ISM ORIGINAL WORK DOCUMENTATION

MANAV SOOD, AKASH BASKARAN

Below, are all the articles, publications, and documents used in the development and creation of our revision of the IoT Security Improvement Act.

Technative, 8 Ways IoT & AI are Impacting Financial Services
https://www.technative.io/8-ways-iot-ai-are-impacting-financial-services/

AI & IoT are already having a huge impact in financial services
Artificial intelligence has been around for quite a while now but both interest and development in the field have increased exponentially in the past decade. Computational costs have decreased allowing for more and more powerful computers being made. These machines do not lack the hardware and processing power to correctly perform intelligent decisions based on collected data.

Artificial intelligence is the future, revolutionizing our lifestyle and the way we do even the simplest of tasks. At the same time, IoT is gaining popularity rapidly and it will inevitably come to rely on artificial intelligence. The data collected through the interlinking of all computational devices around us is too vast for manipulation by humans but is easily comprehended and evaluated by a computer to make the best use of it. Both these phenomena are set to shape and change the future by impacting not only our lives but also every industry vertical. One in partcular that is likely to benefit massively is financial services.

The Internet of Things is no longer just a concept. Manufacturers have released products designed to work with each other and are also working on interoperability between devices from different vendors because only then will a smooth and useful experience be provided to the user. These intelligent devices will integrate seamlessly into our lifestyle and their interconnection with each other is what will

make them have a huge impact on our financial lives. Insurance, healthcare, and banking will benefit the most from this and provide better and more options for using IoT with advanced financial products and services.

Personalized Financial Services
Automated financial advisors make use of AI to assist the user in handling and making decisions related to their financial issues. These roboadvisors monitor the user's financial goals and stock prices to offer suggestions on which stocks or bonds to buy or sell. AI applications installed and working in user devices analyze huge amounts of data to offer relevant financial advice and forecasts.

Smart wallets use AI to learn user's habits and needs and warn them about their expenditures so they can practice restraint.

Healthcare
Smart devices are in use today that monitor all aspects of a person's health. With the evolution of IoT, these devices will only become more intelligent and able. Monitoring data from these devices will allow for monitoring the user's health and act in situations where intervention may be necessary. This process will also allow health insurance companies to be better prepared in advance and prevent and cure diseases at an early stage before they become chronic. Not only will this lead to reduced costs for both patients and the healthcare companies it will also help dynamic pricing in insurance premiums based on the record of a person's health and fitness.

Car Insurance
Internet of Things will allow insurance companies to monitor drivers and their vehicles to record miles driven, driver habits, changes in speed and the time of the day they drive to calculate and assess risk levels. This will deliver better premium rates for users who drive well.

Home Insurance
Even today home insurance companies are encouraging customers to install devices that monitor their property by providing incentives. Intelligent tracking devices can be used to warn of potential danger, track water leaks, carbon monoxide levels, and smoke to detect and warn in case of a fire. Analytics based on IoT data can be used to predict future events like weather patterns in a certain geographical

area. Insurance companies are also employing drones to assess the amount of damage in the case of an incident. All this will allow for better pricing for both service providers and consumers.

IoT in Banking
Customers will be able to make transactions and inquiries using different devices. Banks will be able to collect information and monitor behavior patterns to provide better and sound financial advice and services.

These are just some of the aspects of our financial lives affected by IoT. Use of sensors and data from IoT devices will allow banks to provide more personalized banking and financial services. For example, banks can monitor a user's business and its growth to ensure the loan is returned on time. All this data from thousands of customers coming into the bank's system is impossible to be managed by humans however and cannot be put to meaningful use without employing serious computational power to deduce and predict behaviors and trends. For this purpose, computers will organize and collect this data and employ artificial intelligence to make the most of it. The Internet of Things cannot offer its maximum benefits without artificial intelligence.

The decrease in computational and data storage costs have made making AI systems and applications more practical. With computers being a major part of our lives, we are today making the most of the mobile devices, wearables, and the Internet. The data from our use of all these devices can be used by AI programs so they can operate at the maximum performance level. AI is being employed by different industries everywhere to provide a better and more personalized experience for their users. An example is chat bots. These same AI systems can also be used in the finance sector by banks and other service providers to predict business growth, etc. and track user's behaviors and characteristics to cater their ever-changing financial needs.

