two that I've recently researched: The bionic eye, and the bionic kidney. I know, not quite as awesome as throwing a car, but far more life changing.

The University of California Schools of Pharmacy and Medicine are close to developing an artificial kidney that works better than dialysis and requires no electrical power. The implant uses a combination of nanotechnology and biotechnology to mimic the various functions of the human kidney. To read more about this miraculous device, you can visit http://pharm.ucsf.edu/kidney.

And in Minnesota, a man with damaged photoreceptors in his eyes can see again. He has an microchip prosthesis implanted in the back of his eye that connects directly to the optic nerve.

The system works by capturing images of the world through a pair of glasses similar to Google glass. These glasses send the images to be processed by a computer that the man wears around his waist. The information is then wirelessly sent to the prosthesis.

The prosthesis enables the man to see share and outlines in black and white. As science continues to advance, his eyesight will improve. Imagine that, eyesight improving with age!

Visit mayoclinic.org and search 'bionic eye' to find some fascinating articles.

Unfortunately, bionics don't always benefit mankind. I had a few examples of this to give, but I seem to forgotten them. I'd better go Google it and get back to you*.

*Relying on technology to replace certain memory functions is not recommended.

The Emerging Enterprise Friendliness of Android
[Christopher Johnson]

For over a decade, technology industry insiders have touted the benefits of incorporating mobility into an organization's broader IT strategy. A widely-cited survey released in 2010 by wireless Internet provider iPass found that organizations could realize an annual productivity boost of nearly 240 hours per employee given a robust mobile strategy incorporating devices such as laptops and tablets along with remote access to corporate data. Following the release of its flagship smartphone the iPhone in 2007 and the iPad in 2009, Apple quickly surpassed Blackberry as the dominant provider of business-class mobile devices. While Apple has maintained a solid grip on the enterprise mobile hardware segment for nearly 10 years, Google has overtaken them as overall leader in number of mobile devices in service due to its lead in the consumer marketplace. Google's mobile platform, Android, is the most widely used operating system in the world, surpassing the iOS install base by nearly 3 to 1. Still, Google has struggled to make significant in-roads to the enterprise mobile device market. While the search giant has a great deal of ground to cover, two major developments in the last year show that Google is not ready to concede the enterprise market to their Cupertino rivals.

Google's Rich Communication Services Initiative

Late last year, Google announced a major push to expand adoption of the rich communication services (RCS) protocol for mobile messaging. RCS was introduced nearly a decade ago, but had largely fallen victim to the somewhat fractured Android ecosystem that developed as a result of Google's strategy to incorporate as many hardware partners as possible into their mobile platform. Many phone carriers developed text-messaging apps independently, using the older and less capable, but more broadly supported, SMS protocol to provide a minimalist message platform to allow their customers to easily exchange messages with people on other carrier networks. Business users, looking for a more robust feature set in their messaging apps, flocked to the iOS platform to use the far more advanced iMessage. Google's drive to expand adoption of RCS among its hardware partners and mobile carriers represents a direct challenge to iMessage dominance among business users. RCS will allow feature-rich communications between users, providing business users a way to exchange media and interactive content while integrating with business contact lists. RCS will allow group messaging and other forms of collaboration -- key features for business users and functionality that has been sorely missed in many carrier-developed messaging apps. As more partners sign up to support RCS, the Android platform will evolve to include many more such features that will greatly enhance its utility and favorability among business users.

Google for Work Rebranded as Google Cloud

In September of last year, Google rebranded its 'Google for Work' solution as Google Cloud and introduced more seamless integration with its G Suite of tools (formerly known as Google Apps) to create a comprehensive productivity platform aimed squarely at enterprises. With its Cloud platform, Google provides a convenient means to help businesses leverage local mobility to realize significant gains in productivity and exploit the flexibility and scalability of the cloud to maximize return on technology investment. Google's approach is to capitalize on consumer familiarity with its Android platform by providing enterprise IT professionals a robust set of tools to secure corporate data on Android devices, from phones to tablets to netbooks. With Cloud, Google offers a streamlined work environment for business users who are already comfortable using Android software at home. How much more

April 1, 1976 – Apple Computer was founded by Steve Jobs and Steve Wozniak. With a market cap of around 700+ billion, perhaps April 1st is not "fools" day or maybe it is, given how they've snookered Microsoft and have become a brand to envy!

productive might employees be if the lines between work and home are not only blurred by mobility but eliminated altogether by integration of work and personal data on a single Android device? Android users already have g-mail on their personal devices, and they're already using collaborative apps like Hangouts and Google Chat. If those same tools are brought into the business fold, Google hopes to enterprises will be able to capitalize more efficiently on those extra 240 a year that mobility affords every employee.

