Taste of IT Keynote Speakers

IT Leader Spotlight
Examing Effectiveness: A Lesson From the Golden Goose

By: Jeff Van Fleet, Lighthouse

How can we be more effective in our relationships? Jeff Van Fleet, Lighthouse's CEO, thinks we should all take a lesson from Aesop's Golden Goose...

"Lately I have been thinking about how I can be more effective in my relationships with my wife and daughters, at work, in my community with the Lions Club, in my spirituality, and with my friends.

With all that I have on my plate, how can I stay in balance? How can I help those around me grow? How can I continue to drive high-quality results without burning out my team?"

I hope this message finds you well and enjoying your summer. Lately I have been thinking about how I can be more effective in my relationships with my wife and daughters, at work, in my community with the Lions Club, in my spirituality, and with my friends. With all that I have on my plate, how can I stay in balance? How can I help those around me grow? How can I continue to drive high-quality results without burning out my team?

It brought me back to one of my favorite books: Stephen Covey's 7 Habits of Highly Successful People. In the book, he talks about building a principle-centered approach to improving your effectiveness. Here's an excerpt:

Effectiveness Defined: The Seven Habits are habits of effectiveness. Because they are based on principles, they bring the maximum long-term beneficial results possible. They become the basis of a person's character, creating an empowering center of correct maps from which an individual can effectively solve problems, maximize opportunities, and continually learn and integrate other principles in an upward spiral of growth.

They are also habits of effectiveness because they are based on a paradigm of effectiveness that is in harmony with a natural law, a principle I call the "P/PC Balance," which many people break themselves against. This principle can be easily understood by remembering Aesop's fable of the goose and the golden egg.

The fable is the story of a poor farmer who one day discovers in the nest of his pet goose a glittering golden egg. At first, he thinks it must be some kind of trick. But as he starts to throw the egg aside, he has second thoughts and takes it in to be appraised instead.

The egg is pure gold! The farmer can't believe his good fortune. He becomes even more incredulous the following day when the experience is repeated. Day after day, he awakens to rush to the nest and find another golden egg. He becomes fabulously wealthy; it all seems too good to be true.

But with his increasing wealth comes greed and impatience. Unable to wait day after day for the golden eggs, the farmer decides he will kill the goose and get them all at once. But when he opens the goose, he finds it empty. There are no golden eggs—and now there is no way to get any more. The farmer has destroyed the goose that produced them.

I suggest that within this fable is a natural law, a principle—the basic definition of effectiveness. Most people see effectiveness from the golden egg paradigm: the more you produce, the more you do, the more effective you are. But as the story shows, true effectiveness is a function of two things: what is produced (the golden eggs) and the producing asset or capacity to produce (the goose).

If you adopt a pattern of life that focuses on golden eggs and neglects the goose, you will soon be without the asset that produces golden eggs. On the other hand, if you only take care of the goose with no aim toward the golden eggs, you soon won't have the wherewithal to feed yourself or the goose.

Effectiveness lies in the balance—what I call the P/PC Balance. P stands for production for desired results, the golden eggs. PC stands for production capability, the ability or asset that produces the golden eggs.

This really made me think about how well (or not so well) we're all keeping these factors in balance. Are we clear about what we're producing? Are we clear about how we're producing it? Can we repeat the results? How well are we taking care of our production capability? Are we investing enough in improvement activities to continue generating golden eggs? I'd love to hear if this relevant to you and what you are doing to continue delivering your golden eggs.

If you're interested in joining me on my self-improvement journey, I encourage you to purchase the book and read it. Even if you read it twenty years ago, I encourage you to read it again. It's just as relevant today.
EVENT SPOTLIGHT

Women for Technology

On September 6th, our Women 4 Technology group gathered at LexisNexis to hear from an amazing panel on the Past, Present, and Future of Empowering Women in Leadership. This event was a collaboration between Technology First, LexisNexis, PNC, and Synchrony women’s groups and brought together 170+ individuals.

Empowering Females in Leadership Panelists (L to R): Casey Moran, Pat McDonald, Lori Anello, Barbara Hogan, and Moderator Diana Tullio.

Shoes 4 the Shoeless was chosen as the Community Outreach beneficiary for this event. Together we donated $182 and a box of socks to the organization’s Sock Drive for school-age children.

Dayton Dragons

RoundTower Technologies (Technology First Annual Partner) treated IT Leaders in the community to a Family Night Out at the Dayton Dragon’s Game August 31st. Not only was this an enjoyable event for our Leaders, RoundTower and Nutanix donated $10 per attendee toward the Technology First Scholarship Fund. Incredible! Thank you RoundTower and Nutanix!