Fighting Fraud and Crime
Monitored user behavior patterns allow AI tools to notice anomalies and irregular behavior quickly to apply countermeasures and notify the users in case of fraud attempts. Such tools are also capable of collecting the necessary evidence needed for the conviction of the criminals making these attempts.

Advanced Insight

Companies can make use of AI computing to perform analysis of behaviors and trends to offer better and advanced insight that will be useful to their business. For example, firms can use AI to go through thousands of pages of tax information to collect relevant data that may be needed.

Use of Bots

Chatbots are being used by different financial service providing companies and banks to communicate with their customers and meet their needs. These bots are a valuable way of fetching information, providing answers and offering personalization. Customers regularly use Bank Bots to get information about their accounts and make payments. Robo advisors offer meaningful advice and recommendations to each client based on their needs and portfolio.

In short, AI is being currently applied to offer both substantive and personalized services to users as well as to process huge amounts of data to correctly predict business growth, future finance trends and changes as well as to formulate effective banking strategies. It is allowing for better, faster and cheaper decision making and productive changes to systems to get better customer satisfaction.

The Future

IoT and AI both are progressing rapidly and it is more than probable that soon everything we do on any digital device could be connected with all the other digital devices in our use. Currently, most of the financial service providers are limited by resources, budgets, regulations or operations. However, studies show that by 2025 robotics and machine intelligence will be a vital part of our daily lives and this will have great implications for every industry.

Yet a major concern is privacy. With this much information flow and systems relying on digital devices and information through them the users' privacy will have to be taken care of. Intelligent systems will need to identify cases of manipulation or fraud as a result of a crime. Otherwise, all anyone has to do is fool the banking and insurance intelligent systems by tampering with the connected devices or impersonating the account holder. A BBC reporter recently proved HSBC's current voice-recognition security isn't as he impersonated his brother to get access to his account.

Combined, AI and IoT together can thoroughly revolutionize the finance industry and how services are provided to customers but this can only be achieved if banks and insurers cooperate by preparing employees to create products and services that integrate with smart devices. Visa recently announced it's expanding its VisaReady program to include IoT devices. "More and more, consumers are relying on smart appliances and connected devices to make their lives easier," said their EVP of innovation and partnerships, Jim McCarthy in a statement.

By adding payments to these devices, we are turning virtually any Internet connection into a commerce experience – making secure payments seamless, and ultimately more accessible, to merchants and consumers.

A noble aim. The shift to all things digital may be costly at the start but it is the way to go and this time the change will not be stopped due to lack of resources or operational means. The substantial benefits of integrating IoT and AI into our lives and work are numerous and therefore there is no turning back from this. There will be an increase in automated financial services that employ Artificial Intelligence along with Internet of Things in the future. Although this will give rise to rise to security and privacy issues as well, these will eventually be effectively dealt with.

Healthcare IT News, Experts back Senate IoT security legislation
http://www.healthcareitnews.com/news/experts-back-senate-iot-security-legislation

The Internet of Things Cybersecurity Improvement Act would set minimum standards that are immediately needed.
By Bill Siwicki September 14, 201709:47 AM
Senate IoT security legislation
Orgs should formalize their own medical device security policies because IoT security legislation is coming.

The security of the Internet of Things is a key concern today. But in healthcare, IoT security literally can be a matter of life or death.

Healthcare could be on the brink of massive security standard changes when it comes to the IoT. For example, a new U.S. Senate bill – The Internet of Things Cybersecurity Improvement Act of 2017 – would require IoT devices sold by vendors to the federal government to meet minimum security standards. This includes sales to Defense Department and Veterans Affairs healthcare facilities, which would filter out to the rest of the healthcare industry as a result.

[Also: Old legacy devices pose greatest security risk, experts say]

This legislation targets the low-hanging fruit of healthcare device cybersecurity, said Josh Jabs, vice president of public key infrastructure and IoT solutions at Entrust Datacard, a security technology company.

“It requires vendors of Internet-connected healthcare devices to have a higher minimum standard of security,” Jabs said. “For healthcare provider organizations, they can expect their device vendors to supply equipment that can be patched. Healthcare devices have a lifecycle that may include the need to modify the original firmware that controls the device, especially if security issues are found after design and manufacture.”