The Race to the Cloud Will Determine Who Wins the Enterprise Customer

Backed by the vast scale of Google's cloud presence, the Android platform might soon overtake iOS as the business platform of choice. Google continues to boost the security and business-oriented utility its apps, leaving Apple and others hard pressed to compete with the storage and collaborative functionality built right in to the Android OS. Combined with the security and device management features introduced with Google Cloud, Android becomes a formidable competitor to iOS in the enterprise.

Who first used the term cloud computing? Questions like these always lead to heated arguments and we are glad to have provided a topic for a meaningless exchange. It is likely that Eric Schmidt of Google used this term at a search engine strategies conference on August 9, 2006 but… feel free to have a good-natured discussion over a cup of hot chocolate!

OneDrive: The joy of sharing, made simple [By Aaron Powers]

These days everything is about sharing, especially in business. Quick communication of ideas and dissemination of data can help us improve processes and expand services. You probably already use something called a "File Share" within your department, to store information often crucial in keeping your department afloat. However, you may not be familiar with another tool already at your disposal, called OneDriveForBusiness. As an employee of UNT, you're given access to a really vast set of resources, collectively known as Office 365 (o365), and this includes cloud file storage for your individual business use. These files are accessible from a network connection anywhere in the world, they're backed up automatically, and they're managed by the same type of security we use for file storage here on campus. While this OneDrive storage might not be ideal as a final resting place for "departmental data", I think it should be considered as a replacement for your local computer desktops. Whatever you're working on, consider saving it to your OneDrive instead of your desktop, for all of the reasons mentioned above. There are even applications that help automatically sync data from local computers to your cloud storage, so with a little initial setup, you don't even have to consciously choose to save to your cloud space.

Ok, so now that you're thinking about all the things you can use OneDrive to store, I can show you how to share them with your colleagues!
* First, open up your web browser and go to onedrive.untsystem.edu.
* It should redirect you to our campus security portal, which currently look like this…
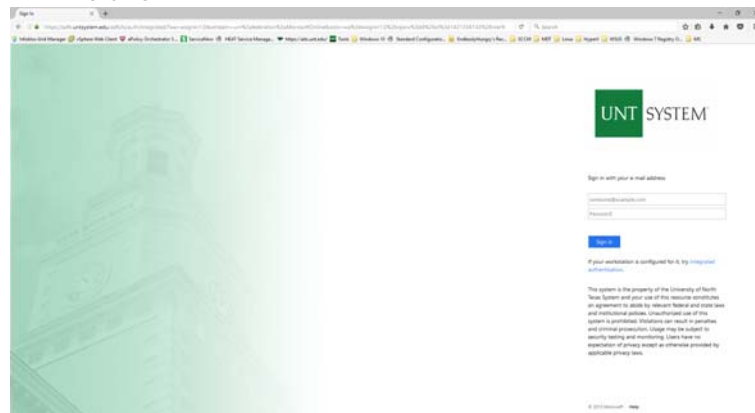
* Here, you sign in with your UPN (think email address), so probably First.Last@unt.edu.
* That should redirect you to the landing spot for your OneDrive, which might look something like this…
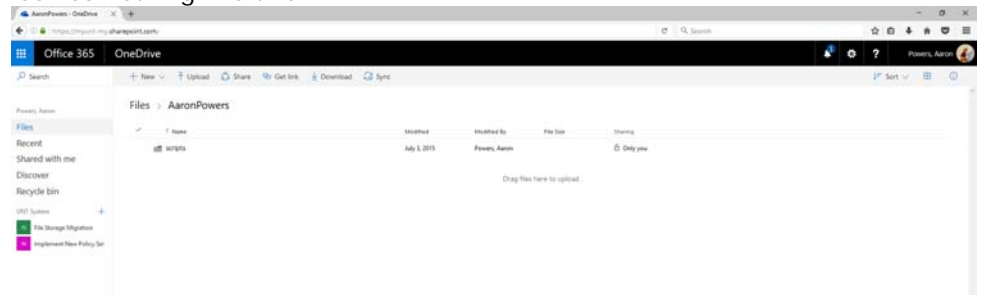
* The main frame is much like the file explorer you use on Windows, allowing you to view files, details, and navigate folders. If you look at the picture above, you see a folder named "scripts", and on the far right of the details there is a column named "Sharing". You can see that I'm not sharing my scripts with anyone, which is a shame since they are so helpful. Let's share
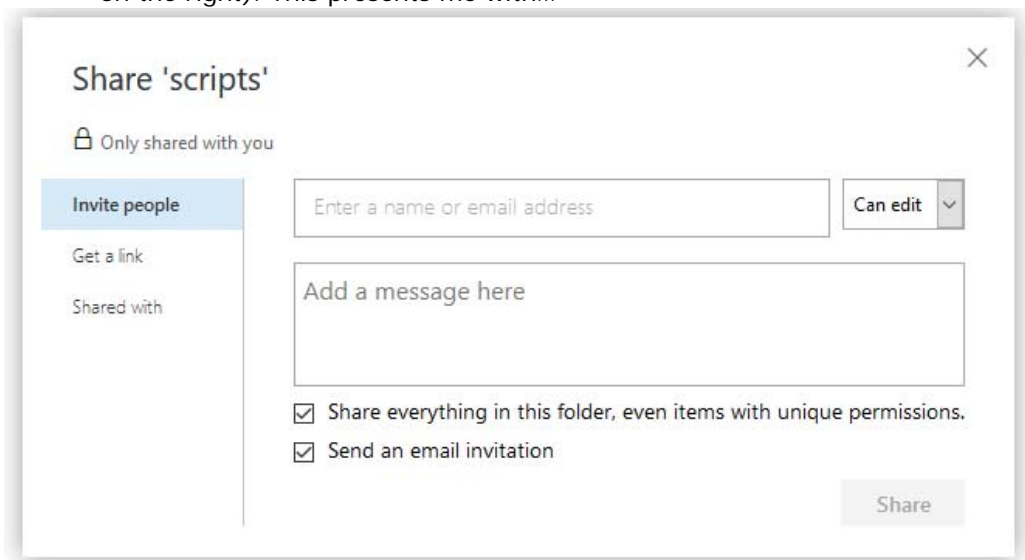
those with others, so I can save them some time doing their work!