Families enjoyed dinner and drinks on the Dragon’s Lair deck overlooking the field. We even made it on the Jumbotron for Take Me Out to the Ball Game!

Technology First’s Kaitlin, Marcia, and Chair Jim Bradley posing with Gem! Go Dragons!
How to Legally Practice Social Engineering

By: Tim O’Connor, Cadre Information Security

Social Engineering is without question the most powerful and successful hacker skill of all time, but how can you become fluent enough in this skill to learn and defend against it if the practice is illegal?

If you want to learn a skill to protect yourself, your employees or your customers, you must be able practice that particular skill on the fly with real humans in real situations.

Social Engineering is like plying the art and skills of a con-man. However, isn’t that unethical and illegal?

There is a form of Social Engineering that is not only legal but often done for fun, profit and education. It is called “mentalism.”

The art and practice of mentalism is often associated with magicians but professional mentalists are often insulted by being called a magician. Magicians use “tricks” and ask their audiences to enter a state of suspended disbelief (you know the lady was not really sawn in half but it’s fun to wonder how it appeared so). The mentalist’s job, however, is to gain the confidence of the audience and make them believe that something real has taken place. Unlike magician’s tricks, mentalist routines are not guaranteed to work because humans have unpredictable reactions based on their biases so the mentalist must gracefully maneuver around unexpected situations.

All Social Engineering exploits conducted in person, remotely or through code are some variation of a con-artists game. The “con” stands for confidence. Mentalists control the behavior and perceptions of people by gaining their confidence and manipulating their biases. Do you see the similarities?

By learning the skills of a mentalist, we are directly practicing and honing the very same skills as the hacker. In a number of good Security Awareness classes, mentalism routines are used to demonstrate and test the students’ ability to identify and defuse Social Engineering attempts. Likewise, many of the skills used in penetration testing are identical to those used by performing mentalists.

So we have established that a mentalist is a hacker of humans that uses Social Engineering to ply the trade and that the skills needed in both cyber-crime and lawful Social are not only closely related but are often the same. Where do we go from here?

One way that you might want to dive into learning Social Engineering through mentalism is to read the book Social Engineering: The Art of Human Hacking by Christopher Hadnagy.

Another approach is to follow the works of famous mentalists that have donated some of their time and careers to exposing Social Engineering fraud such as The Amazing Randi or Penn & Teller productions. While these performers have exposed many con artists, I don’t know any that were using computers and technology hacks as we encounter them in IT. It is important to remember that while the tools used during Social Engineering in IT are technology-based, the routines, skills and human biases leveraged are exactly the same. Since much of the materials produced by these entertainment professionals is in the form of video, it can be a more amusing and an easy introduction to mentalism.

If you are convinced by this article to dive into mentalism and Social Engineering the best place to start is by reading Thirteen Steps to Mentalism by Tony Corinda. This collection of articles first codified the cold reading techniques and other skills used by con artists from the turn of the century. Alternatively you may consider the works by Banachek. Banachek, at 18 years of age, with oversight by James Randi, used Social Engineering skills to hack a $500,000 grant awarded to Washington University in St. Louis, Missouri for the establishment of the McDonnell Laboratory. He has written many books on mentalism useful to the Social Engineering practitioner such as Psychological Subtleties Vol. 1, Vol. 2 and Vol. 3, Psychophysiological Thought Reading, and Muscle Reading and the Ideomotor Response Revealed.

Once you have some basic routines down you can start to practice them on friends, fellow employees or even strangers in public places. Once you can read strangers on the spot, ad hoc in public you will have achieved the knowledge, skills and understanding to recognize and reverse engineer almost any Social Engineering attack you choose to analyze.

I hope that I have stimulated your interest in Social Engineering and its psychological underpinnings. Even if you do not decide to learn the arts of mentalism, I hope you will consider employing the most effective response to Social Engineering attacks, which is Security Awareness training. Security Awareness training does not turn your employees into mentalists but it does teach them to recognize cons, both those executed in person or through various technology. Security Awareness training is the best bang for the buck in cyber security and really the only way to stop attacks against the human element.
A Guide to Interconnection: How to Achieve Seamless Connectivity

By: Mike Fuhrman, Chief Product Officer at Flexential

As more organizations make the shift to a hybrid IT infrastructure, data is increasingly dispersed across various networks, often in different geographical locations. As a hybrid IT strategy becomes the norm for organizations, executives and IT decision makers must ensure that public, private and hybrid solutions are accessible to every business, partner, end user and customer. So the question becomes, how do you maintain a cohesive IT strategy among different networks and environments?