[Also: Ransomware and electronic records access, healthcare's biggest threats]

Additionally, the legislation requires vendors to provide devices configured so that their single-factor authentication credential, the username and password, can be changed, rather than being hard-coded. The Mirai botnet, for example, was an example of an attack against default and unchangeable credentials.

The time is ripe for IoT security legislation. Healthcare providers in the U.S. have very little guidance on how to protect IoT/medical devices within their infrastructures today.

[Also: How healthcare providers can curb medical identity theft]

Aside from some guidance from the FDA and PII-centric HIPAA requirements, there are no federal requirements in terms of how to protect, detect and respond to security threats affecting IoT/medical devices that could lead to device manipulation, data exfiltration or, worse, direct patient harm, said Chris Sherman, a security and risk

analyst at Forrester Research who specializes in the Internet of Things and medical device cybersecurity.

“Providers should prepare for legislation in this area,” Sherman said, “by formalizing their own medical device security policies, while demanding their device suppliers adhere to application security best practices and medical security certifications, as well as building out their own device monitoring capabilities.”

Jabs has suggestions for how provider organizations can better protect IoT/medical devices today.

“The WannaCry ransomware attack showed us that patching desktop systems is important for healthcare providers,” he said. “Providers also should take inventory of connected systems, which will help to identify risk beyond privacy measures specified by HIPAA. Even if the cybersecurity maturity of your healthcare organization is low, it is a good first step.”

And, he added, the Presidential Policy Directive 21 (PPD 21) has identified healthcare providers as critical infrastructure. Work is being done to help healthcare providers get the most out of the National Institute of Standards and Technology cybersecurity framework, he said, so that ultimately providers can understand how to measure and remedy risk.

A multiple communication standards compatible IoT system for medical usage
http://ieeexplore.ieee.org/abstract/document/6577775/

Abstract:
With the development of IoT technologies, more and more medical equipments and sensors with wireless communication modules are deployed in the same domain. Confliction of wireless signal in air becomes a serious problem which should be carefully managed. In this paper, we design a communication system model for medical equipments and IoT sensors. The system defines different communication priority for various devices depending on the necessity of functions. Some medical IoT sensors translate and receive the massive data every time and on the other hand some equipment just translate emergency signal for help calling. All these communication process should be treated separately to keep the efficiency of ISM band utility. The system has three patterns: (1) Devices with various communication standard can

sense the existing of other devices.(2) Device can change its working state depending on the priority of itself and others. (3) The system will only change the MAC and upper layer of Device network stack and without touching the PRY layer.

IoT Agenda, Healthcare IoT security issues: Risks and what to do about them
http://internetofthingsagenda.techtarget.com/feature/Healthcare-IoT-security-issues-Risks-and-what-to-do-about-them

In healthcare, the Internet of Things offers many benefits, ranging from being able to monitor patients more closely to using generated data for analytics.

But that increased flow of information also brings risks that health IT professionals need to address.

"There are so many benefits that come with these new connected devices," said Mike Nelson, vice president of healthcare solutions at DigiCert, a security certification company in Lehi, Utah. "But they also present some new risks and vulnerabilities that as an industry we haven't, I would say, firmly dealt with to this point."

Mike NelsonMike Nelson
Those risks include possible harm to the patient's safety and health, loss of PHI and unauthorized access to devices, Nelson said.

However, the healthcare community is beginning to address these Internet of Things (IoT) security issues.

"I think the issue is becoming relevant enough that we're now starting to see real collaboration occur," Nelson said.

He added that this collaboration among healthcare professionals to ensure healthcare IoT security is an indication that the risks are not hypothetical.

"I think that indicates, one, that the threat and the risk is real, and two, that it's becoming painful enough for some of the manufacturers and maybe some of the hospital providers that they're starting to do stuff about the issue," Nelson said.

The risks of IoT in healthcare

When it comes to healthcare IoT security issues, the list can seem overwhelming.

Karl WestKarl West
One problem is devices entering hospitals through a variety of channels, with some of these avenues being unknown, said Karl West, chief information security officer at Intermountain Healthcare located in Salt Lake City. One example of this is BYOD. When this happens it can be difficult to figure out the lifecycle management of that device and identify the operating system.