- If I click on the "Only you" value under Sharing, it opens an information pane like this…
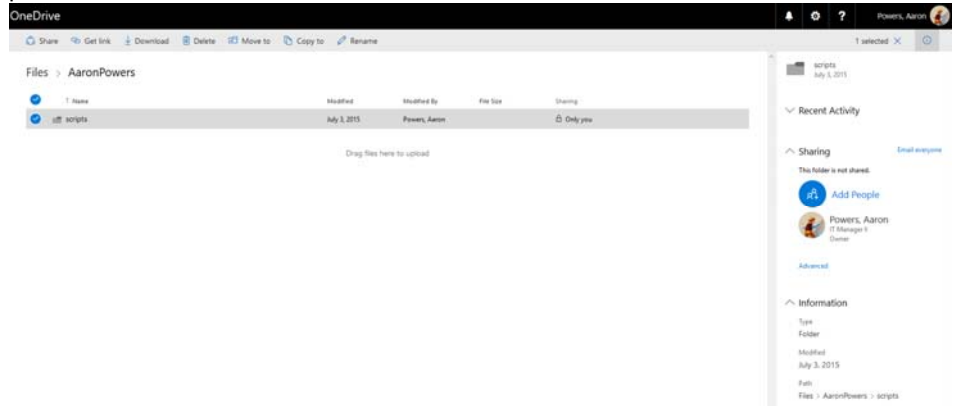
- Next, I can click on Add People (under Sharing, in the new information pane on the right). This presents me with…

- Now all I have to do is find a person to share with, choose a few details/settings, et voila!

I wouldn't be able to sleep at night, if I didn't mention that you need to be careful what you share with whom, so…YOU DO NEED TO BE CAREFUL WHAT YOU SHARE WITH WHOM. And keep in mind if you want them to be able to edit things, or just look around. You're able to remove Sharing permissions the same way, and you can always see whom you are sharing a particular resource with in that main view.

I hope this is useful in your collaboration efforts.

To Agile or Not to Agile... [By Dorothy Flores]

What is Agile? Well, it's the buzzword of the day in project management and software development, as well as service management. But, according to the Project Management Institute (www.PMI.org), "Agile approaches to project management aim for early, measureable ROI (Return on Investment) through defined, iterative delivery of project increments. They feature continuous involvement of the customer throughout the product development cycle."   Sounds a little stuffy for something that many think is all about going whichever the way the wind blows…no rules, no structure, no planning…

Nothing could be further from the truth. It certainly isn't the traditional "waterfall" method of project management for IT projects, but rigor abounds with this approach, when done correctly. However at its core, the Agile Manifesto states the following:

"Individuals and interactions over processes and tools.
Working software over comprehensive documentation.
Customer collaboration over contract negotiation.
Responding to change over following a plan."