Enter interconnection. With seamless integration of your network infrastructures, organizations can ensure maximum uptime and complete IT availability for their business - no matter the data's location. Additionally, interconnection allows an organization to expand its local footprint without the need to move to other facilities as the business scales. In short, implementing efficient processes can allow organizations to focus on growth rather than constantly monitoring, managing and optimizing their network connectivity.

On the surface, interconnection can be complex and intimidating. But if you follow a few simple steps, secure, efficient and sustainable interconnection across your IT landscape can be achievable.

1. Connect All of The Moving Parts
This is one of the most important aspects of transitioning to hybrid IT, but it is also one of the trickiest. Your infrastructure likely has many moving parts and applications that rely on multiple data sets found in disparate locations. To have a successful migration, you must keep in mind that data and applications are intrinsically linked. It is critical that you understand how much each application consumes and produces before simply picking it up and moving it. To do this, companies should consider storing manageable amounts of data in an on-premise location with hyperscalers, or with a data center provider, allowing each application to properly connect to the correct data store. This way, its unique needs are accommodated for and your organization will be set to achieve an efficient and ultimately successful migration process.

2. Focus on the Long Term
When it comes to interconnection, it's not productive to get wrapped up in the "here and now." Always have the future of your workloads in mind. (Side note: This also rings true for enterprises looking to implement a disaster recovery plan or solution). It's critical to recognize your organization's plans to replicate IT processes with interconnection. You’ll also need to carefully consider compliance, your company’s downtime allowance and the most effective ways to store your most sensitive data. While the process can seem challenging and time-consuming, ensuring proper interconnection will, in-turn, allow you to put more time, energy and resources back into your organization. Keep your eye on the prize: a stable and secure IT environment.

3. Master Management and Monitoring
Once a solid interconnection framework is established and your data is sitting in different locations, make sure you set aside time for it to adapt to its new environment. Once you’ve been able to work out the kinks, retaining agile workloads is key to the success of your interconnection strategy. Maintaining agile workloads goes hand-in-hand with creating opportunities for open communication among your peers and colleagues. Discuss the goals you would like to achieve with interconnection and institute a routine for consistent and effective monitoring.

Without proper interconnection, you risk losing time, money and resources -- all of which make an organization's IT operations thrive. By developing a more well-rounded, cohesive approach to planning and executing an interconnection strategy, you are making a smart business investment toward the long-term success of your organization's most sensitive and critical data.

---

A Guide to Interconnection: How to Achieve Seamless Connectivity

By: Mike Fuhrman, Chief Product Officer at Flexential

1. Connect All of The Moving Parts
2. Focus on the Long Term
3. Master Management and Monitoring

---

Master of Information Systems
M.S. Logistics & Supply Chain Management
Unlock Your Career Potential with A Master’s Degree!
12-Month Program
1 Class at A Time
4 Weekends on Campus then All Online
Join us at the Taste Your Master’s event on Saturday, January 5, 2019
Receive program information, enjoy a free lunch, meet current students, and observe a class. Event is Free.

To Register Click Eventbrite bit.ly/TasteYourMasters
Zack Huhn is the Chief Executive Officer of Venture Smarter and Chairman of the Smart Regions Initiatives. His efforts have earned him recognition as a top 50 and top 51 global leader in smart cities two years in a row. Zack is active in standards development efforts within NIST and IEEE, policy development efforts in the United States Congress, and market development in cities and regions across the country. Zack is dedicated to accelerating the implementation of smart technologies, policies, and strategies that create better places to live, work, and visit. He underscores the importance of ensuring that everyone has equal access to the new opportunities created, not just those that can afford it. From defeating the digital divide to combating the heroin and opioid epidemic, Zack has been consistent in delivering a message that ‘smart solutions’ are about a lot more than shared mobility and automation.

In Washington DC, Zack helped stand up the Congressional Smart Cities Caucus where the focus is to empower communities of all sizes to realize smart city success stories. At home, Zack helped to form ‘Smart Cincy’, which was the first Regional Smart Cities Initiative in the United States. This year, the Smart Regions effort, modeled after lessons learned from Smart Cincy, scaled nationally with the launch of the 2018 Smart Infrastructure Challenge. Regions from across the country submitted 80 project proposals competing for access to more than $50 million in project financing, funding, and other support resources. The teams include multi-jurisdictional collaborators throughout urban, suburban, and rural cores. Projects fit within at least one of four categories: smart and connected development, smarter and safer streets, critical infrastructure, and next-generation infrastructure. Teams will be presenting their projects at the Second Annual Smart Regions Conference on October 25th and 26th in Columbus, OH.