Furthermore, "because [devices] come in through a different process, they wouldn't necessarily have any common controls surrounding them," West said, meaning having passwords, encryption, and the latest versions of hardware and software on the device. When it comes to common controls, "that doesn't exist today."

Another issue, West added, is standalone devices that have developed networks and connectivity glitches. "With those connectivity issues comes transference and movement of data, and so data migration is occurring," he said. "We're unaware of it because they haven't come in through normal channels."

That level of concern goes up when someone -- a vendor, rogue IT staff member or maybe even a hacker -- puts standalone devices onto an isolated network. "I don't even know that that network exists, I don't know who put it in, I don't know how it's contained, I don't know if someone bridged that network to my network," West said. "So that's a huge issue for me."

He explained that some of these devices can also come onto the hospital's network without his network team knowing about it.

Consider this scenario from West: A medical device vendor puts a network connection together for 10 new devices, and then the vendor feeds those devices onto the hospital's network. It's a security headache waiting to happen.

Such a scenario is especially concerning, West said, because he hasn't been alerted that these devices have even been connected, which means multiple risks and vulnerabilities are introduced.

These vulnerabilities, which largely have not been addressed in healthcare, in turn can pose potential harm to patients.

Scott ErvenScott Erven
"We don't have evidence that vulnerability in devices, or a cybersecurity issue in a medical device, has caused a direct patient safety issue," said Scott Erven, associate director at Protiviti, a consulting firm based in Menlo Park, Calif. "But due to these devices lacking evidence capture and forensic logging capabilities, I like to say that we have low assurance that something hasn't happened."

And while many would assume that the threat to a patient would come from an outside hacker with malicious intent, that notion is not always the case, Erven said.

"There were two individuals in Austria in a hospital that were hooked up to an infusion pump and felt their pain management wasn't under control," Erven said. These pair went online, found service documentation, got the hard-coded service credentials to their infusion pumps, logged in and upped their doses. The overdoses caused respiratory problems, Erven said.

"I think it goes to show that a patient that was on an infusion pump was able to figure out how to locate credentials on the Internet and log in to the device," he said. "That isn't something that requires advanced understanding or knowledge of a device."

What to do to achieve better healthcare IoT security
Despite these risks, it seems the healthcare community has accepted the fact that IoT is coming. In order to prepare and remain as secure as possible, there are steps that providers and manufacturers alike can take.

Firstly, "basic security hygiene" is a must, Nelson said, such as authentication. If this step is properly followed, device access is limited, firmware being sent to the device is verified, and device-to-device communication undergoes scrutiny, Nelson said.

Other basic security actions that providers and manufacturers can take include encryption and conducting a secure boot, Nelson said. A secure boot is making sure that when a device is turned on, none of its configurations have been modified.

It is also important to not just take inventory of all devices and applications, but also create a "data dictionary," West said.

"We recognized that having an application inventory doesn't solve the problem," he said. "You really need to know and have a data dictionary. That is, you need to know and have in a dictionary where all data resides, where it originates, where it moves, [and] what its transmission capabilities are."

Temenos, What the IoT Brings to Banking
https://www.temenos.com/globalassets/mi/wp/16/wp1605_what_iot_brings_to_banking.pdf

Sensors and Wi-Fi are changing how we interact with the world around us, bringing a new era of connectivity – dubbed the Internet of Things. With this enhanced connectivity comes the chance to tap into and use any data collected, opening up almost boundless opportunities for business, communities, personal and civic benefit. Central to facilitating much of that potential will be banks. Our very relationship with banks will be transformed, as will the way they operate. Branches will disappear as we no longer require face-to-face service. Wearables and biometric devices, cars, homes, offices and even the built environment will initiate transactions directly with banks in real time, while banks' role as custodians of our money will grow to include management services to help with budgeting and even health. The extent of change is limited only by our imagination. Already there are game-changing applications and services being trialled and implemented. It is time for financial services to be provided by the "Bank of Things". 4 Over the past 10 years, I've seen analysts forecasts of the number of devices connected to the internet grow from 2 billion to 50 billion. The reality is we simply don't know – and the ever-spiralling statistic is a sign of just how big the potential for this new technology is. It seems it will soon be possible to connect anything and everything. We already have a mattress cover that monitors your health; socks that tell you how many times they've been worn and washed; 3D printed clothes that adjust to temperature; and milk bottle tops that tell you if the contents have gone off. Meanwhile, toothbrushes, light bulbs, door handles and even pens can all be connected and deliver new services as a result. New types of information A new era of connectivity has begun and with it comes a whole different level of Big Data, as devices emit a constant flow of information. In addition, just as the number and variety of things connected to the internet continues to