The name "Agile" implies that it's quick and flexible, and it definitely has its benefits, but it isn't a silver bullet and it's not right for every project or every organization. Here is some basic information that may provide a bit of insight and aid in future decision-making for whether or not to use it.

Waterfall vs. Agile Methodology
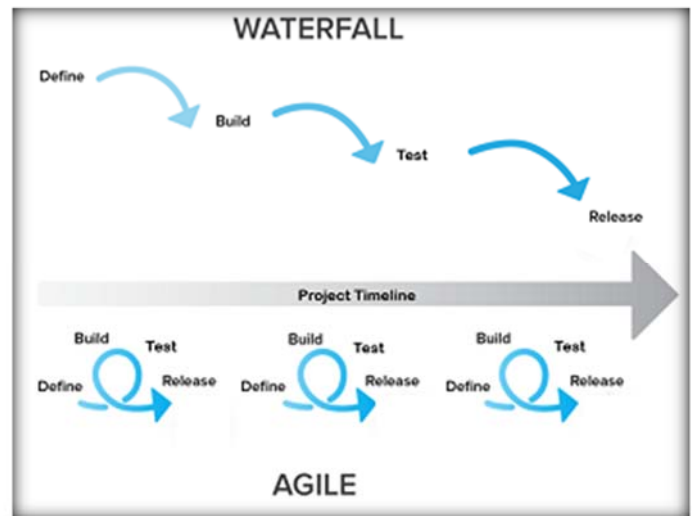
3 Common Myths about Agile:

1. You don't have to plan! FACT: You still have to plan; it's just done a little differently.
2. You don't have to document! FACT: You still need to document, but the primary focus is on people and outcomes of the work.
3. You're free to do it however you want because it's so flexible! FACT: There is plenty of structure, otherwise you'd never get anything done.

Top 10 Key Facts about Agile:

1. There is new terminology to learn, like…
   - Burn-down Chart – A graphical representation that shows the progress made during a sprint.
   - Scrum – A type of Agile project management used in software development.
   - Sprint – A 2-4 week increment of software development activities that delivers working software and the end of the iteration.
   - User Story – A high-level definition of requirements in business language describing what the users wants to achieve; generally "who," "what," and "why."
2. Agile can be used for large or small projects, and can scale just as any other method.
3. Project team (generally 4 to 8 members) should be completely dedicated to the project and co-located to enhance the ability to move and respond quickly.
4. Collaboration and partnership between IT and the users is critical.
5. Agile provides continuous delivery of features, instead a big-bang at the end.
6. Scrums do not alone make up an Agile implementation.
7. User stories are about the business needs and flow, and may not easily translate into the level of detail required for the purposes of developing the technology.
8. It's sometime difficult to describe what "done" really looks like for the project.
9. An Agile project can fail just as easily as one done using the waterfall method.
10. AND, it's important to keep it simple!

Don't build this … if all you need is this.

Thinking about using Agile? Here are some things to consider:

1. Get some training and engage with an expert in Agile, if possible.
2. Learn the terminology and be consistent in its use.
3. Educate the project team and especially users on what to expect in a project using Agile.
4. Stick to the core principles of Agile.
5. Start with a small project.
6. Communicate, communicate, communicate…of course, this is the case with any project!

If you want to learn more, check out these sites and videos:
- Agile Methodology and Scrum defined: http://agilemethodology.org/
- Agile in a Nutshell: http://www.agilenutshell.com/

*Want a good software engineering book that you can, probably, finish, before falling asleep – check out the "**Mythical Man-Month: Essays on Software Engineering**".*

- Scrum Alliance: https://www.scrumalliance.org/
- Project Management Institute: http://www.pmi.org/
- Videos Tutorial on Agile and Scrum – many more available:
  - http://www.youtube.com/watch?v=XU0llRItyFM
  - https://www.youtube.com/watch?v=DvBKevrItcc
  - https://www.youtube.com/watch?v=-zDct5d2smY

*If you are keen on picking up a Pulitzer prize winning book on computing then you may find **"The Soul of a New Machine" by Tracy Kidder** engrossing.*

What is Internal Audit? [By Mickie Tate]

Well, by definition per *Wikipedia, The Free Encyclopedia*, Internal Audit is an independent, objective assurance and consulting services agency designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes. Internal auditing is a catalyst for improving an organization's governance, risk management and management controls by providing insight and recommendations based on analyses and assessments of data and business processes. With commitment to integrity and accountability, internal auditing provides value to governing bodies and senior management as an objective source of independent advice.