Areas of Coverage: • Emerging Trends & Technologies, Roles and Responsibilities
David Cearley is a Vice President and Gartner Fellow in Gartner Research and is a leading authority on information technology. As a member of Gartner Research, Mr. Cearley analyzes emerging and strategic business and technology trends and explores how these trends shape the way individuals and companies derive value from technology. As a member of the Enterprise Architecture & Technology Innovation research group, he focuses on cloud computing, emerging and strategic technology trends, and how enterprises establish technology innovation programs.

Background: Previous Experience - Mr. Cearley’s expertise spans software architectures and standards, component software models, application design, the internet, business-IT alignment, and the IT services market. He has worked with a wide range of end-user and vendor organizations assisting in strategy creation, technology selection, implementation planning and organizational development. Prior to joining Gartner, Mr. Cearley held various senior-level research positions at Meta Group. Before that, he was vice president of R&D for Revelation Technologies, served as program director at Gartner Group, and held various managerial/director-level positions at Innovative Software and Informix.

Professional Background: • Informix, Director, Product Management, 8 years • Meta Group, Senior Vice President & Principal Analyst, 12 years • Revelation Technologies, Vice President, Research & Development, 2 years

Education: B.S., Finance and Economics, Rockhurst University

Industry Awards/Accolades: Gartner Fellow
Backups are an Essential Aspect of your Organization’s Cyber Security Protection

David Owens, Vice President of Sales and Marketing, FSN

Reliable and restorable backups are one of the fundamental foundations provided by IT personnel. Ensuring business continuity and the integrity of your data, including your customers’ sensitive information, is paramount in today’s digital age.

Traditionally, backups have been deployed as an insurance practice for when things go wrong in terms of hardware failures or disaster recovery events, including building fires or other natural occurrences, like floods and tornadoes.

In today’s era of prevalent cyber security threats, backups are equally important for restoring data as a result of a cyber-attack, where your data gets encrypted then held for ransom by criminal elements.

According to Cybersecurity Ventures, cybercrime damage costs are expected to hit $6 trillion annually by 2021. Cybercrime has become the most insidious and destructive threat that businesses and organizations of all types face today.

While it was once thought that cyber threats were only a concern for major corporations and other large businesses, hackers are now frequently targeting small and middle-market organizations.

- 43% of cyber-attacks target businesses with less than 100 employees
- Over 90% of cyber-attacks start with a phishing email

Cyber criminals are working hard to find ways to breach your security. You need to do all you can to protect your business and your customer data. Among the data security defense tools in your arsenal are reliable and restorable backups.

If companies don’t have the ability to restore data from a backup job prior to the phishing event that encrypts your data – then paying the ransom to the cyber criminals might be the only recourse. Besides being a costly endeavor, your data might not be restored, as there is no honor among thieves.

The more data that is lost or compromised, the greater the negative business impact. Clients might lose faith in your ability to safely deliver products and services, either resulting in lost revenue or liability that could ultimately end in bankruptcy.

Part of a good backup protocol is being able to restore business operations to the condition it was in before your data and software applications were encrypted by the cyber criminals.

Below is the best practice 3-2-1-0 backup strategy:

1: Consider when a catastrophe occurs at your primary data center, whether on-premises or hosted in a private cloud, if all your data is in one place then you are at risk of losing all your critical business data.

For your offsite disaster recovery copy, the hardware storing your secondary copy should be in a physically distant data center.

2: Verify your recovery plan has zero errors. It is not uncommon for organizations to deploy a data recovery plan but fail to validate that it performs as required. Daily monitoring of successful backup jobs and regularly scheduled recovery testing are essential to ensure if you lose data, either to an unexpected event or a criminal act, your organization can be operational in a nominal amount of time.

Regarding your backup solution, two other aspects to consider include having an image based backup vs. file level backup to improve your Recovery Time Objective (RTO). Determine the Recovery Point Objective (RPO) of how often incremental snapshots should occur, with the goal of keeping a full backup for restoration, in case of a cyber security episode.

In case of an incident where you need to restore a backup due to a hardware failure, having the entire server or PC image backup will allow recovery in a significantly lesser period of time vs. individually installing operating system functions, the software applications, and then the numerous files. RTO is important to critical business functions, where hours of downtime vs. days widely impacts your business operations.