grow, so does the range of information coming from them. Sensors can provide data on location (GPS), movement (accelerometer), temperature, pressure and light, for example. And it quickly becomes apparent that the possibilities for this continuous stream of information are limitless. Interconnected “things” Nor does it stop there, because these connected “things” can also communicate with each other. Imagine a washing machine that warns you that you’ve left your phone in the pocket of the jeans you’ve just placed inside it to wash. Or curtains that open when the alarm on your phone wakes you up in the morning (possibly a little later than usual because it has checked your diary for the day ahead and detected that you haven’t slept well). Again, the possibilities of what could result from devices that are able to talk to each other are endless. Children are today learning the basics of wiring up sensors and finding ways to employ the resulting data using kits such as Wunderbar, SAM and Kano to build their own gadgets. These are the skill sets of the future – electronics (circuits), APIs/scripting and analytics. Dawn of the “Bank of Things” Introduction 5 The future of banking The implications of this new connected world are only just starting to be felt. Every industry is in a state of transformation and none more so than banking. Banks are considering how Big Data could potentially transform what they offer to customers and their relationship with them. This is what I call the “Bank of Things” and in this new world it is likely that banks will want to become the trusted: • Custodian of the customer’s data – helping to manage privacy and control sharing • “Infomediary” – acting as an adviser between the customer and sellers • Payments manager for the customer’s “things”. A report from The World Economic Forum forecasts that smart chip implants could be commonplace by 2023. These might range from simple chips for identity and payments to health devices such as cochlear implants or heart pacemakers. The report also highlights progress in research by Brown University into technology that connects directly with the brain to enable mind control of devices. This moves us into Zero UI, controlling devices beyond a touch screen, whether through voice control, gestures or even thought processes. Google’s project Ara is a modular phone that permits you to upgrade individual parts such as the camera or battery, putting an end to the need to replace the whole phone when you want an upgrade. Taking this concept further, perhaps the Personal Area Network could mean that eventually you only need one GPS, one camera, one battery and so on – each wirelessly communicating to other devices like your phone, car stereo and watch. The changing face of finance Into this world of possibilities come banks. biometrics, devices and chips – wherever they are located on

the human body – make payments possible without having to use cards. Meanwhile, if banks have access to ever-richer data about people's lifestyles they will be able to play the role of infomediary and provide more relevant and targeted offers, advice and rewards. Banks will need to act round the clock to make the most of the information coming from these sources and respond to real-time events. With increased information it's clear that products such as insurance will change dramatically to become more personalised to suit individual lifestyles. The key for banks is to look for opportunities to engage in creating compelling new customer experiences based on these devices and the data they provide, while always respecting privacy. A huge amount of innovation has already been brought to market – too much to cover in any white paper or even book. Even five-year-olds (and maybe younger) are learning how to use the Internet of Things, and the time is ripe for banks to define how they might engage customers in their own "Bank of Things". The Internet of Things is only limited by imagination – the time is ripe for banks to define how they might engage customers in their own 'Bank of Things'.

Finextra, How the Internet of Things will change Banking
https://www.finextra.com/blogposting/12707/how-the-internet-of-things-will-change-banking

The Internet of Things (IoT) is, without a doubt, one of the biggest technological transformations on the horizon, with many already claiming that we are entering the second major digital revolution.

Analysts at Gartner predict there will be 25 billion smartphones, smartwatches, wearables, connected cars and other connected devices by 2020. An amazing forecast, that strongly indicates the influence that machine-to-machine (M2M) connectivity is going to have on our society, culture and business.

In a very short space of time, we are all going to be surrounded by intuitive connected devices, from our smartphones and wearable tech, through to millions of sensors in our homes, on our roads and in our workplaces. For consumers, the real promise of the ubiquitous connectivity of the IoT era is to help us save time, work smarter, drive safer and live a healthier and more active lifestyle. For business, there are multiple opportunities to benefit from IoT, with $2 trillion of economic benefit predicted on a global level by Gartner.