So how do we see our role at the University of North Texas? Our primary focus is to provide excellent service to the UNT System. We are internal business partners here to help; we are here to be a part of the solution to help make the UNT System a better institution for all. We provide advisory, consulting and assurance services to all components of the UNT System. We strive to make improvements through process improvements, discovering control weaknesses and offering recommendations as to how to remediate any findings discovered. We accomplish this through annually developed audit plans but also leaving time available for management requests. We are committed to the highest degree of fairness, integrity, and ethical conduct in the performance of our mission.

Our Chief Audit Executive (CAE) reports to the Audit Committee of the Board of Regents. Internal Audit activities and audit reports are communicated by the CAE to the Board of Regents and all other applicable reporting entities including the State of Texas. This helps to maintain our independence. We adhere to the Code of Ethics as established by the Association of Certified Fraud Examiners (ACFE) and Institute of Internal Auditors (IIA). Furthermore, we will not issue a report without first allowing the recipient the opportunity to review, challenge, question, and respond to our findings and conclusions. Our relationships with the UNT community will be characterized by respect, helpfulness, sharing, patience, and openness. And although we are a part of UNTS, we are committed to maintaining our professionalism in providing UNT with independent and objective findings to make clear and well-informed decisions based on facts and the best information available. We believe that when the University systems are working efficiently and effectively, we all win together.

Information on the UNTS Internal Audit function can be found at http://www.untsystem.edu/service-teams/internal-audit.

"Information is a significant component of most organizations' competitive strategy either by the direct collection, management, and interpretation of business information or the retention of information for day-to-day business processing. Some of the more obvious results of IS failures include reputational damage, placing the organization at a competitive disadvantage, and contractual noncompliance. These impacts should not be underestimated." – **Institute of Internal Auditors**

Self-Driving Car [By Christopher Horiates]

We have reached a point in our world where we rely on technology to do many things for us that are rather basic or day to day tasks. While most of these items are fairly mundane some are more complex than others. AI and the technology that powers it has reached a point now where we have the self-driving cars. For or against it the technology is here and we as humans have a big decision ahead of us. Cruise control for vehicles have been used for many years now. They still rely on a human to do most of the work but it will keep a constant speed for you. There has even been self-parking cars out for a few years now. This is a basic low risk task. We have accident avoidance that will help stop your car so you can check that post on Facebook in stop and go rush hour traffic and not rear-end someone. The complete self-driving car however is still very new and while it seems to work there are too many questions we as humans need to ask ourselves and technological issues that still need to be addressed.

First the technological issues. Currently while the cars can drive themselves what safeguards are in place to handle variants such as weather, construction, new roads and such? The questions are how fast will accurate data get to the cars to tell them don't drive into that flash flood at night that's 4ft deep. Right now any rational person would stop and turn around, right? Would the car? Ice and pot holes are another issue. The cars currently seem to have issues discerning both and what to do so as not to hit that patch of ice or that major pothole that just showed up. What about construction and sudden lane changes? Look at the current work being done on I35 right now, the data to get all those variants loaded into the cars would take so much overhead and how does the programming get to them? Lane closures are another issue too. It's all about how we get that data to the cars in a real time manner or code the AI to be able to identify it in real time and adjust.

Now the human element. None of us want to ever be an accident. While self-driving cars might cut down on the accidents we get into at what cost does the come at? Will the cars be programmed to no matter what self-preservation is top priority? What about that time a kid runs into a street after a ball? Will the car decide do I swerve left or right and hit other cars or trees and kill my occupant, stop suddenly and get rear-ended by the car behind me killing the four occupants in it, or hitting the child will kill them and save my occupant along with the four behind me and only cause minor damage to my vehicle if any? While this might be an extreme example this instance will come at some point due to the human element and environmental variance outside the car. What would you do if you were in that situation? How then do we charge someone for a crime if they are not "driving the car" but the computer is? Is the developer or manufacturer of the vehicle held liable or is will it be just an unfortunate event with no punishment? We can't put a car in jail for simply doing what it was programmed to do.

While technology is great and can do many things for us we must decide how much control in our lives we want to give it. At what point do we stop becoming human if we rely too much on it? AI cannot, for now if ever, be programmed with emotions. It can simply be programmed to quickly take the best solution for self-preservation with no regard to human life for variances that it cannot be programmed for. We still have many issues to resolve and questions to ask. Until then it's not perfect technology but perhaps has a place in a very controlled environment.

"If a car parks itself you won't need as many parking garages." – **Joe Derhake, CEO, Partner Engineering and Science Inc.**