Further, the frequency of the backup and the total retention time need to be determined based on specific business needs. Part of this decision is the financial calculation of the total amount of storage investment for both local and offsite backups necessary to accomplish the defined RPO.

For the local backup target, we recommend a Network Attached Storage (NAS) appliance as a cost-effective storage solution – independent of your active production data on either your server or a storage area network (SAN) under a high-availability configuration.

3: Maintain at least three copies of your data. One active production copy of your software application running on your server platform (either on-premises, hosted or co-located) and two backup jobs. The first backup job is local for quick file restores, when a user accidentally deletes a file. The second copy is located at a different geographical location in case of a disaster recovery scenario.

2: Store your backups on two different hardware platforms. One reason for this is to avoid your backup targets processing the same vulnerabilities. Backups jobs should never be susceptible to the same point of failure. As an example, hard drives on the same computing platform could be corrupted by the same virus or hardware failure. By leveraging different hardware platforms, you can reduce your exposure to the same incident on your backups jobs.
1. **What was your first job?**

My first job earning money was a paperboy delivering the Dayton Daily News, however my first Data Processing job was keypunch operator in the morning and 402 operator in the afternoon. After doing poorly as a freshman at Wright State attending with all my high school friends I decided to seek full time employment and attend school full time at night. I fortunately found a job in my field of study, it just happen to be using some relatively old technology, punched cards, sorters and tabulating equipment.

2. **Did you always want to work in IT?**

Actually was opposed to Data Processing, because that is what my Father did. All through high school I wanted to be an Architect, studying drafting and Architectural drawing, up until my Senior year when I signed up to take a programming course in Basic. I enjoyed the class so much I decided that I didn't want to go through all the extra years of college and have to get licensed when I could have a lot more fun working with computers.

3. **Tell us about your career path.**

As I mentioned I got started in operations punching cards and operating the system, but my career probably started much earlier in life, given my Father was in Data Processing, as it was called back then. When I was 6 years old, I could remember going into work with my Dad on a Saturday and playing tic tac toe against the computer by feeding in my move with a punched card. The computer would print a new page with my move and the computer's move printed on it and ask for my next move. The program couldn't be beat. You could tie it, but never win. Jumping back to my career, I learned to program the 402 by wiring the program boards. I moved on from there to Computer Operator on what I thought was a huge step forward in technology, running a IBM 370/125 for the Peter Kuntz Company. Still processing cards and storing data on large disk platers that reminded me of the Star Trek Enterprise spaceship body. I finished my Bachelor of Science in Computer Science from Wright State University. With degree in hand I changed jobs when I got a chance to program COBOL and then got a call from Good Samaritan Hospital for a programming position, programming in COBOL on the same IBM 370/125 that I used to operate on. Peter Kuntz leased computer time on Good Samaritan's computer during an off shift. While at Good Samaritan, I moved up the career ladder to Programmer Analyst and got the chance to supervise a new programmer as the department grew. I changed gears for a while and became the Systems Programmer, handling all the operating system configurations and changes along with debugging the problems that took a deeper dive into what was going on. I gained more responsibilities and had more staff reporting to me and moved up to a Project Leader. I went back to UD to earn my MBA, to further my career in management and later became the MIS Director at Good Samaritan Hospital. Feeling like I had reached a plateau at Good Samaritan, I ventured into the manufacturing industry as a Director at a small company in Monroe, OH. Due to an acquisition, I moved back into healthcare as the Director of IS at Middletown Regional Hospital. After several years, the Vice President of Systems at The Cincinnati Enquirer opened up and I was selected. Being a part of a large for-profit, quarterly driven, organization of Gannett, taught me that I was much more comfortable in a smaller organization. Middletown Regional Hospital called me back and it was an offer that I couldn't refuse even if it meant losing my VP title. Middletown Regional Hospital became Atrium Medical Center and joined Premier Health and I was back in a much larger organization, again. The opening at Graceworks Lutheran Services opened up and the opportunity to be in an organization that was the right size for me was too good to pass up. And here I am, within a few years of retirement!

4. **What advice would you give to aspiring IT leaders?**

Integrity, perform your job with integrity. You'll earn the respect of those that work for you and those that you work for. For me integrity is knowing your business, business being the IT side and the business your company is in, knowing it well enough that you can match up the right technology for the right purpose. And then not overselling the technology or your team or yourself, but providing realistic expectations, goals and timeframes. And finally making it happen, achieve what you said and set out to achieve. That would be living out integrity in the IT world. No hype, no smoke and mirrors, no vaporware. And the second piece of advice would be to surround yourself with people that are smarter and better than you are. Build your team to compliment your weaknesses and accentuate you strengths.

5. **What has been your greatest career achievement?**

I like to think that even though I have come and gone from several organizations I never left on bad terms, tried not to burn a bridge, remained in contact with and on good terms with the people I worked for and worked with, even after leaving, which hopefully speaks to my integrity. From a project perspective, I like to think that implementing an Electronic Health Record system at Middletown Regional Hospital early on was one of my career highlights. Hearing the nurses claim they would quit before using a computer and then afterwards complain when you had to take the system down for maintenance because they couldn't work without it was rewarding. The experience repeated itself when I came to Graceworks Lutheran Services as I got the opportunity to assist in leading a long-term care organization through the same process. The other project that was personally satisfying to me was the design and building of the technology in Atrium Medical Center. It appealed to my technology passion at the same time appealed to my high school training in Architecture.

6. **Looking back with 20:20 hindsight, what would you have done differently?**

I don't know that I would have done anything differently. I have often looked back and thought what if I'd stayed here, or there. Would things have been different, and I am sure they would have. I lost a lot of perks and opportunities when I stepped down from The Cincinnati Enquirer position for example, but it was the right decision for me personally, especially at that time in my life.
IT LEADER SPOTLIGHT

JD Whitlock - Dayton Childrens

CIO

1. **What was your first job?**
   Paperboy when I was 13. Woke up at 6am in blizzards in upstate NY to deliver your morning paper on my bicycle. Went through a lot of rusted out bicycles. And I put the newspaper inside your storm door, didn’t just throw it in the bushes from the sidewalk. Customer service!

2. **Tell us about your career path.**
   Started out in the Navy driving ships around the Pacific and Middle East and Caribbean, then switched to healthcare administration in the Air Force, and got into healthcare IT from there.

3. **What are the CEO’s top priorities for you in the coming year? How do you plan to support the business with IT?**
   We have a crack team of visionary Execs, the entire C-suite, that push hard on IT to deliver transformative capabilities for our providers, nurses, patients, and of course in our special case as a children’s hospital, the families of our patients. Dayton Children’s has had significant growth in the last couple years (new patient tower with a lot of new IT capability) so the focus this year in IT is on a better support model for the wide variety of new applications added in the last couple years, while still doing a double-upgrade to our Epic electronic health record (EHR) in November, and a significant expansion of our WorkDay ERP into supply chain in the spring. Also tossing in a transition to O365 and several other new clinical applications just for fun. My Air Force analogy for this year is that we are easing off the supersonic afterburner (we don’t build new patient towers every year) and now we need to keep cruising at 500mph and innovating while implementing a better support model for all the applications we added recently.

4. **What advice would you give to aspiring IT leaders?**
   One of the many great things about working in IT is that there are both supervisory and individual contributor paths to career progression, a bigger paycheck, and hopefully some simultaneous net positive effect on the universe. Let’s face it, the personality characteristics that make great geeks do not always also make good bosses. We all know IT leaders that got promoted because they were smart and stuck around, but probably should have focused on honing their coding skills in a dark room rather than trying to supervise other human beings. So take a deep breath and ask yourself where your strengths lie. If you want to be a leader of people in addition to a leader of technology, great, go get an MBA, and realize you may need to switch employers a few times to find the right progression of supervisory roles. On the other hand, if you are a super-geek, embrace that, and go deep with data science or cybersecurity or whatever floats your boat. That is one of the many awesome things about working in IT – you can make a good living as an individual contributor. Of course if you want to make more coin as an individual contributor you have to be smart about where the technology AND industry are headed. Don’t bother getting smart on something that AI will do well in 5 years. I am available for career counseling on this topic for the small price of buying me a beer at Lock 27 or an Old Fashioned at The Century Bar after work. Just look me up on LinkedIn.
As cryptocurrencies are still a relatively new introduction to the world, concerns about security introduce a degree of risk into this payment system. Cybercriminals are working relentlessly to find ways to take advantage of this new technology and exploit cryptocurrencies for their own financial gain and to access and acquire the data flowing through this newer payment system. For this reason, you might be thinking, “is cryptocurrency safe?” And, “what can I do to protect my investment?”

Since the introduction of Bitcoin in 2009, which is generally considered the first decentralized cryptocurrency, over 4,000 variations of cryptocurrency have been created worldwide. Bitcoin itself has never been compromised to date, so the coins themselves and the Bitcoin alternatives are considered safe and secure. However, cryptocurrency exchanges have been hacked and individuals’ accounts have been compromised – resulting in hundreds of millions of dollars in cryptocurrency being stolen.

Phishing, malware and ransomware are common tactics used by cybercriminals to mine for cryptocurrency. These tactics exploit vulnerabilities in the exchanges, access cryptocurrency wallets and exploit third-parties that are connected to this payment system.

There are four ways to protect your cryptocurrency investment and enhance security by using features built into the currencies or the networks they run on.

1. **Avoid Cryptocurrency Scams**
   
   There are currently over 1,000 Active Cryptocurrencies on the market, and many come and go each month. Some of these are nothing more than just an online Bitcoin scam used as a way to pilfer coins from unsuspecting investors.

   One of the common ways fraudsters scam cryptocurrency users is by advertising a new coin and building up interest. Next, they offer an initial coin offering (ICO). Before users notice something has gone wrong, the fraudsters have pocketed the cryptocurrencies, and the site and the coin have vanished. Because of these scams, a great deal of research should be done to find a currency with a solid background.

2. **Secure Crypto Wallets**

   When investing or applying cryptocurrencies for use, it is necessary to store cryptocurrencies in a secure wallet.

   Although there are hot wallets which are ideal for usability, hot wallets can be hacked. Cold wallets are the most secure.

   There are two types of cold storage wallets to choose from: paper and hardware. A paper wallet may be one of the simplest, but your keys are printed to paper, which is not the safest medium.

   The hardware wallet, which is much the same as a USB drive, is the more secure cold storage option. Not only is it more secure, it can also support many varying types of cryptocurrency. A prime example of the best is the Trezor hardware wallet. This comes with 2-factor authentication, and password manager – should the device be damaged, lost or stolen.

3. **Cryptocurrency Exchange Theft**

   Cryptocurrency exchanges exist around the globe, though many of these are not the ideal places to leave your coins. When looking at which cryptocurrency to invest in, the chosen must be considered.

   Up until recently, Mt. Gox was the most well-known exchange to be hacked. Over $450 million worth of Bitcoin was stolen from their Hot Wallet over a period of time. This shows how crucial it is to conduct due diligence on the exchange, and never leave your coins in any one exchange for any length of time.

4. **How Crypto Coins Help Secure Your Investment**

Many security weaknesses and fraudulent breaches happen at the exchange level, the wallet level, or other third-party level. Many cryptocurrencies
themselves aim to make their own security tighter to help protect your investment, including:

**Dash** - With the peer-to-peer network and the 4,500 plus nodes, Dash utilizes 200 TerraHash of X11 ASIC of processing power to confirm transactions.

The miners are rewarded for securing the network while validating, storing and distributing the Blockchain to users.

The master-node of servers form Quorums to enhance privacy and governance while eliminating threats of low-cost network attacks.

**Monero** - This coin enforces security by not re-using addresses. Ring signatures allow private transactions as any user on the ring can be a sender or receiver of a transaction.

Monero also uses CryptoNight as their proof-of-work algorithm which was designed to reduce the gap in performance between GPU and CPU mining.

Compared to BTC, the block-time is reduced to 2 minutes rather than 10.

A crypto wallet for this crypto also uses mnemonic seeds. Here you are given a list of 25 words which are the only ones that can be used to restore a wallet.

**IOTA** - This coin uses what they call the TANGLE which is a blockless distributed ledger. When the IOTA network has more users, and the number of transactions is increased the more efficient and secure the Tangle becomes.

**Skycoin** - The wonder of the pack is Skycoin, as it totally decouples any of its coins from the mining process.

As a way of doing this, they use their new Obelisk algorithm that rids the need for POW and POS in transactions. A web of trust is created, and decisions are decided upon through network consensus.

The network it runs on is called Skywire. Skywire is built with nodes, so there is no one point of failure. Data is broken into chunks so only the application and the P2P network knows where it is.

Using a proven and reliable exchange, a secure network and a coin like Bitcoin (or another that mitigates flaws by using Blockchain), you can conduct business with cryptocurrency while knowing that your investment is safe.
Upcoming Events

Register today at: www.technologyfirst.org

**Data Analytics - Special Interest Group**

"R vs Python"
- Friday, October 5th; 8:30 - 10:00 am
- Business Solutions Center
- 1435 Cincinnati Street, Suite 300
- Dayton, Ohio 45417

**Infrastructure/Cloud - Special Interest Group**

"Disaster Recovery aaS"
- Friday, October 5th; 11:30 - 1:00 pm
- Business Solutions Center
- 1435 Cincinnati Street, Suite 300
- Dayton, Ohio 45417

**Tech Forum (Open to Everyone)**

“The Moneyball CIO – Learning the Science of IT Decision Making”
- Thursday, October 11th; 11:30 – 1:00 pm
- Business Solutions Center
- 1435 Cincinnati Street, Suite 300
- Dayton, Ohio 45417

**Data Analytics - Special Interest Group**

TBD
- Friday, December 7th; 8:30 - 10:00 am
- Business Solutions Center
- 1435 Cincinnati Street, Suite 300
- Dayton, Ohio 45417

**Infrastructure/Cloud - Special Interest Group**

"Penetration Testing"
- Friday, December 7th; 11:30 - 1:00 pm
- Business Solutions Center
- 1435 Cincinnati Street, Suite 300
- Dayton, Ohio 45417

**Municipality IT - Special Interest Group**

"Public-Private Partnerships"
- Thursday, December 13th; 11:30 – 1:00 pm
- Business Solutions Center
- 1435 Cincinnati Street, Suite 300
- Dayton, Ohio 45417

---

Announcing the 16th Annual Ohio Information Security Conference
March 13, 2019 | Dayton, Ohio

**Call for Papers – Submissions OPEN**
Call for Papers – Submissions OPEN
Proposals are due by November 9, 2018

Technology First is seeking proposals for speaker participation in the 2019 Ohio Information Security Conference. A session can be a formal presentation of a successful implementation, administrative solution, or technical solution. Topic content must focus on information security and may range from introductory to advanced or from operational to strategic.

[ surveymonkey.com/r/OISC19CallForPresentations ](http://surveymonkey.com/r/OISC19CallForPresentations)
People are at the heart of every successful business initiative. At TEKsystems, a leading provider of IT staffing and IT services, we understand people. Every year we deploy over 80,000 IT professionals at 6,000 client sites across North America, Europe and Asia. Our deep insights into the IT labor market enable us to help clients achieve their business goals while optimizing their IT workforce strategies.
Did you know that as part of your Technology First Membership you can post job openings on our website? Select “Find A Job” on the Employment Tab at www.technologyfirst.org.

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.

Marcia Albers  
Executive Director  
Technology First

Diana Bolden  
Former CIO  
Teradata

Jim Bradley - CHAIR  
Global IT Vice President  
Tecomet

Gary Codeluppi  
Regional VP  
Remote Dba Experts

Doug Couch  
Vice President, Information Technology Services  
Speedway

Tim Ewart  
Technical Director and Chief Technology Officer  
Air, Space and Cyberspace HQ  
Air Force Materiel Command, WPAFB

Lisa Heckler  
Vice President and Chief Information Security Officer  
CareSource

Treg Gilstorf  
Senior Director of IT  
Yaskawa Motoman

Gary Ginter  
System Vice President, CIO  
Premier Health

Bryan J. Hogan  
President / CEO  
Afidence

John Huelsman  
Director of Business Support Solutions  
Hobart Service

Tim Hull  
Director, Bitstorm Connect Think Patented

Scott McCollum  
Chief Information Officer  
Sinclair Community College

Monique McGlinch  
VP, Information Technology & Project Management Office  
MidMark Corporation

Dave Mezera  
President  
DataYard

Paul Moorman  
Former IT Strategist  
ND Paper

Shu Schiller  
Associate Professor and Chair Information Systems and Operations Management  
Wright State University

Thomas Skill  
Associate Provost & CIO  
University of Dayton

Diana Tullio  
Principal, North America  
CC&C Americas

Jeff Van Fleet  
President  
Lighthouse Technologies

Writers: Our mission is to support the growth of Greater Dayton’s information technology industry. Technology First provides a forum for educators, business, and technical professionals to communicate their expertise and lessons learned while working in the field. Please submit the article in Word, preferably with 500 to 700 words, with any graphics in pdf to malbers@technologyfirst.org. Please include your name, business organization, business address, phone number, fax number, e-mail address, and a brief description of any professional accomplishments. Please also include a digital photograph if available.

Subscriptions: Non-member business/home delivery of this publication is available at $120/year (11 issues). Mail name, address and check made payable to Technology First.
Take control of your data security.
workforce.sinclair.edu
937.512.2428

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

Applied Cybersecurity Training at Austin Landing

Focusing on the need for training in cybersecurity, 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

SINCLAIR
CYBER TECHNOLOGY CENTER
workforce.sinclair.edu
Are you generating high web traffic but low conversion rates? You need to increase income, not just statistics. Contact Bitstorm Connect for a free analysis of the situation.