Some industries, such as commercial real estate and the insurance industry, have been quick to embrace the benefits of IoT innovation. Insurers, for example, have been quick to learn about and welcome the opportunities to develop new ways of using increasingly widespread sensor data in wearable and smart car technologies to gain much more detailed and valuable risk data on their customers.

Following on from these types of FinTech innovations, the banking industry is now starting to see the various potential ways in which IoT can help to take it to the next level.

IoT generated data adds value for banks and customers

Today’s consumers demand always-on convenience and a personalised service whenever possible, as is clear from the mass adoption of online banking, mobile banking apps and, most recently, contactless payment technologies. Additionally, they also want the highest levels of digital security from their banks, with any data breach or security threat posing a major problem to banks in the IoT era.

Machine-to-machine connectivity that enables the mass collection and exchange of information from sensors and objects also opens up multiple opportunities for banks, who will be able to better track and analyse the behaviours, wants and demands of their customers. This, in turn, will allow banks to provide customers with a far more personalised experience, with targeted advice, context-aware offers and insight. The bank is able to achieve a new level of understanding of the needs of both consumer and business clients, attaining a new level of customer intimacy.

Banks might use IoT technologies to create more engaging and context-aware customer rewards, or to generate more intelligent and personalised customer cross sell opportunities, for example. And IoT will help banks to innovate and devise better ways to improve risk management, reduce costs and improve overall operational efficiency.

Business clients and consumers will be able to access a much more holistic view of their finances wherever and whenever they like. And banks will offer far more tailored products and solutions to help customers make the best financial decisions at all times.

The increased amount of real time data available to banks, from information on residential and commercial properties through to

personal data from social media, spending habits and credit behaviour, will all allow banks to make better commercial decisions, based on far more accurate financial risk data.

How the IoT helps banks to stay ahead of the curve

Banks are going to be far more technologically-empowered to assist business customers and help them to achieve better commercial results, due to the banks' ability to obtain and access data from across the business customers' value chain, from suppliers through to distributors and retailers, for example.

Biometric and positional sensors, for example, are highly likely to help banks to track both the physical performance of individuals and to track the shipping of goods and manufacturing quality control better than ever before, which in turn will help to improve underwriting processes and reach new markets.

It will be those banks that best use these new types of IoT-generated data streams to make vital decisions on business lending that stay ahead of the curve. One example here might be the potential benefits to banks from new types of sensor that monitor the activity and condition of retail industrial and agricultural businesses, such as connected field devices in manufacturing or agricultural sensors that monitor livestock.

On which note, farming, in particular, could well be a major beneficiary of real-time data feeds which will allow farmers and their banks to continuously assess and value the farm's crops and livestock, accurately gauging yields, property and overall business value.

In terms of consumer-facing retail banking branches, IoT could also be used to assist customers with new and improved video tellers and kiosks that will be equipped with sensing technology that will be able to biometrically recognise the customer from the moment they enter the branch.

New security challenges for banks in the IoT era

Over the next five to ten years, the banking industry is going to see major changes from IoT technologies, which will also present banks with new security challenges to manage. The need to ensure that the

whole connected banking experience is safe and secure will be increasingly vital in order to gain customer trust and ease clients' concerns around personal and business banking data being hacked.

Sensitive data, from a customer's financial history to their location history, is always potentially a target while it is stored on or moving around the network. No matter where the data is held, whether it be on a device or moving along the network from the bank to the customer's connected car, for example, it needs to be properly protected.

Which is exactly where tools such as encryption to protect the data itself and authentication tools to authorise access to this data by only those allowed to, are vital. We're already starting to see the development of biometric data – fingerprints, voice-recognition software and iris-scans – come into play to prove the customer is who they say they are.

Banks will have a far more detailed and useful picture of the customer, with the abundance of IoT devices, which at the same time means that banks will need to add an extra layer of security across the entire IoT ecosystem – from the devices being used through to the network and cloud level.

Cybercriminals have more opportunities to sneak in or hack a network as there are more points of entry and devices there are connected to that network. All of which means, for banks to fully embrace IoT, they will need to build in security from the start, at every level, to win and maintain customer trust.

OnApproach, Internet of Things: Retail Banking
http://blog.onapproach.com/bank-of-things-internet-of-things-retail-banking

The Internet of Things (IoT) has gained a considerable amount of hype as the "Next Big Thing" to change the world as we know it. Applications of IoT are thought by some to be limited only by the human imagination. From simply controlling your home (e.g. - lights, thermostat, etc.) with a smartphone, to life saving medical and healthcare systems, IoT is pervasive and growing rapidly.

The financial services industry has recently started experiencing the IoT disruption in the form of mobile banking. While mobile banking is seen as an incredible advancement in financial services, it may only be the tip of the iceberg for the Bank (or Credit Union) of Things.

In recently published whitepaper, The Bank of Things: How the Internet of Things will Transform Financial Services, Author Ian Webster of Accenture discusses what he refers to as 'Customer 3.0.' Much like I discussed in one of my pervious articles, Why Attracting Millennials Requires Big Data/Analytics, Webster's 'Customer 3.0' is "hyper-connected, highly informed, very demanding and spoilt for choice. They expect to be engaged as individuals, and on their terms — when, where and how they want." This new information expectation is requiring banks/credit unions to think of innovative ways to transform their data into valuable assets that provide a better customer experience.

Examples of IoT in Financial Services

'Customer 3.0' is being conditioned to expect much more information in all areas of their lives with retail banking being no exception. IoT is still in its adolescence in the financial services industries but there are several practical example of IoT in banking that do not seem far-fetched, consider the following example:

Loans are a major source of revenue for financial institutions but with interest rates at historical lows, differentiating one loan from another is difficult. So how do you ensure someone uses your financial institution for their next loan? By being the first image a customer sees when deciding to make their next big purchase. With advanced geo-tracking using beacons (IoT technology), financial institutions can send out the most accurate and timely marketing alerts.
Imagine walking onto a car dealership and receiving an alert from your mobile banking app that automatically tells you how much financing you've been approved for. Even better, the auto loan application can be completed using your smartphone and contain prepopulated data stored from previous transactions (e.g. current address). Imagine an app offering you a deal if you purchase the exact car you're looking at. With beacon technology you can send offers such as, "Save $1,000 on that new 2015 Chevy Impala if you use Sample Federal Credit Union financing." This may seem like a "too

good to be true" scenario, but with IoT (beacons) and Big Data, this is something retail banking institutions could start doing today.
Living in Harmony: Internet of Things (IoT) and Big Data & Analytics

IoT presents a tremendous opportunity for financial services, but it also presents a serious challenge. In addition to the countless new applications for internet connected banking, IoT is also expected to generate a plethora of data. This data is coming from a variety of new sources, at high-velocity and in increased volumes (also known as Big Data).

"...Internet of things-related technology and services revenue is forecasted to grow from US$4.8 trillion in 2012 to US$8.9 trillion by 2020. The future is coming fast — and to capitalize on these opportunities, today's banks need to invest in developing the ecosystems and capabilities that will drive tomorrow's Bank of Things." -Ian Webster, Accenture

Time is of the Essence

Without the proper technology to store, process, and analyze the data generated from Internet of things-related banking, retail banking institutions will not be able to serve 'Customer 3.0' in the way they desire. Failure to address the needs of 'Customer 3.0' will challenge the future viability of most banks and credit unions. The financial services industry is at a cross roads and needs to think about how to reinvent itself before it's too late. There are several companies that have noticed this tremendous opportunity and have started investing in similar technology. A few of these companies worth mentioning are Apple (Apple Pay), PayPal, and Lending Club (backed by investment from Google).

As we enter the era of IoT and the ensuing massive data explosion, how will your institution react? Will it sit on the sidelines and wait for the innovators of the industry or will it get ahead of the curve, start investing in Big Data/Analytics, and be one of those innovators?

HITRUST, US Healthcare Data Breach Trends
https://infosec.uthscsa.edu/sites/default/files/HITRUST_Report-US_Healthcare_Data_Breach_Trends.pdf

InfoSys, IoT-Enabled Banking Services
https://www.infosys.com/industries/financial-services/white-papers/Documents/IoT-enabled-banking.pdf

NIST, Framework for Improving Critical Infrastructure Cybersecurity
https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf